1. Governança e Gestão de Segurança da Informação

1.1. A CONTRATADA deverá dotar o PJERJ de meios para proteger e garantir a confidencialidade, integridade, disponibilidade e privacidade das informações produzidas e ou armazenadas.

1.2. A CONTRATADA deverá realizar o levantamento e planejamento de ações juntamente com a DGTEC, para a implantação da política de segurança do PJERJ, para garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade de todos os serviços e informações do PJERJ;

1.3. Garantir que os recursos estejam disponíveis por meio de mecanismos seguros.

1.4. Definir e atualizar políticas de acesso ao conteúdo protegido.

1.5. Estabelecer processos para proteger a integridade dos dados armazenados.

1.6. Assegurar a confidencialidade do conteúdo.

1.7. Evitar o roubo de informações sigilosas ou o seu vazamento.

1.8. Selecionar e instalar produtos e equipamentos voltado à proteção de informações sigilosas, de acordo com as normas e padrões da CONTRATANTE.

1.9. Realizar recomendações das melhores práticas de segurança, provenientes de análises globais e melhorias na proteção do ambiente, observando os pilares das ações de proteção de dados.

1.10. Elaborar um Programa de Política de Segurança da Informação e Plano de Gerenciamento de Projetos.

1.11. Avaliar a política de segurança da informação existente no PJERJ e sugerir modificações caso seja necessário.

1.12. Deverá realizar, nos primeiros 40 (quarenta) dias de execução deste serviço, uma avaliação completa do ambiente do PJERJ com o objetivo de identificar lacunas ou oportunidades de melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança do PJERJ, contendo no mínimo:

1.12.1. Avaliação de maturidade do ambiente da CONTRATANTE;

1.12.2. Assessment de CASB;

1.12.3. Teste de invasão;

1.12.4. Scan de vulnerabilidade.

1.13. Realizar anualmente para cada formato (White Box, Gray Box e Black Box) as tentativas de invasão a sistemas e equipamentos, assim como analisar as regras atuais de firewall, IDS, IPS, antivírus, proxy e AntiSpam.

1.14. Realizar análise de código em aplicações críticas, onde os sistemas críticos serão definidos pelo PJERJ.

2. Gestão de Riscos de Segurança da Informação

2.1. 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.

2.1.1. **Das atividades**

2.1.1.1. A CONTRADADA deverá capacitar o CONTRATANTE para lidar com os riscos nas decisões de qual selecionar dependerá de uma série de fatores tangíveis e incerteza intangível, consequências da realização do risco (bom ou ruim). Além dessa 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.

2.1.1.2. A CONTRATADA deverá manter uma rotina mensal de avaliação dos processos e práticas em todas as áreas de atuação do escopo deste contrato com o objetivo de avaliar a eficácia, propor melhorias e auxiliar na implementação desses ajustes.

2.1.1.3. Estabelecer o processo de gerenciamento de risco envolvendo a revisão das informações coletadas como parte das avaliações de risco (e preocupação), passando pelas etapas de identificação, análise e avalição 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.

2.1.1.4. 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.

2.1.1.5. Quanto ao gerenciamento de riscos a CONTRATADA deverá:

2.1.1.5.1. Estabelecer uma matriz de riscos juntamente com a Administração do PJERJ e propor ações de tratamento desses riscos (evitar, aceitar, mitigar, eliminar e transferir);

2.1.1.5.2. Realizar ações de análise de riscos, visando a criação de uma matriz em conformidade com as diretrizes da administração da Contratada;

2.1.1.5.3. Elaborar um documento para que seja avaliado e homologado pela Contratante, contendo minimamente a matriz de riscos, os processos de tratamento dos riscos reportados;

2.1.1.5.4. Realizar análises de risco de segurança para cada contratação tecnológica a ser realizada pela CONTRATANTE;

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

2.1.2. **Avaliação de riscos**

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

2.1.2.2. Os riscos a processos ou serviço em particular;

2.1.2.3. Níveis de ameaças e vulnerabilidades;

2.1.2.4. Níveis de risco;

2.1.2.5. Medidas iniciais de redução de riscos.

2.1.3. **Ferramenta**

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

2.1.3.1.1. Administração

2.1.3.1.1.1. 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;

2.1.3.1.1.2. Registrar atividades em trilhas de auditoria;

2.1.3.1.1.3. Permitir que o administrador parametrize quais funções do sistema cada usuário terá acesso através de perfis de acesso. Entende-se funções do sistema todos os menus contidos no sistema;

2.1.3.1.1.4. Suportar autenticação Single Sign-On (SSO) através do protocolo SAML. O recurso deve ser nativo e ter interface de configuração na própria solução para que o administrador realize as configurações;

2.1.3.1.1.5. Permitir a sincronização de usuários com o Active Directory da Microsoft de forma nativa e configurável dentro da própria solução em um ambiente on premise do

Contratante onde a solução está hospedada em outro servidor, preferencialmente sem necessidade de abertura de portas de firewall entre servidor de aplicação e AD do cliente, garantindo segurança do ambiente do cliente;

2.1.3.1.1.6. Permitir realizar testes de sincronização e envio de relatório de sincronização de usuários a cada execução;

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

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

2.1.3.1.2. Usabilidade

2.1.3.1.2.1. Permitir utilizar soluções de código aberto como requisitos do sistema, incluindo: servidor web, servidor de aplicação Java, sistema operacional e banco de dados;

2.1.3.1.2.2. Ser compatível com os navegadores internet: Google Chrome, Microsoft Internet Explorer; Edge e Firefox;

2.1.3.1.2.3. Permitir rodar em ambiente virtualizado;

2.1.3.1.2.4. Permitir a configuração do armazenamento de conteúdo (documentos e anexos) de forma visual pelo administrador do sistema, com as opções de armazenamento em banco de dados (campo Blob) ou diretório em rede;

2.1.3.1.2.5. Permitir a conversão de conteúdo para o formato PDF;

2.1.3.1.2.6. Suportar idiomas padrão UTF8;

2.1.3.1.2.7. Suportar o uso de Load balancing tanto na camada de banco de dados, quanto de aplicação, permitindo que a carga do sistema seja distribuída entre dois ou mais nós da solução;

2.1.3.1.2.8. Possuir visualizador nativo HTML 5 para PDF sem a necessidade de instalação de softwares adicionais para visualização nas estações clientes.

2.1.3.1.3. Segurança

2.1.3.1.3.1. Realizar comunicação segura entre os diferentes componentes da solução e com a estação de trabalho usando padrões de criptografia e protocolos, ambos não proprietários (ex: SSL);

2.1.3.1.3.2. Deve possuir controle de acesso por identificação e senha, com cadastro de usuários, grupos e transações, onde as permissões para cada uma das transações possam ser dadas diretamente ao usuário ou implicitamente através de um grupo do qual ele faça parte;

2.1.3.1.3.3. 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;

2.1.3.1.3.4. A ferramenta deve prover mecanismos de segregação de usuários através de nível de atuação (usuários, gerentes de projeto, consultor do escritório de projetos, suporte, administração);

2.1.3.1.3.5. A ferramenta deve possuir mecanismos para restringir as operações no sistema conforme o perfil dos usuários;

2.1.3.1.3.6. A ferramenta deve possibilitar o controle de restrições de acesso por usuário e por grupo de usuários;

2.1.3.1.3.7. A ferramenta deve manter registro das alterações feitas nos dados e documentos com data, hora e usuário;

2.1.3.1.3.8. A ferramenta deve possibilitar registro e consulta a dados estatísticos sobre acesso de usuários como acesso simultâneo, tempo de logon, origem do acesso;

2.1.3.1.3.9. Todas as senhas de usuários devem ser armazenadas utilizando algoritmos de criptografia salted hash;

2.1.3.1.3.10. A ferramenta deve 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.

2.1.3.1.3.11. Gestão de riscos - Permitir a definição da metodologia de avaliação de pontuação do risco em qualquer nível da organização;

2.1.3.1.3.12. 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;

2.1.3.1.3.13. Classificar os riscos de acordo com a severidade para a organização e com a probabilidade da ocorrência no processo;

2.1.3.1.3.14. Permitir a avaliação periódica do risco, monitorando a sua evolução analiticamente e graficamente;

2.1.3.1.3.15. Permitir a criação de modelos (template) de plano de riscos, para facilitar a replicação de estruturas similares nas organizações;

2.1.3.1.3.16. Permitir uma abordagem estratégica na identificação dos principais objetivos da organização e dos riscos existentes para o alcance desses objetivos;

2.1.3.1.3.17. Permitir que os riscos possam ser facilmente identificados e associados a um processo;

2.1.3.1.3.18. 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;

2.1.3.1.3.19. Permitir a definição de equipes responsáveis pela avaliação;

2.1.3.1.3.20. Manter o cadastro e acompanhamento das alterações (revisão) dos objetos e dos planos de risco;

2.1.3.1.3.21. Permitir a definição do custo dos controles e o valor do impacto ou ganho do risco possibilitando a realização de análises quantitativas do risco;

2.1.3.1.3.22. 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;

2.1.3.1.3.23. Possibilitar a abertura de um workflow específico caso a avaliação do risco esteja acima do esperado;

2.1.3.1.3.24. Possibilitar a aprovação do plano de riscos ao final do planejamento e a revalidação dentro de frequência pré-estabelecida;

2.1.3.1.3.25. Permitir que os riscos possam ser associados a mais de um processo, porém, que sejam analisados e documentados individualmente para cada processo;

2.1.3.1.3.26. Permitir a avaliação considerando o risco potencial, o risco inerente e o risco residual;

2.1.3.1.3.27. Permitir o cálculo automático do risco residual;

2.1.3.1.3.28. Permitir a associação de anexos e documentos controlados ao Risco;

2.1.3.1.3.29. Executar as avaliações de maneira on-line;

2.1.3.1.3.30. Permitir a análise de risco dos processos mapeados;

2.1.3.1.3.31. Apresentar graficamente, no fluxograma do processo, as atividades que possuem riscos associados;

2.1.3.1.3.32. Mapear os processos e modelar todas as atividades relacionadas;

2.1.3.1.3.33. Permitir a análise de risco dos ativos;

2.1.3.1.3.34. Permitir a análise de risco dos projetos;

2.1.3.1.3.35. Permitir o planejamento do projeto com a definição de atividades, responsabilidades, recursos, prazos e custos;

2.1.3.1.3.36. Permitir o preenchimento da árvore de decisão na gestão dos riscos de segurança alimentar;

2.1.3.1.3.37. Permitir a gestão dos riscos relacionados ao planejamento estratégico (Scorecard);

2.1.3.1.3.38. Definir o Scorecard corporativo com todos os seus elementos (perspectivas, objetivos e indicadores);

2.1.3.1.3.39. Permitir a habilidade de desenvolver ou adotar um framework para a gestão de riscos (COSO ERM, ISO 27005, FERMA, OCEG ou outros frameworks similares);

2.1.3.1.3.40. Mapear os riscos operacionais de acordo com framework COSO;

2.1.3.1.3.41. Permitir a associação de tratamentos e planos de ação no momento da criação da análise de risco;

2.1.3.1.3.42. Permitir a associação de controles aos riscos durante o cadastro, facilitando a utilização posterior;

2.1.3.1.3.43. Apresentar o histórico das avaliações do risco atualizado conforme última versão do método de avaliação;

2.1.3.1.3.44. Oferecer método de avaliação para a definição do nível do risco. Critérios quantitativos podem ser informados para a obtenção do resultado;

2.1.3.1.3.45. Personalizar as colunas para serem visualizadas na estrutura do plano de risco e controle;

2.1.3.1.3.46. Permitir a visualização da Matriz de Risco de todos os riscos de um plano de risco;

2.1.3.1.3.47. Permitir a visualização da Matriz de Risco agrupando quantitativamente as avaliações dos riscos;

2.1.3.1.3.48. Permitir a associações do risco no momento que está cadastrando um evento, ou seja, um incidente, problema ou workflow;

2.1.3.1.3.49. Permitir registrar uma justificativa, anexo ou documento para cada resultado da avaliação do risco;

2.1.3.1.3.50. Permitir associar causas, consequências, fontes de risco e melhores práticas ao risco;

2.1.3.1.3.51. Permitir criar e gerenciar KRI (Indicadores chave de risco), com geração de eventos casos do KRI estejam fora dos valores aceitáveis;

2.1.3.1.3.52. Permitir enviar e-mail a aprovação da avaliação do risco;

2.1.3.1.3.53. Permitir solicitar a avaliação de risco para o responsável no momento da Auditoria.

2.1.3.1.3.54. Supervisionar a implantação do plano de ação de risco e realizar a revisão periodicamente.

2.1.3.1.4. Problemas e tratamento

2.1.3.1.4.1. Permitir a identificação de problemas nas atividades de controle;

2.1.3.1.4.2. Permitir a identificação de problemas na avaliação do risco;

2.1.3.1.4.3. Permitir a associação de prioridade aos problemas;

2.1.3.1.4.4. Permitir a definição de responsáveis aos problemas;

2.1.3.1.4.5. Permitir o monitoramento de prazos de planejamento e de execução;

2.1.3.1.4.6. Permitir o envio de e-mail automaticamente para o responsável assim que uma ocorrência for registrada;

2.1.3.1.4.7. Permitir a criação e o monitoramento de múltiplos planos de ação para cada problema;

2.1.3.1.4.8. Permitir que os responsáveis pelos planos de ação possam ser diferentes dos responsáveis pelo problema;

2.1.3.1.4.9. Permitir que os planos de ação sejam revisados e aprovados por um usuário específico ou pelo responsável pelo problema;

2.1.3.1.4.10. Permitir que a situação de execução dos planos de ação seja monitorada;

2.1.3.1.4.11. Permitir que as notificações por e-mail possam ser definidas pelos usuários;

2.1.3.1.4.12. Permitir que o gestor tenha fácil acesso a todos os problemas e planos de ação de sua área de responsabilidade;

2.1.3.1.4.13. Permitir que trilhas de auditoria para qualquer alteração nas atividades e prazos relacionados aos problemas e planos de ação façam parte do sistema;

2.1.3.1.4.14. Permitir a análise de causa e de tendência;

2.1.3.1.4.15. Permitir a personalização da resposta ao risco;

2.1.3.1.4.16. Permitir a criação ou a associação de um ou mais planos de ação para cada tratamento do risco;

2.1.3.1.4.17. Permitir a gestão de iniciativas de acordo com o PMBOK;

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

2.1.3.1.5. Consultas e relatórios

2.1.3.1.5.1. 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;

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

2.1.3.1.5.3. Permitir salvar relatórios no formato PDF;

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

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

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

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

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

2.1.3.1.5.9. 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;

2.1.3.1.5.10. Apresentar a matriz de riscos para a fácil identificação da relação entre riscos e atividades;

2.1.3.1.5.11. Apresentar o cálculo do risco médio gerado automaticamente e agrupado por Unidade Organizacional, Processo, Risco, Tipo de Risco com visões gráficas da matriz de risco em um portal interativo;

2.1.3.1.5.12. Permitir comparar os resultados entre as revisões do plano de risco e controle;

2.1.3.1.5.13. Permitir a definição de indicadores de desempenho associados aos processos e acompanhamento do cumprimento das metas estabelecidas;

2.1.3.1.5.14. Possibilitar a geração de diversos tipos de relatórios e gráficos contendo informações detalhadas ou resumidas sobre os processos e atividades;

2.1.3.1.5.15. Possuir semáforos que sinalizam visualmente o nível de cumprimento dos resultados;

2.1.3.1.5.16. Possuir indicador de tendência sobre possíveis problemas futuros;

2.1.3.1.5.17. Permitir a formatação dos resultados em planilhas e gráficos configuráveis pelo usuário;

2.1.3.1.5.18. Permitir a visualização dos recursos e custos requeridos para a execução dos processos.

2.1.3.1.5.19. Efetuar a manutenção das regras e políticas do parque monitorado para responder a incidentes, à exceção dos ativos sob gestão exclusiva do PJERJ, cujos incidentes ou resultados de monitoração devem ser informados ao PJERJ.

2.1.4. **Análise de impacto no negócio (AIN)**

2.1.4.1. A CONTRATADA deverá elaborar a Análise de Impacto no Negócio - AIN, para quantificará o impacto que a perda do serviço de SI impactará no negócio do CONTRATANTE.
2.1.4.2. A CONTRATADA Através de análise de Risco deverá identificar potenciais ameaças para a continuidade e a probabilidade que porventura acontecer. Precisando também incluir medidas para gerenciar as ameaças identificadas, quando o custo se justificar.
2.1.4.3. A CONTRATADA efetuará análise contendo:
2.1.4.3.1. A identificação dos serviços críticos ao negócio do CONTRATANTE;
2.1.4.3.2. Determinar os efeitos da indisponibilidade;
2.1.4.3.3. Avaliação do cenário que será impactado;
2.1.4.3.4. Análise das obrigações legais junto ao cumprimento pela CONTRATADA e CONTRATANTE;
2.1.4.3.5. Análise do tempo que o CONTRATANTE se manterá em caso de indisponibilidade total da TI;
2.1.4.3.6. Avaliação dos requisitos mínimos de restabelecimento (pessoal, infraestrutura e serviços) para assegurar os processos críticos para o CONTRATANTE;
2.1.4.4. Determinar o tempo mínimo e máximo dos níveis de serviços a serem recuperados;
2.1.4.5. Determinar quais processos do CONTRATANTE devem ser recuperados por completo.

3. Privacidade e Proteção de Dados Pessoais

3.1. A CONTRATADA deverá executar serviços para estabelecer um programa de governança e gerenciamento de privacidade conforme os requisitos estabelecidos na Lei Geral Proteção de Dados.
3.2. Deverá ser realizado o levantamento prévio de informações para alinhar as expectativas com a CONTRATANTE e a definição do cronograma de execução das atividades. Nesta fase serão realizadas reuniões entre a CONTRATANTE e a CONTRATADA.
3.3. Atividades a serem desenvolvidas
3.3.1. Planejamento
3.3.1.1. Na fase de planejamento a CONTRATADA deverá:
3.3.1.1.1. Identificar e tomar conhecimento da estrutura organizacional da CONTRATANTE;
3.3.1.1.2. Definir quais as pessoas envolvidas da empresa CONTRATADA e da CONTRATANTE;
3.3.1.1.3. Auxiliar o Comitê de Proteção de Dados Pessoais da CONTRATANTE;

3.3.1.1.4. Detalhar todos os procedimentos, normativos e processos que serão objeto da análise;

3.3.1.1.5. Definir as principais áreas / departamentos afetados;

3.3.1.1.6. Definir o formato das entrevistas iniciais (cronograma, quais os envolvidos, datas, local da entrevista, forma de divulgação e documentação);

3.3.1.1.7. Identificar e definir os entrevistados;

3.3.1.1.8. Documentar todas as fases da execução do diagnóstico;

3.3.1.1.9. Avaliar e definir, de forma preliminar, o grau de conhecimento da CONTRATANTE acerca da Lei Geral de Proteção de Dados;

3.3.1.1.10. Definir o formato do seminário inicial para nivelamento das pessoas que serão afetadas pelo Projeto (localização, datas, horário, público, recursos áudio visuais necessários) em conjunto com o CONTRATANTE;

3.3.1.1.11. O workshop deverá contemplar a participação de toda a organização e aprovada pelo CONTRATANTE;

3.3.1.1.12. A CONTRATADA deverá realizar o mapeamento dos processos de negócio que envolvem o tratamento de dados pessoais, assim como o entendimento do ambiente de segurança da informação e identificação dos principais contratos impactados, avaliação de políticas e demais documentos relevantes;

3.3.1.1.13. As atividades dever-se-ão desenvolver por meio da coleta de evidências (testemunhais, físicas, documentais e analíticas) com a finalidade de mapear preliminarmente os dados pessoais dentro das principais áreas/departamentos/unidades de negócio da CONTRATANTE, que permitindo a compreensão do nível de conformidade da organização perante a Lei Geral de Proteção de Dados Pessoais;

3.3.1.1.14. As atividades desenvolvidas na fase de Diagnóstico servirão de subsídios para a realização das demais atividades;

3.3.1.1.15. As entrevistas deverão ser realizadas preferencialmente de forma presencial com os departamentos identificados como afetados, e são necessárias para que a empresa a ser contratada possa entrar em contato com os colaboradores de áreas chave, e possa determinar o grau de maturidade e adequação a Lei LGPD e às boas práticas de segurança da informação;

3.3.1.2. Na fase de diagnóstico a CONTRATADA deverá:

3.3.1.2.1. Mapear os repositórios de dados pessoais existentes e conhecidos na CONTRATANTE;

3.3.1.2.2. Mapear os repositórios de dados não estruturados (planilhas, documentos e outros arquivos), indexar o conteúdo desses arquivos e classificá-los caso o arquivo contenha Dados Pessoais ou Dados Pessoais Sensíveis;

3.3.1.2.3. Identificar o fluxo dos dados pessoais dentro e fora da CONTRATANTE, quer seja através de entrevistas ou através de análise de processos;

3.3.1.2.4. Identificar e analisar a estrutura atual de governança de dados, políticas, controles de segurança e de acesso às informações, assim como as vulnerabilidades;

3.3.1.2.5. Identificar e analisar os normativos existentes (Instruções normativas, resoluções, códigos, comunicados internos, regimentos), tendo por parâmetro a LGPD;

3.3.1.2.6. Desenvolver um mapa com identificação dos principais tipos/grupos de contratos existentes;

3.3.1.2.7. Identificar as hipóteses de transferência internacional de dados;

3.3.1.2.8. Identificar os GAPs existentes quanto ao tratamento de dados pessoais;

3.3.1.2.9. Definição de conformidade

3.3.1.2.10. A CONTRATADA deverá, com o apoio da CONTRATANTE, esclarecer dúvidas e validação de processos que envolvem dados pessoais;

3.3.1.3. Na fase de definição de conformidade a CONTRATADA deverá:

3.3.1.3.1. Avaliar, a partir das informações coletadas na fase anterior, os níveis de aderência à LGPD e definir o status de conformidade com as regulamentações;

3.3.1.3.2. Apresentar os principais GAPs endereçados;

3.3.1.3.3. Definir, em conjunto com a CONTRATANTE, o apetite de risco da organização, perante a sua estratégia de produtos e serviços.

3.3.1.3.4. A CONTRATADA deverá coordenar e executar plano de ação para implementação da Lei Geral de Proteção de Dados no âmbito do PJERJ contendo no mínimo as seguintes fases:

3.3.1.3.4.1. **Organização e Comunicação**;

3.3.1.3.4.1.1. Identificar contatos no departamento jurídico, RH e outros grupos interessados/envolvidos no processo;

3.3.1.3.4.1.2. Identificar papéis na própria organização e de parceiros: controladores de dados/processadores de dados;

3.3.1.3.4.1.3. Comunicar campanha para todos os grupos relevantes de interessados / plano de comunicação;

3.3.1.3.4.1.4. Criar novo aviso de privacidade e publicar (externamente);

3.3.1.3.4.1.5. Criar uma nova política de privacidade e publicar (internamente);

3.3.1.3.4.2. **Processos;**

3.3.1.3.4.2.1. Criar inventário de todos os processos de negócios que envolvem dados de identificação pessoal;

3.3.1.3.4.2.2. Identificar quais dados pessoais são processados e em quais processos de negócio;

3.3.1.3.4.2.3. Identificar motivos para processar dados pessoais ("propósito de processamento");

3.3.1.3.4.2.4. Determinar e documentar bases legais para o processamento de dados pessoais;

3.3.1.3.4.2.5. Identificar processadores de dados envolvidos em processos de negócios (ver item 7) com apoio DGTEC;

3.3.1.3.4.2.6. Identificar de que forma os dados são processados em cada processo;

3.3.1.3.4.2.7. Identificar todo e qualquer subprocesso (onde se aplicar);

3.3.1.3.4.2.8. Alterar os processos de negócios existentes para garantir a minimização dos dados utilizados;

3.3.1.3.4.2.9. Lista de Remoção todos os dados pessoais que não cumpram os critérios do propósito do processamento;

3.3.1.3.4.2.10. Realizar avaliação de impacto à: privacidade (PIA), proteção de dados (DPIA), quando necessários;

3.3.1.3.4.2.11. Criar ou alterar processo de avaliação de risco com apoio DGTEC;

3.3.1.3.4.3. **Direitos do Titular de Dados;**

3.3.1.3.4.3.1. Criar processo para tratar direito de acesso pelo titular dos dados;

3.3.1.3.4.3.2. Criar processo para tratar direito de retificação;

3.3.1.3.4.3.3. Criar processo para tratar direito de apagamento;

3.3.1.3.4.3.4. Criar processo para tratar direito de restrição de processamento;

3.3.1.3.4.3.5. Criar processo para tratar notificação;

3.3.1.3.4.3.6. Criar processo para tratar direito de portabilidade de dados;

3.3.1.3.4.3.7. Criar processo para tratar direito de se opor;

3.3.1.3.4.3.8. Criar processo para tratar direito de não estar sujeito a decisões baseadas em perfis, etc;

3.3.1.3.4.4. **Proteção de Dados;**

3.3.1.3.4.4.1. Revisar o atual armazenamento de dados pessoais;

3.3.1.3.4.4.2. Conduzir avaliação de risco (quando apropriado);

3.3.1.3.4.4.3. Identificar e implementar medidas técnicas e organizacionais adequadas para proteger os dados pessoais.

3.3.1.3.4.5. **Gestão de Consentimento e Preferências;**

3.3.1.3.4.5.1. Identificar todos os pontos de contato onde é obtido o consentimento do titular dos dados;

3.3.1.3.4.5.2. Identificar os processos para os quais é necessário o consentimento;

3.3.1.3.4.5.3. Identificar processadores e controladores de dados envolvidos com dados para os quais é necessário consentimento;

3.3.1.3.4.5.4. Revisar gestão de consentimento existente no website/portal e alterar de acordo com LGPD;

3.3.1.3.4.5.5. Revisar gestão de consentimento existente em formulários de papel e alterar de acordo com LGPD;

3.3.1.3.4.5.6. Desenvolver processo para obter o consentimento dos pais nos casos em que dados de menores são coletados;

3.3.1.3.4.6. **Retenção de Dados e de backup;**

3.3.1.3.4.6.1. Revisar os requisitos de retenção de dados existentes;

3.3.1.3.4.6.2. Revisar processos de backup existentes;

3.3.1.3.4.6.3. Alterar políticas de retenção de dados e processos de backup;

3.3.1.3.4.7. **Contratos;**

3.3.1.3.4.7.1. Criar acordos de processador-controlador onde ainda não existe ou não está em vigor;

3.3.1.3.4.7.2. Atualizar acordos do controlador-processador (uso intencional e requisitos de segurança);

3.3.1.3.4.7.3. Atualizar processo de aquisição (critérios de seleção para novos serviços);

3.3.1.3.4.7.4. Atualizar processo de aquisição (novas exigências incluídas nos novos contratos).

3.3.1.3.4.8. **Preparação para Possível Violação de Dados.**

3.3.1.3.4.8.1. Identificar dados de contato relativos a Autoridade Nacional de Proteção de Dados (DPA);

3.3.1.3.4.8.2. Desenvolver o processo de gerenciamento de violações para permitir a notificação dentro de 48 (quarenta e oito) horas;

3.3.1.3.4.8.3. Testar o processo de gerenciamento de violações (semestralmente).

3.4. **Boas práticas a serem recomendadas pela CONTRATADA**

3.4.1. A CONTRATADA deverá documentar, consolidar e encerrar o projeto, com o registro detalhado de todas as atividades realizadas nas etapas anteriores, a análise crítica da situação atual da CONTRATANTE perante a LGPD e, a emissão de um relatório detalhado com as

recomendações de atividades e projetos a serem implementados para adequação à lei. Essa fase deverá se refletir em um Relatório executivo que deverá conter:

3.4.1.1. Gráficos do Grau de Maturidade da Organização;

3.4.1.2. Os níveis de conformidade de cada item analisado;

3.4.1.3. Inventário dos repositórios de dados pessoais e dados pessoais sensíveis;

3.4.1.4. Mapa do Fluxo dos principais processos que envolvem dados pessoais identificados no contexto da CONTRATANTE, da coleta até o descarte;

3.4.1.5. Análise dos resultados obtidos na fase de Diagnóstico e Definição;

3.4.1.6. Identificação de normativos e procedimentos a serem modificados;

3.4.1.7. Identificação como agente de tratamento e responsabilidades;

3.4.1.8. Indicação de cláusulas a serem inseridas em contratos;

3.4.1.9. Apresentação de uma carteira de projetos, contendo as ações e projetos que devem ser implementados para adequação à Lei.

3.4.2. Todas as recomendações de melhoria e adequação à LGPD devem ser apresentadas individualmente por meio de fichas de projetos dentro de uma linha do tempo, contendo os detalhes:

3.4.2.1. Qual o problema ou vulnerabilidade encontrada;

3.4.2.2. Qual a recomendação de adequação;

3.4.2.3. Qual o dispositivo da Lei é afetado;

3.4.2.4. Quais as alternativas possíveis;

3.4.2.5. Quais os custos estimados.

3.4.3. As recomendações realizadas, após aprovação da CONTRATANTE, devem ser incluídas na matriz de risco, sendo acompanhadas até sua resolução;

3.4.4. Deverá ser fornecida e implantada uma Plataforma de Privacidade para que possam ser implementados os requisitos exigidos pela Lei.

3.4.5. Atividades básicas

3.4.5.1. A CONTRATANTE e CONTRATADA se compromete a seguir todas as orientações da ATO NORMATIVO TJ N.º 08/2019, ATO NORMATIVO TJ Nº 10/ 2019 e ATO NORMATIVO TJ Nº 27/ 2020 e os que vierem a substituí-los.

3.4.5.2. A CONTRADADA não pode armazenar dados classificados do CONTRATANTE, no seu ambiente de nuvem da CONTRATANTE, devendo observar o disposto sobre tratamento da informação em computação em nuvem do ATO NORMATIVO TJ N.º 08/2019, exceto a documentação e dados das ferramentas.

3.4.5.3. A CONTRATADA deve assegurar que os dados, metadados, informações e conhecimento, tratados no ambiente de computação em nuvem, não serão fornecidos a terceiros e/ou uso para fins diferentes do escrito neste Termo de Referência, sob nenhuma hipótese, sem concordância formal da CONTRATANTE.

3.4.5.4. Os Serviços objeto deste Termo de Referência deverão seguir as orientações condas na Lei Nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD).

3.5. **Plataforma de Privacidade**

3.5.1. Especificação técnica da ferramenta de gestão de privacidade

3.5.1.1. Requisitos do Fabricante e Integrador da solução

3.5.1.1.1. O fabricante da solução deve ser uma empresa líder global, evidenciado por relatórios de analistas (Forrester, Gartner, IDC ou similares)

3.5.1.1.2. O fabricante da solução deve possuir time próprio presente no Brasil

3.5.1.1.3. O fabricante da solução deve oferecer um portal para clientes com conteúdo, treinamento e certificação gratuita na solução

3.5.1.1.4. O fabricante do software ofertado e/ou integrador devem possuir pessoal treinado e certificado em privacidade (Exin ou IAPP) e segurança (ISC2, SANS, EC-Council ou CompTIA)

3.5.1.1.5. O fabricante da solução deve possuir certificações como SOC 2 tipo I ou tipo II, ISO 27001, ou similares

3.5.1.1.6. O fabricante da solução e/ou integrador devem oferecer suporte 24x7 de primeiro nível

3.5.1.1.7. O fabricante da solução deverá ter informação clara e disponível online sobre problemas e indisponibilidades na plataforma, bem como histórico e agendamento de manutenções programadas no sistema, listando o que será afetado nas mudanças.

3.5.1.1.8. O fabricante da solução deverá garantir disponibilidade superior a 99,5%.

3.5.1.1.9. A solução deve permitir a partir de seu portal de gerenciamento abrir tickets de suporte técnico com o fabricante da solução, os quais poderão ser acompanhados diretamente deste portal.

3.5.1.2. Arquitetura da solução

3.5.1.2.1. Todas as funcionalidades e módulos da solução devem ser do mesmo fabricante, com finalidade de maior integração nativamente e ganhos operacionais, portanto não sendo aceitas composições de ferramentas e diferentes tecnologias de mercado

3.5.1.2.2. A solução deve ser licenciada de forma modular, permitindo a escolha dos módulos desejados e possibilidade de inclusão/upgrade futuro de outros módulos

3.5.1.2.3. A solução deve ser oferecida com arquitetura e implementação no modelo SaaS para seu console de gerenciamento e demais módulos, hospedada em serviço de nuvem AWS, Azure ou GCP

3.5.1.2.4. A solução não deve requerer VPN para acesso ao ambiente ao cliente nem publicação de serviços/portas do cliente para internet

3.5.1.2.5. A solução não deve requerer banco de dados para funcionamento básico do seu console e principais módulos

3.5.1.2.6. Para o acesso a fontes de dados on-premises ou IaaS, a solução deve oferecer a opção de uso de máquina virtual no ambiente on-premises ou IaaS do cliente, especificamente para o componente de Data Discovery que acessará o ambiente local, e que este tenha comunicação de saída HTTPS com opção de uso de proxy, para o SaaS do fabricante da solução

3.5.1.2.7. A máquina virtual citada deve suportar virtualizador VMWare e Hyper-V, e sistema operacional Ubunto, RedHat e SUSE.

3.5.1.2.8. Para o acesso a fontes de dados SaaS a solução deve permitir o acesso diretamente nuvem-nuvem sem a necessidade de componentes na infraestrutura on-premises ou IaaS do cliente

3.5.1.2.9. Todo o gerenciamento dos componentes e funções administrativas devem ser feitas através de uma única interface web, acessível por navegador web moderno, sem a necessidade de instalação de aplicações ou plug-ins adicionais

3.5.1.2.10. A solução deve ser multiusuário, isto é, permitir logins simultâneos ilimitados e não restringir no licenciamento e tecnicamente a quantidade de usuários cadastrados para uso do console

3.5.1.2.11. Deve oferecer API nativa e documentada para os módulos de Requisições de Titulares (DSR), Consentimento do titular, consentimento de Cookies e Mapeamento de dados, fornecendo documentação online das funções disponíveis nas APIs e também no formato swagger.

3.5.1.2.12. A autenticação dos usuários ao console da solução deve suportar Single Sign-on no padrão SAML 2.0

3.5.1.2.13. A solução deve oferecer autenticação com duplo fator (MFA) para usuários que administrarão a solução

3.5.1.2.14. A solução deve permitir a criação de usuários internos de maneira ilimitada no Console da ferramenta

3.5.1.2.15. A solução deve ter a capacidade de permitir o cadastramento de usuários internos através de um ou mais domínios da empresa.

3.5.1.2.16. A solução deve permitir a criação de usuários externos, com perfil de Parceiro/Consultor, permitindo o registro por e-mail de domínio externo autorizado

3.5.1.2.17. A solução deve permitir a criação de usuários em massa, através de importação de arquivo CSV, incluíndo nome, email e perfil do usuário

3.5.1.2.18. A solução deve permitir a geração automática de senhas para os usuários cadastrados, quando não integrada a um SSO, e envio desta por email ao usuário em questão

3.5.1.2.19. A solução ofertada deve oferecer perfis de acesso com níveis ao menos Administrador, Operador e Usuário, permitindo criar novos perfis

3.5.1.2.20. A solução deve permitir limitar por perfil de acesso que módulos podem ser acessados pelos usuários, ocultando os que não têm acesso

3.5.1.2.21. Deve possuir trilha de auditoria com logs de atividades administrativas e de gerenciamento executadas no portal

3.5.1.2.22. A solução deve permitir a inserção do Logotipo da empresa nas telas que forem externas, destinadas a titulares de dados e fornecedores

3.5.1.2.23. A solução deve oferecer log de auditoria de todas as operações do sistema, acessível diretamente pelo Console Web, protegido contra deleção (somente leitura)

3.5.1.2.24. A solução deve permitir o envio de notificações e alertas configuráveis por e-mail

3.5.1.2.25. A solução deve permitir o envio de notificações e alertas de maneira resumida, sendo possível selecionar a periodicidade exemplo (Dia e Hora)

3.5.1.3. Experiência do Usuário

3.5.1.3.1. A solução deve prover interface (console) nos idiomas Português Brasileiro, Inglês e Espanhol ao menos, definidos de forma global mas também configuráveis como preferência individual de usuários

3.5.1.3.2. A solução deve possuir interface amigável ao usuário, também para usuários que não sejam técnicos de TI

3.5.1.3.3. A solução deve permitir acesso por navegador web Chrome, Safari e Firefox, de desktop e dispositivos móveis Android e IOS

3.5.1.3.4. A solução deve oferecer integração nativa de todos os módulos, dando ao usuário uma interface uniformizada e navegação coerente

3.5.1.3.5. A solução deve oferecer Ajuda Online no próprio console, incluíndo vídeo tutorial dos principais módulos da solução

3.5.1.3.6. A solução deve fazer log-off automático de sessões inativas de usuários, notificando-os com pop-up e contador de tempo decrescivo antes do log-off

3.5.1.4. Módulo de Direitos de Titulares - DSAR

3.5.1.4.1. A solução deve receber, organizar e apoiar no processamento de requisições de titulares de dados que exerçam seus direitos da LGPD

3.5.1.4.2. A solução deve permitir a criação de formulários web (DSR) seguros (HTTPS), hospedado na própria solução com possibilidade de "incorporar" no site da empresa, onde o titular de dados fará suas requisições

3.5.1.4.3. O formulário web (DSR) deve permitir customização de campos, cores, logotipo, títulos, de acordo com a necessidade da empresa, através de editor de formulários online da própria ferramenta

3.5.1.4.4. A solução deve prover um Portal de Direitos de Titular, onde o titular de dados possa acessar o histórico e detalhes das suas requisições já finalizadas e ativas, com retenção online configurável para até 5 anos

3.5.1.4.5. O formulário web (DSR) deve possibilitar o envio de Anexos (configurável e opcional) para apoiar no atendimento da requisição e na validação de identidade, e estes anexos serão anexados à requisição

3.5.1.4.6. Deve permitir a integração com provedores externos de validação de identidade (biometria, face-match, documentos) como uma opção configurável

3.5.1.4.7. O formulário web (DSR) e Portal de Direitos de Titular devem ser multi-idioma, tendo Português Brasileiro como padrão, e permitindo ao titular de dados escolher o idioma alternativo (Inglês e Espanhol ao menos) no próprio formulário online

3.5.1.4.8. A solução deve permitir a criação manual de requisições diretamente no Console, em nome de titular de dados, pelo time de Privacidade da empresa internamente, caso tenha sido recebido por outro canal

3.5.1.4.9. A solução deve oferecer APIs nativas e documentadas para permitir o recebimento de requisições de titulares oriundas de outro sistema/canal de atendimento da empresa

3.5.1.4.10. A solução deve requerer validação do e-mail do titular que submeter requisições pelo Formulário Web, gerando um código numérico ou link enviado ao e-mail preenchido, e somente aprovar a requisição caso tenha o e-mail validado

3.5.1.4.11. A solução deve possuir um painel central onde o time de Privacidade da empresa possa visualizar e gerenciar a fila de todas as requisições recebidas dos titulares, com filtros por data, titular, tipo de requisição, dentre outros

3.5.1.4.12. A solução deve permitir exportar a lista de requisições filtradas no Console, para formato CSV

3.5.1.4.13. A solução deve permitir definir o prazo/meta de atendimento das requisições e indicar no console quantos dias faltantes, com possibilidade de notificar o time de Privacidade antes do vencimento

3.5.1.4.14. A solução deve gerar uma notificação automática de prorrogação da requisição para o titular de dados, caso ultrapasse o prazo definido, utilizando de um template customizável da empresa

3.5.1.4.15. A solução deve gerar um protocolo individual para cada requisição feita pelos titulares de dados

3.5.1.4.16. Deve ter a capacidade comunicação por mensagens entre o DPO e o titular de dados de maneira segura, rápida e instantânea, para facilitar a validação ou o atendimento de requisições recebidas;

3.5.1.4.17. Deve prover automatização de requisições nativa da ferramenta, sem requerer criação de fluxos de trabalho (workflow), para atendimento aos direitos de titulares.

3.5.1.4.18. Deve gerar indicador de % de tempo salvo pela automatização das requisições de titulares.

3.5.1.4.19. A solução deve alimentar de forma automatizada as requisições recebidas com os seguintes recursos:

3.5.1.4.20. Dados pessoais identificados nas fontes de dados estruturados e não estruturados, que sejam referentes ao titular da requisição em questão e criar tarefas e subtarefas para cada fonte de dado estruturado e não estruturado e cada objeto que tenha encontrado informações pessoais do titular, como ações que são requeridas para validação e atendimento da requisição recebida.

3.5.1.4.21. Atribuir responsáveis para cada tarefa de forma automatizada para revisão da solicitação.

3.5.1.4.22. Correlacionar dados pessoais estruturados e não estruturados por titularidade.

3.5.1.4.23. Deve ter a capacidade de criar registros de entrega e o resultado de cada requisição DSR, documentando exatamente "o que" foi feito, "quando" foi feito e "por quem" foi feito, permitindo exportação destes logs pelo console gráfico se preciso, para uma ou mais requisições

3.5.1.4.24. Deve ter a capacidade de processar uma requisição de maneira automática e caso não detecte dados pessoais do titular pelo módulo de Data Discovery, deve fechá-la

automaticamente informando ao requerente que nenhum dado foi encontrado, através de uma mensagem padrão (modelo customizável).

3.5.1.4.25. A solução deve permitir a configuração da retenção e armazenamento das requisições de titulares por um prazo de até 5 anos online na própria solução.

3.5.1.4.26. Deve permitir o reprocessamento de requisições recebidas e ainda abertas, para o caso de adição de novas fontes de dados ao módulo de Data Discovery ou mudança na lógica de automação seja incorporada ao sistema.

3.5.1.4.27. Deve prover a possibilidade de armazenar os anexos das requisições em infraestrutura de propriedade do cliente, tendo como opção GCP, Azure ou AWS S3

3.5.1.4.28. A solução deve oferecer uma interface web responsiva a dispositivos como Desktop, Tablets e Smartphones

3.5.1.4.29. A solução deve permitir filtrar a lista de requisições de titulares (DSR)c om no mínimo os seguintes campos: Status; Tipo de Requisição; Data da criação; Proprietário da requisição; Titular; Prazo de Atendimento;

3.5.1.4.30. Deve possuir modelos predefinidos e customizáveis para comunicação por mensagens com um titular de dados em relação à sua solicitação.

3.5.1.5. Módulo de Mapeamento de Processos, Ativos e Fluxos de Dados - Data Mapping

3.5.1.5.1. Deve ter a capacidade de suportar as iniciativas de mapeamento de dados (Data Mapping), incluindo catálogo de Ativos de TI, Fornecedores e Entidades, Processos de negócio (atividades de tratamento).

3.5.1.5.2. Deve integrar o módulo de Mapeamento de Dados (Data Mapping) com o módulo de Descoberta de Dados (Data Discovery), de forma a atualizar automaticamente os elementos de dados pessoais detectados pelo Discovery no Ativo de TI catalogado no Data Mapping.

3.5.1.5.3. Deve suportar customizar os campos e em qualquer quantidade que sejam compatíveis para o upload via CSV

3.5.1.5.4. Deve gerar mapas gráficos do fluxo de dados automaticamente ao se relacionar itens catalogados dentro de um processo (atividade de tratamento).

3.5.1.5.5. Deve permitir catalogar atributos de dados pessoais dentro de Ativos de TI

3.5.1.5.6. Deve se integrar ao módulo de Avaliações permitindo o envio de questionários web para coleta de dados de ativos, processos, fornecedores entre outros para criação destes itens no catálogo do Data Mapping e atualização dos mesmos.

3.5.1.5.7. Deve permitir enviar questionários atrelados a um processo, ativo, fornecedores e instituições, para mapear novos riscos associados a estes objetos catalogados.

3.5.1.5.8. Deve permitir conceder acesso ao console para visualização e edição dos objetos do catálogo, registrando quaisquer alterações feitas no catálogo no log de auditoria.

3.5.1.5.9. Deve permitir o versionamento de Processos catalogados.

3.5.1.5.10. Deve permitir a geração de relatórios tipo RoPA, de um processo selecionado em PDF e CSV, e de múltiplos processos em CSV.

3.5.1.5.11. Deve prover capacidade de chat interno na ferramenta, dentro do contexto do objeto catalogado (ex: Processo, Ativo) que está sendo trabalhado, para facilitar a comunicação com os times envolvidos

3.5.1.5.12. Deve oferecer um portal de autoatendimento via web, onde áreas de negócio podem registrar voluntariamente novos Processos, que devem ser direcionados dentro da ferramenta para aprovação do time de privacidade, sendo automaticamente incorporados ao catálogo se aprovados

3.5.1.6. Módulo de Descoberta de Dados - Data Discovery

3.5.1.6.1. Deve ter a capacidade de integração com soluções de mercado do tipo SaaS e On-Premises

3.5.1.6.2. Deverá ter a capacidade de permitir a criação de Atributos de Dados adicionais aos padrões, por meio de:

3.5.1.6.2.1. Expressões regulares (regex);

3.5.1.6.2.2. Dicionário;

3.5.1.6.2.3. Palavras-Chave.

3.5.1.6.3. Os Atributos de Dados criados deverão ter a configuração de taxa esperada de falha.

3.5.1.6.4. Deve permitir configurar qual o tipo de fonte de dados utilizará esse novo atributo, exemplo: Se afetará só fontes não estruturadas, só fontes estruturadas ou ambos.

3.5.1.6.5. Deverá oferecer por padrão mecanismo de detecção próprio de grande diversidade de dados pessoais, sem a necessidade de criação manual de regras, contemplando ao menos:

3.5.1.6.5.1. Dados de contato

3.5.1.6.5.2. Dados de educação

3.5.1.6.5.3. Dados financeiros

3.5.1.6.5.4. Dados médicos

3.5.1.6.5.5. Documentos diversos, incluindo ao menos CPF, CNH, RG, Passaporte

3.5.1.6.5.6. Contas de rede social

3.5.1.6.5.7. Dados de localização e endereço

3.5.1.6.5.8. Dados de veículos

3.5.1.6.5.9. Dados profissionais e de renda

3.5.1.6.5.10. Atributos físicos de pessoas

3.5.1.6.5.11. Idioma, raça e etnia

3.5.1.6.5.12. Opiniões políticas, crenças religiosas, orientação sexual

3.5.1.6.6. Para fontes de dados SaaS, a solução deve permitir a conexão direta com a fonte de dados (SaaS para SaaS), sem requerer infraestrutura no ambiente da empresa

3.5.1.6.7. Deve ter a capacidade de detectar e descobrir automaticamente a estrutura de bases de dados, suas tabelas, colunas, views, índices e relacionamento

3.5.1.6.8. Deve ser capaz de analisar fontes de dados tipo banco de dados através de amostragem (linhas de base de dados), automaticamente identificando que tabelas e colunas contém dados pessoais, e quais são estes atributos, sem necessidade de especificar que tabelas e campos verificar, nem ao menos requerer definir queries manuais.

3.5.1.6.9. No caso de dados estruturados, deve permitir revisar e alterar a classificação feita automaticamente, bem como informar campos adicionais que não forem padrão da ferramenta

3.5.1.6.10. Deve ser capaz de analisar dados não estruturados em formatos de arquivos comuns de mercado, como pdf, csv, xlsx, xls, msg, doc, docx, google docs, ppt, pptx, json, 7zip, zip, mdb, dentre outros

3.5.1.6.11. Deve permitir definir a periodicidade e janelas de exclusão de horário para execução da descoberta de dados incremental

3.5.1.6.12. Deve prover maneira escalável de realizar o Discovery de dados de sistemas on-premises, permitindo instalar uma máquina virtual local no ambiente da empresa, não requerendo VPN site to site ou publicação de serviços e portas para internet para conexão da solução em nuvem com a fonte de dados on-premises

3.5.1.6.13. A Solução deve prover o módulo de Descoberta de Dados de maneira nativa, não será aceito composição com softwares de terceiros de outro fabricante

3.5.1.6.14. Deve ter a capacidade de executar automaticamente a descoberta e seleção de elementos de Dados em cada fonte de dados conectada à solução

3.5.1.6.15. Deve se integrar ao módulo de Mapeamento de Dados (Data Mapping) para registro automático no Ativo catalogado dos atributos de dados pessoais localizados pelo módulo de Descoberta de Dados (Data Discovery).

3.5.1.6.16. Deve oferecer conectores nativos da solução para conexão aos principais sistemas da empresa como:

3.5.1.6.16.1. Bases de Dados Relacionais como SQL Server, MySQL, PostgreSQL, Oracle, Sybase, DB2, Progress, MS Access

3.5.1.6.16.2. Aplicações de bigdata e NoSQL como Amazon Athena, Amazon Postgres, DynamoDb, Redshift, Azure Data Warehouse, Elasticsearch, Google BigQuery, MongoDB

3.5.1.6.16.3. Aplicações de CRM como SAP ECC, SAP HANA, SAP SuccessFactors, Zoho CRM, Oracle ERP, Microsoft Dynamics CRM

3.5.1.6.16.4. Aplicações Salesforce e Salesforce Marketing Cloud

3.5.1.6.16.5. Aplicações de marketing como Mailchimp, Surveymonkey, Facebook Workplace, SendGrid, Google Analytics, Tableau, Salesforce Marketing Cloud

3.5.1.6.16.6. Aplicações de colaboração como ServiceNow, Zendesk, Jira, Trello, Asana e Slack

3.5.1.6.16.7. Servidor de arquivo on-premises via SMB e NFS

3.5.1.6.16.8. Soluções de armazenamento de arquivos SaaS como Dropbox, Box, Google Drive, OneDrive

3.5.1.6.16.9. Suite do Office 365 incluindo Outlook, Sharepoint, Onedrive e Celandário

3.5.1.6.16.10. Suite do Google incluindo GMail, Calendário e Google Drive

3.5.1.6.17. A solução deve ter conector de replicação de base de ativos, compatível com AWS e ServiceNow CMDB ao menos, detectando automaticamente novos sistemas através destas integrações, e cadastrando-os na base de ativos da solução

3.5.1.6.18. A solução deve prover recursos de verificação de configurações de segurança para AWS S3, com capacidade de remediação destas, com objetivo de identificar se o repositório de dados pessoais está seguro

3.5.1.6.19. A solução deve possuir a capacidade de leitura de etiquetas de classificação nos arquivos encontrados

3.5.1.6.20. A solução deve possuir a capacidade de integração com o Microsoft Information Protection para aplicação de etiquetas de classificação nos arquivos armazenados em fontes de dados do tipo SMB

3.5.1.7. Módulo de Gestão de Consentimento Universal

3.5.1.7.1. Deve ter a capacidade de registrar eventos de novos consentimentos concedidos, negados, e revogados, com o detalhe da data, identificador do titular, fonte de consentimento (ponto de coleta) e finalidade associada.

3.5.1.7.2. Deve ter a capacidade de suportar múltiplas maneiras de coleta de dados como por API, por integração com formulário web, e por um formulário de consentimento para o titular.

3.5.1.7.3. A Solução deve prover API Restful própria e documentada, permitindo integração por get e post para coleta de novos eventos de consentimento oriundos de soluções externas e para leitura dos consentimentos armazenados centralizadamente na ferramenta

3.5.1.7.4. A solução deve relacionar o evento de consentimento ao titular de dados por identificador como CPF e EMAIL.

3.5.1.7.5. A solução deve prover workflow para orquestração de ações referentes ao consentimento registrado, com ações internas da própria ferramenta e também com integração a outras soluções externas como, SQL, ORACLE, SALESFORCE, SLACK, outros, para facilitar o cumprimento de revogações e mudanças de preferência dos titulares

3.5.1.7.6. A solução deve prover um dashboard que permita filtrar por, no mínimo:

3.5.1.7.6.1. Consentimentos de um titular de dados específico

3.5.1.7.6.2. Ponto de coleta do consentimento

3.5.1.7.6.3. Consentimentos aceitos, revogados e negados.

3.5.1.7.6.4. Finalidade de Processamento

3.5.1.7.6.5. Por período

3.5.1.7.7. A solução deve permitir a criação de uma central de preferências para o titular de dados que exiba todos os consentimentos registrados em seu nome, permitindo também que os altere ou revogue se desejar, como autoatendimento (self-service);

3.5.1.7.8. Para pontos de coleta de consentimento via integração a formulários web, a solução deve analisar a página em questão e automaticamente gerar o código fonte e scripts para inserção na página-alvo de coleta de consentimento.

3.5.1.7.9. A solução deve permitir filtrar e exportar a lista de consentimentos em formato CSV, através de seu console gráfico

3.5.1.7.10. O consentimento recebido deve ter a possibilidade de visualização em uma tela de administração mostrando os seguintes dados:

3.5.1.7.10.1. Identificador do Titular;

3.5.1.7.10.2. Proposito de do consentimento;

3.5.1.7.10.3. Status do Consentimento;

3.5.1.7.10.4. Data do Consentimento;

3.5.1.7.10.5. O ponto de coleta utilizado;

3.5.1.7.10.6. Dados fornecidos pelo titular atrelados ao evento do consentimento

3.5.1.8. Módulo de Gestão de Consentimento de Cookies

3.5.1.8.1. Solução deverá ter a funcionalidade de Gerenciamento de Consentimento de Cookies.

3.5.1.8.2. A solução deve ter a capacidade de realizar varredura em sites hospedados em domínios de internet

3.5.1.8.3. Deve classificar automaticamente os cookies detectados nos sites verificados, classificando-os por uma base global de cookies de terceiros conhecidos mantida e atualizada pelo próprio fabricante

3.5.1.8.4. Deve ter a capacidade de classificar os cookies com no mínimo as seguintes categorias relativas: Essencial, Publicidade, Análise e Personalização, Desempenho e Funcionalidade e, Não Classificado.

3.5.1.8.5. A categorização dos cookies deve permitir ao administrador renomear as categorias, marcar individualmente que categorias são obrigatórias e quais podem ser incluídas no opt-in/opt-out dos titulares

3.5.1.8.6. A categorização dos cookies deve permitir ao administrador mover cookies entre categorias, caso seja necessário reclassificar cookies não classificados automaticamente

3.5.1.8.7. A solução deve incluir a funcionalidade de script bloqueador de Cookies nativo da solução.

3.5.1.8.8. A solução deve ter a opção de integração com GTM (Google Tag Manager) caso este esteja presente no site em questão

3.5.1.8.9. A solução deve ter a capacidade de permitir as seguintes configurações ao banner de cookies:

3.5.1.8.9.1. Posição do banner na tela, incluindo ao menos: Barra inferior, Barra superior, Bloco à direita/esquerda

3.5.1.8.9.2. Estilo visual dos botões do banner, ao menos: Sem Borda, preenchido com cor

3.5.1.8.9.3. Customização de cores para os elementos visuais do banner, usando código de cor Hexadecimal e RGB

3.5.1.8.9.4. Link para Política de Privacidade da empresa

3.5.1.8.9.5. Customização dos títulos de cada botão, categoria de cookies, textos de cabeçalho e demais elementos do banner

3.5.1.8.9.6. Exibição do Centro de Preferências de Cookies;

3.5.1.8.9.7. Customização de logo no Centro de Preferências de Cookies

3.5.1.8.10. A solução deve ter a capacidade de fornecer ao menos 3 tipos de conformidade para o gerenciamento de cookie dentre eles:

3.5.1.8.10.1. Apenas a informação que é utilizado cookie;

3.5.1.8.10.2. Permitir que os usuários optem por não receber cookies (opt-out)

3.5.1.8.10.3. Permitir que os usuários optem por quais os cookies receber (opt-in)

3.5.1.8.10.4. Deve ter a capacidade de realizar o gerenciamento de gravação do cookie baseado na resposta do usuário, bloqueando aqueles não autorizados

3.5.1.8.10.5. Deve ter a capacidade de registrar o identificador do titular no log do gerenciamento de cookie.

3.5.1.8.10.6. Deve ter a capacidade de registrar no log quais os cookies foram ou não permitidos pelo titular, detalhando a categoria e os cookies específicos negados e aceitos.

3.5.1.8.10.7. Deve ter a capacidade de registrar o país de origem do acesso do titular e o domínio da página referente ao consentimento de cookie do titular de dados.

3.5.1.8.11. O consentimento recebido deve ter a possibilidade de visualização em uma tela de administração mostrando os seguintes dados:

3.5.1.8.11.1. Identificador do Titular;

3.5.1.8.11.2. Categoria do Cookie;

3.5.1.8.11.3. Status do Consentimento;

3.5.1.8.11.4. Data do Consentimento;

3.5.1.8.11.5. País de origem do acesso do titular

3.5.1.8.11.6. Deve possui um dashboard que informe de qual região (país) origem do consentimento dado

3.5.1.8.12. A solução deve prover um dashboard que permita filtrar por, no mínimo:

3.5.1.8.12.1. Por um titular de dados

3.5.1.8.12.2. Ponto de coleta

3.5.1.8.12.3. Consentimentos aceitos, revogados e negados.

3.5.1.8.12.4. Categoria de Cookie

3.5.1.8.12.5. Por período

3.5.1.8.13. O banner de cookie 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

3.5.1.8.14. O Centro de Preferências de cookies do banner (detalhamento dos cookies) deve ser capaz de exibir a relação e descrição dos cookies identificados, agrupados por categorias

3.5.1.8.15. A solução deve prover a capacidade de realizar varreduras recorrentes e automáticas nos sites da empresa, permitindo ao menos um scan mensal para detecção de alteração de cookies e novos cookies identificados

3.5.1.8.16. A solução deve notificar ao time de TI e DPO por e-mail, caso novos cookies sejam detectados automaticamente

3.5.1.9. Módulo de Gestão de Riscos e Avaliações internas

3.5.1.9.1. Deve ter a capacidade de enviar convites por e-mail para destinatários internos, sem requerer o cadastro destes usuários dentro da ferramenta previamente, convidando-os a acessar uma avaliação via web hospedada na própria ferramenta

3.5.1.9.2. A solução deve ter a capacidade de importar modelos externos de questionário, utilizando arquivos em CSV e JSON

3.5.1.9.3. Deve possuir modelos de questionários que atendam a LGPD, GDPR entre outras regulamentações e frameworks reconhecidos globalmente, e que permita cloná-los e alterá-los livremente para incorporar customizações locais e necessidades da organização

3.5.1.9.4. Deve possuir modelo de questionário sugerido e customizável para Avaliação de Impacto de Privacidade (PIA).

3.5.1.9.5. Deve permitir atrelar nível de risco a opções de resposta de perguntas do questionário, tanto por definição no modelo do questionário quanto diretamente na revisão/aprovação de um questionário preenchido

3.5.1.9.6. Deve permitir convidar e atribuir e convidar diversos usuários para colaborarem na resposta de um mesmo questionário, incluindo a opção de fazê-lo no nível da pergunta, seção de perguntas e para todo o questionário

3.5.1.9.7. Deve permitir atribuir um responsável para cada item de risco pontuado no questionário, incluindo também data de limite e comentários internos

3.5.1.9.8. A definição de risco deve ser por escala como Muito Alto, Alto, Médio, Baixo e Muito Baixo, e por quadrantes visuais com 2 vetores de Probabilidade e Gravidade

3.5.1.9.9. Deve ter chat em tempo real entre o convidado e o remetente do questionário, dentro da própria interface de resposta, para facilitar a interação durante o preenchimento do questionário.

3.5.1.9.10. Deve possuir painel que centralize todos os itens de risco derivados de questionários enviados, com filtros para identificar quais os riscos estão relacionados por cada usuário convidado, severidade, data, dentre outras opções.

3.5.1.9.11. Deve ter a capacidade de criar automações via workflow para caso um risco seja detectado na resposta de uma avaliação.

3.5.1.9.12. A customização do modelo do questionário deve oferecer diferentes tipos de campos, como:

3.5.1.9.12.1. Sim e Não

3.5.1.9.12.2. Caixa de Texto

3.5.1.9.12.3. Múltipla Escolha

3.5.1.9.12.4. Período de Data

3.5.1.9.12.5. Lista de seleção

3.5.1.9.12.6. Tabela

3.5.1.9.13. Deve ter um portal de self service para usuários, permitindo que eles possam voluntariamente iniciar uma avaliação, selecionando um dos modelos de questionário publicados em tal portal, para apoio ao esforço de "Privacy by Design". Uma vez respondidos, estes questionários devem ser roteados internamente para aprovação do time de privacidade.

3.5.1.9.14. Deve oferecer integração nativa ao módulo de Mapeamento de Dados (Data Mapping) permitindo usar do recurso de Questionários para também atualização de registros de Processos, Ativos de TI e Fornecedores.

3.5.1.9.15. A solução deve oferecer a opção de envio periódico de um mesmo questionário, provendo as respostas anteriores para revisão e com versionamento das respostas

3.5.1.9.16. Os questionários devem suportar lógica condicional, isto é, omitir ou expor novas questões de acordo com respostas de questões anteriores

3.5.1.9.17. A solução deve permitir realizar o upload de anexos em um questionário

3.5.1.10. Módulo de Gestão de Fornecedores

3.5.1.10.1. Deve compartilhar os modelos de questionário com o módulo de Avaliações internas

3.5.1.10.2. A solução deve ter a capacidade de enviar e-mails para convidar contatos externos à empresa, sem necessidade de criar login na ferramenta para estes, com convite enviado por e-mail pela ferramenta com link para acesso online à avaliação

3.5.1.10.3. A solução deve ter a capacidade de revisar e aprovar cada pergunta recebida no questionário e permitir atribuir riscos a cada questão com no mínimo: Nível de risco, Descrição do Risco, Recomendação, Notas internas não visíveis ao Fornecedor convidado

3.5.1.10.4. Deve permitir que o fornecedor convide membros adicionais da sua empresa que está sendo avaliada para apoiar na resposta, adicionando-os ao questionário e a pergunta específica. Estes convidados adicionais poderão colaborar especificamente no questionário aberto a que foram convidados, através da interface web da ferramenta.

3.5.1.10.5. Deve ter a capacidade de realizar uma importação em massa de uma lista de contatos de fornecedores a serem convidados, utilizando-se de arquivo CSV

3.5.1.10.6. A solução deve ter uma base de inteligência global de avaliações de fornecedores de mercado, mantida e atualizada periodicamente pelo fabricante da solução, baseado em dados públicos como políticas de privacidade, e indicador de nível de maturidade de

privacidade, incluindo aspectos como Direitos do Titular, Coleta de Dados, Armazenamento de Dados, Compartilhamento de Dados, Violações e Certificações de Segurança.

3.5.1.10.7. Deve gerar um dashboard com as empresas fornecedoras com os seus principais riscos, conforme mapeados anteriormente nas avaliações.

3.5.1.10.8. Deve permitir visualizar itens agrupados por fornecedor, incluindo: Avaliações enviadas com status de preenchimento, Nível de Risco, Arquivos anexos

3.5.1.10.9. A solução deve oferecer um painel central de inventário de fornecedores

3.5.1.11. Módulo de Gestão de Incidentes

3.5.1.11.1. A solução deve oferecer módulo nativo e integrado para o registro de possíveis incidentes e violações de dados pessoais

3.5.1.11.2. Deve permitir a publicação de um portal nativo da ferramenta onde os funcionários da empresa possam relatar possíveis violações e incidentes, submetendo-os para avaliação do time de privacidade

3.5.1.11.3. Deve permitir a customização dos formulários utilizados internamente em cada etapa de triagem dos incidentes em trabalho

3.5.1.11.4. Deve permitir triagem e relacionar a regulamentação e seção das normas de privacidade para contextualizar possíveis incidentes

3.5.1.11.5. Deve integrar-se ao módulo de Workflow para permitir ações customizadas quando um novo incidente é reportado

3.5.1.11.6. Deve permitir o acompanhamento de uma violação através das seguintes etapas:

3.5.1.11.6.1. Verificação do incidente

3.5.1.11.6.2. Detecção

3.5.1.11.6.3. Análise do incidente

3.5.1.11.6.4. Remediações

3.5.1.11.6.5. Notificações

3.5.1.11.6.6. Status final

3.5.1.11.7. Deve possuir a capacidade de informar quais os tipos de atributos de dados pessoais podem ter relação ao incidente e qual a região geográfica dos titulares afetados.

3.5.1.11.8. Deve possuir a descrever a remediação da causa raiz do incidente, permitindo a descrever o motivo da causa raiz, documentação comprobatória da remediação e status da remediação;

3.5.1.11.9. Deve possuir a capacidade de gerenciar a comunicação do incidente, permitindo a triagem sobre a comunicação para diferentes atores, exemplo comunicação governamentais e titulares.

3.5.1.11.10. A solução deve possuir mecanismos para informar o risco do incidente

3.5.1.11.11. A solução deve possuir base de jurisdição para LGPD.

3.5.1.11.12. Deve permitir a configuração de outros modelos de notificações, permitindo realizar o registro das atividades.

3.5.1.11.13. Deve prover um resumo detalhado do incidente com todos os itens descritos nos módulos de verificação, detecção, análise e remediação do incidente.

3.5.1.11.14. Deve prover capacidade de chat interno na ferramenta, dentro do contexto do incidente sendo trabalhado, para facilitar a comunicação com os times envolvidos

3.5.1.11.15. Deve oferecer um portal de autoatendimento via web, onde usuários da empresa possam registrar possíveis violações de dados para análise do time de privacidade

3.5.1.12. Módulo de Gestão da Política de Privacidade

3.5.1.12.1. A solução deve oferecer a funcionalidade de criação, gerenciamento e publicação de políticas de privacidade

3.5.1.12.2. A solução deve gerar automaticamente o texto sugerido para cada seção da política de privacidade, através de um assistente online, e permitir a edição do texto gerado

3.5.1.12.3. A solução deve permitir a hospedagem da política gerada, em link web público da própria solução, para que seja integrada ao site da empresa

3.5.1.12.4. A solução deve oferecer modelo de política de privacidade, contemplando áreas como Definições legais, Atividades de Processamento de dados, Dados de menores, Cookies, Compartilhamento de dados com terceiros, Medidas de segurança, Direitos de titulares

3.5.1.12.5. A solução deve ter integração com o módulo de Data Mapping, de forma a obter os elementos de dados pessoais catalogados e importá-la para a política de privacidade, de forma customizável

3.5.1.12.6. A solução deve ter integração com o módulo de Consentimento de Cookies, de forma a obter as categorias de cookie realmente utilizadas nos sites da empresa e importá-las para a política de privacidade, de forma customizável

3.5.1.13. Módulo de Fluxo de Trabalho e Automações Gerais Customizáveis

3.5.1.13.1. A solução deve ter a capacidade de criação de workflows customizados, através de módulo nativo e integrado da própria ferramenta e compatível com todos os demais módulos ofertados

3.5.1.13.2. A solução deve ter a capacidade de criar workflows de forma visual, com gatilhos e ações interligáveis suportando lógica condicional entre eles

3.5.1.13.3. Deve permitir a exportação do fluxo criado, bem como a importação de fluxos externos, no formato JSON

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

3.5.1.13.4.1. Requisições DSR são criadas, alteradas e fechadas

3.5.1.13.4.2. Consentimentos são registrados, aceitos e revogados

3.5.1.13.4.3. Dados são detectados pelo Data Discovery

3.5.1.13.4.4. Objetos catalogados no Data Mapping são criados e alterados

3.5.1.13.4.5. Incidentes são registrados

3.5.1.13.4.6. Questionários são recebidos e dependendo do risco associado

3.5.1.13.4.7. Determinado dia/hora, periodicidade e intervalo de tempo

3.5.1.13.4.8. Acionamento externo por API Webhook da ferramenta

3.5.1.13.5. A solução deve permitir criação de múltiplos fluxos de automação independentes

3.5.1.13.6. A solução deve permitir que um fluxo acione outro fluxo da ferramenta, para reaproveitamento e cascateamento de ações

3.5.1.13.7. A solução deve oferecer diversas ações de workflow, incluindo:

3.5.1.13.7.1. Criar tarefas e subtarefas nas requisições de titular (DSR)

3.5.1.13.7.2. Alterar proprietários de tarefas e subtarefas das requisições de titular

3.5.1.13.7.3. Anexar arquivos à requisições de titular

3.5.1.13.7.4. Criar e alterar itens do catálogo de Data Mapping, incluindo Ativos de TI e Processos

3.5.1.13.7.5. Iniciar avaliações/questionários

3.5.1.13.7.6. Gerenciar fornecedores cadastrados na ferramenta

3.5.1.13.7.7. Criar incidentes no módulo de gestão de incidentes

3.5.1.13.7.8. Criar e Consumir arquivos no formato CSV

3.5.1.13.7.9. Criar e Consumir arquivos no formato de Planilha

3.5.1.13.7.10. Transferir arquivos via SFTP, Box, Dropbox, Onedrive

3.5.1.13.7.11. Executar queries, inserts e updates em SQL Server, MySQL, Postgres e Oracle

3.5.1.13.7.12. Localizar e atualizar documentos em MongoDB

3.5.1.13.7.13. Ler e extrair conteúdo de arquivos no formato PDF

3.5.1.13.7.14. Ler e atualizar registros no Salesforce

3.5.1.13.7.15. Consumir APIs externas através de HTTP Request, com Post, Get, Put, suportando autenticação via Header

3.5.2. Ferramenta para auxiliar contra vazamento de dados

3.5.2.1. O licenciamento da solução proposta deve contemplar todo o software, ou seja, todas as funcionalidades descritas neste edital.

3.5.2.2. As configurações de todos os módulos devem ser gerenciadas por uma console.

3.5.2.3. Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS).

3.5.2.4. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, no Sistema Operacional:

3.5.2.4.1. Microsoft Windows Server;

3.5.2.4.2. Suportar funcionamento em sistemas de virtualização de hosts.

3.5.2.4.3. Capacidade de excluir incidentes em lote para gestão eficiente de espaço utilizado pela base de dados.

3.5.2.4.4. Suportar funcionamento em plataformas de Single Sign-On (SSO)

3.5.2.5. A solução deverá criptografar toda a comunicação que ocorre entre os servidores de gerenciamento e os agentes instalados em terminais.

3.5.2.6. A solução deverá criptografar a comunicação entre o servidor principal e os servidores adicionais da plataforma.

3.5.2.7. Possuir registros detalhados de auditoria de atividades de sistema.

3.5.2.8. Permitir a instalação em Sistema Operacional restrito, com serviços e configurações de porta limitados (Hardening).

3.5.2.9. Deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações confidenciais detectadas;

3.5.2.10. Deve possuir módulos de detecção distintos, para:

3.5.2.10.1. Localizar dados confidenciais armazenados em servidores de arquivos, bancos de dados e servidores de e-mail;

3.5.2.10.2. Localizar dados confidenciais armazenados em desktops e laptops;

3.5.2.10.3. Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP;

3.5.2.10.4. Detectar vazamento de dados a partir de conexão direta com servidores de e-mail;

3.5.2.10.5. Detectar vazamento de dados a partir de conexão direta com appliances responsáveis pelo processamento de tráfego WEB (Proxy ou UTM);

3.5.2.11. Capacidade de obter a “impressão digital” de dados estruturados e não estruturados.

3.5.2.12. Capacidade de normalizar variações comuns de apresentação de dados para aprimorar a precisão de políticas de monitoramento.

3.5.2.13. Capacidade de identificar dados estruturados e não estruturados, sem necessidade de utilização de servidores adicionais ou dedicados para este fim.

3.5.2.14. Detectar documentos não estruturados, após usar capacidades nativas de aprendizado automático, a partir da análise de um conjunto de amostras.

3.5.2.15. Permite a criação de padrão de identificação utilizando dados internos da instituição de modo a customizar a ferramenta.

3.5.2.16. Permitir detecção de acordo com expressões regulares configuráveis.

3.5.2.17. Permitir detecção por tipo de arquivo, por nome e extensão de arquivo, remetente/destinatário e protocolo de transmissão.

3.5.2.18. Capacidade de integrar diretamente com LDAP (MS Active Directory) para criar regras de detecção de terminal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada.

3.5.2.19. Possuir mecanismo de envio de notificações personalizadas por e-mail aos administradores.

3.5.2.20. Permitir a criação de perfis para administração de servidores, administração de usuário, criação e edição de política.

3.5.2.21. Armazenar e exibir a mensagem original ou arquivo que gerou o incidente.

3.5.2.22. Exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo.

3.5.2.23. Permitir a exportação da lista de incidentes no formato HTML, PDF ou CSV.

3.5.2.24. Interface de administração única para visualização de todos os incidentes.

3.5.2.25. Possuir interface WEB, compatível, no mínimo, com os navegadores Internet Explorer, Mozilla Firefox e Google Chrome.

3.5.2.26. Permitir a configuração de ações automáticas, dependendo da quantidade de dados expostos.

3.5.2.27. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado.

3.5.2.28. Deve possuir integração com Active Directory, para autenticação de usuários da solução.

3.5.2.29. Deve possuir logs detalhados de auditoria de alterações de políticas.

3.5.2.30. A solução deve ter capacidade de descoberta de vazamento de dados nos seguintes canais:

3.5.2.30.1. Nuvem;

3.5.2.30.2. E-mail;

3.5.2.30.3. Web;

3.5.2.30.4. Terminais;

3.5.2.30.5. Smartphones (A partir de um APP a ser instalado);

3.5.2.30.6. Plataforma de armazenamento de dados.

3.5.2.30.7. Proteger os dados contra exposição ou roubo em tempo real.

3.5.2.31. Deve suportar a verificação de arquivos compactados recursivos (exemplos .zip, .rar dentro de .zip, .rar).

3.5.2.32. Deve suportar de forma comprovada a detecção de dados no idioma português brasileiro.

3.5.2.33. Deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails.

3.5.2.34. Deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem.

3.5.2.35. Deve identificar os conteúdos armazenados em colunas específicas de planilhas eletrônicas e em bancos de dados.

3.5.2.36. Deve possuir capacidade para identificar os conteúdos específicos com base em um padrão pré-determinado, para no mínimo:

3.5.2.36.1. CPF;

3.5.2.36.2. CNPJ;

3.5.2.36.3. Cartões de Crédito;

3.5.2.36.4. Número de eleitor;

3.5.2.36.5. RG;

3.5.2.36.6. IBAN;

3.5.2.36.7. Dados de tecnologia com o IP Address, Mac Address e IMEI de telefones.

3.5.2.36.8. Deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo.

3.5.2.37. A solução deve possuir integrada na console a funcionalidade de workflow (Condições de acionamento) resposta a incidentes.

3.5.2.38. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente para, no mínimo:

3.5.2.38.1. Dados para análise como: Origem, Destino, detalhes de qual Canal de detecção foi acionado e nome/caminho do arquivo;

3.5.2.38.2. Dados de qual regra foi acionada;

3.5.2.38.3. Dados de qual informação acionou a regra;

3.5.2.38.4. Severidade do incidente;

3.5.2.38.5. Status do incidente;

3.5.2.38.6. Nome da aplicação;

3.5.2.38.7. Data e hora do evento;

3.5.2.38.8. Volume de dados trafegados no incidente;

3.5.2.38.9. Nome do usuário referenciado no incidente;

3.5.2.38.10. Atributos do usuário coletados do Active Directory;

3.5.2.38.11. Nome da estação de trabalho;

3.5.2.38.12. Informações de destino para qual o dado seria copiado;

3.5.2.38.13. Histórico completo de alteração de incidentes.

3.5.2.39. Deve ter a capacidade de importar um conjunto de pré-configurações do sistema otimizadas para verticais das indústrias específicas, contando com dados de pesquisa em português.

3.5.2.40. Deve possibilitar a realização de backup e restore de configurações, incidentes e políticas da plataforma.

3.5.2.41. Deve possibilitar integração nativa com soluções de classificação da informação, de forma a monitorar o uso de dados classificados nos canais de detecção e também a possibilidade de imposição de classificação durante a descoberta de dados em servidores de arquivos, por exemplo.

3.5.2.42. Criação de Políticas e Detecção de Conteúdo Confidencial

3.5.2.43. Deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:

3.5.2.43.1. Palavra ou conjunto de palavras chave;

3.5.2.43.2. Identificadores pré existentes o customizados (CPF, CNPJ, Cartão de crédito, etc.);

3.5.2.43.3. Expressões regulares com possibilidade de adaptação para qualquer padrão de dados existentes;

3.5.2.43.4. Nível de classificação da informação;

3.5.2.43.5. Tipo de arquivo;

3.5.2.43.6. Nome e extensão de arquivos;

3.5.2.43.7. Bases de indexação previamente carregadas;

3.5.2.43.8. Tamanho de dados trafegados;

3.5.2.43.9. Quantidade de anexos de um e-mail;

3.5.2.43.10. Usuários/E-mails internos;

3.5.2.43.11. Estações de trabalho/servidores específicos;

3.5.2.43.12. Localização da estação de trabalho (Dentro ou fora da rede interna);

3.5.2.43.13. Tipo de estação (Laptop ou desktop);

3.5.2.43.14. E-mails ou domínios externos;

3.5.2.43.15. Direção do tráfego (Entrada ou saída);

3.5.2.43.16. Protocolos de rede ou canais da estação;

3.5.2.43.17. E-mails em dispositivos móveis;

3.5.2.43.18. Dados enviados para impressora;

3.5.2.43.19. Qualquer aplicação em execução na estação de trabalho;

3.5.2.43.20. Cópias para caminhos de rede.

3.5.2.44. Deve possibilitar criação de regras de exclusões para as políticas de acordo com grupos de usuários fornecidos pelo active directory.

3.5.2.45. O produto deve possuir modelos de políticas de detecção com base em regulamentações e melhores práticas de mercado, para no mínimo:

3.5.2.45.1. SOX;

3.5.2.45.2. PCI;

3.5.2.45.3. HIPAA;

3.5.2.45.4. GDPR.

3.5.2.46. A solução deve possibilitar a criação de regras para adequação a LGPD.

3.5.2.47. A solução deve possuir templates de políticas de detecção, para no mínimo os seguintes temas:

3.5.2.47.1. Imagens com conteúdo inapropriado;

3.5.2.47.2. Linguagem ofensiva ou racismo;

3.5.2.47.3. Cyber Bullying;

3.5.2.47.4. Problemas relacionados a jogos de azar;

3.5.2.47.5. Dados confidenciais e propriedade intelectual;

3.5.2.47.6. Dados que envolvem segurança de redes;

3.5.2.47.7. Busca de informações relacionadas a indicadores de comprometimento.

3.5.2.48. Deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:

3.5.2.48.1. Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);

3.5.2.48.2. Compactados (ZIP, RAR, GZ, LHA, HQX, JAR, 7z);

3.5.2.48.3. CAD (DWG, DXF, VSD, DGN);

3.5.2.48.4. Planilhas (XLS, XLSX, 123, SXC, ODS, CSV);

3.5.2.48.5. Apresentações (PPT, PPTX, SXI, SXP, ODP);

3.5.2.48.6. Outros (PDF, MDB).

3.5.2.49. Deve permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU" lógicas e de exceção.

3.5.2.50. Permitir a escrita de expressões lógicas para configuração das regras de detecção, exemplo:("Condição 1" OU "Condição 2") E NÃO "Condição 3".

3.5.2.51. Deve ter a capacidade de construir políticas de detecção, configurando-se o grau de severidade adotado para cada regra criada, conforme o número de correspondências que se deseja encontrar em cada possível violação.

3.5.2.52. As políticas de detecção devem possuir, no mínimo:

3.5.2.52.1. A capacidade de normalização de todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "123-45-6789", "123456789", "123.45.6789", etc.);

3.5.2.52.2. A capacidade de detecção usando palavras e frases-chave totalmente configuráveis;

3.5.2.52.3. A capacidade de colocar múltiplas palavras/frases em uma única regra de detecção.

3.5.2.52.4. A capacidade nativa de detectar documentos de identificação e números de impostos internacionais, para no mínimo, os países EUA, França e Brasil.

3.5.2.53. A capacidade de detectar faixas de números válidos para determinados tipos de dados, tal como no mínimo, número de cartão de crédito válido.

3.5.2.54. Resposta a incidentes

3.5.2.55. Deve possuir notificações personalizáveis através de e-mail em caso de violação de política.

3.5.2.56. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações.

3.5.2.57. Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:

3.5.2.57.1. Permitir o envio, deletar anexos, quarentenar ou criptografar e-mails;

3.5.2.57.2. Permitir ou bloquear tráfego de dados sensíveis via FTP;

3.5.2.57.3. Permitir ou bloquear tráfego de dados sensíveis via HTTP/HTTPs;

3.5.2.57.4. Através do agente, permitir, bloquear ou solicitar justificativa para o tráfego em pelo menos: Qualquer tipo de aplicação executada pelo Sistema operacional, cópia para armazenamentos de rede, impressão de arquivos, E-mails enviados, upload para páginas Web e cópias para dispositivos USB.

3.5.2.58. Permitir a possibilidade de busca ou não de detalhes sobre o incidente durante o registro;

3.5.2.59. Execução de atividades customizadas;

3.5.2.60. Enviar mensagens para servidores de syslog;

3.5.2.61. Enviar notificações por e-mail;

3.5.2.62. Manipular arquivos durante a descoberta de rede.

3.5.2.63. Deve permitir vários botões de reposta na interface gráfica dos incidentes totalmente configuráveis.

3.5.2.64. Os botões de resposta na interface gráfica dos incidentes devem possibilitar no mínimo:

3.5.2.64.1. Designar o incidente para resposta de alguém específico;

3.5.2.64.2. Modificar o status do incidente;

3.5.2.64.3. Modificar a severidade do incidente;

3.5.2.64.4. Ignorar o incidente;

3.5.2.64.5. Adicionar TAG no incidente;

3.5.2.64.6. Adicionar comentários no incidente;

3.5.2.64.7. Fazer Download do incidente;

3.5.2.64.8. Deletar o incidente;

3.5.2.64.9. Acionar scripts ou tarefas customizadas;

3.5.2.64.10. Escalar o incidente para o gerente do usuário envolvido;

3.5.2.64.11. Escalar o incidente para uma pessoa específica.

3.5.2.64.12. Deve exibir todos os detalhes do incidente em uma única página.

3.5.2.64.13. Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo.

3.5.2.65. Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente.

3.5.2.66. Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente.

3.5.2.67. Workflow com retenção de e-mails em quarentena InLine, e fluxo de aprovação automatizado;

3.5.3. Relatórios

3.5.3.1. Deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:

3.5.3.1.1. Ação aplicada;

3.5.3.1.2. Responsável pela análise;

3.5.3.1.3. Nome da aplicação;

3.5.3.1.4. Departamento;

3.5.3.1.5. Canal de detecção;

3.5.3.1.6. Nível de classificação da informação;

3.5.3.1.7. Destino de tráfego da informação;

3.5.3.1.8. Tipo estação (Desktop ou Laptop);

3.5.3.1.9. ID do incidente

3.5.3.1.10. Hora do incidente

3.5.3.1.11. Nome do arquivo trafegado;

3.5.3.1.12. Histórico do incidente;

3.5.3.1.13. Incidentes marcados como ignorados;

3.5.3.1.14. TAGs de incidentes;

3.5.3.1.15. Quantidade de informação sensível trafegada;

3.5.3.1.16. Propriedades do arquivo;

3.5.3.1.17. Política acionada;

3.5.3.1.18. Nome da regra acionada;

3.5.3.1.19. Severidade do incidente;

3.5.3.1.20. Origem do incidente;

3.5.3.1.21. Status do incidente;

3.5.3.1.22. Tamanho da transação;

3.5.3.1.23. Dados relacionados as violações encontradas.

3.5.3.2. Deve exportar relatórios para os formatos HTML, PDF e CSV.

3.5.3.3. Deve apresentar um painel para visualização dos relatórios.

3.5.3.4. Deve ter a capacidade para configurar, salvar relatórios e painéis personalizados por usuário.

3.5.3.5. Dashboard de incidentes baseado em risco de usuários.

3.5.3.6. Deve possuir painéis (Dashboards) para, no mínimo os seguintes itens:

3.5.3.6.1. Incidentes criados nos últimos X dias;

3.5.3.6.2. Políticas mais acionadas;

3.5.3.6.3. Incidentes por severidade;

3.5.3.6.4. Incidentes por ação tomada;

3.5.3.6.5. Incidentes por canais de detecção;

3.5.3.6.6. Incidentes por origem/destino;

3.5.3.6.7. Usuários que mais violam políticas.

3.5.4. Módulo de Área de Armazenamento

3.5.4.1. Deve verificar existência de conteúdo confidencial em file systems sem a necessidade de agentes de coleta (agent-less) para no mínimo CIFS, NFS, SMB e NTFS.

3.5.4.2. Deve permitir a análise dos file systems através de agentes ou sem agentes em sistemas operacionais, para no mínimo:

3.5.4.2.1. Windows Server 2008 R2;

3.5.4.2.2. Windows Server 2012;

3.5.4.2.3. Windows Server 2016;

3.5.4.2.4. Red Hat Enterprise Linux 6 e demais releases da versão;

3.5.4.2.5. Red Hat Enterprise Linux 7 e demais releases da versão.

3.5.4.3. Deve analisar conteúdo sigiloso armazenado em ambientes complexos, para no mínimo:

3.5.4.3.1. Microsoft Sharepoint;

3.5.4.3.2. Lotus Notes;

3.5.4.3.3. Microsoft SQL Server;

3.5.4.3.4. Oracle;

3.5.4.3.5. MySQL

3.5.4.3.6. Microsoft Exchange;

3.5.4.4. Deve analisar conteúdo sigiloso em aplicações em nuvem:

3.5.4.4.1. Salesforce,

3.5.4.4.2. AW

3.5.4.4.3. ServiceNow

3.5.4.4.4. Facebook Workplace

3.5.4.4.5. G-Suite

3.5.4.4.6. Google Cloud Platform

3.5.4.4.7. Azure.

3.5.4.4.8. One Drive

3.5.4.4.9. Trello

3.5.4.4.10. Dropbox

3.5.4.4.11. Slack

3.5.4.4.12. GitHub

3.5.4.4.13. LinkedIn

3.5.4.5. Deve possuir a capacidade de verificar arquivos Microsoft "PST", possibilitando executar varreduras tanto nas mensagens, assim como, nos arquivos anexos as mensagens.

3.5.4.6. Possibilidade de mover para quarentena arquivos que violam políticas de segurança.

3.5.4.7. Deve manter o arquivo no local original, substituindo seu conteúdo por uma mensagem customizável, como aviso e orientação para o usuário.

3.5.4.8. Deve possuir capacidade de remover permissões de compartilhamento dos arquivos que violam as políticas de segurança.

3.5.4.9. Permitir a remoção do arquivo que está em quarentena e restaurá-lo de volta ao local original.

3.5.4.10. Deve permitir coleta automática de arquivos que violem políticas para análise legal (evidência).

3.5.4.11. Permitir a criação de respostas personalizadas para incidentes.

3.5.4.12. Exibir detalhes, no incidente, dos arquivos que violam as políticas.

3.5.4.13. Permitir a visualização das permissões do arquivo.

3.5.4.14. Deve possibilitar notificação através de e-mail e alerta Syslog em caso de violação de política.

3.5.4.15. Deve permitir agendamento de varreduras automáticas.

3.5.4.16. Possuir mecanismo de verificação incremental, na qual apenas arquivos novos, ou alterados, sejam verificados.

3.5.4.17. Deve permitir configurar janelas de tempo para verificações, interrompendo o processo automaticamente ao fim do período configurado.

3.5.4.18. Preservar os atributos originais do arquivo, inclusive o atributo "Acessado em", enquanto realiza a verificação.

3.5.4.19. Possuir capacidade de pausar, manualmente, a verificação.

3.5.4.20. Deve utilizar técnicas de paralelismo e controle de banda.

3.5.4.21. Permitir o controle da velocidade das verificações para limitar o uso da largura de banda da rede.

3.5.4.22. Deve ter a capacidade de reutilizar uma única credencial (nome de usuário/senha) em múltiplos alvos a serem verificados.

3.5.4.23. Permitir a verificação simultânea em várias fontes distintas.

3.5.4.24. Permitir limitar quais portas de comunicação serão utilizadas entre o sistema-alvo e o servidor que faz a verificação.

3.5.4.25. Deve permitir aplicar filtros para verificar na varredura de arquivos de um determinado tipo ou em certo diretório.

3.5.4.26. Deve permitir aplicar filtros para verificar na varredura de arquivos a idade E/ou o tamanho de arquivos.

3.5.5. Módulo de Terminal de Usuário

3.5.5.1. Capacidade de descobrir fuga de informações sensíveis, por meio de agente.

3.5.5.2. Ações de proteção baseadas em risco comportamental.

3.5.5.3. Possibilidade de aplicação de políticas mesmo quando o agente não tem comunicação com o servidor de gerenciamento.

3.5.5.4. Possibilidade de armazenamento em cache, dos arquivos que causaram o incidente até que o usuário se conecte, novamente, à rede corporativa.

3.5.5.5. A solução possuir a funcionalidade de OCR em arquivos do tipo imagem, no mínimo para:

3.5.5.5.1. Jpeg

3.5.5.5.2. Bmp

3.5.5.5.3. Png

3.5.5.5.4. Gif

3.5.5.5.5. Tiff

3.5.5.6. Monitorar e bloquear dados copiados para dispositivos de armazenamento removível (USB).

3.5.5.7. A solução deverá possuir capacidade de analisar arquivos menos de 1 kbyte.

3.5.5.8. Possibilidade de criptografar dados sensíveis copiados para dispositivos USB, sem a necessidade de soluções adicionais.

3.5.5.9. Permitir a monitoração e bloqueio para dados copiados para CD/DVD.

3.5.5.10. Permitir a monitoração e bloqueio para dados enviados a qualquer tipo de impressora local e de rede.

3.5.5.11. Permitir a monitoração e bloqueio para ações de copiar e colar.

3.5.5.12. Permitir a monitoração e bloqueio de dados sensíveis trafegados via e-mail corporativo.

3.5.5.13. Permitir a monitoração e bloqueio para transmissões HTTPS pelo menos nos seguintes navegadores:

3.5.5.13.1. Internet Explorer;

3.5.5.13.2. Microsoft Edge;

3.5.5.13.3. Mozilla Firefox;

3.5.5.13.4. Google Chrome;

3.5.5.13.5. Safari.

3.5.5.14. Permitir a monitoração e bloqueio para transmissões HTTP.

3.5.5.15. Permitir a monitoração e bloqueio para transmissões via FTP.

3.5.5.16. Permitir a monitoração e bloqueio para uso de dados confidenciais por qualquer aplicativo, incluindo programas de criptografia não autorizados.

3.5.5.17. Permitir a monitoração e bloqueio para dados copiados para compartilhamentos de rede pelo Windows Explorer.

3.5.5.18. A Solução deve possuir monitoramento, por padrão, para pelo menos os seguintes aplicativos:

3.5.5.18.1. Chrome;

3.5.5.18.2. Firefox;

3.5.5.18.3. Internet Explorer (IE);

3.5.5.18.4. Microsoft Edge;

3.5.5.18.5. Opera;

3.5.5.18.6. Safari;

3.5.5.18.7. Tor;

3.5.5.18.8. Torch;

3.5.5.18.9. Acoustica MP3 CD Burner;

3.5.5.18.10. Alcohol 120%;

3.5.5.18.11. CD-Mate;

3.5.5.18.12. Disk Utility;

3.5.5.18.13. iTunes;

3.5.5.18.14. Nero Burning ROM;

3.5.5.18.15. Roxio – Easy Media Creator;

3.5.5.18.16. Windows Media Player;

3.5.5.18.17. Amazon Cloud Drive;

3.5.5.18.18. Box;

3.5.5.18.19. Dropbox;

3.5.5.18.20. Egnyte;

3.5.5.18.21. Google Drive;

3.5.5.18.22. iCloud;

3.5.5.18.23. OneDrive;

3.5.5.18.24. Salesforce Files;

3.5.5.18.25. ShareFile;

3.5.5.18.26. Syncplicity;

3.5.5.18.27. WatchDox;

3.5.5.18.28. Apple Mail;

3.5.5.18.29. Eudora;

3.5.5.18.30. Lotus Notes;

3.5.5.18.31. MailMate;

3.5.5.18.32. Microsoft Outlook;

3.5.5.18.33. Microsoft Outlook Express;

3.5.5.18.34. Mozilla Thunderbird;

3.5.5.18.35. Pegasus Mail;

3.5.5.18.36. Postbox;

3.5.5.18.37. Sparrow;

3.5.5.18.38. Windows Live Mail;

3.5.5.18.39. Windows Mail;

3.5.5.18.40. DK2 Network Server Remote Monitor - DK2 DESkey;

3.5.5.18.41. File Encryption XP;

3.5.5.18.42. Windows Privacy Tray (WinPT);

3.5.5.18.43. Core FTP LE;

3.5.5.18.44. Cute FTP Home 8.2;

3.5.5.18.45. File Transfer Program (Microsoft Utility);

3.5.5.18.46. FileZilla FTP Client;

3.5.5.18.47. Flash FXP 3.6 build 1240;

3.5.5.18.48. FTP Voyager 15;

3.5.5.18.49. Ipswitch WS FTP Home;

3.5.5.18.50. Leech FTP;

3.5.5.18.51. Serv-U;

3.5.5.18.52. Smart FTP Client;

3.5.5.18.53. Adium;

3.5.5.18.54. AIM;

3.5.5.18.55. Apple Messages;

3.5.5.18.56. Camfrog;

3.5.5.18.57. Cisco WebEx;

3.5.5.18.58. GoToMeeting;

3.5.5.18.59. ICQ;

3.5.5.18.60. Jabber Messenger;

3.5.5.18.61. ManyCam;

3.5.5.18.62. Microsoft Lync 2010;

3.5.5.18.63. Miranda IM;

3.5.5.18.64. ooVoo;

3.5.5.18.65. Pidgin;

3.5.5.18.66. Skype for Business;

3.5.5.18.67. TeamViewer;

3.5.5.18.68. Teccent QQ;

3.5.5.18.69. Trillian;

3.5.5.18.70. Viber;

3.5.5.18.71. Yahoo! Instant Messenger;

3.5.5.18.72. Adobe Reader;

3.5.5.18.73. Bean;

3.5.5.18.74. Eclipse;

3.5.5.18.75. Emacs;

3.5.5.18.76. Evernote;

3.5.5.18.77. Keynote;

3.5.5.18.78. LibreOffice/Apache OpenOffice;

3.5.5.18.79. Mellel;

3.5.5.18.80. Microsoft Office Access;

3.5.5.18.81. Microsoft Office Excel;

3.5.5.18.82. Microsoft Office InfoPath;

3.5.5.18.83. Microsoft OneNote;

3.5.5.18.84. Microsoft Office PowerPoint;

3.5.5.18.85. Microsoft Office Project;

3.5.5.18.86. Microsoft Office Publisher;

3.5.5.18.87. Microsoft Office Visio;

3.5.5.18.88. Microsoft Office Word;

3.5.5.18.89. Notepad;

3.5.5.18.90. Numbers;

3.5.5.18.91. OpenOffice.org Calc;

3.5.5.18.92. OpenOffice.org Draw;

3.5.5.18.93. OpenOffice.org Math;

3.5.5.18.94. OpenOffice.org Writer;

3.5.5.18.95. Pages;

3.5.5.18.96. Reminders;

3.5.5.18.97. Stickies;

3.5.5.18.98. TextEdit;

3.5.5.18.99. WordPad;

3.5.5.18.100. AllegianceMD;

3.5.5.18.101. eClinicalWorks;

3.5.5.18.102. ECLIPSYS;

3.5.5.18.103. INGENIX;

3.5.5.18.104. inteGreat;

3.5.5.18.105. Sequel;

3.5.5.18.106. Ares;

3.5.5.18.107. Azureus;

3.5.5.18.108. BearShare;

3.5.5.18.109. BitComet;

3.5.5.18.110. BitLord;

3.5.5.18.111. BitTornado;

3.5.5.18.112. BitTorrent;

3.5.5.18.113. eMule;

3.5.5.18.114. FrostWire;

3.5.5.18.115. Kazaa Lite;

3.5.5.18.116. LimeWire;

3.5.5.18.117. Pando;

3.5.5.18.118. Transmission;

3.5.5.18.119. uTorrent;

3.5.5.18.120. 7-Zip File Manager;

3.5.5.18.121. iArchiver;

3.5.5.18.122. WinRAR;

3.5.5.18.123. WinZip;

3.5.5.18.124. Bluetooth Stack COM Server - BTStackServer;

3.5.5.18.125. Fsquirt;

3.5.5.18.126. iTunes;

3.5.5.18.127. Wireless Link File Transfer App – Irftp;

3.5.5.18.128. WCESMgr;

3.5.5.18.129. Aplicor (online);

3.5.5.18.130. CRM.com;

3.5.5.18.131. HostAnalytics;

3.5.5.18.132. Intacct;

3.5.5.18.133. NetSuite;

3.5.5.18.134. Oracle CRM on demand;

3.5.5.18.135. RightNow;

3.5.5.18.136. Salesforce;

3.5.5.18.137. WorkDay;

3.5.5.18.138. FoxPro;

3.5.5.18.139. Ld;

3.5.5.18.140. MSTSC;

3.5.5.18.141. NT backup tool;

3.5.5.18.142. Vista backup tool;

3.5.5.18.143. VMWare.

3.5.5.19. A solução deve permitir a criação de qualquer aplicativo existente que não venha cadastrado por padrão.

3.5.5.20. Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceções de políticas para esses dispositivos.

3.5.5.21. O agente deverá suportar, no mínimo, Windows 7 (32 e 64 bits), Windows 2008 R2 Enterprise (64bit), Windows 10, Windows Server 2012, Windows Server 2016 e Apple MacOS.

3.5.5.22. Todas as funções devem ser executadas por um único agente.

3.5.5.23. Permitir a desativação do agente pela console de gerenciamento.

3.5.5.24. Possuir mecanismo que reinicie o agente caso o usuário tente interromper o serviço.

3.5.5.25. Possuir proteção contra desinstalação do agente.

3.5.5.26. Capacidade de apresentar as mensagens de notificações em português.

3.5.5.27. Possuir a capacidade de envio de notificação automática, por e-mail, para o usuário e administrador durante a ocorrência de um incidente.

3.5.5.28. Possuir a capacidade de gerenciamento da saúde dos agentes.

3.5.5.29. Deve permitir a distribuição do agente através de GPO ou por ferramenta de terceiros.

3.5.5.30. Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em “pop-up”, escolhendo opções de justificativa configuráveis pelo administrador da ferramenta.

3.5.5.31. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial.

3.5.5.32. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados.

3.5.5.33. Permitir a instalação do agente de modo oculto ou em modo de interação com o usuário.

3.5.5.34. Quando utilizado em modo interativo, permitir sincronização de políticas de forma manual, através de acionamento de botão no agente.

3.5.5.35. Alimentar a console de gerenciamento, com pelo menos, as seguintes informações do agente:

3.5.5.35.1. Nome do computador;

3.5.5.35.2. IP Address;

3.5.5.35.3. Usuário logado;

3.5.5.35.4. Última vez que o agente se comunicou com a o servidor central;

3.5.5.35.5. Identificador do grupo de políticas utilizados;

3.5.5.35.6. Campo que informa se o agente está em sincronismo com as últimas políticas/configurações disponibilizadas pelo administrador;

3.5.5.35.7. Versão do agente;

3.5.5.35.8. Versão da política instalada.

3.5.6. Módulo de rede

3.5.6.1. Permitir a monitoração/bloqueio do e-mail corporativo, evitando que e-mails com dados sigilosos sejam enviados para fora da organização, inclusive em smartphones e tablets.

3.5.6.2. Possibilidade de colocar mensagens de correio eletrônico em quarentena para análise.

3.5.6.3. Permitir a monitoração/bloqueio de tráfego WEB, evitando que dados sigilosos saiam da organização por este canal, inclusive em smartphones e tablets.

3.5.6.4. Capacidade de monitorar/bloquear o tráfego informações sensíveis em posts de redes sociais.

3.5.6.5. Permitir a monitoração de qualquer protocolo baseado em TCP, como o SMTP, inclusive anexos; HTTP, inclusive arquivos de upload; FTP ativo e passivo.

3.5.6.6. Capacidade de monitorar o vazamento de dados por meio de softwares de Mensagens Instantâneas.

3.5.6.7. Permitir a classificação dos protocolos, mesmo quando executados em portas que não são padrão.

3.5.6.8. Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP e remetente/destinatário de e-mail.

3.5.6.9. Ferramenta para auxiliar o acesso em nuvem

3.5.6.9.1. Deve prover detalhes do cloud service provider de quais tipos de armazenamentos e informações o aplicativo utiliza.

3.5.6.9.2. Deve possuir riscos para cada aplicação nuvem (Baixo, médio e alto).

3.5.6.9.3. Deve possuir métodos de implementação nos formatos, API, Reverse Proxy e Forward Proxy.

3.5.6.9.4. Possuir relatório com métricas de utilização dos usuários, atividades e volume de tráfego.

3.5.6.9.5. Deve configurar os riscos das aplicações para que o Discovery de informação seja realizado de acordo com o contexto do cliente.

3.5.6.9.6. A sua solução análise risco baseadas em múltiplos critérios.

3.5.6.9.7. Deve prover visibilidade dos usuários da aplicação para melhor identificar as altas áreas de risco.

3.5.6.9.8. Deve possuir Assessment de segurança baseado em boas práticas da indústria (PCI, ISO, etc) para visibilidade de vulnerabilidade de segurança.

3.5.6.9.9. Deve possui workflow integrado para o gerenciamento de risco.

3.5.6.9.10. Deve possuir habilidade de identificar configurações de senha, custos excessivos e outros atributos que podem ser sinais de riscos de segurança.

3.5.6.9.11. Deve possuir controle de informações através das cloud apps baseado em tipos de dados como PCI, PII, dados de TI, informações sensíveis e outras.

3.5.6.9.12. Deve possuir controle de informações com tipos de dados customizados utilizando dicionários, palavras chaves e Expressões Regulares.

3.5.6.9.13. Deve analisar em tempo real ações com informações nas aplicações nuvem SaaS, IaaS e PaaS.

3.5.6.9.14. Deve possuir descoberta de arquivos em repouso baseado em tipos de dados como PCI, PII, dados de TI, informações sensíveis e outras.

3.5.6.9.15. Deve possuir as seguintes ações ao realizar a mitigação

3.5.6.9.15.1. Auditoria.

3.5.6.9.15.2. Cancelar Compartilhamento para todos.

3.5.6.9.15.3. Cancelar Compartilhamento para usuários externos.

3.5.6.9.15.4. Cancelar Compartilhamento para usuários Internos.

3.5.6.9.15.5. Quarentena.

3.5.6.9.15.6. Quarentena com justificativa.

3.5.6.9.16. Deve possuir habilidade de gerar relatórios por tipos de dados, políticas e categorias de dados.

3.5.6.9.17. Deve possuir análise de risco baseado em analíticos de incidentes de vazamento de informação.

3.5.6.9.18. Deve possuir solução de Bring Your Own Encryption (BYOK) para no mínimo Office 365, One Drive e SharePoint Online.

3.5.6.9.19. Deve possuir suporte para todas os principais Apps de armazenamento de dados em nuvem suportados (Exemplo possibilidade de reportar operações de criação, deleção, upload e download para os arquivos e pastas incluindo o nome da pasta e o nome do arquivo)

3.5.6.9.19.1. Salesforce,

3.5.6.9.19.2. AWS

3.5.6.9.19.3. ServiceNow

3.5.6.9.19.4. Facebook Workplace

3.5.6.9.19.5. G-Suite

3.5.6.9.19.6. Google Cloud Platform

3.5.6.9.19.7. Azure.

3.5.6.9.19.8. One Drive

3.5.6.9.19.9. Trello

3.5.6.9.19.10. Dropbox

3.5.6.9.19.11. Slack

3.5.6.9.19.12. GitHub

3.5.6.9.19.13. LinkedIn

3.5.6.9.20. Deve possuir configurações personalizadas para os seguintes aplicativos em Officer 365 com as seguintes ações, Auditar, Bloquear Ação, Bloquear Usuário, Remover Compartilhamento, Quarentena.

3.5.6.9.20.1. OneDrive (SharePoint)

3.5.6.9.20.2. Outlook

3.5.6.9.20.3. Skype

3.5.6.9.20.4. Microsoft Teams

3.5.6.9.20.5. Power BI

3.5.6.9.20.6. Mobile Apps

3.5.6.9.21. Deve possuir configurações personalizadas para os seguintes aplicativos em G Suite com as seguintes ações, Auditar, Bloquear Ação, Bloquear Usuário, Remover Compartilhamento, Quarentena.

3.5.6.9.21.1. GDrive

3.5.6.9.21.2. Gmail

3.5.6.9.21.3. GCalendar

3.5.6.9.21.4. Hangouts

3.5.6.9.21.5. Sites

3.5.6.9.22. Deve possuir alertas contra brute force - Ataques de tentativa de senha e risco de conta ser comprometida.

3.5.6.9.23. Deve possuir alertas de Malicious insiders (acesso suspeito de dados) - Alta quantidade de download em curto espaço de tempo.

3.5.6.9.24. Deve possuir análise de comportamento de usuários automática para detecção de utilização anômala e comportamento suspeito.

3.5.6.9.25. Deve possuir integração com soluções de SIEM, Syslog e SOC/MSSPs.

3.5.6.9.26. Deve possuir controle de políticas de acesso customizadas para controle de BYOD e dispositivos corporativos.

3.5.6.9.27. A solução deve possuir nativamente motores de DLP com ações de bloqueio em real-time.

4. Gestão de Segurança de Ativos

4.1. A CONTRATADA deverá executar os serviços necessários para implantar o gerenciamento de ativos, bem como seguir todos os requisitos nele contido, planejando, implantando e coordenando ações juntamente com a área operações, contemplando segurança de infraestrutura, de software e de dados.

4.2. **Segurança de hardware**

4.2.1. Garantir a segurança dos ativos, prevenindo incidentes e impedindo a repetição de erros cometidos no passado. Garantindo a análise pormenorizada de vulnerabilidades de todos os itens de TI ao longo de todo o seu ciclo de vida ou período de propriedade, pois são onde as informações são criadas, processadas, armazenadas e compartilhadas.

4.2.2. Medir, informar e disponibilizar através de dashboard a segurança dos hardwares utilizando ferramentas de medições padrões de mercado de avaliação concentrando-se principalmente aos critérios aplicáveis à segurança de TI em geral.

4.2.3. Supervisionar e propor melhorias em relação ao Módulo de Segurança de Hardware (HSM) juntamente com os analistas técnicos e supervisores.

4.2.4. Estabelecer padrões para garantir que os ativos de tecnologia da informação estejam identificados corretamente; definir responsabilidades apropriadas para proteção e

divulgação da gestão dos ativos da informação, por meio do estabelecimento e manutenção de inventários, além de assegurar que o ciclo de vida dos ativos seja realizado e gerenciado para garantir a Segurança da Informação e o atendimento as legislações, normas e boas práticas recomendadas.

4.2.5. A CONTRATADA deverá elaborar procedimentos e instruções de segurança para os ativos de tecnologia.

4.2.6. A CONTRATADA deverá, através dos serviços prestados, identificar os pontos fracos examinando os ativos conectados à rede em busca de vulnerabilidades conhecidas, configurações incorretas e malware.

4.2.7. A CONTRATADA deverá:

4.2.7.1. Priorizar impactos ao PJERJ, mostrando a probabilidade de uma determinada ação ser explorada;

4.2.7.2. Identificar rapidamente quais patches priorizar para a maior redução de risco;

4.2.7.3. Fornecer uma série de pesquisas salvas que contenha atributos de hardware, coletadas ativamente como parte de um inventário de hardware;

4.2.7.4. Fornecer uma visão mais abrangente e integrada da postura de segurança corporativa para que você possa identificar, investigar e priorizar vulnerabilidades com precisão;

4.2.7.5. Fornecer uma análise histórica dos sistemas digitalizados, em comparação com os dados do BIOS e do Tipo de Dispositivo;

4.2.7.6. Fornecer o resumo dos sistemas operacionais detectados.

4.2.8. A CONTRATADA deve elaborar e coordenar um plano de ação para estabelecer procedimentos padronizados com relação a configuração de ativos de TIC e SI, de forma a facilitar os técnicos, bem como definir os responsáveis por sua atualização, onde esse trabalho deve abranger os seguintes tipos de ativos, entre outros:

4.2.8.1. Sistema Operacional;

4.2.8.2. Firewall

4.2.8.3. Balanceador de Carga;

4.2.8.4. Switch;

4.2.8.5. IPS - IDS/IPS;

4.2.8.6. IIS – Servidor Web/Apache;

4.2.8.7. Banco de Dados.

4.2.9. Todos os serviços de manutenção corretiva e preventiva aprovados através de um plano de ação, deverão minimizar a necessidade de parada do ambiente em produção,

testando todos os serviços após a realização de manutenções preventivas e/ou corretivas relacionadas à segurança da informação e suas vulnerabilidades.

4.2.10. A CONTRATADA deverá fazer o inventário de todos os ativos de hardware.

4.2.11. ACONTRATADA deverá fazer o inventario de ativos de hardwares conectados à rede.

4.2.12. A CONTRATADA deve manter um inventário preciso e atualizado de todos os ativos de tecnologia com o potencial de armazenar ou processar informações.

4.2.13. O inventario deve ter no mínimo:

4.2.13.1. Endereço de rede;

4.2.13.2. Endereço do hardware;

4.2.13.3. Nome da máquina;

4.2.13.4. Proprietário do ativo;

4.2.13.5. Departamento de cada ativo.

4.2.14. As manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), deverão ser agendadas e realizadas fora do horário regular, salvo quando expressamente autorizado pelo PJERJ.

4.2.15. As manutenções programadas, basicamente nos equipamentos mais críticos, que impliquem em extensiva parada do ambiente serão realizadas durante um final de semana.

4.2.16. A CONTRATADA deverá monitorar permanente e avaliar criticamente os serviços, identificando comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços.

4.2.17. 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.

4.3. **Segurança do Sistema distribuído**

4.3.1. A CONTRATADA deverá identificar as necessidades técnicas gerais em um sistema distribuído, consequentemente, que se relacionam com a orquestração dos recursos distribuídos de forma que o usuário possa acessar de forma transparente os serviços aprimorados decorrentes da distribuição de recursos sem ter que lidar com os mecanismos técnicos que fornecem as várias formas de recursos e serviços distribuídos orquestrações.

4.3.2. A CONTRATADA deverá prover uma ferramenta de segurança para essa transação de suporte a essas funcionalidades incluindo:

4.3.2.1. Um esquema de coordenação de recursos (Coordenação Serviços);

4.3.2.2. Gestão de inventario de vulnerabilidades.

4.3.3. A CONTRATADA deverá:

4.3.3.1. Fornecer ferramentas para análise do perímetro da rede com localização as fronteiras e onde estão logicamente conectadas;

4.3.3.2. Fornecer identificação das portas detectadas em hosts que estão ouvindo ou tem conexões de portas ativas;

4.3.3.3. Identificar e disponibilizar no dashboard ações maliciosas nos serviços web associados às portas comuns dos serviços.

4.4. **Segurança de software**

4.4.1. A CONTRATADA deverá:

4.4.1.1. Identificar e disponibilizar através de dashboard aplicativos e sistemas operacionais sem suporte e com patches ausentes na rede;

4.4.1.2. Identificar e disponibilizar através de dashboard aplicativos e sistemas operacionais sem suporte por tipo de produto, como servidores de banco de dados, servidores WEB, Windows ou outros sistemas operacionais;

4.4.1.3. Identificar softwares instalados nos hosts;

4.4.1.4. Manter uma lista atualizadas de todos os softwares autorizados;

4.4.1.5. Remover softwares não autorizados.

4.5. **Ciclo de Vida Seguro do Software**

4.5.1. A CONTRATADA deverá fornecer uma visão geral dos processos de desenvolvimento de software para a implementação de software seguro, desde o design do software até o uso operacional do software.

4.5.2. Essa implementação envolverá nova codificação, bem como a incorporação de bibliotecas e componentes de terceiros. O objetivo é o uso na área de segurança de software e para orientar os profissionais do Departamento de Desenvolvimento de Sistemas (DESIS).

4.5.3. A CONTRATADA deverá:

4.5.3.1. Fornecer uma visão geral estruturada do desenvolvimento, codificação de software seguro e as categorias conhecidas de vulnerabilidades de implementação de software e de técnicas que podem ser usadas para prevenir ou detectar tais vulnerabilidades ou para mitigar sua exploração;

4.5.3.2. Subsidiar de conhecimentos necessários nos processos de ciclo de vida de software seguro com abordagens proativas para construir segurança em um produto, tratando na raiz o software mal projetado e inseguro na fonte, em vez de interromper os sintomas por meio de uma abordagem reativa de penetração e correção;

4.5.3.3. Adotar práticas que abrangem a prevenção de defeitos de segurança, a detecção de defeitos de segurança e a mitigação de defeitos de segurança quando um produto está em campo;

4.5.3.4. Auxiliar os profissionais que devem considerar a incorporação de práticas de cada um desses processos em seu próprio processo de software seguro.

4.5.4. A CONTRATADA deverá prover orientações dos modelos de ciclo de vida de software seguro pelas diversas atividades mapeadas nas possíveis fases de desenvolvimento de software:

4.5.4.1. Educação e conscientização;

4.5.4.2. Início do projeto;

4.5.4.3. Análise e requisitos;

4.5.4.4. Projeto arquitetônico e detalhado.

4.5.5. A CONTRATADA deverá propor e fornecer informações sobre adaptações para proteger o ciclo de vida do software:

4.5.5.1. Desenvolvimento de software Ágil e DevOps;

4.5.5.2. Móvel;

4.5.5.3. Computação em Nuvem;

4.5.5.4. Internet das coisas (IoT).

4.5.6. A CONTRATADA deverá acompanhar a avaliação da maturidade do ciclo de vida seguro do software com os métodos abaixo:

4.5.6.1. Software Assurance Maturity Model (SAMM);

4.5.6.2. Building Security In Maturity Model (BSIMM);

4.5.6.3. Common Criteria (CC).

4.5.7. Adotar um ciclo de vida seguro de software - Escolher quais práticas de segurança incluir em um ciclo de vida de software seguro, o CONTRATANTE pode considerar olhar para os resultados da maturidade adotada que fornecem informações atualizadas sobre a adoção de práticas.

4.6. **Segurança de rede**

4.6.1. A CONTRATADA deverá:

4.6.1.1. Criar mecanismos e suporte operacional para os desafios associados à proteção da rede contra uma variedade de ataques para uma série de tecnologias de rede e protocolos de segurança amplamente usados no PJERJ, juntamente com desafios e soluções de segurança emergentes.

4.6.1.2. Fazer uma abordagem aplicada para entender quais técnicas ajudam a construir uma rede segura na arquitetura de internet, permitindo entender os problemas de segurança em cada camada e a interação entre eles.

4.6.1.3. Evitar ataques da rede, examinando a segurança em cada camada da pilha de protocolo de rede a busca de vulnerabilidades.

4.6.2. A CONTRATADA deverá prover segurança da camada de aplicação observando:

4.6.2.1. A infraestrutura de chave pública (PKI);

4.6.2.2. Extensões de segurança DNS;

4.6.2.3. Protocolo de transferência de hipertexto seguro (HTTPS);

4.6.2.4. Segurança de protocolo de tempo de rede (NTP).

4.6.3. A CONTRATADA deverá prover segurança da camada de transporte observando:

4.6.3.1. Handshake;

4.6.3.2. Key-Derivation;

4.6.3.3. Data-Transfer;

4.6.3.4. Conexões rápidas com a Internet UDP (QUIC).

4.6.4. A CONTRATADA deverá prover segurança da camada de rede observando:

4.6.4.1. Mascaramento de IP;

4.6.4.2. Segurança IPv6;

4.6.4.3. Segurança do protocolo de roteamento.

4.6.5. A CONTRATADA deverá prover segurança da camada de link observando:

4.6.5.1. Autenticação baseada em porta IEEE 802.1X;

4.6.5.2. Ataque no switch Ethernet.

4.6.6. Suporte a segurança dos protocolos das redes sem fio, devido à natureza de transmissão da mídia, o que simplifica a escuta.

4.6.7. A CONTRATADA deverá fornecer lições importantes sobre os protocolos de segurança projetados para fornecer integridade, confidencialidade e autenticação.

4.6.8. A CONTRATADA deverá apoiar na implantação de ferramentas que abordará em detalhes a área de Conhecimento de Operações de Segurança e Gerenciamento de Incidentes nas camadas da pilha de protocolos onde os ataques devem ser detectados o mais cedo possível, ou mesmo previstos antes de começarem, para que possam ser evitados por completo. Onde essa ferramenta deve contemplar:

4.6.8.1. Filtros de pacotes / firewalls;

4.6.8.2. Gateway de Aplicativo (AG);

4.6.8.3. Gateway em nível de circuito (CG);

4.6.8.4. Sistemas de detecção de intrusão (IDS);

4.6.8.5. Sistema de prevenção de intrusão (IPS);

4.6.8.6. Projeto de Arquitetura de Rede.

4.6.9. A CONTRATADA deverá observar as determinações do Ato Normativo TJ n.º 10/2019 e executar pelo pessoal técnico para conformidade das atividades técnicas da segurança de rede avançada (Rede definida por software (SDN), virtualização e Segurança da Internet das Coisas (IoT)), referenciados ao Data Center.

5. Gestão de Incidentes, Vulnerabilidades e Ameaças

5.1. A CONTRATADA deverá executar serviços para o gerenciamento incidentes, com ferramentas automatizadas, levantar e monitorar vulnerabilidades e ameaças, baseando-se no modelo ISO/IEC 27005, além da legislação e normas do Poder Judiciário.

5.2. Propor e coordenar a criação de protocolos de prevenção de incidentes e gestão de crises.

5.3. Propor ações preventivas e corretivas, de forma proativa, bem como testes periódicos de segurança.

5.4. Coordenar ações defensivas e ofensivas de segurança, incluindo ataques cibernéticos

5.5. Serão considerados incidentes de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do PJERJ, tais como:

5.5.1. Acessos indevidos;

5.5.2. Instalação de códigos maliciosos;

5.5.3. Indisponibilidade dos serviços causados por agentes externos / maliciosos;

5.5.4. Ataques por força bruta;

5.5.5. Exploração de vulnerabilidades.

5.6. Avaliar periodicamente a customização dos softwares do PJERJ e ajusta as suas configurações, de maneira que ocorrências de problemas, incidentes ou irregularidades sejam devidamente notificadas.

5.7. Proteger servidores de contra-ataques, zero-day por meio de políticas comportamentais, sem a necessidade de atualização da base de assinaturas.

5.8. Monitorar a proteção dos servidores executando ações como controle de acesso a processos, por IP ou porta.

5.9. Ações de monitoramento.

5.9.1. Realizar monitoração diária.

5.9.2. Priorizar e pontuar o grau de riscos cibernéticos automatizados.

5.9.3. Realizar buscas automatizadas por endereços de e-mails pertencentes aos domínios que tenham sido alvo de exposições de credenciais.

5.9.4. Monitorar a ocorrência de incidentes globais

5.9.5. Monitoramento de aplicações web, servidores, virtualizadores e rede de forma proativa e reativa no ambiente internet e intranet da instituição.

5.9.6. 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.

5.10. Análise de Incidentes Globais

5.10.1. A CONTRATADA deve monitorar a ocorrência de incidentes globais, através de RSS Feeds, de modo a antever eventuais ataques a CONTRATANTE;

5.10.2. Ataques direcionados ao mesmo segmento de mercado do CONTRATANTE devem ser imediatamente sinalizados para que seja tomada uma decisão em relação à atuação dos serviços contratados.

5.11. Monitoração de Marca e Fraudes Digitais

5.11.1. O serviço a ser contratado deve possuir como requisito básico a proteção da presença digital da CONTRATANTE, e de suas marcas, conteúdos e aplicativos nos diversos canais digitais (web, mídias sociais especificas, lojas de aplicativos, e-mail) de forma a impedir, no Brasil ou no exterior.

5.11.2. O uso inadequado ou associação, sem a devida autorização das suas marcas, serviços, produtos ou eventos, organizações, empresas da CONTRATANTE;

5.11.3. Utilização de identidade, senha, dados cadastrais ou credenciais de usuários da internet, através do envio de e-mails falsos que direcionam para sites fraudulentos, utilizando indevidamente as características da presença digital da CONTRATANTE;

5.11.4. O uso indevido das marcas relacionadas a CONTRATANTE, por terceiros em “anúncios pagos” ou “busca orgânica” de mecanismos de busca (Google, Yahoo, Bing, entre outros), com o objetivo de desviar o tráfego do site original para sites não oficiais;

5.11.5. O uso não autorizado do nome (ou marca) da CONTRATANTE ou similares (com erro de grafia, adição ou troca de caracteres) no registro de nomes de domínios no Brasil e no exterior;

5.11.6. O uso não autorizado das marcas da CONTRATANTE de forma figurativa ou nominativa na criação de perfis e páginas em determinadas redes sociais;

5.11.7. A associação das marcas da CONTRATANTE de forma figurativa ou nominativa, para ofertar produtos ou serviços fraudulentos ou falsos relacionados às atividades da CONTRATANTE;

5.11.8. A associação das marcas da CONTRATANTE de forma figurativa ou nominativa, na disponibilização ou comercialização de serviços ou de conteúdos da CONTRATANTE;

5.11.9. A oferta ou disponibilização de credenciais de acesso aos websites das marcas da CONTRATANTE;

5.11.10. O uso não autorizado das marcas da CONTRATANTE de forma figurativa ou nominativa por aplicativos de terceiros;

5.11.11. A reprodução não autorizada dos aplicativos oficiais das marcas da CONTRATANTE em canais não oficiais ou não autorizados pela CONTRATANTE;

5.11.12. A divulgação ou comercialização de listas que contenham endereços eletrônicos relacionados aos domínios das marcas da CONTRATANTE;

5.11.13. A divulgação, uso ou comercialização de modelos de telas para web similares ou idênticas das marcas da CONTRATANTE com o objetivo de criação de Phishings;

5.11.14. A divulgação ou comercialização de informações sensíveis da CONTRATANTE ou dos contribuintes.

5.11.15. Dessa forma, a empresa CONTRATADA, deverá viabilizar à CONTRATANTE, em conjunto com a CONTRATADA ou de forma isolada, a adoção das seguintes ações:

5.11.15.1.1. Monitorar sites com conteúdo não autorizado, compreendendo a abrangência da internet, com o objetivo de gerar uma resposta através de notificações até mesmo da remoção completa do site infrator da internet;

5.11.15.1.2. Nos serviços de envio de e-mail da CONTRATANTE, implementar e monitorar, com o apoio da CONTRATANTE, o padrão Domain-Based Message Authentication, Reporting and Conformance (DMARC), que passará a dotar este padrão para obter a redução da exposição dos usuários às mensagens não legítimas ou fraudulentas enviadas por servidores não autorizados (e-mail spoofing);

5.11.15.1.3. Gerar um histórico de eventos identificados contra as marcas da CONTRATANTE, de acordo com os cenários demandados pela CONTRATANTE;

5.11.15.1.4. Realizar gestão preventiva para evitar que novas fraudes ou uso indevido das marcas ocorram;

5.11.15.1.5. Gerar um conjunto de evidências sobre o incidente, como screenshots, cópia do site, informações do whois, histórico de comunicação para notificação e todos os demais

artefatos que poderão ser utilizados em uma possível investigação ou processo criminal contra os fraudadores;

5.11.15.1.6. Realizar relacionamento com entidades nacionais e internacionais para facilitar o processo de desligamento de sites hospedeiros de fraudes.

5.11.15.1.7. Para tal, a CONTRATADA deverá disponibilizar a ferramenta de monitoramento e prestar apoio para operacionalização conjunta dos serviços com a CONTRATANTE;

5.11.16. Além dos requisitos básicos para atender as necessidades do negócio da CONTRATANTE, a CONTRATADA deverá:

5.11.16.1. Realizar takedowns ou shutdowns ilimitados para incidentes digitais detalhados neste documento;

5.11.16.2. Disponibilizar através de um website/portal, uma plataforma integrada, que permita à CONTRATANTE verificar todos os incidentes, desde a detecção de sua origem, passando pela criação até sua conclusão;

5.11.16.3. Disponibilizar website/portal que ofereça conexão segura através do protocolo HTTPS (Hyper Text Transfer Protocol Secure) e também autenticação em dois fatores;

5.11.16.4. Possuir mecanismos próprios de monitoramento e análise de dados, como relatórios de spam dos principais provedores da internet, relatórios de empresas de antivírus, adotando uma abordagem proativa com o objetivo de encontrar previamente os tipos de incidentes digitais detalhados no Anexo A;

5.11.16.5. Possuir mecanismos próprios que realizem a monitoração das principais Redes Sociais (Blogs, sites de notícias, Twitter, Google Groups, etc.) e lojas de Aplicativos para Smartphones (Google Play Store, Apple Store e outras lojas não oficiais.);

5.11.16.6. Prover os mecanismos acima baseados em machine learning;

5.11.16.7. Prover serviço de monitoramento de domínios nacionais e internacionais, incluindo TLDs e gTLDs, que verifique a utilização do uso indevido das marcas da CONTRATANTE no nome do domínio ou na URL cadastrada, disponibilizando relatórios a cada 24 horas no máximo, contendo o domínio/URL cadastrado, a empresa que administra o registro do domínio, e os dados do proprietário do domínio;

5.11.16.8. Prover o serviço de validação de e-mail baseado no padrão DMARC, incluindo a verificação da adoção mecanismos de segurança dos domínios SPF (Sender Policy Framework) e no DKIM (DomainKeys Identified Mail) e apoio ao tratamento das mensagens;

5.11.16.9. Acatar novas palavras-chave, listas de palavras, sempre que demandados pela CONTRATANTE para elaboração dos parâmetros de busca a serem executados;

5.11.16.10. Disponibilizar web service que permita consultar, pesquisar e obter informações referentes aos incidentes, através de REST, JSON, ou alguma outra abordagem desde que acordada pela CONTRATANTE;

5.11.17. A CONTRATADA deve monitorar a DEEP WEB em monitoramento de lista vip a partir dos bins informados pela CONTRATANTE;

5.11.18. Permitir o envio de weblogs e abuse inbox, tratando-os a fim de avaliar se existem ameaças que sejam objeto deste termo;

5.11.19. Fornecer scripts que deverão ser inseridos de forma ofuscada nas páginas do seu(s) site(s) que a CONTRATANTE queira monitorar. Esse script deverá gerar uma conexão com variáveis de navegação que serão analisadas pela CONTRATADA, a fim de detectar anomalias na conexão feita pelo usuário website do CONTRATANTE. Se a conexão for anômala, um alerta deverá ser enviado à CONTRATADA para revisão final. Caso o ataque seja confirmado, a CONTRATADA deverá gerenciar a desativação do site fraudulento;

5.11.20. Mostrar nas estatísticas informações sobre possíveis vítimas de ataques de phishing, com os seguintes dados:

5.11.20.1. Listagem de todos os tickets abertos de ataques de phishing;

5.11.20.2. Possíveis vítimas dos ataques;

5.11.20.3. Estatísticas resumidas.

5.11.21. Prover os seguintes monitoramentos:

5.11.21.1. Proteção contra defacement de websites: O defacement é um tipo de ataque que altera a aparência visual do website. A proteção de defacement do DMS cria uma impressão digital do website e monitora alterações nas páginas protegidas a cada 2 minutos. Quando uma falta de correspondência é detectada, a equipe DMS investiga se se trata de um ataque;

5.11.21.2. Monitoramento de DNS: O DNS é usado para associar nomes de sites a endereços IP. O serviço DMS previne o sequestro de DNS, fazendo um snapshot de todas as resoluções DNS dos sites protegidos e comparando-as em tempo real com as resoluções de DNS no mundo inteiro, para garantir que nenhum ataque esteja em andamento. Quando um evento é detectado, a equipe DMS determina se está ocorrendo um ataque e contata o cliente imediatamente;

5.11.21.3. Verificação de certificados SSL: O DMS realiza validações periódicas do certificado SSL e sua criptografia para proteger o site transacional e garantir que os usuários finais do cliente sempre obtenham um certificado válido e não expirado.;

5.11.22. A CONTRATADA deve realizar o monitoramento de disponibilidade do site: Continua supervisionando o status do website para acompanhar se ele está on-line, carregando lentamente ou se está inativo.

5.11.23. Notificar o responsável pela hospedagem ou publicação do material ou serviço fraudulento, até o seu Takedown ou Shutdown ser confirmado, além de manter monitoração contínua, por 15 dias consecutivos, para identificar possíveis reincidências, para todos os tipos de incidentes, listados a seguir:

5.11.23.1. Prover o serviço em regime 24x7 todos os dias da semana, inclusive finais de semana e feriados.

5.11.23.2. Tratamento de Incidentes, Relatórios Operacionais e Consulta

5.11.23.3. Cada incidente deve conter, no mínimo, as seguintes informações em seu conteúdo:

5.11.23.3.1. Código para identificação do incidente;

5.11.23.3.2. Tipo do incidente;

5.11.23.3.3. Data e hora de abertura do incidente;

5.11.23.3.4. Data e hora de fechamento do incidente

5.11.23.3.5. Tempo de tratamento do incidente;

5.11.23.3.6. URL/IP, nome do Host, país, ISP, domínio, informações do whois;

5.11.23.3.7. Fonte de origem (responsável pela detecção);

5.11.23.3.8. Evidências que comprovam o incidente.

5.11.23.4. Cada incidente deve conter a descrição da sua fonte originária, informando quem detectou o incidente, se a CONTRATANTE ou a CONTRATADA, devendo essa informação estar visível quando o incidente for consultado;

5.11.23.5. Cada incidente deve ser comprovado, permitindo que através de uma simples consulta seja possível constatar suas evidências;

5.11.23.6. São aceitos como evidências: screenshots, artefatos, informações do whois ou código fonte da página;

5.11.23.7. As evidências poderão ser utilizadas desde que acordadas pela CONTRATANTE, priorizando-se sempre que possível pelo código fonte da página como uma das evidências;

5.11.23.8. Para incidentes que envolvam Phishing, é imprescindível a presença de screenshots como evidência;

5.11.23.9. Para cada incidente aberto, o serviço deverá emitir um e-mail automaticamente para a CONTRATANTE informando em seu conteúdo os detalhes da criação do incidente;

5.11.23.10. Para cada incidente finalizado, o serviço deverá emitir um e-mail automaticamente para a CONTRATANTE informando em seu conteúdo os detalhes referentes ao fechamento do incidente, ficando a critério da CONTRATANTE a ativação e desativação dessa rotina.

5.11.23.11. O serviço de proteção de aplicativos para Smartphones deverá:

5.11.23.11.1. Realizar o monitoramento das principais lojas de aplicativos para mobile (Google Play Store, Apple Store), com varreduras diárias;

5.11.23.11.2. Realizar monitoramento a fim de encontrar aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas.

5.12. Apropriação de Identidade

5.12.1. Apropriação do nome ou das marcas, utilizando a credibilidade da CONTRATANTE para passar pelo site oficial ou explorar a marca para atividades indevidas ou fraudulentas.

5.12.2. Prover relatórios operacionais e consultas

5.12.3. Desejável prover interface web para gerenciamento, monitoramento, painéis de alerta e relatórios consolidados e analíticos, para consulta imediata, de todos os incidentes tratados e analisados;

5.12.4. Desejável prover funcionalidades que permitam realizar a personalização de filtros e ordenações para gerar informações por tipo de incidente, tempo de shutdown ou Takedown, URL/IP, Host, país, e a fonte de origem do incidente (quem realizou a detecção do incidente);

5.12.5. Desejável disponibilizar painel que demonstre no mínimo as seguintes informações para um período de consulta a ser executado no website/portal:

5.12.5.1. Total de incidentes abertos, com opção para visualizar por tipo de incidente;

5.12.5.2. Total de shutdowns realizados, com opções para visualizar por tipo de incidente e agrupar por tempo de shutdown realizado;

5.12.5.3. Tempo médio de shutdown atingido, com opção para visualizar por tipo de incidente.

5.12.6. Deve permitir a exportação dos dados do website/portal de forma simplificada, através de formatos populares, como, por exemplo: doc, odt, csv, xls, pdf, entre outros;

5.12.7. Deve preservar e suportar armazenamento de dados históricos de acordo com a tabela de armazenamento especificada a seguir;

5.12.8. Lista de Incidentes a serem tratados

5.12.8.1. Aplicativos não oficiais

5.12.8.2. A proteção de aplicativos para Smartphones e Tablets, objetiva encontrar aplicativos falsos, ou maliciosos, ou que utilizam a marca da CONTRATANTE sem autorização,

nas principais lojas de aplicativos (Google Play Store, Apple Store) e também em nas lojas e sites não oficiais;

5.13. Domínios similares

5.13.1. Domínios são nomes que servem para localizar e identificar conjuntos de computadores na Internet;

5.13.2. Domínios realizam a função de relacionar nomes a endereços IP (Internet Protocol) e vice-versa;

5.13.3. O serviço de proteção de domínios de internet deverá realizar monitoramento:

5.13.3.1. Da utilização da marca no domínio;

5.13.3.2. Da utilização da marca no domínio através de palavras semelhantes ou alusivas a marca CONTRATANTE, com ou sem erros ortográficos;

5.13.3.3. Da divulgação em anúncios pagos, além de permitir a realização de buscas por termos específicos indicados pela CONTRATANTE.

5.13.4. A CONTRATADA deverá propor mecanismo para evitar danos por Malware ou código malicioso desenvolvido para causar danos, alterações ou roubo de informações ao usuário final, combatendo dentre os mais conhecidos:

5.13.4.1. vírus, worms, trojans, C&C (Command and Control), rootkit, backdoor, Remote Access Trojan (RAT), etc.

5.14. Perfis Falsos

5.14.1. Páginas ou perfis que se apropriam indevidamente da identidade da CONTRATANTE ou de seus servidores, utilizando a credibilidade da marca para promoção da página ou para auferir benefícios financeiros ou não.

5.15. Phishing

5.16. Vazamento de e-mails corporativos

5.16.1. Monitoramento de lista vip que será fornecida pelo PJERJ, pois requer cuidados especiais.

5.16.2. Prática ilícita divulgação ou comercialização de programas ou serviços da CONTRATANTE ou criados por hackers para realizar consultas e divulgar ou vender informações sensíveis de cidadãos.

5.16.3. Cabe destacar que além do quadro de Ameaças ou Incidentes Digitais apresentado, o serviço contratado abrange a proteção do nome ou da marca da CONTRATANTE, de seus conteúdos ou que ela seja fiel depositária, bem como de aplicativos, sendo:

5.16.3.1. Proteção de Marca

5.16.3.1.1. O serviço de proteção de marca deverá abranger a marca CONTRATANTE contemplando os sites institucionais do seu conglomerado;

5.16.3.1.2. O serviço de proteção de marca deverá realizar monitoramento da utilização da marca em nomes de domínios, sites de internet, blogs e fóruns, redes sociais específicas, lojas de aplicativos para smartphones, que estejam atuando de forma abusiva, fraudulenta ou não autorizada.

5.16.3.2. Proteção de Conteúdo

5.16.3.2.1. O serviço de proteção de conteúdo contempla a distribuição não autorizada de conteúdo digital;

5.16.3.2.2. O serviço de proteção de conteúdo deverá realizar monitoramento acerca da distribuição de documentos e informação confidenciais, divulgações relacionadas a produtos e sistemas da CONTRATANTE, além do monitoramento do site de compartilhamento de arquivos e informações Pastebin como exemplo.

5.16.3.3. Proteção de Aplicativos

5.16.3.3.1. O serviço de proteção de aplicativos para Smartphones deverá:

5.16.3.3.1.1. Realizar o monitoramento das principais lojas de aplicativos para mobile (Google Play Store, Apple Store) com varreduras diárias;

5.16.3.3.1.2. Realizar monitoramento a fim de encontrar aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas.

5.16.3.4. Políticas de retenção de dados

5.16.3.4.1. A CONTRATADA irá coletar dados para descobrir ataques avançados contra a CONTRATANTE. Os dados deverão permanecer disponíveis para visualização no portal do cliente, pelo período definido abaixo:

DADOS	PERÍODO DE RETENÇÃO
Informações sobre o ticket Qualquer incidente registrado pelo CONTRATADO que é uma ameaça potencial para o CONTRATANTE. O ticket pode incluir screenshots de websites, outros relacionadas às partes.	5 anos
Domínios semelhantes Registros de domínio da Internet com uma ortografia semelhante ao CONTRATANTE ou suas marcas	5 anos
Mídias sociais Mídia social (podendo ser indicadas algumas em específico	3 anos

posteriormente pelo PJERJ) ou artigos de notícias que mencionam o CONTRATANTE ou suas marcas.	
Alertas do SSL do Web site Qualquer problema de certificado SSL identificado em um site do CONTRATANTE.	3 anos
Site Disponibilidade Alertas Qualquer tempo de inatividade identificado em um site do CONTRATANTE.	3 anos
Alertas de Desfiguração do Site (Defacement) Qualquer alteração significativa que não tenha sido causada pela CONTRATANTE em um site do CONTRATANTE. O monitoramento deve ser automatizado e gerar alertas quando existir alteração de atualização ou publicação de documentos.	3 anos
Detectar conexões no site Qualquer tipo de conexão fora do padrão de atividade adotado pelo PJERJ, incluindo inatividade identificado em um site do CONTRATANTE.	2 anos

5.17. **Das atividades técnicas de gestão de vulnerabilidades**:

5.17.1. Dispor de meios para identificação e correção de vulnerabilidades de segurança da informação no ambiente e sistemas do PJERJ, com a capacidade de detectar, inventariar e avaliar vulnerabilidades a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas. Especialmente quanto ao impacto no ambiente computacional e ao risco inerente à segurança das informações custodiadas.

5.17.2. A atividade de Gestão de Vulnerabilidades poderá ser realizada in loco ou remotamente, conforme determinação do CONTRATANTE, e terá como objetivo principal a análise geral do, ambiente do CONTRATANTE quanto a segurança da informação para identificar, mapear, documentar controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do CONTRATANTE, bem como apresentar recomendações de melhorias e/ou correções das vulnerabilidades identificadas durante os testes;

5.17.3. Fazem parte do processo de gestão de vulnerabilidades as fases de Varredura de vulnerabilidades, Teste de Invasão, Alerta de Vulnerabilidades e Controle das

vulnerabilidades. Estas fases devem atuar de forma integrada com o objetivo de proverem informações suficientes para uma proteção mais eficaz do ambiente da contratada.

5.17.4. A periodicidade da execução das fases supracitadas dentro da vigência contratual de 24 meses deverá seguir as exigências da tabela abaixo:

FASE	PERIODICIDADE	EXECUÇÕES NO CONTRATO
Varredura de vulnerabilidades (interno)	Mensal	24
Teste de invasão (interno e externo) White Box, Gray Box e Black Box	Semestral	4
Simulação de ataque phishing	Trimestral	8
Alerta de vulnerabilidades	Semanal	106
Controle de vulnerabilidades	Diária	730

A quantidade total de IPs para o monitoramento de vulnerabilidades e URLs para aplicações, assim como a quantidade de localidades que deverão ser monitorados serão informados durante a visita técnica.

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

5.17.6. Os testes de infraestrutura só poderão acontecer mediante autorização da CONTRATANTE, com anuência da DI – Diretoria de Informática.

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

5.17.8. Todos os testes a serem realizados deverão ser precedidos de escopo pré-definido e aprovado, 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 do CONTRATANTE.

5.17.9. Todas as fases dos testes serão acompanhadas e supervisionadas a critério da CONTRATANTE.

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

5.17.11. O Responsável Técnico deverá estar presente, no mínimo, 1 (um) dia por semana nas dependências do CONTRATANTE para efetuar o acompanhamento dos serviços e repassar as informações para o CONTRATANTE, durante a execução dos Testes de Invasão;

5.17.12. Varredura de Vulnerabilidades:

5.17.12.1. Deverá ser realizada mensalmente uma varredura interna de vulnerabilidades no escopo descrito abaixo;

5.17.12.2. A varredura de vulnerabilidades do ambiente de TI deve considerar as seguintes etapas:

5.17.12.3. 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 e as informações das janelas de manutenção e mudança caso seja necessário aplicar patch e/ou correções;

5.17.12.4. Execução da varredura de vulnerabilidades

5.17.12.5. Análise dos resultados e priorização das vulnerabilidades;

5.17.12.6. Elaboração e entrega de um Plano de Remediação, com a supervisão e execução do plano, considerando a criticidade da vulnerabilidade identificada e, também, os critérios definidos na fase de Levantamento de Ativos, utilizando-se o conceito de ativo estabelecido no Ato Normativo TJ n.º 10/2019.

5.17.12.7. Para toda vulnerabilidade encontrada, a CONTRATADA deverá descrever de forma detalhada as ações para correção. Caso precise ter acesso as configurações dos ativos de tecnologia ou o código fonte para propor as soluções de correção, a Contratada deverá justificar a necessidade, ficando a cargo do CONTRATANTE decidir pela liberação;

5.17.12.8. Deve ser também apresentado a Matriz de Risco das vulnerabilidades detectadas e o grau de maturidade do CONTRATANTE em cada item analisado.

5.17.13. **Ferramenta**

5.17.13.1. Para auxiliar na atividade de varredura de vulnerabilidades deve ser entregue uma ferramenta com as seguintes características:

5.17.13.2. O gerenciamento da ferramenta deverá ser no ambiente da CONTRATANTE;

5.17.13.3. A solução de gestão de vulnerabilidades deverá ter a capacidade de realizar varreduras em busca de vulnerabilidades, configurações incorretas e inconformidade dos

ativos de rede, além da identificação de indícios e padrões de códigos maliciosos. Também fazem parte da aquisição o fornecimento, instalação, configuração de softwares da solução, garantia pelo período de 24 meses.

5.17.13.4. A ferramenta deve ser licenciada para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);

5.17.13.5. A ferramenta deverá ser instalada nas dependências do órgão, de forma on-premisse, sendo aceito qualquer dos seguintes cenários:

5.17.13.6. Uso de Appliance físico, sem uso de virtualização;

5.17.13.7. Appliance "bare metal" de terceiros, desde que, oficialmente suportados e homologados pelo fabricante da solução de gestão de vulnerabilidades;

5.17.13.8. Uso de Appliance virtual compatível com Hypervisor do órgão;

5.17.13.9. Uso de Appliance virtual junto com Servidor e Hypervisor oficialmente suportados e homologados pelo fabricante da solução de gestão de vulnerabilidades.

5.17.13.10. Os produtos utilizados devem ser licenciados de forma integral para todas as funcionalidades especificadas neste termo de referência;

5.17.13.11. A ferramenta deve ser licenciada para uso perpétuo. As funcionalidades da ferramenta devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na ferramenta.

5.17.13.12. Deve ser entregue comprovação ponto a ponto de atendimento das características técnicas dos equipamentos aos requisitos exigidos neste Termo de Referência por meio da transcrição de trecho do documento oficial do fabricante ou qualquer outra documentação que comprove expressamente o atendimento da funcionalidade, informando:

5.17.13.12.1. Qual é o documento;

5.17.13.12.2. Onde encontrar o documento;

5.17.13.12.3. Qual a página do documento;

5.17.13.12.4. Qual o parágrafo do documento.

5.17.13.13. REQUISITOS TÉCNICOS PARA PLATAFORMA DE GESTÃO DE VULNERABILIDADES

5.17.13.13.1. Deverá possuir um módulo de gerenciamento único, centralizado, responsável pela aplicação das políticas de segurança, administração e controle das demais funcionalidades da ferramenta.

5.17.13.13.2. A plataforma de gerenciamento da ferramenta de gestão de vulnerabilidades deverá ser instalada nas dependências do cliente (On-premise) e deverá ser compatível para instalação nos seguintes sistemas operacionais:

5.17.13.13.2.1. Red Hat Enterprise Linux 6;

5.17.13.13.2.2. Red Hat Enterprise Linux 7;

5.17.13.13.2.3. CentOS 6, 64-bit;

5.17.13.13.2.4. CentOS 7, 64-bit;

5.17.13.13.3. A ferramenta deve ser licenciada para uso ilimitado de sensores ativos;

5.17.13.13.4. A ferramenta de gerenciamento deverá permitir hardening via controles SELinux para impedir explorações no servidor;

5.17.13.13.5. Deve ter a possibilidade de armazenar localmente a base de dados de vulnerabilidades;

5.17.13.13.6. Deve ser capaz de identificar no mínimo 60.000 CVE´S;

5.17.13.13.7. Deve permitir a autenticação com certificados SSL, smart cards, PIV (Personal identity verification) e common access cards (CAC);

5.17.13.13.8. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv2 score ou CVSSv3;

5.17.13.13.9. A ferramenta também deve possuir um sistema próprio de pontuação e priorização das vulnerabilidades;

5.17.13.13.10. O sitema de priorização deve aplicar algoritimos de inteligência artificial (Machine learning) para analizar mais de 120 características relacionadas a vulnerabilidades listadas na National Vulnerability Database(NVD);

5.17.13.13.11. O sistema de priorização deve ser dinâmico, a medida que as variáveis relacionadas a uma determinada vulnerabilidade se alterem o algoritmo deve levar essas mudanças em consideração ao realizar o cálculo do score;

5.17.13.13.12. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

5.17.13.13.12.1. CVSSv3 Impact Score;

5.17.13.13.12.2. Idade da Vulnerabilidade;

5.17.13.13.12.3. Número de produtos afetados pela vulnerabilidade;

5.17.13.13.12.4. Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;

5.17.13.13.12.5. Lista de todas as fontes (canais de mídia social, dark web etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade;

5.17.13.13.13. A ferramenta deve possuir sistema de alertas com ações definidas para cada alerta, entre elas:

5.17.13.13.13.1. Criação de Ticket no sistema de chamados interno da ferramenta;

5.17.13.13.13.2. Envio de e-mail;

5.17.13.13.13.3. Envio de mensagem syslog;

5.17.13.13.13.4. Iniciar scan sob demanda com base em condições definidas;

5.17.13.13.13.5. Gerar relatório sob demanda filtrado nas condições do alerta;

5.17.13.14. REQUISITOS DE RELATÓRIOS E PAINÉIS GERENCIAIS

5.17.13.14.1. A ferramenta deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados.

5.17.13.14.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento.

5.17.13.14.3. Deve possuir mais de 300 relatórios e painéis pré-configurados que podem ser utilizados sem a necessidade de customização.

5.17.13.14.4. A ferramenta deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;

5.17.13.14.5. A ferramenta deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e RTF;

5.17.13.14.6. A ferramenta deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

5.17.13.14.7. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;

5.17.13.14.8. A ferramenta deve suportar o envio automático de relatórios para destinatários específicos;

5.17.13.14.9. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

5.17.13.14.10. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

5.17.13.14.11. Deve permitir a customização de relatórios podendo incluir no mínimo as seguintes opções:

5.17.13.14.12. Marca d'agua customizada em cada página do relatório;

5.17.13.14.13. Customização de logo;

5.17.13.14.14. Header pré-definido;

5.17.13.15. REQUISITOS DE VARREDURA

5.17.13.15.1. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

5.17.13.15.2. A ferramenta deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;

5.17.13.15.3. Deve ser capaz de realizar varreduras em dispositivos móveis suportando no mínimo: Apple Profile Manager, ActiveSync, Airwatch e MobileIron;

5.17.13.15.4. Os resultados da varredura em dispositivos móveis devem conter no mínimo os seguintes filtros:

5.17.13.15.4.1. Modelo;

5.17.13.15.4.2. Número Serial do dispositivo;

5.17.13.15.4.3. Severidade da vulnerabilidade;

5.17.13.15.5. A ferramenta deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;

5.17.13.15.6. A ferramenta deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;

5.17.13.15.7. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou;

5.17.13.15.8. A ferramenta deve ser configurável para permitir a otimização das configurações de varredura;

5.17.13.15.9. A ferramenta deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

5.17.13.15.10. A ferramenta deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

5.17.13.15.11. A ferramenta deve ser capaz de realizar pesquisas de dados confidenciais;

5.17.13.15.12. A ferramenta deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

5.17.13.16. REQUISITOS DE CONFORMIDADE

5.17.13.16.1. A ferramenta deve ser totalmente licenciada para realizar scans de auditoria e compliance;

5.17.13.16.2. A ferramenta deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

5.17.13.16.3. A ferramenta deve ser licenciada para realizar scans de conformidade e compliance de forma ilimitada;

5.17.13.16.4. Toda a ferramenta deve ser licenciada de modo a realizar scans de conformidade para os seguintes padrões: CIS, SCAP e OVAL;

5.17.13.16.5. Deve suportar a verificação de compliance para no mínimo:

5.17.13.16.5.1. Bluecoat ProxySG;

5.17.13.16.5.2. Adtran AOS;

5.17.13.16.5.3. Brocade Fabric OS;

5.17.13.16.5.4. Checkpoint;

5.17.13.16.5.5. Cisco IOS;

5.17.13.16.5.6. Citrix Xenserver;

5.17.13.16.5.7. Fireeye;

5.17.13.16.5.8. Fortinet FortiOS;

5.17.13.16.5.9. Extreme ExtremeXOS;

5.17.13.16.5.10. HP Procurve;

5.17.13.16.5.11. Huawei VRP;

5.17.13.16.5.12. IBM iSeries;

5.17.13.16.5.13. MongoDb;

5.17.13.16.5.14. Netapp Data ONTAP;

5.17.13.16.5.15. Openstack;

5.17.13.16.5.16. Palo Alto Firewall;

5.17.13.16.5.17. Red Hat Enterprise Virtualization;

5.17.13.16.5.18. Salesforce;

5.17.13.16.5.19. SonicWall;

5.17.13.16.5.20. Unix Configuration;

5.17.13.16.5.21. Windows Configuration;

5.17.13.16.6. A ferramenta deve mostrar se o critério de compliance foi atendido ou não;

5.17.13.16.7. A ferramenta deve suportar os seguintes padrões de compliance:

5.17.13.16.7.1. COBIT;

5.17.13.16.7.2. CIS (Center for Internet Security Benchmarks);

5.17.13.16.7.3. DISA;

5.17.13.16.7.4. ISO 27001;

5.17.13.16.7.5. NIST;

5.17.13.16.8. Deverá possuir documentação, de maneira pública ou ser criada e entregue junto com a instalação da ferramenta, referenciando como implementar os controles CIS, apresentando o controle CIS e como configurar e monitorar o atendimento a este controle usando a plataforma de Gestão de Conformidade;

5.17.13.16.9. A ferramenta deve permitir medir, analisar e visualizar a postura de segurança da organização através da definição de políticas de segurança estabelecidas pelo administrador da ferramenta;

5.17.13.16.10. A ferramenta deve mostrar quais resultados estão em conformidade e quais não estão;

5.17.13.17. Análise de Risco do Ambiente

5.17.13.17.1. A ferramenta deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

5.17.13.17.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

5.17.13.17.3. Deve ser capaz de calcular a criticidade dos ativos da organização;

5.17.13.17.4. A ferramenta deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

5.17.13.17.5. A ferramenta deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro

5.17.13.17.6. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

5.17.13.17.7. A ferramenta deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo).

5.17.13.17.8. A ferramenta deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos.

5.17.13.17.9. A ferramenta deve permitir um acompanhamento histórico do nível de exposição da organização;

5.17.13.17.10. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela ferramenta.

5.17.13.17.11. A ferramenta deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades criticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade.

5.17.13.17.12. A ferramenta deve possuir um gráfico indicativo do percentual de ativos com soluções de proteção de endpoint instaladas, bem como o nome e a versão da ferramenta.

5.17.13.17.13. A ferramenta deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área.

5.17.13.17.14. A ferramenta deve permitir a segregação lógica entre aplicações distintas da empresa afim de obter a pontuação referente exposição cibernética por aplicação.

5.17.14. **Teste de Invasão**

5.17.14.1. Os termos “Pentest”, "teste de penetração", "teste de intrusão" e "teste de invasão", são considerados sinônimos.

5.17.14.2. Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, nem ativo porventura relacionado, sem explícita e prévia autorização e monitoração pela equipe técnica responsável da CONTRATANTE.

5.17.14.3. Caso a CONTRATANTE entenda haver algum risco na execução do Pentest que possa comprometer, em qualquer grau, o funcionamento de sistema, ativo ou processo da CONTRATANTE, poderá solicitar a mudança de metodologia e/ou do cronograma, inclusive podendo requerer a execução dos testes em finais de semana, feriados ou fora do horário comercial.

5.17.14.4. A CONTRATADA deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante qualquer das fases de realização do Pentest, conforme disposições contidas no Anexo VII “Modelo de Termo de Confidencialidade de Informações”.

5.17.14.5. O pentest externo é o tipo de pentest realizado em qualquer dos serviços e sistemas de TI publicados na internet em qualquer porta lógica e que pertençam ao domínio e faixas de IP da CONTRATANTE.

5.17.14.6. O pentest interno é o tipo de pentest realizado em serviços e sistemas publicados na intranet (rede interna) da CONTRATANTE, podendo ser concedido acesso remoto à CONTRATADA por meio de VPN, à critério do CONTRATANTE.

5.17.14.7. Os sistemas, serviços e ativos de TI da CONTRATANTE a serem submetidos aos testes, serão definidos em Ordens de Serviços (O.S.).

5.17.14.8. As modalidades de pentest serão classificadas da seguinte maneira:

5.17.14.8.1. Black-box: Quando o executor do teste não possui informações acerca do ambiente tecnológico e arquitetura do alvo;

5.17.14.8.2. Gray-box: Quando o executor do teste tem conhecimento limitado ou algumas informações acerca do ambiente tecnológico e arquitetura do alvo;

5.17.14.8.3. White-box: Quando o executor tem pleno conhecimento e vasta informação acerca do ambiente tecnológico e arquitetura do alvo;

5.17.14.9. Durante os testes, não poderão ser executados quaisquer variações dos seguintes ataques sem explícita autorização prévia e monitoração pela equipe técnica responsável da CONTRATANTE:

5.17.14.9.1. Ataques de negação de serviços e flooding;

5.17.14.9.2. Engenharia social, por exemplo, phishing, vishing, pharming, personificação, roubo de identidade e outros;

5.17.14.9.3. Ataques que possam causar danos físicos, por exemplo, arrombamentos, danos às fechaduras eletrônicas, ativação de sistemas de alarme.

5.17.14.9.4. Ataques que envolvam vetores de infecção, tais como, ransomware, vírus, worms, trojan, rootkits e outros.

5.17.14.9.5. Todos os testes deverão ser acompanhados e supervisionados por setor competente e a critério do CONTRATANTE.

5.17.14.10. A O.S. será elaborada por setor competente do CONTRATANTE, que ficará responsável pelo acompanhamento da execução do teste junto à CONTRATADA.

5.17.14.11. Nas O.S. deverão ser contemplados, no mínimo, os seguintes tópicos (escopo):

5.17.14.11.1. O sistema ou ativo de tecnologia a ser testado;

5.17.14.11.2. A modalidade de pentest a ser realizado (Black Box, Grey Box, White Box);

5.17.14.11.3. Tipo de realização do pentest (Pentest Interno ou Externo);

5.17.14.12. Os testes de invasão serão realizados periodicamente com a solicitação da CONTRATANTE. Para entendimento de atividade ofensiva, temos a análise do ambiente alvo e a exploração das falhas encontradas sendo o produto final um relatório detalhado da atividade.

5.17.14.13. A CONTRATADA deve elaborar junto com a DGTEC o plano de ação para correção e falhas. Supervisionando a execução e emissão de um relatório.

5.17.14.14. As vulnerabilidades encontradas que ainda não foram corrigidas de acordo com o relatório anterior, não podem ser objetos do próximo pentest.

5.17.14.15. Ferramentas:

5.17.14.15.1. As ferramentas utilizadas nos testes de intrusão são de responsabilidade da CONTRATADA,

5.17.14.15.2. Os testes de invasão deverão envolver, necessariamente, o uso de técnicas e ferramentas específicas mais atualizadas e comumente utilizadas no mercado de segurança da informação, para tentar obter acesso não autorizado e privilegiado aos ativos e informações, simulando um ataque real.

5.17.14.15.3. Para a análise de vulnerabilidades, executada durante a fase de descobertas, a CONTRATADA deverá utilizar ferramentas que atenda, no mínimo, as seguintes características:

5.17.14.15.3.1. Realize escaneamento utilizando base de dados atualizada com as mais recentes ameaças e vulnerabilidades;

5.17.14.15.3.2. Faça avaliação de riscos com apresentação de score utilizando metodologia CVSS (Common Vulnerability Scoring System) versão CVSS3.0 ou superior;

5.17.14.15.3.3. Apresente formas de resolução ou mitigação das vulnerabilidades, detalhando atualizações e configurações necessárias para eliminar ou, não sendo possível, para reduzir a exposição ao risco;

5.17.14.15.3.4. Deverá utilizar identificadores CVE (Common Vulnerabilities and Exposures) associados as vulnerabilidades identificadas, quando disponíveis. Caso o CVE ainda não esteja disponível, a vulnerabilidade deverá ser reportada ao ser identificada.

5.17.14.15.4. As ferramentas deverão ser apresentadas para ciência e aprovação, antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades.

5.17.14.15.5. Suportar o armazenamento seguro de credenciais, para uso em varreduras autenticadas, usando as credenciais para se autenticar em sistemas Windows, UNIX ou qualquer ativo de infraestrutura, tais como dispositivos de rede, etc.

5.17.14.15.6. O processo de varredura deve ter um impacto mínimo sobre a rede.

5.17.14.15.7. Ferramentas de análise vulnerabilidades e enumeração de sistemas web, deverão possuir minimamente as seguintes características:

5.17.14.15.7.1. Ser capaz de detectar, no mínimo, as vulnerabilidades elencadas no guia OWASP TOP 10 em sua versão mais atualizada;

5.17.14.15.7.2. Ser capaz de realizar escaneamento ativo e passivo;

5.17.14.15.7.3. Ser capaz de realizar crawling/spidering para descobertas de urls, hiperlinks, páginas, dentre outros.

5.17.14.15.8. A utilização de ferramentas não deve integralizar a atuação do analista quando da realização do Pentest, sendo apenas auxiliares no processo de identificação, análise e posterior exploração de vulnerabilidades.

5.17.14.16. FASES - Cada teste de intrusão, necessariamente, deverá seguir as seguintes fases, nesta ordem:

5.17.14.16.1. PLANEJAMENTO - A partir de Ordem de Serviço (OS) requisitada pela CONTRATANTE inicia-se a fase de Planejamento, quando serão apresentados e discutidos os itens constantes na OS.

5.17.14.16.1.1. Na fase de planejamento serão definidos:

5.17.14.16.1.2. Pacote de invasão/Pentest ou a quantidade de horas a serem consumidas.

5.17.14.16.1.3. Objetivo de "comprometer o ambiente" para ser alcançado como por exemplo. Caso o objetivo mude durante a tentativa, deve ser reportado em relatório posterior.

5.17.14.16.1.4. Processos e atividades permitidas ou proibidas.

5.17.14.16.1.5. O detalhamento do cronograma.

5.17.14.16.1.6. As informações e acessos necessários para a realização do Pentest (especialmente nos casos de Pentests Graybox e Whitebox).

5.17.14.16.1.7. A fase de Planejamento será formalizada através de declaração de aceite contendo todas as informações discutidas e definidas.

5.17.14.16.2. DESCOBERTA - Após formalmente autorizado pela CONTRATANTE, inicia-se a fase de Descoberta, que tem como objetivo a obtenção de informações relevantes dentro do escopo do teste que possibilitam reconhecer possíveis ameaças/vulnerabilidades. Importante frisar que esta fase não deve se restringir à utilização de ferramentas automatizadas, sendo esperada atuação manual da equipe técnica contratada, aprofundando a análise da superfície de ataque à procura de vulnerabilidades não facilmente identificáveis. Deverão ser realizadas, no mínimo, as seguintes atividades:

5.17.14.16.2.1. Coleta passiva, caracterizada pela obtenção de informações utilizando-se, no mínimo, as seguintes técnicas/serviços/ferramentas, quando aplicáveis:

5.17.14.16.2.1.1. Whois e nslookup (consultas DNS);

5.17.14.16.2.1.2. Sites de busca;

5.17.14.16.2.1.3. Listas de discussão;

5.17.14.16.2.1.4. Blogs de colaboradores;

5.17.14.16.2.1.5. Dumpster diving ou trashing;

5.17.14.16.2.1.6. Informações livres;

5.17.14.16.2.1.7. Packet sniffing "passive eavesdropping";

5.17.14.16.2.1.8. Captura de banner.

5.17.14.16.2.1.9. Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas, quando aplicáveis:

5.17.14.16.2.1.10. Port scanning (Mapeamento de rede);

5.17.14.16.2.1.11. Varredura de vulnerabilidade, que deverá verificar/identificar no mínimo:

5.17.14.16.2.1.12. Hosts ativos na rede;

5.17.14.16.2.1.13. Portas e serviços em execução;

5.17.14.16.2.1.14. Serviços ativos e vulneráveis nos hosts;

5.17.14.16.2.1.15. Fingerprinting de Sistemas operacionais dos hosts;

5.17.14.16.2.1.16. Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;

5.17.14.16.2.1.17. Configurações feitas nos hosts sem observância de boas práticas em segurança computacional;

5.17.14.16.2.1.18. Identificação de rotas e estimativa de impacto, caso estas sejam modificadas ou reconfiguradas;

5.17.14.16.2.1.19. Identificação de vetores de ataque e cenários para exploração;

5.17.14.16.2.1.20. Vulnerabilidades Detectadas (CVE), classificadas com alto, médio ou baixo risco.

5.17.14.16.2.1.21. Informações a serem aplicadas na fase de ataques;

5.17.14.16.2.1.22. Em relação a serviços e aplicações web, deve-se ter/verificar:

5.17.14.16.2.1.23. Uso indevido de sistema de arquivos e arquivos temporários;

5.17.14.16.2.1.24. Evasão de informação por configurações padrão de tratamento de erros;

5.17.14.16.2.1.25. Tratamento indevido de entrada;

5.17.14.16.2.1.26. Problemas relacionados à má configuração dos serviços;

5.17.14.16.2.1.27. Gerenciamento inseguro de sessões web.

5.17.14.16.3. EXPLORAÇÃO - Nesta fase, o objetivo é confirmar as vulnerabilidades e identificar os impactos e riscos das ameaças porventura encontradas a partir de simulações de ataques reais. As ações desta fase devem utilizar metodologias reconhecidas no mercado e elencadas neste estudo e não devem comprometer o correto funcionamento dos equipamentos e sistemas, nem afetar o desempenho das atividades ora realizadas neste PJERJ, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável da CONTRATANTE. Além disso, deve-se atender os seguintes itens:

5.17.14.16.3.1. A empresa CONTRATADA deverá ser capaz de aplicar, no mínimo, os seguintes tipos de ataques, quando aplicáveis:

5.17.14.16.3.1.1. Violações do protocolo HTTP;

5.17.14.16.3.1.2. SQL Injection;

5.17.14.16.3.1.3. LDAP Injection;

5.17.14.16.3.1.4. Cookie Tampering;

5.17.14.16.3.1.5. Cross-Site Scripting (XSS);

5.17.14.16.3.1.6. Directory Transversal;

5.17.14.16.3.1.7. Buffer Overflow;

5.17.14.16.3.1.8. OS Command Execution;

5.17.14.16.3.1.9. Command Injection;

5.17.14.16.3.1.10. Remote Code Inclusion;

5.17.14.16.3.1.11. Server Side Includes (SSI) Injection;

5.17.14.16.3.1.12. File disclosure;

5.17.14.16.3.1.13. Information Leak;

5.17.14.16.3.1.14. Problemas com o SNMP;

5.17.14.16.3.2. Para testes de invasão direcionados, especialmente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, no mínimo, os testes baseados na publicação OWASP TESTING GUIDE (The Open WebApplication Security Project) em sua versão mais recente.

5.17.14.16.3.3. Qualquer vulnerabilidade crítica e de fácil exploração encontrada deverá ser imediatamente comunicada à equipe técnica da CONTRATANTE, contendo detalhes técnicos e ações necessárias para a correção da vulnerabilidade e disponibilizado de forma segura em até 1 (um) dia útil. Caso ocorra antes do término do teste, deverá ser reportado no relatório se houve impacto na continuidade do teste.

5.17.14.16.4. RELATÓRIO PARCIAL - Após a fase de Exploração, deve ser elaborado pela CONTRATADA um relatório do teste de intrusão. Este relatório deve conter ao menos:

5.17.14.16.4.1. Escopo, tipo e modalidade do teste;

5.17.14.16.4.2. Metodologias, técnicas, fontes de pesquisa, referências, equipamentos e ferramentas utilizadas;

5.17.14.16.4.3. Atividades realizadas, em ordem cronológica.

5.17.14.16.4.4. Tempo do analista utilizado em cada atividade;

5.17.14.16.4.5. Informações acessadas e detalhes da infraestrutura descoberta (caso aplicável).

5.17.14.16.4.6. Confirmação ou refutação de existência das vulnerabilidades.

5.17.14.16.4.7. Descrição de todas as vulnerabilidades e ameaças porventura encontradas, informando, no mínimo:

5.17.14.16.4.7.1. Nome;

5.17.14.16.4.7.2. Nível de Risco;

5.17.14.16.4.7.3. Intrusiva (sim / não);

5.17.14.16.4.7.4. Descrição;

5.17.14.16.4.7.5. Observação;

5.17.14.16.4.7.6. Recomendação de Remediação;

5.17.14.16.4.7.7. Link do patch ou da correção;

5.17.14.16.4.7.8. Número CVE, se houver;

5.17.14.16.4.7.9. SANS / FBI referência Top 20; e

5.17.14.16.4.7.10. IAVA (Information Assurance Vulnerability Alert) Referência.

5.17.14.16.4.7.11. Detalhamento do caminho utilizado e evidências da exploração das vulnerabilidades porventura encontradas;

5.17.14.16.4.8. Tipos de ataques realizados;

5.17.14.16.4.9. Avaliação de riscos e impacto da vulnerabilidade e consequente exploração;

5.17.14.16.4.10. Contramedidas para correção ou mitigação dos riscos decorrentes das vulnerabilidades encontradas.

5.17.14.16.4.11. Anexos com os resultados dos testes automatizados e vídeos de realização dos ataques bem-sucedidos, quando assim solicitados.

5.17.14.16.4.12. Assinatura do profissional certificado, conforme subitem 8.9 deste Termo de Referência.

5.17.14.16.4.13. A CONTRATADA deverá elaborar e coordenar um plano de ação para a correção das vulnerabilidades encontradas.

5.17.14.16.4.14. Prover informações sobre a efetividade da simulação, apresentando ao menos:

5.17.14.16.4.14.1. Quantidade de usuários testados;

5.17.14.16.4.14.2. Quantidade de usuários que somente visualizaram;

5.17.14.16.4.14.3. Quantidade de usuários que clicaram em algum link/anexo;

5.17.14.16.4.14.4. Quantidade de usuários enganados;

5.17.14.16.4.14.5. Tempo decorrido desde a última simulação.

5.17.14.16.4.14.6. Deve estar disponível, pelo menos, em português e inglês.

5.17.14.16.4.14.7. Alerta de Vulnerabilidades

5.17.14.16.4.15. A CONTRATADA deverá abrir chamados no sistema de atendimento da CONTRATANTE de modo a solicitar às áreas pertinentes a correção das vulnerabilidades identificadas;

5.17.14.16.4.16. Tais chamados devem ser abertos por ação corretiva, agrupando todas as vulnerabilidades eliminadas pela execução daquela ação;

5.17.14.16.4.17. Avaliar o tratamento de vulnerabilidades Altas, além das críticas, levando em consideração a classificação (Crítica - Alta - Media - Baixa).

5.17.14.16.4.18. A CONTRATADA deverá acompanhar a resolução dos chamados abertos, validando as evidências e dando baixa nas vulnerabilidades tratadas no sistema de gestão de vulnerabilidades.

5.18. **Das atividades técnicas de gestão de ameaças**

5.18.1. A CONTRATADA deverá apresentar uma caracterização dos adversários que executam ações maliciosas. Esta caracterização é baseada em sua motivação as informações referentes a justiça.

5.18.2. Atividades

5.18.3. Apresentar estudo de crimes comportamentais em:

5.18.3.1. Crimes cibernéticos e ciberdependentes;

5.18.3.2. Ofensores interpessoais;

5.18.3.3. Criminosos organizados cibernéticos;

5.18.3.4. Organizações criminosas ciberdependentes que utilizam técnicas de:

5.18.3.5. E-mail spam;

5.18.3.6. Phishing;

5.18.3.7. Malware Financeiro;

5.18.3.8. Clique fraude;

5.18.3.9. Ransomware

5.18.3.10. Negação de serviço.

5.18.3.11. Ataques hackers

5.18.3.12. Hacktivismo:

5.18.3.13. Negação de serviço;

5.18.3.14. Vazamentos de dados;

5.18.3.15. desfiguração da web.

5.18.3.16. State actors:

5.18.3.17. Sabotagem;

5.18.3.18. Espionagem;

5.18.3.19. Desinformação.

5.18.4. Garantir que as necessidades dos criminosos não sejam atendidas no cenário do PJERJ, fornecendo ao corpo técnico do CONTRATANTE uma visão geral dos elementos necessários usados em operações de crime cibernético que se aplicam aos comportamentos adversários como:

5.18.4.1. Programas de afiliados

5.18.4.2. Vetores de infecção:

5.18.4.3. Anexos maliciosos;

5.18.4.4. Otimização de mecanismo de pesquisa de black hat;

5.18.4.5. Ataques de download drive-by;

5.18.4.6. Comprometimento de dispositivos conectados à Internet.

5.18.5. Infraestrutura:

5.18.5.1. Provedores de serviços de hospedagem Bulletproof;

5.18.5.2. Infraestrutura de comando e controle.

5.18.6. Serviços especializados:

5.18.6.1. Kits de exploração;

5.18.6.2. Serviços de pagamento por instalação.

5.18.7. Serviços Humanos:

5.18.7.1. Serviços de resolução de CAPTCHA;

5.18.7.2. Contas falsas;

5.18.7.3. Geração de conteúdo;

5.18.7.4. Mules Money

5.19. **Operações de segurança e Gerenciamento de incidentes**

5.19.1. Monitoração de Incidentes

5.19.2. No processo de monitoração de incidentes a CONTRATADA deve:

5.19.2.1. Monitorar aplicações web, servidores, virtualizadores e rede de forma proativa e reativa (com anuência do CONTRATANTE) no ambiente internet e intranet da instituição.

5.19.2.2. Customizar os alarmes, de maneira que ocorrências de incidentes e problemas sejam devidamente notificadas tempestivamente ao monitoramento da empresa;

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

5.19.2.4. Realizar a gestão dos incidentes (criação de alertas, detecção e abertura de chamados);

5.19.2.5. Acompanhar do início ao fim os incidentes;

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

5.19.2.7. Correlacionar o processo de eventos (gerenciar eventos durante todo o seu ciclo de vida) e o processo de incidentes de forma automatizada entre a ferramenta de ITSM e ferramenta de monitoramento;

5.19.2.8. Acompanhar os processos através de indicadores de desempenho;

5.19.2.9. Para a execução deste serviço deverá ser fornecido uma ferramenta de segurança para Defesa Cibernética baseada em análise de comportamento completamente licenciada, conforme as especificações gerais dos serviços deste Termo de Referência.

5.20. **Ferramenta**

5.20.1. A ferramenta de Defesa Cibernética tem que ser que capaz de identificar qualquer comportamento anômalo na rede em tempo real através de tecnologias de Inteligência Artificial e Machine Learning.

5.20.2. Características gerais da ferramenta:

5.20.2.1. A ferramenta deve permitir Threat Hunting, análise comportamental da rede e seus componentes, detecção de anomalia(s) o e visibilidade de rede.

5.20.2.2. Não serão aceitos produtos ou serviços OpenSource.

5.20.2.3. Todos os componentes devem ser oficialmente suportados pelo(s) fabricante(s) da ferramenta em acordo com as condições especificadas.

5.20.2.4. A ferramenta deve ser dotada de tecnologia baseada em Inteligência Artificial afim de identificar anomalias de comportamento e ataques sutis não identificados pelas tecnologias tradicionais de segurança da informação.

5.20.2.5. Deve utilizar no mínimo os seguintes métodos de inteligência artificial para criação de perfis de uso e identificação de desvios comportamentais na rede:

5.20.2.5.1. Machine learning não supervisionado

5.20.2.5.2. Machine learning supervisionado

5.20.2.5.3. Deep Learning

5.20.2.5.4. Redes Neurais

5.20.2.6. A ferramenta não deve depender de pré-configurações baseadas na rede do órgão para que identifique associações entre múltiplos elementos da rede para que consiga identificar anomalias de comportamento.

5.20.2.7. A ferramenta deve ser capaz de aprender o comportamento da rede e de seus componentes (dispositivos e usuários) de forma autônoma e contínua se adaptando a variações de comportamento destes durante o tempo.

5.20.2.8. A ferramenta deve realizar todas as inspeções, processamento, análise e detecção de anormalidades e gerenciamento localmente, ou seja, é vedada qualquer forma de envio de dados para fora da rede do órgão para o funcionamento da ferramenta.

5.20.2.9. A ferramenta deve possuir mecanismos de DPI (Deep Packet Inspection).

5.20.2.10. A ferramenta deve realizar o aprendizado do ambiente de rede e inspeção do tráfego de forma off-line através de tráfego espelhado de porta nos switches, ou seja, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede.

5.20.2.11. A ferramenta deve inspecionar e analisar os dados brutos da rede através de espelhamento de porta (SPAN/Port Mirror) ou através do uso de TAP – Terminal Access Point.

5.20.2.12. A ferramenta deve suportar a ingestão de dados através de mecanismos de tunelamento de tráfego na camada 2 (enlace) do modelo OSI como VXLAN e ERSPAN.

5.20.2.13. A ferramenta deve ser capaz de tomar ações autônomas de resposta contra ameaças e/ou ataques cibernéticos baseadas em sua inteligência artificial.

5.20.2.14. A ferramenta deve ser capaz de integrar-se a soluções de segurança terceiras a fim de permitir ações adicionais de bloqueio contra ataques cibernéticos.

5.20.2.15. A ferramenta deve permitir a inspeção de plataformas como:

5.20.2.15.1. Amazon AWS

5.20.2.15.2. Microsoft Azure

5.20.2.15.3. Google G-Suite

5.20.2.15.4. Office 365

5.20.2.15.5. SalesForce

5.20.2.15.6. Dropbox enterprise

5.20.2.15.7. Componentes virtuais (máquinas virtuais)

5.20.2.15.8. Endpoint para Sistemas Operacionais.

5.20.2.15.9. Docker, Kubernetes e AWS Fargate.

5.20.2.15.10. Box

5.20.2.15.11. Slack

5.20.2.15.12. Zoom

5.20.2.16. Deve ser dotada de única interface gráfica a qual permite o gerenciamento centralizado de todos os componentes da ferramenta.

5.20.3. Características técnicas da ferramenta

5.20.3.1. A ferramenta deve identificar de forma autônoma, sem intervenção humana, todas as redes ativas no ambiente (que tiveram tráfego inspecionado) e apresentar uma relação com todas as redes, máscara de rede, primeira vez em que a rede foi observada e quantidade de dispositivos observados na rede correspondente.

5.20.3.2. A ferramenta deve identificar de forma autônoma, sem intervenção humana, todos os endereços IPs que trafegaram nas redes inspecionadas apresentando uma relação com no mínimo os seguintes dados:

5.20.3.2.1. Classificação do tipo de dispositivo (desktop, servidor, Impressora, câmera, iot, etc.)

5.20.3.2.2. IP do dispositivo

5.20.3.2.3. Mac Address

5.20.3.2.4. Nome DNS do dispositivo

5.20.3.2.5. Primeira vez que o dispositivo/IP foi visto na rede

5.20.3.2.6. Última vez que o dispositivo foi visto na rede.

5.20.3.2.7. Deve ser possível visualizar o histórico de IPs de um determinado dispositivo baseado no IP provido pelo servidor DHCP.

5.20.3.3. A ferramenta deve criar métricas, de forma autônoma, de raridade de Ips, Domínios DNS, Dispositivos, etc. baseado na frequência que estes são acessados através da rede.

5.20.3.4. A ferramenta deve criar métricas, de forma autônoma, de anormalidades comparando a ação atual de um dispositivo, usuário, IP, domínio, etc. contra as ações de mesmo escopo realizadas no passado.

5.20.3.5. A métrica de anormalidade deve apresentar o percentual de desvio do comportamento atual de um dispositivo comparado com o comportamento passado aprendido.

5.20.3.6. A ferramenta deve ser comprovadamente baseada em análise de comportamento permitindo a detecção de, no mínimo, as seguintes anomalias:

5.20.3.7. Dispositivo realizando conexões para destinos raros na internet não frequentemente visitados com por dispositivos da rede interna.

5.20.3.8. Dispositivo se comunicando com um servidor externo usando um certificado auto assinado.

5.20.3.9. Dispositivo se comunicando com um servidor usando um certificado expirado.

5.20.3.10. Dispositivo se comunicando com um dispositivo externo usando um certificado inválido.

5.20.3.11. Dispositivo iniciando várias conexões para um IP externo raro de maneira regular. (Beaconing)

5.20.3.12. Dispositivo gerando muitas solicitações para servidores Web internos o qual está retornando códigos de erro HTTP.

5.20.3.13. Novo dispositivo entrou na rede e começou a utilizar o software de teste de penetração ou escaneamento de rede.

5.20.3.14. Vários dispositivos internos começaram a desviar de suas atividades normais e escanearam a rede interna.

5.20.3.15. Dispositivo fazendo requisições de DNS repetidas recebendo respostas com registro TXT. (Tunelamento via DNS)

5.20.3.16. Dispositivo se comunicando externamente via DNS de maneira consistente com o tunelamento de DNS.

5.20.3.17. Dispositivo fazendo conexões criptografadas para um domínio relacionado a DNS Dinâmico

5.20.3.18. Dispositivo gerando um volume anormalmente alto de solicitações DNS.

5.20.3.19. Dispositivo fazendo uma série de conexões utilizando Hostnames raros que parecem não ter uma resolução de DNS legítima.

5.20.3.20. Um servidor DNS interno está agindo como um resolvedor de DNS aberto (OpenDns).

5.20.3.21. Dispositivo se comunicando com o serviço de anonimização da rede TOR.

5.20.3.22. Dispositivo se comunicando com a rede Tor por meio de um Web Service intermediário.

5.20.3.23. Atividade anormal de PowerShell e o Windown Romote Mamagement, seguido por uma conexão a um destino externo raro seguido de download de arquivo suspeito.

5.20.3.24. Dispositivo executando comandos PsExec em uma máquina remota que nunca havia recebido tráfego similar anteriormente.

5.20.3.25. Dispositivo se conectando repetidamente a destinos externos que não possuem nomes legíveis para humanos.

5.20.3.26. Dispositivo detectado conectando-se a hostnames identificados como trojans financeiros.

5.20.3.27. Dispositivo fazendo conexões com hostnames raros associados a uma botnet.

5.20.3.28. Dispositivo solicitando um domínio conhecido por hospedar malwares.

5.20.3.29. Dispositivo gravando arquivos com nomes suspeitos, relacionado a ransomware, em Servidores de arquivos da rede SMB.

5.20.3.30. Dispositivo transferindo um volume de moderado a grande de dados para fora da rede durante um período de 24 horas ou mais por meio de um grande volume de conexões.

5.20.3.31. Dispositivo fazendo download dados de um sistema interno e fazendo upload de volumes de dados semelhantes para destino externo.

5.20.3.32. Dispositivo se comunicando com domínios suspeitos na internet e, ao mesmo tempo, realizando comportamentos incomuns de SMB na rede interna.

5.20.3.33. Dispositivo acessando uma grande quantidade de compartilhamentos SMB que não foram acessados anteriormente pelo mesmo dispositivo.

5.20.3.34. Dispositivo não conseguiu estabelecer uma sessão SMB2 seguida de uma configuração bem-sucedida da sessão SMB1 usando credenciais administrativas.

5.20.3.35. Dispositivo lendo e gravando volumes de dados semelhantes para compartilhamentos de arquivos remotos.

5.20.3.36. Dispositivo acessando arquivos que possuem de senhas não criptografadas.

5.20.3.37. Dispositivo enviando um grande volume de dados para um IP externo que raramente é utilizado por qualquer dispositivo na rede interna.

5.20.3.38. Dispositivo fazendo conexões web externas sem usar um proxy web.

5.20.3.39. Dispositivo sendo bloqueado repetidamente por um proxy web durante um período de várias horas.

5.20.3.40. Dispositivo solicitando informações de configuração de proxy (WPAD) para um IP externo.

5.20.3.41. Dispositivo fazendo conexões HTTP suspeitas, de forma repetitiva, diretamente para um endereço IP sem utilizar um Hostname.

5.20.3.42. Dispositivo foi redirecionado para um Hostname HTTP raro e em seguida baixou um executável ou outro arquivo binário.

5.20.3.43. Dispositivo causando repetidos picos de conexões HTTP ou SSL na rede interna ou para a internet.

5.20.3.44. Dispositivo fazendo requisições HTTP suspeitas repetidamente em portas não padrão.

5.20.3.45. Dispositivo informando no cabeçalho User-Agent que possui um sistema operacional o qual é diferente do SO que realmente está utilizando.

5.20.3.46. Dispositivo fazendo download de um arquivo que não corresponde ao seu 'File Type' de uma fonte externa que a rede normalmente não acessa.

5.20.3.47. Dispositivo fazendo download de arquivo executável vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

5.20.3.48. Dispositivo fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

5.20.3.49. Dispositivo fazendo download de um arquivo suspeito e em seguida fez uma conexão para um destino externo com o qual a rede normalmente não se comunica.

5.20.3.50. Dispositivo usando uma plataforma externa de armazenamento de arquivos de terceiros.

5.20.3.51. Dispositivo enviando dados para o Pastebin, Zerobin.net, ghostbin.com, rentry.co, controlc.com, hastebin.com

5.20.3.52. Dispositivo usando um sistema terceiro de mensageria (Whatsapp ou similares).

5.20.3.53. Dispositivo acessando rede social (Facebook ou similares).

5.20.3.54. Dispositivo se comunicando com um destino raro na internet usando portas normalmente usadas apenas na rede interna.

5.20.3.55. Dispositivo fazendo conexões peer-to-peer BitTorrent.

5.20.3.56. Dispositivo recebeu um número anormalmente grande de conexões de entrada de IP externos raros.

5.20.3.57. Dispositivo fazendo conexões SQL para IPs externos a rede.

5.20.3.58. Dispositivo enviando uma quantidade anormal alta de dados para destinos fora da rede.

5.20.3.59. Dispositivo trocando um volume de dados anormal com outro dispositivo na rede interna.

5.20.3.60. Dispositivo enviando uma quantidade anormalmente alta de dados externamente para um local para o qual a rede não enviou dados anteriormente.

5.20.3.61. Dispositivo explorado vulnerabilidade Heartbleed na rede interna.

5.20.3.62. Dispositivo se conectando a um DNS SinkHole conhecido.

5.20.3.63. Dispositivo realizando grandes volumes de pequenas conexões SSH e/ou RDP.

5.20.3.64. Dispositivo iniciando um grande número de conexões para um servidor RDP e/ou SSH.

5.20.3.65. Dispositivo recebendo um grande número de conexões RDP de entrada de IPs externos raros.

5.20.3.66. Alteração de bloco CIDR de uma subrede.

5.20.3.67. Alteração no comportamento de tráfego DHCP.

5.20.3.68. Novo servidor DNS na rede.

5.20.3.69. Novo servidor de proxy web na rede.

5.20.3.70. Adição ou remoção de domínios DNS na rede.

5.20.3.71. Perda de pacotes é superior a X% na rede.

5.20.3.72. Uma senha de credencial de alto privilégio foi alterada no domínio Windows.

5.20.3.73. Uma credencial efetuando login de uma origem incomum.

5.20.3.74. Uma credencial foi usada em múltiplos dispositivos internos.

5.20.3.75. Um dispositivo gerou um grande número de falhas de sessão SMB.

5.20.3.76. Um dispositivo desviou de suas atividades normais criando várias falhas de login Kerberos.

5.20.3.77. Deve ser possível criar regras utilizando um ou mais dos componentes do item acima.

5.20.3.78. Todos os dados processados pela ferramenta devem ser armazenados para posterior análise independentemente de terem gerado alertas ou não.

5.20.3.79. A ferramenta deve possuir mecanismos para exportar os dados armazenados no padrão de extensão '.pcap'.

5.20.3.80. Deve ser capaz de agrupar de forma autônoma dispositivos em grupos baseado em sua similaridade de comportamento.

5.20.3.81. Deve ser capaz de tomar ações baseadas em desvio de comportamento.

5.20.3.82. Deve possuir a capacidade de quarentenar ou semi-quarentenar temporariamente dispositivos na rede.

5.20.3.83. Deve possuir a habilidade para responder, desacelerar e/ou parar ameaças autonomamente.

5.20.3.84. Deve ser capaz de marcar dispositivos automaticamente para decisões de resposta e ajuste fino.

5.20.3.85. Deve ser altamente configurável permitindo vários níveis de resposta a uma anomalia na rede.

5.20.3.86. Deve ser capaz de registrar todas as ações de resposta para propósitos de auditoria.

5.20.3.87. Deve ser configurável para supervisão e aprovação de analistas em ações de tomada de decisão / resposta.

5.20.4. Características de gerenciamento da ferramenta

5.20.4.1. O gerenciador deve possuir controle de interface gráfica (GUI: Graphical User Interface) e interface texto (CLI);

5.20.4.2. A interface de texto (CLI) deve possuir comandos para permitir a realização de troubleshooting.

5.20.4.3. A interface gráfica não deve ser desenvolvida ou conter componentes baseados em Java por questões de compatibilidade com browsers modernos.

5.20.4.4. A interface gráfica deve possuir no mínimo:

5.20.4.4.1. Sumário dos dados aprendidos como: Dados totais processados por dia, Quantidade de Redes, Dispositivos e usuários identificados na rede.

5.20.4.4.2. Lista de alertas de anormalidade identificadas.

5.20.4.4.3. Critérios de filtro dos alertas de anormalidade por categoria de alerta, dispositivo ou usuários.

5.20.4.4.4. Critérios de filtro de período (data e horário) para os alertas de anormalidade.

5.20.4.4.5. Critérios de filtro de prioridade (risco) para os alertas de anormalidade.

5.20.4.4.6. Apresentar a posição geográfica das redes no ambiente de TI.

5.20.4.4.7. Opções de configuração do sistema

5.20.4.4.8. Área de gerenciamento de usuários

5.20.4.4.9. Área para gerenciamento de arquivos ".pcap", exportação e visualização na própria interface.

5.20.4.4.10. Área de busca de dados na base de dados da ferramenta.

5.20.4.5. Os alertas de anomalia devem conter no mínimo os seguintes dados:

5.20.4.5.1. Identificador único (Unique ID).

5.20.4.5.2. Data e horário.

5.20.4.5.3. Dispositivo que originou a ação.

5.20.4.5.4. Apresentar o IP de origem do Dispositivo.

5.20.4.5.5. Apresentar o MAC address do Dispositivo.

5.20.4.5.6. Apresentar o Hostname (DNS) do Dispositivo.

5.20.4.5.7. Apresentar o (s) usuário(s) que se eventualmente se logaram no Dispositivo nas últimas horas.

5.20.4.5.8. Apresentar o a rede a qual o dispositivo estava conectado.

5.20.4.6. Descrição técnica do evento.

5.20.4.6.1. Gráfico apresentando a quantidade de eventos similares e evolução do nível de risco.

5.20.4.6.2. Atalho para acesso rápido às configurações da política que gerou o alerta.

5.20.4.6.3. Dados técnicos resumidos das ações que causaram a anomalia e subsequente alerta.

5.20.4.6.4. Atalho para acessar dados detalhados das ações que causaram a anomalia e subsequente alerta.

5.20.4.6.5. Durante a investigação de uma anomalia/alerta o administrador pode acessar os dados abaixo utilizando apenas o mouse.

5.20.4.6.6. Dados detalhados do dispositivo que originou a anomalia.

5.20.4.6.7. IP do dispositivo

5.20.4.6.8. Mac Address

5.20.4.6.9. Nome DNS do dispositivo

5.20.4.6.10. Primeira vez que o dispositivo/IP foi visto na rede

5.20.4.6.11. Última vez que o dispositivo foi visto na rede

5.20.4.6.12. Apresentar o (s) usuário(s) que se eventualmente se logou(aram) no Dispositivo.

5.20.4.6.13. Apresentar o a rede a qual o dispositivo estava conectado.

5.20.4.6.14. Acesso a todas as comunicações realizadas pelo dispositivo na rede.

5.20.4.6.15. Acesso a todas as anomalias as quais o dispositivo gerou na rede.

5.20.4.6.16. Acesso a ferramenta para geração de gráficos que facilitem a investigação utilizando critérios como, mas não limitados a:

5.20.4.6.16.1. Dados relacionados a conexões.

5.20.4.6.16.2. Tráfego de dados.

5.20.4.6.16.3. Requisições DNS.

5.20.4.6.16.4. Erros de Login.

5.20.4.6.16.5. Ações utilizando SMB.

5.20.4.6.17. Apresentar gráfico representando os fluxos de comunicação entre os dispositivos que originaram e receberam tráfego anômalo.

5.20.4.6.18. A ferramenta deve possuir mecanismo para automação de investigação de alertas permitindo a correlação entre múltiplos evento apesentando em uma única tela as seguintes informações:

5.20.4.6.19. Linha do tempo apontando a correlação entre alertas emitidos para um determinado dispositivo, data e horário em que cada alerta foi emitido bem como o período em que cada ação anômala, que gerou o alerta, ocorreu.

5.20.4.6.20. Apresentação individual de cada alerta contendo: Descrição do comportamento anômalo e riscos associados.

5.20.4.6.21. Dados técnicos relacionados ao alerta como:

5.20.4.6.21.1. Período em que a anomalia foi observada.

5.20.4.6.21.2. IP de origem

5.20.4.6.21.3. IP(s) de destino

5.20.4.6.21.4. Credencial de usuário observada no dispositivo

5.20.4.6.21.5. Ação anômala identificada pela ferramenta.

5.20.4.6.21.6. Acesso aos logs do tráfego anômalo.

5.20.4.6.22. Deverá classificar cada alerta baseado em fases de ataque.

5.20.4.6.23. Deve permitir ao administrador exportar todas as informações acima em documento padrão .pdf.

5.20.4.6.24. A interface deve permitir a procura e navegação de qualquer dispositivo, usuário, Ips, etc. que tenham sido inspecionados em qualquer data armazenada pela ferramenta.

5.20.4.6.25. Ao navegar pelas comunicações do dispositivo o administrador pode utilizar filtros baseados em IP, Porta e Protocolo para facilitar a visualização.

5.20.4.6.26. Ao navegar pelas comunicações do dispositivo o administrador pode utilizar um IP de destino como filtro permitindo a investigação de 'Origem > Destino' ou 'Destino > Origem'.

5.20.4.6.27. Ao navegar pelas comunicações de um usuário o administrador pode analisar todo o histórico de login do mesmo contendo a data, o ip de origem do dispositivo que utilizou a credencial do usuário e estado da autenticação.

5.20.4.6.28. O administrador pode gerar arquivos ".pcap" para quaisquer comunicação inspecionada pela ferramenta.

5.20.4.6.29. A ferramenta deve se integrar com serviço LDAP a fim de possibilitar a autenticação e autorização de usuários na interface de administração e para consultas com objetivos de enriquecer os dados inspecionados.

5.20.4.6.30. A ferramenta deve permitir a utilização de segundo fator de autenticação para logins na interface web.

5.20.4.6.31. A ferramenta deve possuir mecanismo de gerenciamento de usurários da interface web permitindo:

5.20.4.6.31.1. Criação, modificação ou remoção de usuários

5.20.4.6.31.2. Gerenciamento de permissionamentos dos usuários.

5.20.4.6.31.3. Opção de gerar usuário com permissão de leitura apenas.

5.20.4.6.32. Deve possuir interface para visualização dos aspectos do sistema como:

5.20.4.6.32.1. A versão de software, espaço utilizado em disco, consumo de CPU e consumo de memória

5.20.4.6.32.2. Informação de todas as interfaces ativas e respectivo tráfego recebido através de cada uma delas.

5.20.4.6.32.3. Total de banda processada no momento, a média de banda processada e o pico de banda registrado nas últimas semanas.

5.20.4.6.32.4. Uma análise detalhada de todo o tráfego recebido no dispositivo bem como a última vez em que os principais protocolos foram vistos dentre eles, HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, dentre outros.

5.20.4.6.32.5. Listagem de todas as sub redes identificadas no ambiente bem como a quantidade de dispositivos em cada sub rede.

5.20.4.6.32.6. Deve permitir o envio de e-mails de alertas emitidos pela ferramenta.

5.20.4.6.33. Deve permitir o envio de logs para sistemas externos utilizando os seguintes padrões:

5.20.4.6.33.1. CEF

5.20.4.6.33.2. LEEF

5.20.4.6.33.3. JSON

5.20.4.6.33.4. Syslog

5.20.4.6.34. Deve permitir a integração nativa com plataforma de gerenciamento de chamados como HPSM, Atlassian, JIRA e ServiceNow.

5.20.4.6.35. Deve permitir a integração com plataformas de Threat Inteligence utilizando os protocolos STIX/TAXII.

5.20.4.6.36. A ferramenta deve possuir OPEN API para suportar integração com sistemas terceiros.

5.20.4.6.37. Deve possuir Inteligência artificial para automatizar triagens, análises e investigações de ameaças.

5.20.4.6.38. Deve possuir um aplicativo mobile capaz de visualizar, responder a incidentes, notificar, reportar e aprovar remediações para Android e iOS.

5.20.4.6.39. Deve possuir painel incorporado para executar consultas em metadados no tráfego inspecionado.

5.20.5. Características de gerenciamento de relatórios:

5.20.5.1. Deve permitir a criação automática de relatórios executivos cobrindo no mínimo:

5.20.5.2. Indicação da quantidade total de dispositivos, quantidade total de sub redes e banda média processada.

5.20.5.3. Sumário das violações por fase do ataque.

5.20.5.4. Sumário dos dispositivos com maior nível de brechas não usuais.

5.20.5.5. Sumario dos top dispositivos que mais violaram comportamentos anômalos.

5.20.5.6. Violações mais frequentes a principais itens de compliance como: uso de USB no dispositivo, google drive, tráfego RDP saindo da rede, acesso a servidor SQL através da internet, dentre outros.

5.20.5.7. Sumário dos dispositivos que mais violaram os itens de compliance gerando risco a organização.

5.20.5.8. Deve permitir que o relatório seja exportado para documento padrão .PDF e/ou .csv

5.20.5.9. Deve possuir mecanismo para busca de dados diretamente na base de dados da ferramenta.

5.20.5.10. O administrador pode gerar pesquisas e relatório dos seguintes critérios, mas não limitados a:

5.20.5.10.1. Data e Horário

5.20.5.10.2. Endereços IPs de origem e destino

5.20.5.10.3. Versão do protocolo IP

5.20.5.10.4. Protocolo de comunicação

5.20.5.10.5. Estado da conexão

5.20.5.10.6. Dados trafegados de entrada e saída.

5.20.5.10.7. Método HTTP

5.20.5.10.8. Cabeçalhos HTTP

5.20.5.10.9. Versão do SSL

5.20.5.10.10. Cifragem da Conexão SSL

5.20.5.10.11. Logins Kerberos

5.20.5.10.12. Comunicações DNS

5.20.5.10.13. Comunicações FTP

5.20.5.10.14. Comunicações LDAP

5.20.5.10.15. Comunicações Kerberos

5.20.5.10.16. Comunicações SMB

5.20.5.10.17. Comunicações Radius

5.20.5.10.18. Comunicações RDP

5.20.5.10.19. Comunicações SIP

5.21. **Respostas aos incidentes**

5.21.1. A CONTRATADA deve assessorar a equipe de respostas a incidentes e o Comitê Gestor de Segurança da Informação do PJERJ.

5.21.2. A CONTRATADA deve elaborar e implantar o protocolo de prevenção de incidentes cibernéticos e o protocolo de gerenciamento de crises cibernéticas. Tais protocolos devem conter todos os requisitos contidos na Portaria CNJ n.º 162/2021.

5.21.3. O controle de incidentes deve conter minimamente:

5.21.3.1. Tipos de incidentes;

5.21.3.2. Ações a serem realizadas;

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

5.21.3.4. O chamado playbook prevendo alguns cenários de possíveis incidentes.

5.21.4. Os incidentes não cobertos nesses cenários previstos no playbook, caso ocorram, devem ser incluídos em uma próxima revisão, assim como as respostas ao incidente.

5.21.5. Em caso de ocorrência de um incidente grave que implique na indisponibilidade parcial ou total de ativos do CONTRATANTE, a CONTRATADA, juntamente com a DGTEC, deve elaborar e coordenar um plano de ação para garantir a recuperação no menor tempo possível, com a preservação de todas a evidências sempre que possível, para posterior investigação.

5.21.6. A CONTRATADA deverá comunicar ao CONTRATANTE todos os incidentes, mas a orquestração das respostas, incluindo as ações a serem tomadas e os responsáveis pela execução de tais ações será da CONTRATADA.

5.21.7. A implantação dos controles e ajustes necessários durante um eventual incidente deverão ser realizados pela CONTRANTADA em comum acordo com o CONTRATANTE.

6. Gestão de Usuários

6.1. A CONTRATADA deverá executar serviços necessários para implementar a proteção adequada para as informações do CONTRATANTE, baseada nas pessoas, contemplando o gerenciamento de identidades, acessos e privilégios, abrangendo usuários comuns, internos e externos, administradores e desenvolvedores.

6.2. Os usuários devem se comportar conforme especificado pelas políticas de segurança, a maioria dos profissionais de segurança enfrentam uma barreira para conscientização e educação de segurança, ou seja, "adequar o ser humano à tarefa".

6.3. Das atividades – Gestão de identidades

6.3.1. Revisar e propor melhorias para a gestão de identidades atual, conforme Ato Normativo TJ n.º 27/2020 a partir da análise dos processos vigentes no CONTRANTANTE com o objetivo de propor ações preventivas, corretivas ou elaborar novas em comum acordo com a DGTEC, para controle de políticas de identidade, acessos e privilégios.

6.3.2. A CONTRATADA, em conjunto com a DGTEC, realizar o controle e verificação periódica de usuários, bem como seu grupo e permissões de acesso aos vários recursos tecnológicos da empresa como os sistemas, dispositivos, aplicativos, sistemas de armazenamento, redes e serviços. Utilizando o período de um ano para sistemas e acessos considerados críticos e dois anos para os demais.

6.3.3. Supervisionar a manutenção (planejamento junto ao departamento responsável pelo AD), propor sugestões, melhores práticas na árvore do AD.

6.3.4. Planejar e Supervisionar os níveis de segurança;

6.3.5. Analisar a eficiência na gestão de acessos;

6.3.6. Implementar políticas de acesso;

6.3.7. Verificar as rotinas de backup do AD.

6.3.8. Propor a redução da complexidade dos acessos de forma segura, eliminando a necessidade de que os colaboradores mantenham infinitas senhas, que normalmente são esquecidas.

6.3.9. Hierarquização das permissões controlando os privilégios de cada tipo de funcionário aos ambientes, construindo e avaliando a hierarquização de permissões existente de forma que cada colaborador tenha acesso apenas ao necessário.

6.3.10. Propor a exigência de senhas seguras com a finalidade de não permitir que os usuários utilizem senhas fracas que possam ser descobertas com facilidade. Desse modo, uma política de controle deve exigir a obrigatoriedade de senhas complexas, que misturem caracteres, números e símbolos especiais.

6.3.11. A CONTRATADA deve emitir um relatório no final de cada supervisão e serviços realizados.

6.4. **Gestão de Acessos**

6.4.1. O controle de acesso baseia-se na autorização e autenticação. Apresentado os fundamentos gerais do controle de acesso e algumas instanciações significativas que surgiram à medida que a TI continuou se espalhando para novas áreas de aplicação. A CONTRATADA pesquisará os modos de autenticação do usuário e a forma como eles são implantados atualmente, os protocolos de autenticação para a web, observando como novos casos de uso levaram a uma mudança dos protocolos de autenticação para os de autorização e a formalização das propriedades de autenticação usadas nas ferramentas de análise de protocolo atuais.

6.4.2. Orientar e apresentar para PJERJ o conceito de autorização no contexto do controle de acesso.

6.4.3. Implantar, após avaliação em conjunto com o CONTRATANTE:

6.4.3.1. O conceito de Controle de acesso, onde o processo deve conceder ou negar solicitações específicas a partir das entradas corretas.

6.4.3.2. Os conceitos básicos que estipulam os recursos confidenciais que devem ser protegidos, quanto para as regras aplicadas pelos sistemas de TI nos recursos que gerenciam.

6.4.3.3. As políticas de segurança automatizadas que se trata de um conjunto de regras que especificam os direitos de acesso um objeto.

6.4.3.4. O Controle de acesso baseado em função que são uma camada intermediária entre os usuários e as permissões para executar certas operações.

6.4.3.5. O controle de acesso baseado em atributos (ABAC) - controle de acesso lógico em que a autorização para realizar um conjunto de operações é determinada pela avaliação de atributos associados ao assunto, objeto, operações solicitadas e, em alguns casos, condições ambientais em relação política, regras ou relacionamentos que descrevem as operações permitidas para um determinado conjunto de atributos.

6.4.3.6. O controle de acesso baseado em código (CBAC) que atribui direitos de acesso a executáveis.

6.4.3.7. Aplicar controle para as políticas regular o número de vezes que o conteúdo pode ser acessado, por quanto tempo o conteúdo pode ser apresentado, o número de dispositivos de onde pode ser acessado.

6.4.3.8. Aplicar o Controle de Uso (UCON) proposto como uma estrutura que englobará autorizações com base nos atributos de sujeito e objeto, obrigações e condições.

6.4.3.9. Aplicação do controle de acesso para política de segurança, que deve ser definida para uma determinada solicitação, que envolvam, Pontos de administração de política, Pontos de decisão de política, Pontos de informação de política e Pontos de aplicação da política.

6.4.3.10. A delegação e a concessão de direitos de acesso referem-se a situações em que um principal, ou um sujeito, obtém um direito de acesso de outra pessoa.

6.4.3.11. Aplicar mecanismo de revogação, como o Protocolo de Status de Certificado Online (OCSP) para certificados X.509.

6.4.4. Tipos de monitores de referência

6.4.4.1. Propor mecanismos para transmitir com segurança solicitações de acesso, atributos, políticas e decisões entre os nós para o controle de acesso em sistemas distribuídos.

6.4.5. Conceitos Básicos sobre certificado, credencial e token.

6.4.6. Políticas Origin-based em aplicativos da web, clientes e servidores que se comunicam por meio do protocolo HTTP.

6.4.7. Cross-site Scripting - Ataques de script entre sites em aplicativos da web.

6.4.8. Cross-origin Resource Sharing.

6.4.9. Apoiar o gerenciamento de Federated Access Control.

6.4.10. Propor mecanismos de controle de acesso em um sistema operacional que implementam uma defesa lógica - Criptografia e controle de acesso.

6.4.11. Criptografia baseada em atributos.

6.4.12. Controle de acesso centrado em chave.

6.4.13. Orientar e apresentar para PJERJ o conceito de autenticação em um sentido restrito verificando a identidade de um usuário que efetua login - local ou remotamente - e vincular a identidade do usuário correspondente a autenticação do usuário com base em senhas é um método comum.

6.4.14. Sistemas de gerenciamento de identidade são responsáveis pela criação, uso e encerramento de identidades eletrônicas

6.4.15. A autenticação deverá ser vista como o serviço que valida os atributos de segurança de um assunto quando ele é criado.

6.4.16. Propor implantação/estudos de senhas empregadas para autenticação do usuário, as medidas de proteção no sistema incluem o armazenamento de senhas com hash (Unix, Linux) ou criptografadas (Windows).

6.4.17. Propor alternativas, para evitar a carga cognitiva associada à autenticação baseada em senha, tais como impressão digital e reconhecimento facial.

6.4.18. Propor a autenticação multifator combinando vários métodos de autenticação do usuário para aumentar a segurança ou token de autenticação.

6.4.19. Autenticação em Sistemas Distribuídos

6.4.20. Propor protocolo Needham-Schroeder que estabelece chave que emprega um servidor de autenticação como intermediário entre um cliente e um servidor.

6.4.21. Propor protocolo Kerberos para autenticação de usuário.

6.4.22. Propor Security Assertion Markup Language (SAML) v2.0 para metaprotocolos para autenticação em serviços da web.

6.4.23. Propor protocolos OAuth 2.0 e OpenID Connect, que são executados diretamente sobre HTTP e fornecem autenticação e autorização.

6.4.24. Orientar e apresentar para PJERJ a responsabilidade como a meta de segurança que gera a exigência de ações de uma entidade a serem rastreadas exclusivamente para essa entidade.

6.5. **Gestão de privilégios**

6.5.1. A CONTRATADA deve propor regras padronizadas e objetivas para criação de níveis acessos privilegiados aos ativos do PJERJ.

6.5.2. A CONTRATADA deve propor ações otimização, controle e melhoria do controle de privilégios.

7. Gestão de Problemas

7.1. A CONTRATADA deverá executar serviços que possibilitem a identificação da causa raiz de incidentes, apresentando e coordenando plano para correção definitiva ou solução de contorno.

7.2. A CONTRATADA deverá gerenciar o problema incluindo atividades requeridas para diagnosticar a causa raiz de incidentes e determinar a resolução dos problemas associados.

7.3. Relatório de análise e diagnóstico das causas (causa raiz) dos incidentes e problemas ocorridos, manutenções evolutivas e corretivas realizadas e sugestão de melhorias.

7.4. Detecção, resposta e análise da causa raiz dos incidentes, com auxílio de ferramentas informatizadas, com a finalidade de restaurar a operação normal do serviço o mais rápido possível de modo a minimizar o impacto adverso nas operações, garantindo que os níveis acordados de qualidade do serviço sejam mantidos.

7.5. A CONTRATADA irá manter as informações sobre problemas e soluções de contorno apropriadas.

7.6. Detecção de problema

7.6.1. Gatilhos para o gerenciamento de problema reativo:

7.6.1.1. Suspeita ou detecção de causa de um ou mais incidentes feita pela central de serviço, resultando na criação de registro de problema;

7.6.1.2. Análise de um incidente feita pelo grupo de suporte técnico que revela que um problema relacionado existe ou possam vir a existir;

7.6.1.3. Detecção automática de uma falha na infraestrutura ou em aplicativo;

7.6.1.4. Notificação de um fornecedor que um problema existe e precisa ser resolvido.

7.6.2. Gatilhos para o gerenciamento de problema proativo:

7.6.2.1. Análise de incidente que resulta na necessidade de criar um registro de problema;

7.6.2.2. Tendência do histórico de registro de incidentes para identificar uma ou mais causas relacionadas que, se removidas, podem prevenir suas recorrências;

7.6.2.3. Atividades realizadas para melhorar a qualidade de um serviço que resultam na necessidade de criar um registro de problema para identificar mais ações de melhoria que precisam ser tomadas.

7.7. Registro de problema

7.7.1. Todo o detalhamento descrito nesse caput referente a problema deve ser registrado em nossa ferramenta interna de gestão do CONTRATANTE para que conste em nosso banco de dados o histórico completo do incidente. A contratada deverá manter uma referência cruzada entre o(s) incidente(s) que iniciaram o registro do problema – e os detalhes importantes precisam ter continuidade e serem tratados a partir do(s) registro(s) de incidentes.

7.8. Categorização de problema

7.8.1. Problemas podem ser categorizados da mesma forma que o incidentes (é aconselhável usar o mesmo sistema de codificação), assim a natureza do problema pode ser facilmente rastreada no futuro e informação gerencial significativa pode ser obtida.

7.9. Priorização de problema

7.9.1. Identificar e ordenar as melhorias em potencial e criar um plano de implementação (matriz de priorização). A frequência e o impacto dos incidentes relacionados precisam ser levados em consideração.

7.10. Investigação e diagnóstico

7.10.1. Uma investigação deve ser conduzida para tentar diagnosticar a causa raiz do problema. A velocidade e a natureza desta investigação irão variar dependendo de impacto, severidade e urgência dos problemas.

7.10.2. Há várias técnicas que podem ser úteis para o diagnóstico, como análise cronológica, análise do valor do impacto, kepner e trogoe, brainstorming, 5W2H, isolamento de falha, mapa de afinidade, diagrama de Ishikawa, análise de Pareto, etc.

7.11. Descoberta de soluções de contorno

7.11.1. Em alguns casos pode ser possível descobrir uma solução de contorno para os incidentes causados pelo problema – uma forma temporária de superar as dificuldades. Quando uma solução de contorno é descoberta, ainda assim é importante que o registro do problema permaneça aberto e que os detalhes da solução de contorno sejam documentados no registro do problema.

7.12. Criação de registro de erro conhecido

7.12.1. Assim que o diagnóstico estiver completo e particularmente onde uma solução de contorno foi descoberta (ainda que não exista uma resolução permanente), um registro de

erro conhecido pode ser colocado no BDEC para ser utilizado para resolver novos incidentes. Às vezes pode ser vantajoso abrir um registro de erro conhecido ainda no início do processo.

7.13. Resolução do problema

7.13.1. Uma vez que a causa raiz foi descoberta e uma solução para removê-la foi desenvolvida, esta deve ser aplicada para resolver o problema.

7.13.2. Se qualquer mudança em uma funcionalidade é requerida, uma RDM deve ser criada e autorizada antes de a resolução se aplicada. Se uma correção urgente é necessária, uma RDM emergencial deve ser criada.

7.14. Encerramento de problema

7.14.1. Quando uma resolução final foi aplicada, o registro do problema pode ser encerrado formalmente – mesmo que registros de incidente estejam ainda abertos. Uma verificação é feita nesse momento para assegurar que o registro do problema contém uma descrição histórica completa e todos os eventos – e se não, o registro deve ser atualizado.

7.15. Revisão de problema grave

7.15.1. Após cada problema grave e enquanto a memória ainda estiver fresca, é aconselhável conduzir uma revisão para aprender quaisquer lições para o futuro. Especialmente, a revisão deve examinar:

7.15.1.1. Coisas que foram feitas corretamente;

7.15.1.2. Coisas que foram feitas errado;

7.15.1.3. O que poderia ser feito melhor no futuro;

7.15.1.4. Como prevenir a recorrência do problema;

7.15.1.5. Se houve qualquer responsabilidade de terceiro e se ações de acompanhamento são necessárias.

8. Gestão de Continuidade de Serviços de Segurança da Informação

8.1. A CONTRATADA deverá executar serviços para planejar e coordenar ações e procedimentos padronizados para recuperação de desastres e continuidade de serviços essenciais no menor tempo possível, mesmo em condições adversas.

8.2. Os objetivos da gestão de continuidade de serviços de SI do CONTRATANTE são:

8.2.1. Mapear os serviços tecnológicos do PJERJ a fim de elaborar um documento consolidado contendo as informações dos serviços e suas dependências;

8.2.2. Elaborar um plano de continuidade de serviços essenciais visando a redução do impacto na produção e manutenção do mesmo nível de segurança aplicado no repositório principal.

8.3. Produzir periodicamente uma análise de impacto do negócio (AIN) para assegurar que todos os planos de continuidade são mantidos em conformidade com os requisitos e impactos das mudanças no CONTRATANTE;

8.4. Administrar periodicamente uma análise e gerenciamento de risco, principalmente em conjunto com o gerenciamento de disponibilidade e o gerenciamento de segurança da informação;

8.5. Orientar a todas as demais áreas do CONTRATANTE, TI e SI sobre assuntos relacionados à continuidade e o resgate de informações;

8.6. Garantir que a continuidade e os mecanismos adequados de recuperação estejam estabelecidas para atender ou transpor as metas acordadas de continuidade do negócio;

8.7. Estimar o impacto de todas as mudanças nos planos de continuidade de serviço de TI e manter metodologias e procedimentos;

8.8. Assegurar medidas proativas para melhorar a disponibilidade dos serviços de SI;

8.9. A gestão de continuidade de serviço de SI considera os ativos e configurações de SI que suportem os processos de negócios e não cobre riscos de longo prazo tais como mudança de direção, reestruturação, diversificação do negócio, entre outros.

8.10. A CONTRATADA deverá elaborar e coordenar, juntamente com o CONTRATANTE, protocolo e plano de ação para recuperação de desastres e continuidade de serviços essenciais em condições adversas. Devem ser baseadas nos conceitos elementares das melhores práticas de mercado.

9. Gestão do Conhecimento

9.1. A CONTRATADA deverá executar serviços que permitam a criação, em conjunto com o CONTRATANTE, de uma base de conhecimento de boas práticas e lições aprendidas, permanente e sempre atualizada, com auxílio de ferramenta automatizada.

9.2. A CONTRATADA deverá implantar e incrementar uma base de conhecimento relacionada a segurança da informação, contendo informações dos incidentes ocorridos durante a vigência do contrato, os processos adotados para a devida resposta a esses incidentes e as soluções encontradas.

9.3. A CONTRATADA deverá homologar ou recomendar ajustes nos processos previamente estabelecidos de respostas a incidentes e demais operações, através da análise das informações presentes nessa base de conhecimento.

9.4. A CONTRATADA deverá garantir que a informação correta esteja disponível para a pessoa certa e na hora certa, permitindo tomada de decisão bem embasada.

9.5. A CONTRATADA deverá implementar o gerenciamento do conhecimento agregando valor às informações, filtrando, resumindo e sintetizando estas, e dessa forma, desenvolvendo um perfil de utilização pessoal que ajuda a levá-las à ação. Transformando a informação em conhecimento a partir de:

9.5.1. Comparação: entendimento sobre como as informações relativas a um determinado assunto podem ter alguma relação ou aplicação em outras situações;

9.5.2. Consequência: implicação que determinada informação pode trazer para a tomada de alguma decisão e/ou ação;

9.5.3. Conexão: relação entre a informação adquirida e um conhecimento já existente;

9.5.4. Conversação: interpretação daquela informação a partir do entendimento sobre o que as pessoas pensam sobre ela.

9.6. O processo de gestão do conhecimento será composto por:

9.6.1. Criação e aquisição do conhecimento;

9.6.2. Identificar o conhecimento relevante para melhorar a qualidade do processo, produto ou serviço.

9.6.3. Definir o indicador e a meta de melhoria a serem alcançados com o uso do conhecimento.

9.6.4. Definir o método para identificar e captar e ou criar o conhecimento.

10. Gestão de Comunicação e Educação

10.1. A CONTRATADA deverá executar serviços necessários para criação de um plano de comunicação permanente e institucionalizado, com procedimentos padronizados, em especial, no caso de incidentes graves, promovendo também uma política educacional e de conscientização de segurança da informação.

10.2. A CONTRATADA deverá é apoiar o CONTRATANTE na elaboração e implantação de um plano de comunicação institucional permanente e atualizado para divulgação dos procedimentos e ações a serem adotadas em caso de incidentes, pelos usuários internos do PJERJ.

10.3. Estabelecer procedimentos técnicos de orientação e comunicação das autoridades e o público sobre as informações estritamente necessárias de forma transparente de incidentes.
10.4. Estabelecer um programa em comum acordo com o CONTRATANTE, de conscientização e aculturamento em segurança da informação, em conformidade com as leis e normas vigentes, em todos o ambiente do PJERJ através da educação, promovendo, cursos, campanhas, eventos, palestras e outros com o objetivo de promover o maior conhecimento sobre o tema e engajar os usuários a participar da segurança.
10.5. A CONTRATADA e CONTRATANTE deve definir um processo de comunicação e tratamento de incidentes de segurança em redes computacionais, considerando as exigências da legislação vigente, em até XX dias após a realização da reunião inicial. Os serviços objeto deste Termo de Referência serão executados contemplando as diretrizes acordadas na Política de Segurança da Informação do PJERJ, aprovada pela Resolução TJ/OE n.º 05/2019, de 27 de fevereiro de 2019.
10.6. **Atividades da comunicação**
10.6.1. Propor uma Gestão da comunicação dentro das equipes de SI, seus departamentos, usuários, clientes, para uma política de comunicação em cada equipe ou departamento/diretoria e também para cada processo de operação.
10.6.2. Propor a criação de canais de comunicação estabelecidos apropriadamente podem ajudar prevenir ou mitigar problemas internos., estabelecendo que tipos de comunicação que podem ser utilizados: reuniões, e-mail, Telefone, documentos, sistemas.
10.6.3. O gerenciamento das comunicações deverá abranger processos imprescindível para assegurar que as informações sejam planejadas, coletadas, criadas, distribuídas, armazenadas, recuperadas, gerenciadas, controladas, monitoradas e estabelecida de maneira oportuna e apropriada. Os autores que estiverem envolvidos em projetos passam a maior parte do tempo se comunicando entre si e outras partes interessadas, tanto internas como externas ao CONTRATANTE.
10.6.4. Fazer com que a comunicação seja eficaz para diminuir a distância e estreitar relações entre as diversas partes interessadas, que podem ter diferentes visões, diferentes níveis de conhecimento, e diversas perspectivas e interesses que podem impactar ou influenciar a execução das atividades ou resultado do projeto.
10.6.5. Fornecer uma visão geral dos processos do gerenciamento das comunicações baseadas nos conhecimentos de projeto, que são:
10.6.5.1. Planejar o gerenciamento das comunicações;
10.6.5.2. Gerenciar as comunicações;

10.6.5.3. Controlar as comunicações.

10.7. **Plano de Comunicação**

10.7.1. A CONTRATADA deve elaborar um plano de comunicação, que além de outros requisitos que podem ser acordados com o CONTRATANTE, deve conter no mínimo:

10.7.1.1. Lista dos ativos abrangidos no escopo do trabalho;

10.7.1.2. Nomes e contatos dos responsáveis por cada sistema de proteção da informação;

10.7.1.3. Nomes e contatos dos consultores contratados como objeto deste edital;

10.7.1.4. Matriz de acionamento da estrutura de Segurança da Informação da CONTRATANTE;

10.7.1.5. Método de acionamento baseado na criticidade do incidente;

10.7.1.6. Também deverá ser desenvolvido um plano de comunicação referente a disseminação da consciência de segurança, para ações de divulgação e aculturamento de segurança da informação, projetos de conscientização, eventos e campanhas, entre outros.

10.7.2. O Plano de Comunicação elaborado deve atender a todos os requisitos estabelecidos no Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário e do Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário normatizados pela Portaria CNJ n.º 162 de 10 de junho de 2021.

10.8. **Meios de Comunicação**

10.8.1. Todas as solicitações de serviço, sejam de suporte ou consultoria, deverão ser realizadas apenas pelos contatos cadastrados, através dos métodos abaixo:

10.8.1.1. Ferramenta de comunicação de mensagens e videoconferência Microsoft ou outra utilizada pelo PJERJ;

10.8.1.2. Ferramenta de service desk web, E-mail e Telefone.

10.8.2. A fim de agilizar o tratamento, em casos de incidentes relacionados à Segurança das Informações, os consultores alocados pela CONTRATADA, objeto deste edital, organizarão a comunicação entre o SOC da CONTRATADA e os recursos da CONTRATANTE, sejam estes funcionários ou terceiros.

10.9. **Atividades da Educação**

10.9.1. Construir um referencial teórico que possa subsidiar a análise sobre todas as áreas no item 2.2.

10.9.2. Deverá criar material próprio e disponibilizar no site do PJERJ.

10.9.3. Todas as solicitações de aculturamento, conscientização, eventos e campanhas deverão ser realizadas apenas pelos contatos cadastrados, através dos métodos abaixo:

10.9.3.1. Ferramenta de comunicação de mensagens e videoconferência Microsoft ou outra utilizada pelo PJERJ;

10.9.3.2. Ferramenta de service desk, web, E-mail e Telefone.

10.9.4. Incorporar como parte do processo de segurança da CONTRATANTE a documentação detalhada de todas as iniciativas e processos.

10.9.5. A CONTRATADA deverá contemplar toda e qualquer evolução tecnológica que requer o planejamento, implementação e ações de educação integradas aos demais serviços que compõem esta contratação, aumentando a maturidade de TIC.

10.9.6. Todas as ações de implantação das mudanças e/ou melhorias deverão abranger uma etapa de educação, sendo definida em comum acordo entre a CONTRATANTE e a CONTRATADA a melhor forma de execução desta educação;

10.9.7. A CONTRATADA deverá promover também a conscientização dos principais riscos existentes, realizando também simulações em períodos anteriores e posteriores as campanhas ou eventos realizados com os usuários e colaboradores, principalmente os afetados pela simulação teste.

10.9.8. Tais eventos, campanhas, aculturamento deverão ser integrado com a ferramenta especializada em simulação de ataque phishing.

11. Gestão de Projetos e Inovações de Segurança da Informação

11.1. A CONTRATADA deverá executar serviços necessários para prospecção de soluções ou inovações que possam contribuir para a melhoria da qualidade da segurança da informação do CONTRATANTE, apoiando tecnicamente os projetos e aquisições.

11.2. Elaborar o plano de gerenciamento de projetos focado em ações de inovações e mudanças de segurança da informação.

11.3. A CONTRATADA deve estabelecer e coordenar projetos dedicados à segurança da informação em geral abrangendo todos os temas constante da tabela do item 2.2, além do monitoramento constante e acompanhamento da evolução das novas técnicas e tecnologias

11.4. A CONTRATADA deve apoiar tecnicamente o CONTRATANTE na aquisição e implantação de soluções que visem ampliar e melhorar a segurança da informação no ambiente do PJERJ.

11.5. A CONTRATADA deve prospectar e propor inovações na área de segurança da informação que sejam compatíveis com o ambiente tecnológico do PJERJ.

12. Auditoria e Investigação

12.1. A CONTRATADA deverá executar serviços que permitam a verificação periódica de conformidade dos normativos e procedimentos implantados, propondo e coordenando ações corretivas e a criação de normas e procedimentos de investigação, correlacionado histórico de eventos, em especial, os relacionados a ilícitos, que permitam a preservação de evidências de forma integrada com a continuidade dos serviços.

12.2. O objetivo principal da CONTRATADA será fornecer uma visão geral das técnicas e capacidades investigativas de segurança da informação e colocá-las em uma perspectiva mais ampla em relação a outras áreas relacionadas no domínio da segurança cibernética.

12.3. A CONTRATADA deve elaborar e implantar o protocolo de investigação de ilícitos cibernéticos, que deve conter todos os requisitos contidos na Portaria CNJ n.º 162/2021.

12.4. A CONTRATADA deverá elaborar e coordenar plano de ação, bem como, executar auditoria de segurança da informação de:

12.4.1. Procedimentos;

12.4.2. Processos de trabalhos;

12.4.3. Ativos;

12.4.4. Conformidade normativa; e

12.4.5. Outros que impactem na segurança da informação.

12.5. Atividades

12.5.1. A CONTRATADA deverá:

12.5.1.1. Executar o plano de ação periodicamente para auditoria prevista no item anterior, aprovado pelo CONTRATANTE;

12.5.1.2. Apresentar relatório completo após o término da auditoria, apontando as possíveis não conformidades;

12.5.1.3. Apresentar e coordenar plano de correções dos problemas encontrados.

12.5.1.4. A CONTRATADA deverá executar Serviços de Modelos Conceituais a partir de duas abordagens possíveis para reconstruir a sequência relevante de eventos na análise de um sistema cibernético a partir das fontes de dados disponíveis.

12.5.1.5. A CONTRATADA deve identificar o ponto de partida para abordagens centradas no estado instantâneo do sistema de interesse;

12.5.1.6. Usando o conhecimento de como um determinado sistema/aplicativo opera, a CONTRATADA deverá deduzir um estado anterior de interesse.

12.5.1.7. Abordagens centradas em log contam com um histórico de eventos explícito com data/hora que documenta as atualizações do estado do sistema.

12.5.1.8. A CONTRATADA deverá garantir que esses logs estarão disponíveis sempre que necessário onde, os sistemas operacionais devem manter uma variedade de logs de monitoramento que detalham vários aspectos da operação do kernel do sistema operacional e diferentes aplicativos; ferramentas adicionais de auditoria e monitoramento de segurança que fornecem eventos ainda mais potencialmente relevantes.

12.5.1.9. A CONTRATADA deverá aplicar em vários níveis de abstração e a uma ampla variedade de artefatos sobre o prisma do modelo de Tarefa Cognitiva a análise diferencial é um bloco de construção básico do processo investigativo.

12.5.1.10. Aplicação do processo analítico geral que é de natureza iterativa com dois loops de atividades principais: um loop que envolve as ações tomadas para encontrar fontes potenciais de informação e que então às consultas e filtra quanto à relevância; e um ciclo de criação de sentido no qual o analista desenvolve - de uma forma iterativa - um modelo conceitual que é apoiado pela evidência.

12.5.1.11. Aplicação dos processos de transformação da informação nos dois loops podem ser classificados em bottom-up (organização de dados para construir uma teoria) ou top-down (localização de dados com base em uma teoria).

12.5.1.12. Construir representações de informações de alto nível (mais abstratas) a partir de evidências mais específicas a partir de Processos Bottom-Up:

12.5.1.12.1. Pesquisa e filtro: fontes de dados externas, discos rígidos, tráfego de rede, etc. são pesquisados em busca de dados relevantes com base em palavras-chave, restrições de tempo e outros em um esforço para eliminar a grande maioria dos dados irrelevantes.

12.5.1.12.2. Ler e extrair: as coleções na shoebox são analisadas para extrair fatos e relações individuais que podem apoiar ou refutar uma teoria. As peças de artefatos resultantes (por exemplo, mensagens de e-mail individuais) são geralmente anotadas com sua relevância para o caso.

12.5.1.12.3. Esquematizar: nesta etapa, fatos individuais e implicações simples são organizados em um esquema que pode ajudar a organizar e identificar a importância e as relações entre um número crescente de fatos e eventos. A análise da linha do tempo é uma das ferramentas básicas do mercado; no entanto, qualquer método de organizar e visualizar os fatos, gráficos, tabelas, etc., pode acelerar muito a análise.

12.5.1.12.4. Construir caso: a partir da análise dos esquemas, o analista eventualmente apresenta teorias testáveis, ou hipóteses de trabalho, que podem explicar a evidência. Uma hipótese de trabalho é uma conclusão provisória e requer mais evidências de apoio, bem como testes rigorosos com explicações alternativas. É um componente central do processo investigativo e é um ponto de referência comum que reúne as partes jurídica e técnica para a construção de um caso.

12.5.1.12.5. Conte a história: o resultado típico de uma investigação forense é um relatório final e, talvez, uma apresentação oral no PJERJ. A apresentação real pode conter apenas a parte da história que é fortemente apoiada pela evidência digital; os pontos mais fracos podem ser estabelecidos com base em evidências de outras fontes.

12.5.1.13. Conclusões parciais ou provisórias são usadas para conduzir a busca por evidências de apoio e contraditórias. Processos Top-Down são analíticos fornecendo contexto e direção para a análise de pesquisas de dados menos estruturadas e ajudam a organizar as evidências.

12.5.1.14. Reavaliar: O feedback dos usuários dos sistemas do CONTRATANTE pode exigir reavaliações, como coletar evidências mais fortes ou buscar teorias alternativas;

12.5.1.15. Busca por suporte: uma hipótese pode precisar de mais fatos para ter interesse e, idealmente, seria testada contra todas as explicações alternativas (razoavelmente) possíveis;

12.5.1.16. Busca por evidências: a análise de teorias pode exigir a reavaliação das evidências para determinar sua significância/procedência, ou pode desencadear a busca por mais/ melhores evidências;

12.5.1.17. Busca de relações: evidências no arquivo podem sugerir novas buscas de fatos e relações com os dados;

12.5.1.18. Busca de informações: o ciclo de feedback de qualquer um dos níveis mais elevados pode, em última instância, resultar em uma busca por informações adicionais; isso pode incluir novas fontes ou o reexame de informações que foram filtradas em fases anteriores.

12.5.1.19. Aplicar o ciclo de Foraging Loop - ato de equilíbrio entre três tipos de processamento que um analista pode realizar - explorar, enriquecer e explorar. A exploração expande efetivamente a shoebox, incluindo grandes quantidades de dados; o enriquecimento o reduz, fornecendo consultas mais específicas que incluem menos objetos para consideração; exploração é a leitura e análise cuidadosa de um artefato para extrair fatos e inferências.

12.5.1.20. Aplicar o Sense-Making Loop que se trata do processo de criação de consciência situacional e compreensão para apoiar a tomada de decisão em face da incerteza - um esforço para entender as conexões entre pessoas, lugares e eventos, a fim de antecipar suas trajetórias e agir com eficácia. Existem três processos principais envolvidos no ciclo de criação de sentido: estruturação do problema - a criação e exploração de hipóteses, raciocínio probatório - o emprego de evidências para apoiar/refutar uma hipótese e tomada de decisão - selecionar um curso de ação a partir de um conjunto de alternativas.

12.5.1.21. Utilizar extração de dados x análise x interpretação jurídica com o auxílio de ferramentas deve fornecer principalmente os meios para adquirir a evidência digital dos alvos forenses, extrair (e reconstruir logicamente) objetos de dados deles e as ferramentas essenciais para pesquisar, filtrar e organizá-los.

12.5.1.22. A CONTRATADA deve ser tecnicamente proficiente o suficiente para compreender o significado dos artefatos extraídos das fontes de dados e devem ser capazes de ler a literatura técnica relevante (artigos revisados por pares) na íntegra.

12.5.1.23. A Análise de Sistema empregada ao conhecimento de como os sistemas operacionais funcionam para chegar a conclusões sobre eventos e ações de interesse para um caso específico.

12.5.1.24. Exame completo de dados persistentes para a maioria das investigações forenses digitais a partir de Análise de armazenamento persistente na forma de unidades de disco rígido (HDDs), unidades de estado sólido (SSDs), discos óticos, mídia externa (conectada por USB) etc.

12.5.1.25. Camadas de abstração de dados a análise forense de dispositivos de armazenamento deve ser realizada em vários níveis de abstração:

12.5.1.25.1. Meios físicos;

12.5.1.25.2. Dispositivo de bloco;

12.5.1.25.3. Sistema de arquivo;

12.5.1.25.4. Artefatos de aplicação.

12.5.1.26. A Aquisição de dados seguindo as melhores práticas, a análise de dados em repouso não será realizada em um sistema ativo. A máquina de destino estará desligada, uma cópia exata dos bits da mídia de armazenamento será criada, o original deverá ser armazenado em um armário de evidências e todo o trabalho forense é executado na cópia.

12.5.1.27. Recuperação de dados - Esse processo de recuperação e reconstrução do conteúdo do arquivo diretamente do armazenamento em bloco, sem usar os metadados do sistema de arquivos.

12.5.1.28. Escultura de dados (estrutura) - Esse processo reconstrói objetos lógicos (como arquivos e registros de banco de dados) a partir de uma captura de dados em massa (imagem de disco/RAM) sem usar metadados que descrevem a localização e o layout dos artefatos.

12.5.1.29. Estudos para demonstrar que os dados tendem a persistir por muito tempo na memória volátil.

12.5.1.30. Armazenamento dos logs de auditoria:

12.5.1.30.1. A CONTRATADA será responsável pela guarda dos logs coletados pelo SIEM;

12.5.1.30.2. A CONTRATANTE, caso julgue insuficiente as informações gravadas nos arquivos de logs, poderá solicitar alterações na configuração junto à CONTRATADA;

12.5.1.30.3. O tempo de retenção dos logs gerados deverá ser equivalente ao prazo da vigência contratual. Ao final do contrato, a CONTRATADA não deverá ficar com nenhuma cópia dos mesmos, assim como, toda documentação necessária para sua utilização, repassando-as para a CONTRATANTE em meio magnético e ou ótico, antes da sua destruição.

12.5.1.31. Ocorrência de Incidentes

12.5.1.31.1. No caso de detecção de algum incidente de segurança, a CONTRATADA deverá acionar a CONTRATANTE, de acordo com o SLA constante deste documento, para que sejam tomadas as medidas corretivas e legais necessárias, de acordo com o procedimento de resposta a incidentes;

12.5.1.31.2. Serão considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, indisponibilização dos serviços (DoS), ataques por força bruta, ou qualquer outra ação que possa comprometer a confidencialidade, disponibilidade ou integridade das informações da CONTRATANTE;

12.5.1.31.3. A CONTRATADA deverá disponibilizar todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que sejam apurados os incidentes de segurança reportados;

12.5.1.31.4. Dependendo do grau do incidente, a CONTRATADA poderá deslocar recurso técnico capaz de dar suporte ao problema, além do time de suporte local, para reduzir o tempo de resposta a CONTRATANTE e minimizar os possíveis impactos;

12.5.2. A CONTRATADA, em casos de identificação de um problema e/ou reincidência de um evento, deve:

12.5.2.1. Garantir o registro, identificação e classificação de criticidade de um problema;

12.5.2.2. Assegurar investigação e diagnóstico;

12.5.2.3. Realizar análise de tendência, permitindo detectar possíveis reincidências;

12.5.2.4. Possibilitar inclusão e atualização dos dados contidos em uma Base de Conhecimento, mantida pela CONTRATADA;

12.5.2.5. Assegurar que um registro de problema contenha todo o histórico de sua análise, diagnóstico e possa estar associado a uma Solicitação de Mudanças.

13. Melhoria contínua

13.1. A CONTRATADA deverá executar serviços para planejar e coordenar ações que visem permanentemente a melhoria da qualidade da segurança da informação do CONTRATANTE.

13.2. 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.

13.3. Tal ação incluirá a análise do ambiente atual, mas também a busca e proposição de soluções tecnológicas e inovações que sejam viáveis e possam melhorar a qualidade da segurança da informação para o PJERJ.

13.4. A Melhoria de Serviço Continuada aplicando metodologias do mercado voltados para SI fornecerá orientação em quatro áreas principais:

13.4.1. A saúde geral do SI como uma disciplina;

13.4.2. O alinhamento contínuo do portfólio de serviços com as necessidades atuais e futuras do CONTRATANTE;

13.4.3. A maturidade e capacidade da organização, gestão, processos e pessoas utilizadas pelos serviços;

13.4.4. Melhoria contínua de todos os aspectos do serviço de TI e os ativos de serviço que os suportam.

13.5. Revisar as informações de gestão e tendências para garantir que os serviços atendam ao acordado níveis de serviço;

13.6. Revisar as informações de gestão e tendências para garantir que a saída da habilitação processos estão alcançando os resultados desejados;

13.7. Realizar periodicamente avaliações de maturidade de encontro as atividades do processo e regras associadas para demonstrar melhoria das áreas ou, inversamente, áreas de interesse;

13.8. Realizar auditorias internas periodicamente, verificando funcionários e conformidades do processo;

13.9. Revisar as entregas existentes para adequação;

13.10. Propor periódicas recomendações para oportunidades de melhoria;

13.11. Realizar análises de serviço externos e internos para identificar oportunidades Melhoria Contínua De Serviço;

13.12. Medir e identificar o valor criado pelas Melhorias aplicadas.

13.13. Elaborar, coordenar e executar plano de ação para a aplicação das melhorias propostas.

13.14. Os resultados da Melhoria Contínua De Serviço devem ser revisados em uma base contínua para verificar a integridade, funcionalidade e viabilidade, e para garantir que eles permaneçam relevantes e não se tornam obsoletos e inutilizáveis.