PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

PAGAMENTO

5.17. A emissão do termo de recebimento provisório será feita após a entrega e apresentação dos relatórios indicados nesta especificação:

5.17.1. Incidentes de segurança cibernética (item 5.14.5);

5.17.2. Deep/Dark Web (item 5.14.6.3);

5.17.3. Breach and Attack Simulation (item 2.32.5), quando a solução tiver essa capacidade;

5.17.4. SLA (itens 5.22.2 e 5.23.8).

5.18. A emissão do termo de recebimento definitivo será feita após a verificação dos serviços prestados e sua aderência às condições estabelecidas nesta especificação.

5.19. O pagamento do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser mensal, sendo realizado somente após a emissão do termo de recebimento definitivo, descontadas eventuais glosas do período avaliado, conforme Fator de Desconto (FD) calculado no período (item 5.25 e subitens) e das multas aplicadas, quando houver.

CONFIDENCIALIDADE E DESCARTE DE INFORMAÇÕES

5.20. Confidencialidade:

5.20.1. A CONTRATADA deve ser responsável pelo ciclo de vida das informações coletadas pela solução proposta, atendendo aos critérios definidos pela CONTRATANTE, devendo processar, armazenar e, após o término da sua finalidade, descartar os dados de maneira segura.

5.20.1.1. A CONTRATADA obriga-se a tratar como "segredos comerciais e confidenciais" quaisquer informações, dados, processos, fórmulas, códigos, obtidos em consequência ou por necessidade desta contratação, utilizando-os apenas para as finalidades previstas no contrato, não podendo revelá-los ou facilitar a revelação a terceiros, mediante assinatura dos Termos de Confidencialidade conforme anexos A1 e A2;

5.20.2. Ao final do contrato, o descarte das informações deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital.

GARANTIA E ACORDO DE NÍVEL DE SERVIÇO

5.21. Da garantia:

5.21.1. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado.

5.21.2. A solução deve contar com garantia integral do fabricante (Garantia Compreensiva) durante toda a vigência do contrato e deve comportar a garantia comumente utilizada pelo comércio e prevista no Código de Defesa do Consumidor acrescida de suporte técnico nos moldes desta especificação.

5.22. Um acordo de nível de serviço (SLA – Service Level Agreement) define os índices a serem atingidos para o cumprimento do conjunto de compromissos acordados entre CONTRATANTE e CONTRATADA.

5.22.1. Tais índices serão medidos e aplicados aos serviços contratados e prestados pela CONTRATADA.

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

5.22.2. Mensalmente, os dados de nível de serviço devem ser apresentados à CONTRATANTE, incluindo informações sobre ações e necessidades para a correção de desvios, visando atingir, manter e melhorar os níveis desejados.

5.22.3. A abrangência e o nível de detalhamento serão definidos conforme as necessidades identificadas pela CONTRATANTE, podendo sofrer alterações ao longo do tempo, as quais serão encaminhadas à CONTRATADA.

5.22.4. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

5.22.4.1. Requisição: solicitação da CONTRATANTE para intervenção preventiva ou corretiva no ambiente gerenciado e nos ativos monitorados (item 1.1.1) e previsto no escopo desta proposta. Cada requisição será identificada unicamente por meio de um código e será classificada conforme seu nível de severidade no momento da sua comunicação à CONTRATADA;

5.22.4.2. Incidentes de segurança: conforme definido nos itens 5.3, 5.4 e 5.5.

5.22.4.3. Severidade: nível de prioridade/emergência atribuído ou solicitado para a realização de um atendimento a uma requisição da CONTRATANTE ou dos alertas gerados para o ambiente gerenciado, conforme critérios descritos a seguir. Solicitações de alteração do nível de severidade poderão ser submetidas à CONTRATADA e, em comum acordo, serão prontamente atendidas.

5.22.4.3.1. Severidade crítica: o serviço está totalmente parado ou inoperante;

5.22.4.3.2. Severidade alta: o serviço está ativo mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;

5.22.4.3.3. Severidade média: o serviço está operativo, mas suas funcionalidades são executadas com restrições;

5.22.4.3.4. Severidade baixa: o serviço está operativo e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;

5.22.4.3.5. Severidade agendado: o atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações;

5.22.4.4. Triagem: notificação, da CONTRATADA para a CONTRATANTE, de que está ciente da requisição ou do incidente, conforme itens 5.14.3 e 5.14.4.

5.22.4.5. Resolução: comunicação, da CONTRATADA para a CONTRATANTE, das ações INICIAIS (podendo incluir soluções paliativas enquanto a CONTRATADA busca a solução definitiva para o incidente ou chamado) a serem executadas para resolução da requisição ou do incidente de segurança, conforme item 5.15.8 e subitens.

5.22.4.5.1. A CONTRATADA deve fornecer, em até 48h, o restante das ações (contendo a resolução paliativa ou definitiva) a serem executadas para a resolução do incidente ou chamado.

5.22.4.5.2. Caso seja fornecida uma solução paliativa, a CONTRATADA deve atuar proativamente na busca de uma solução definitiva, fornecendo o acompanhamento e suporte necessários para a CONTRATANTE, inclusive sugerindo a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente ou chamado.

5.22.4.5.3. Devido à natureza dos incidentes de segurança cibernética, a sua efetiva contenção e remediação não contarão para contagem dos tempos de SLA, não eximindo a CONTRATADA de registrar esses tempos no módulo de gestão de incidentes de segurança da solução e ITSM integrado.

5.22.5. Os seguintes SLAs devem ser cumpridos:

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Atividade	SLA de atendimento
Triagem da requisição/incidente de segurança[1]	Em até 30 (trinta) minutos
Requisição/Incidentes de severidade crítica	Atuação em até 15 (quinze) minutos e resolução[2] em até 01 (uma) hora.
Requisição/Incidentes de severidade alta	Atuação em até 01 (uma) hora e resolução em até 02 (duas) horas.
Requisição/Incidentes de severidade média	Atuação em até 02 (duas) horas e resolução em até 04 (quatro) horas.
Requisição/Incidentes de severidade baixa	Atuação em até 04 (quatro) horas e resolução em até 12 (doze) horas.
Requisição de severidade agendado	Atuação em até 12 (doze) horas e resolução em até 24 (vinte e quatro) horas.

SUPORTE TÉCNICO

5.23. Suporte Técnico:

5.23.1. A abertura de chamados pela CONTRATANTE deve poder ser efetuada:

5.23.1.1. Pela plataforma web, em sistema de atendimento da CONTRATADA;

5.23.1.2. Pelo envio de mensagem de correio eletrônico;

5.23.1.3. Por meio do módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4);

5.23.1.4. Por telefone.

5.23.2. O atendimento aos chamados deve estar disponível em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), conforme SLA apresentado (item 5.22.5).

5.23.3. Todo tipo de comunicação e documentação relacionados aos atendimento de chamados devem ser em Português.

5.23.4. A assistência técnica em garantia deve assegurar o fornecimento de acesso irrestrito (24 horas por dia, 07 dias da semana) da CONTRATANTE à área de suporte do fabricante, especialmente ao endereço eletrônico (web site) e a toda a documentação técnica pertinente (guias de instalação e configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

5.23.5. O suporte técnico do fabricante deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes às soluções de software e hardware (inclusive virtual) dos produtos.

5.23.6. Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, garantir o fornecimento e instalação de novas versões, patches e hotfixes (tanto de componentes on-premises quanto em nuvem), análise de dúvidas sobre melhores práticas de configuração, entre outros.

5.23.7. A CONTRATADA deve fornecer, mensalmente, relatório oriundo da ferramenta de ITSM (conforme item 2.5.4.1) indicando os SLAs de cada chamado e incidente registrado na solução.

[1] Pode ser considerado como o Tempo Médio de Detecção (Mean Time To Detect - MTTD)

[2] Para as atividades de Requisição/Incidentes: pode ser considerado como o Tempo Médio de Resposta (Mean Time To Respond - MTTR)

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

5.23.8. Para a aferição e a avaliação dos níveis de serviço, a CONTRATADA deve fornecer, mensalmente, relatório gerencial de serviços, apresentando-o à CONTRATANTE até o quinto dia útil do mês subsequente ao da prestação do serviço, sendo que devem constar, entre outras informações, os indicadores/metas de níveis de serviço alcançados conforme item 5.22.5, recomendações técnicas, as solicitações de abonos com justificativa e demais informações relevantes para a gestão contratual, em conformidade aos acordos realizados na fase de Planejamento e Projeto (item 4.4.1).

PENALIDADES

5.24. A CONTRATADA está sujeita às seguintes penalidades, desde que não apresente justificativa fundamentada e aceita pela CONTRATANTE, isolada ou cumulativamente:

5.24.1. Advertência;

5.24.2. Multa de 1% (um por cento) do valor mensal contratado em casos de atraso, exceto para as ocorrências verificadas nos subitens, por dia, até o limite de 15 (quinze por cento). Ultrapassado esse limite, poderá ser caracterizada a inexecução total do objeto;

5.24.2.1. Multa de 0,5% (meio por cento) do valor mensal do contrato, quando a CONTRATADA entregar com atraso a documentação exigida nos itens 5.25.13.3 até 5.25.13.8, inclusive subitens, por dia de atraso;

5.24.2.2. Multa de 0,5% (meio por cento) do valor mensal do contrato, quando a CONTRATADA entregar de forma incompleta a documentação exigida nos itens 5.25.13.3 até 5.25.13.8, inclusive subitens, por dia de atraso, até que sejam entregues todos os documentos faltantes;

5.24.2.3. Multa de 0,5% (meio por cento) do valor mensal do contrato, quando a CONTRATADA entregar com atraso os esclarecimentos formais solicitados para sanar as inconsistências ou dúvidas suscitadas durante a análise da documentação exigida nos itens 5.25.13.3 até 5.25.13.8, inclusive subitens, por dia de atraso.

5.24.3. Multa de 0,1% (um décimo por cento) sobre o valor mensal do contrato, multiplicada pelo Fator de Impacto no Serviço (FIS) do indicador, para cada indicador de nível de serviço que apresente discrepância superior a 20% em relação à meta prevista, em determinado mês, limitado a 10% sobre o valor mensal do contrato, que poderá ensejar a inexecução parcial ou total do contrato;

5.24.4. Multa de 0,5% (cinco décimos por cento) sobre o valor mensal do contrato, multiplicada pelo Fator de Impacto no Serviço (FIS) do indicador, para cada indicador de nível de serviço que apresente discrepância superior a 10% em relação à meta prevista em 3 medições consecutivas, ou em 3 medições não consecutivas realizadas no intervalo de 6 meses, limitado a 20% sobre o valor mensal do contrato, que poderá ensejar a inexecução parcial ou total do contrato;

5.24.5. Multa de 5% (cinco por cento) sobre o valor mensal do contrato para cada ocorrência de descumprimento de obrigações contratuais que não sejam relacionadas ao atingimento das metas estabelecidas para os indicadores de nível de serviço;

5.24.6. Multa de 30% (trinta por cento) do valor contratado, em caso de inexecução total ou parcial do objeto, sem prejuízo da responsabilidade civil e criminal; e suspensão, pelo prazo de até 02 (dois) anos, do direito de licitar e contratar com a CONTRATANTE;

INDICADORES DE DESEMPENHO E GLOSAS

5.25. Glosa quando a CONTRATADA não produzir os resultados, ou não executar com a qualidade mínima exigida as atividades contratadas, conforme disposto nos indicadores de níveis de serviço.

5.25.1. Para fins de faturamento, o valor mensal da prestação do serviço será ponderado em função do desempenho mensal alcançado nele. Na medição, será apurado o afastamento dos

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

indicadores de nível de serviço em relação às metas estabelecidas em contrato, aplicando-se um Fator de Desconto (FD);

5.25.2. Nos casos em que o afastamento ensejar o desempenho abaixo da meta exigida, o valor do afastamento será utilizado para abater valores financeiros dos preços previstos em contrato;

5.25.3. Os Fatores de Desconto (FD) serão calculados com base nos resultados alcançados nos indicadores de nível de serviço, previstos nesta especificação técnica (item 5.25.11);

5.25.3.1. Haverá uma tolerância de 5% em relação à meta para a aplicabilidade do fator de desconto, ou seja, caso o índice mensurado ultrapasse a tolerância, o FD será calculado conforme o item 5.25.6.

5.25.4. No cálculo do FD está previsto uma ponderação para cada indicador de nível de serviço, denominada de Fator de Impacto no Serviço (FIS), com o objetivo de adequar os descontos ao grau de importância daquele indicador no contexto do serviço;

5.25.4.1. O FD de cada indicador será limitado à porcentagem representada pelo FIS aplicada ao valor mensal da prestação do serviço.

5.25.5. O FIS será utilizado nas situações em que a meta exigida para o indicador não for efetivamente atingida. Nos casos em que a meta exigida for atingida não haverá abatimento;

5.25.6. No valor mensal do serviço será abatido o FD calculado para cada resultado de indicador não alcançado:

$$FD_{indicador} = Valor\ Mensal \times \frac{FIS_{indicador}}{100} \times \frac{\left| Meta_{indicador} - Resultado_{indicador} \right|}{Meta_{indicador}}$$

$$FD_{total} = \sum_{i=1}^{max(indicadores)} FD_i$$

5.25.7. Não há previsão de bônus ou pagamentos adicionais para os casos em que a contratada superar as metas previstas, ou caso seja necessária a alocação de maior número de profissionais para o alcance das metas;

5.25.8. A superação de uma das metas não poderá ser utilizada para compensar o não atendimento de outras metas no mesmo período, nem o não atendimento da mesma meta em outro período;

5.25.9. Todos os indicadores que dependem de amostra para cálculo serão mensurados com método aleatório de escolha do espaço amostral definido pela CONTRATANTE e serão aferidos com nível de confiança de 90% e margem de erro de 5%.

5.25.10. A CONTRATANTE comunicará a CONTRATADA sobre o recebimento definitivo a fim de possibilitar a emissão da nota fiscal, informando os valores correspondentes às glosas.

5.25.11. Os seguintes Indicadores de Nível de Serviço serão considerados:

Item	Indicador de Nível de Serviço	Fórmula de Cálculo	Unidade de Medida	Meta exigida	Fator de Impacto no Serviço (FIS)
1	Tempo médio de triagem de requisições/incidentes	Somatório dos tempos de triagem de requisições e incidentes / Total	minutos	<= 30	10

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		de requisições e incidentes			
2	Tempo médio de resolução de requisições/incidentes de severidade crítica	Somatório dos tempos de resolução de requisições e incidentes de severidade crítica / Total de requisições e incidentes	horas	<= 1	20
3	Tempo médio de resolução de requisições/incidentes de severidade alta	Somatório dos tempos de resolução de requisições e incidentes de severidade alta / Total de requisições e incidentes	horas	<=2	20
4	Tempo médio de resolução de requisições/incidentes de severidade média	Somatório dos tempos de resolução de requisições e incidentes de severidade média / Total de requisições e incidentes	horas	<= 4	15
5	Tempo médio de resolução de requisições/incidentes de severidade baixa	Somatório dos tempos de resolução de requisições e incidentes de severidade baixa / Total de requisições e incidentes	horas	<= 12	10
6	Tempo médio de resolução de requisições de severidade agendado	Somatório dos tempos de resolução de requisições e incidentes de severidade agendado / Total de requisições e incidentes	horas	<= 24	5
7	Índice de informações inconsistentes, incompletas ou com erros de procedimento, cuja responsabilidade seja da contratada, na documentação dos incidentes de segurança	Total de eventos da amostra registradas de modo inconsistente, incompleto ou com erros de procedimento na documentação dos incidentes de segurança / Tamanho da amostra x 100	%	<= 5%	10
8	Índice de informações inconsistentes, incompletas ou com erros de procedimento, cuja responsabilidade seja da contratada, na documentação das lições aprendidas nos incidentes de segurança	Total de eventos da amostra registradas de modo inconsistente, incompleto ou com erros de procedimento na documentação das lições aprendidas / Tamanho da amostra x 100	%	<= 5%	5
9	Índice de qualificação da equipe conforme itens 5.25.13.3, 5.25.13.4 e 5.25.13.5	Total de certificados da equipe / Quantidade de certificados exigidos, contabilizados depois de 90 dias do profissional entrar em operação	%	= 100%	5

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

QUALIFICAÇÃO TÉCNICA

5.25.12. Qualificação Técnica da CONTRATADA:

5.25.12.1. A CONTRATADA deve apresentar, no momento da sua habilitação no processo licitatório, Atestado(s) de Capacidade Técnica (ACT) em nome da licitante e emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado ou estar prestando:

5.25.12.1.1. Fornecimento de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos similar à proposta, em ambiente computacional contendo no mínimo 4.000 (quatro mil) ativos monitorados;

5.25.12.1.2. Fornecimento de serviço de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), em ambiente computacional contendo no mínimo 4.000 (quatro mil) ativos monitorados;

5.25.12.2. Para cada subitem do item 5.25.12.1, serão considerados somatórios de atestados para atingir as quantidades solicitadas.

5.25.13. Qualificação Técnica do Quadro Profissional:

5.25.13.1. A CONTRATADA deve apresentar, no ato da assinatura do contrato, as certificações e documentos listados nos itens 5.20.7.3, 5.20.7.4 e 5.20.7.5 a fim de comprovar a qualificação técnica dos profissionais alocados para a prestação dos serviços.

5.25.13.1.1. A comprovação dos perfis exigidos para os profissionais se dará por meio de documentação das certificações (dentro do período de validade).

5.25.13.2. É de responsabilidade da CONTRATADA dimensionar a quantidade de profissionais para a adequada prestação dos serviços previstos e delimitados por esta especificação, principalmente no que se refere aos acordos de níveis de serviço (item 5.22.5) e metas estabelecidas.

5.25.13.3. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela sustentação da solução, deverão ter certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (Item 01 da contratação).

5.25.13.3.1. O líder técnico (Item 5.11) deve, obrigatoriamente, ter a certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos.

5.25.13.4. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela detecção, notificação e investigação de ataques cibernéticos, deverão ter certificação em segurança ofensiva, detendo, individualmente ou em conjunto, pelo menos 03 (três) das seguintes certificações, contabilizando no máximo 02 (dois) certificados por profissional:

5.25.13.4.1. CompTIA PenTest+;

5.25.13.4.2. EC-Concil Licensed Penetration Tester (LPT);

5.25.13.4.3. IACRB Certified Expert Penetration Tester (CEPT);

5.25.13.4.4. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);

5.25.13.4.5. GIAC Reverse Engineering Malware (GREM);

5.25.13.4.6. Offensive Security Certified Professional (OSCP);

5.25.13.4.7. Ethical Hacking Post Exploitation (EHPX);

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

5.25.13.4.8. Offensive Security Experienced Penetration Tester (OSEP);

5.25.13.4.9. Offensive Security Web Expert (OSWE);

5.25.13.4.10. Certified Red Team Expert (CRTE);

5.25.13.4.11. Offensive Security Certified Expert (OSCE);

5.25.13.4.12. Certified Ethical Hacker (CEH).

5.25.13.5. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela resposta a ataques cibernéticos, deverão ter certificação em segurança defensiva, detendo, individualmente ou em conjunto, pelo menos 03 (três) das seguintes certificações, contabilizando no máximo 02 (dois) certificado por profissional:

5.25.13.5.1. Certified Information Security Manager (CISM);

5.25.13.5.2. GIAC Experienced Cybersecurity Specialist (GX-CS);

5.25.13.5.3. GIAC Reverse Engineering Malware (GREM);

5.25.13.5.4. Ethical Hacking Post Exploitation (EHPX);

5.25.13.5.5. CompTIA Security+;

5.25.13.5.6. CompTIA Advanced Security Practitioner;

5.25.13.5.7. EC-Council Security Analyst (ECSA);

5.25.13.5.8. Certified Information Systems Security Professional (CISSP);

5.25.13.5.9. CompTIA CYSA+ - Cybersecurity Analyst.

5.25.13.6. Deverá ser comprovado vínculo entre os profissionais detentores dos certificados e a CONTRATADA, através de cópia do livro de registro de funcionários ou cópia da carteira de trabalho contendo as respectivas anotações de contrato de trabalho; ou como contratado, por meio de contrato de prestação de serviços.

5.25.13.7. A CONTRATADA deverá promover, no prazo máximo de 03 (três) meses, a atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido a modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

5.25.13.8. A CONTRATANTE se reserva ao direito de realizar auditorias a qualquer tempo para verificar se as competências mínimas solicitadas são atendidas pela CONTRATADA durante toda a vigência do contrato. Desta forma, quando solicitado, a CONTRATADA deverá apresentar os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas.

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo A-1 - Termo de Confidencialidade - Empresa CONTRATADA

TERMO DE CONFIDENCIALIDADE

CONTRATO <SIGLA DO TRIBUNAL> Nº ____/_____

A **<PESSOA JURÍDICA OU FÍSICA CONTRATADA>**, doravante referida simplesmente como CONTRATADA, inscrita no CNPJ/MF sob o número **<NÚMERO DO CNPJ>**, com endereço **<ENDEREÇO>**, neste ato representada pelo **<VÍNCULO DO SIGNATÁRIO COM A CONTRATADA>**, **<NOME DO SIGNATÁRIO>**, nos termos do **<CONTRATO OU TERMO ADITIVO EM QUE FOI PACTUADO O SIGILO>**, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, firmado perante o <TRIBUNAL>, doravante referido simplesmente como CONTRATANTE, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas à CONTRATADA para que possa desenvolver as atividades contempladas especificamente no Contrato nº ___/_____.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação revelada à CONTRATADA.

Subcláusula Segunda - A CONTRATADA reconhece que, em razão da prestação de serviços ao CONTRATANTE, tem acesso a informações que pertencem ao CONTRATANTE, que devem ser tratadas como sigilosas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, em decorrência da execução do contrato, contendo ela ou não a expressão "CONFIDENCIAL".

Subcláusula Primeira - O termo "Informação" abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, senhas, fotografias, plantas, programas de computador, discos, disquetes, fitas, contratos, projetos, outras informações técnicas, jurídicas, financeiras ou comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal do CONTRATANTE, referido no Contrato, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa do CONTRATANTE poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE

As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que seja comprovadamente de conhecimento público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

A CONTRATADA se obriga a manter sigilo de toda e qualquer informação definida como confidencial neste TERMO DE CONFIDENCIALIDADE, utilizando-as exclusivamente para os propósitos do contrato.

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Subcláusula Primeira - A CONTRATADA determinará a observância deste TERMO DE CONFIDENCIALIDADE, bem como a observância e a assinatura do TERMO DE CONFIDENCIALIDADE - COLABORADOR, a todos os seus empregados, prepostos e prestadores de serviço que estejam direta ou indiretamente envolvidos com a execução do contrato.

Subcláusula Segunda - A CONTRATADA obriga-se a informar imediatamente ao CONTRATANTE qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

Subcláusula Terceira - Compromete-se, ainda, a CONTRATADA a não revelar, reproduzir ou utilizar, bem como não permitir que seus empregados, prepostos ou prestadores de serviço revelem, reproduzam ou utilizem, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas no contrato e neste TERMO DE CONFIDENCIALIDADE.

Subcláusula Quarta - A CONTRATADA deve cuidar para que as informações consideradas confidenciais nos termos do presente TERMO DE CONFIDENCIALIDADE fiquem restritas ao conhecimento dos empregados, prepostos ou prestadores de serviço que estejam diretamente envolvidos nas discussões, análises, reuniões e negócios, devendo cientificá-los da existência deste TERMO DE CONFIDENCIALIDADE e da natureza confidencial das informações.

CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES

A CONTRATADA devolverá imediatamente ao CONTRATANTE, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE CONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com o CONTRATANTE.

CLÁUSULA SEXTA - DO DESCUMPRIMENTO

O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação

CLÁUSULA SÉTIMA - DA VIGÊNCIA

Tendo em vista o princípio da boa-fé objetiva, permanece em vigor o dever de sigilo, tratado no presente TERMO DE CONFIDENCIALIDADE, após o término do Contrato.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo CONTRATANTE.

Por estarem de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

São Paulo, ____ de ____________________ de 20____.

<TRIBUNAL>

Nome:	Nome:
Cargo:	Cargo:

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

NOME DA EMPRESA FORNECEDORA

_____	_____
Nome:	Nome:
Cargo:	Cargo:

TESTEMUNHAS:

_____	_____
Nome:	Nome:
CPF/MF.:	CPF/MF.:

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo A-2 – Termo de Confidencialidade - Colaborador da CONTRATADA

TERMO DE CONFIDENCIALIDADE - COLABORADOR

A **<PESSOA FÍSICA OU JURÍDICA>**, doravante referida simplesmente como COLABORADOR, inscrita no CPF/CNPJ sob o número **<NÚMERO DO CPF/CNPJ>**, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas aos empregados, prepostos ou prestadores de serviço de empresas contratadas pelo <TRIBUNAL> (<SIGLA DO TRIBUNAL>), para que possam desenvolver suas atividades institucionais.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação.

Subcláusula Segunda – O COLABORADOR reconhece que tem acesso a informações que pertencem ao <SIGLA DO TRIBUNAL>, que devem ser tratadas como sigilosas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, contendo ela ou não a expressão "CONFIDENCIAL".

Subcláusula Primeira - O termo "Informação" abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, senhas, fotografias, plantas, programas de computador, discos, pen drives, fitas, contratos, projetos, outras informações técnicas, jurídicas,

financeiras ou comerciais, entre outras a que venha o COLABORADOR ter acesso durante ou em razão da execução de suas atividades profissionais.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, o COLABORADOR deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal do <SIGLA DO TRIBUNAL>, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa do <SIGLA DO TRIBUNAL>poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE

As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que:

I - sejam comprovadamente de conhecimento público no momento da revelação, exceto se tal fato decorrer de ato ou omissão do COLABORADOR;

II - já esteja em poder do COLABORADOR, como resultado de sua própria pesquisa, contanto que o COLABORADOR possa comprovar referido fato; ou

III - tenha sido comprovada e legitimamente recebida de terceiros, contanto que o COLABORADOR possa comprovar referido fato.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

O COLABORADOR se obriga a manter sigilo de toda e qualquer informação definida como confidencial neste TERMO DE CONFIDENCIALIDADE, utilizando-as exclusivamente no desempenho de suas atividades profissionais enquanto contratado.

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Subcláusula Primeira - Compromete-se, ainda, o COLABORADOR a não revelar, reproduzir ou utilizar, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas neste documento.

CLÁUSULA QUINTA - DO DESCUMPRIMENTO

O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação.

CLÁUSULA SEXTA - DA VIGÊNCIA

Tendo em vista o princípio da boa-fé objetiva, permanecem em vigor os deveres de sigilo e de não utilização das informações, tratados no presente TERMO DE CONFIDENCIALIDADE, após o término do vínculo contratual.

CLÁUSULA SÉTIMA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo <SIGLA DO TRIBUNAL>.

Por estar de acordo, o COLABORADOR firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

São Paulo, ____ de _____ de 20____.

_____

Nome:

Cargo / Função:

Empresa:

Anexo B

Anexo B – Comprovação de atendimento aos itens da Especificação Técnica		
Item	**Especificação**	**Comprovação de atendimento ao item**
2	**ITEM 1 – Requisitos mínimos da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos**	
2.3	A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos da CONTRATANTE, por meio da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede dos ativos monitorados e do tráfego de rede.	
2.5	A solução permitirá monitorar em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) eventos de segurança cibernética, identificando incidentes relativos a ataques, violações de conformidade e comportamento suspeito nas aplicações, rede e ativos computacionais da CONTRATANTE, compreendendo:	
2.5.1	Analisar, classificar, categorizar, correlacionar e notificar os eventos e incidentes classificados como ameaças à segurança cibernética, ou que sejam considerados relevantes de acordo com diretrizes estabelecidas pela CONTRATANTE;	
2.5.4	Registrar os incidentes no módulo de gestão de incidentes da solução ofertada, cujo acesso deverá estar disponível para a CONTRATANTE.	
2.5.4.1	O módulo de gestão de incidentes deverá ser nativo da solução ofertada ou ser implementado por meio de ferramenta de ITSM (IT Service Management), complementar e integrado à solução ofertada. As funcionalidades do módulo ou da ferramenta devem conter os dados dos alertas, incidentes e chamados além de informações sobre SLA para acompanhamento do tratamento dos chamados.	
2.5.4.1.1	O módulo ou ferramenta deve ser capaz de, minimamente:	
2.5.4.1.1.1	Permitir a criação e acompanhamento de incidentes cibernéticos, de forma manual e automática, com no mínimo as seguintes características:	
2.5.4.1.1.1.1	Sumário do incidente, incluindo título, sumário, detalhes, e a fonte geradora do incidente. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados e, opcionalmente, prioridade e analistas envolvidos;	
2.5.4.1.1.1.2	Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;	
2.5.4.1.1.1.3	Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;	
2.5.4.1.1.1.4	Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;	
2.5.4.1.1.1.5	Permitir inserir evidências coletadas de eventual análise forense de host e rede como um complemento da análise do incidente;	

Anexo B

2.5.4.1.1.1.6	Permitir registrar ações de remediação que incluam contenção, erradicação, educação de usuários e melhorias no programa do SOC;	
2.5.4.1.1.1.7	Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.	
2.5.4.1.1.2	Permitir o recebimento de alertas de segurança, de forma automática, com no mínimo as seguintes características:	
2.5.4.1.1.2.1	Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;	
2.5.4.1.1.2.2	Dados de origem e destino: IPs e portas; quando disponível, informações de contexto de negócio de cada dispositivo de origem e destino: domínios, endereços MAC, nomes dos dispositivos, tipos, unidades de negócio, geolocalização, índices de criticidade e conformidade e proprietários;	
2.5.4.1.1.2.3	Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas.	
2.5.4.1.1.3	Gerar relatórios mensais do acordo de nível de serviço (SLA – Service Level Agreement) dos alertas, incidentes e chamados.	
2.5.4.1.2	O módulo ou ferramenta de ITSM deverá estar licenciado para a CONTRATANTE, devendo ser hospedado em regime SaaS (Software as a Service) pela CONTRATADA, bem como deve estar protegida por autenticação do tipo MFA - Multi-Factor Authentication e acesso criptografado ponto a ponto.	
2.6	A solução deve ser fornecida no modelo Software as a Service (SaaS) permitindo a instalação de múltiplos coletores e agentes on-premises e em nuvem, a fim de realizar a implantação distribuída da arquitetura.	
2.6.1	O fabricante da solução proposta para monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser atestado SOC 2 Type II;	
2.6.9	O console de gerência deve ser acessado via web, de forma segura (HTTPS) e deve possuir compatibilidade com, no mínimo, os seguintes navegadores:	
2.6.9.1	Google Chrome;	
2.6.9.2	Mozilla Firefox.	
2.6.10	O console de gerência deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.	
2.6.10.3	Os ambientes utilizados pela solução (incluindo do fabricante) devem possuir, ao menos, uma cópia das informações localizadas no Brasil.	
2.6.11	O console de gerência deve possuir a capacidade de autenticação multifator (MFA - Multi-Factor Authentication).	
2.7.1	A solução deve suportar picos de EPS (Eventos Por Segundo) ou GB (gigabytes) acima do licenciado em até 30%.	
2.7.1.1	Caso os picos de EPS ou GB ultrapassem o limite de 30%, a solução não deve descartar os eventos de forma que sejam processados posteriormente.	
2.8	A solução deve possuir retenção mínima de 03 (três) meses de registros prontamente acessíveis ("Logs Quentes"). Após este período, a solução deve suportar, no mínimo, 09 (nove) meses de registros arquivados ("Logs Frios") - totalizando 12 (doze) meses de registros - bem como permitir a exportação destes logs/dados de telemetria/de rede para armazenamento em ambiente de propriedade da CONTRATANTE.	
2.8.1	As análises realizadas e alertas devem estar disponíveis de forma integral por pelo menos 06 (seis) meses.	
2.8.2	Deve haver a opção de exportação de logs/dados de telemetria/de rede em formato aberto (plain text) podendo ser abertos e lidos em editores de texto sem a necessidade de softwares proprietários ou plugins.	

Anexo B

2.8.3	A solução não deve possuir mecanismos que limitem ou onerem a CONTRATANTE com base na quantidade/volume de dados a serem exportados.	
2.9	A solução deve possuir capacidade de monitorar e identificar o comportamento de usuários que representar ameaça (UEBA - User and Entity Behavior Analytics), em nível de ativos monitorados ou em nível de logs de eventos, do Microsoft Active Directory e do Open LDAP, monitorando diferentes vetores de ataque, como:	
2.9.1	Movimentação lateral com uso de credenciais locais de máquina;	
2.9.2	Ataques de força bruta em contas locais de máquinas;	
2.9.3	Usuários locais que tentam apagar arquivos de evento dos registros da máquina.	
2.9.4	Adicionalmente, para ambientes com Microsoft Active Directory:	
2.9.4.1	Movimentação lateral com uso de credenciais de domínio;	
2.9.4.2	Ataques de força bruta em contas de domínio;	
2.9.4.3	Usuários de domínio que tentem apagar arquivos de evento dos registros da máquina;	
2.10	A solução deve permitir, para ambientes com Microsoft Active Directory, monitorar ações de todos os usuários, permitindo campanhas de caças a ameaças, auditoria e criação de alertas para usuários específicos.	
2.11	A solução deve monitorar qualquer tipo de acesso de usuário:	
2.11.1	Em máquinas com credenciais locais – monitoramento com uso de agente da própria solução ou de terceiros;	
2.11.2	Com credenciais do domínio – monitoramento do Microsoft Active Directory;	
2.11.3	Ingress Authentication – como VPN, Google Workspace/Google Apps e Office 365;	
2.11.3.1	Para autenticações vindas de fora do ambiente – Ingress Authentication – a solução deve identificar e correlacionar a informações da origem do acesso – minimamente data, hora e IP.	
2.12	A solução deve suportar IPv4 ou IPv4/IPv6.	
2.13	Para detectar incidentes, a solução deverá implementar o recebimento e análise de logs, dados de telemetria e/ou de rede de, no mínimo:	
2.13.1	Firewalls;	
2.13.2	Web Application Firewalls;	
2.13.3	IPS (Intrusion Prevention System) / IDS (Intrusion Detection System);	
2.13.4	Web filtering;	
2.13.5	Antivírus;	
2.13.6	Microsoft Active Directory;	
2.13.7	Open LDAP;	
2.13.8	IAM (Identity and Access Management) / PAM (Privileged Access Management);	
2.13.9	Servidores HTTP (HTTP Servers);	
2.13.10	Balanceadores de Carga (Load Balancers);	
2.13.11	DNS;	
2.13.12	DHCP;	
2.13.13	ELK Stack;	
2.13.14	Sistemas Operacionais.	
2.14	A solução que fizer uso de parsers para análise dos dados recebidos deve permitir a ingestão de fontes de eventos por meio de, no mínimo, o protocolo Syslog.	
2.14.1	A solução deve permitir a leitura de logs e arquivos nos formatos CSV, XML, JSON e texto puro, de forma a permitir a inclusão de outras fontes de evento que não tenham conectores nativos.	

Anexo B

2.14.2	A solução deve possuir módulo nativo (já incluso) para realização de parsers customizados.	
2.14.2.1	A solução deve permitir utilização de expressões regulares (regex) nos parsers.	
2.14.2.2	A solução deve prover identificação de eventos com erro de parsing e de eventos sem suporte de coleta.	
2.15	A solução deve ter funcionalidade de coleta de eventos de auditoria de bancos de dados por meio de conectores nativos, coleta de logs, dados de telemetria e/ou de rede.	
2.16	Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede, provendo as seguintes informações, no mínimo:	
2.16.1	Sistemas com maior atividade baseada em volume de tráfego;	
2.16.2	Principais aplicações e protocolos trafegados, baseado em volume de dados enviados e recebidos entre endpoints da rede;	
2.16.3	Atividades de rede baseada em porta de destino e endereços de origem e destino;	
2.16.4	Relação dos usuários ou ativos que mais consomem banda de rede, baseado em volume de tráfego.	
2.16.5	Servidores DNS em uso;	
2.16.6	Relação das principais aplicações em uso na rede;	
2.16.7	Identificação de picos de consumo de banda de acesso à rede;	
2.16.8	Relação de dispositivos, servidores e serviços que operam na rede.	
2.17	A solução deve implementar a coleta e análise de diferentes fontes de eventos. A coleta deve ser realizada para logs, dados de telemetria e/ou de rede, devendo ser possível coletar e analisar eventos das seguintes soluções presentes atualmente de forma predominante no ambiente da CONTRATANTE:	
2.17.1	De forma nativa (sem a necessidade de customização de parsers):	
2.17.1.1	Checkpoint para proteção de perímetro (Firewall);	
2.17.1.2	Fortinet FortiGate para proteção de perímetro (Firewall);	
2.17.1.3	Forcepoint para proteção de perímetro (Firewall);	
2.17.1.4	Microsoft Active Directory para serviços de diretório.	
2.17.2	De forma nativa (sem a necessidade de customização de parsers) ou não:	
2.17.2.1	Open LDAP para serviços de diretório;	
2.17.2.2	OpenVPN;	
2.17.2.3	Citrix;	
2.17.2.4	RDP e RDPWeb;	
2.17.2.5	Senha Segura para serviços de gerenciamento de acesso privilegiado;	
2.17.2.6	Cyberark para serviços de gerenciamento de acesso privilegiado	
2.17.2.7	Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;	
2.17.2.8	Keycloak para gerenciamento de identidade e acesso;	
2.17.2.9	midPoint para segurança de identidades (identity security);	
2.17.2.10	ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);	
2.17.2.11	Loqed;	
2.17.2.12	Varonis;	
2.17.2.13	IBM Spectrum Protect Plus para proteção de dados;	
2.17.2.14	Kaspersky para proteção de endpoint;	
2.17.2.15	Blackberry Cylance para proteção de endpoint.	

Anexo B

2.17.2.16	Check Point Harmony para proteção de endpoint;	
2.17.2.17	Tenable One para gerenciamento de exposição (exposure management platform);	
2.17.2.18	Tenable.ep / Nessus para gerenciamento de vulnerabilidades;	
2.17.2.19	Tenable.ad para proteção do Active Directory;	
2.17.2.20	Trivy para varredura de vulnerabilidades;	
2.17.2.21	VMware/vCenter para virtualização de máquinas;	
2.17.2.22	VMware/Horizon para virtualização de estações de trabalho;	
2.17.2.23	Hyper-V para virtualização de máquinas;	
2.17.2.24	Ovirt para virtualização de máquinas;	
2.17.2.25	Docker e Kubernetes;	
2.17.2.26	Apache HTTP Server;	
2.17.2.27	HAProxy;	
2.17.2.28	Ingress;	
2.17.2.29	Nginx;	
2.17.2.30	Switches Cisco MDS;	
2.17.2.31	Switches H3C;	
2.17.2.32	Switches HP;	
2.17.2.33	Switches Huawei;	
2.17.2.34	Roteadores Cisco;	
2.17.2.35	Roteadores Juniper;	
2.17.2.36	Roteadores MikroTik;	
2.17.2.37	Access Points Aruba;	
2.17.2.38	Access Points Ruckus;	
2.17.2.39	Controladoras Virtuais Aruba;	
2.17.2.40	Bacula para serviços de backup;	
2.17.2.41	Commvault (software de backup);	
2.17.2.42	Veeam (software de backup);	
2.17.2.43	Storage Huawei;	
2.17.2.44	Storage IBM;	
2.17.2.45	TSM Server IBM Spectrum Protect para serviços de backup;	
2.17.2.46	Dell EMC Data Domain;	
2.17.2.47	Dell EMC Isilon.	
2.18	A solução deve ser capaz de coletar e processar fontes de eventos oriundas dos seguintes serviços de Cloud:	
2.18.1	De forma nativa (sem a necessidade de customização de parsers):	
2.18.1.1	AWS CloudTrail, via SQS ou API;	
2.18.1.2	Google Cloud Platform, via API;	
2.18.1.3	Google Workspace/Google Apps, via API;	
2.18.1.4	Microsoft Office 365, via API.	

Anexo B

2.19	A solução deve suportar e implementar a coleta e o processamento de fontes de eventos oriundas, no mínimo, dos seguintes sistemas operacionais. Para as soluções que fazem uso de agentes ou outro software externo/nativo do sistema operacional, eles devem ser compatíveis com as versões 32 e 64 bits dos sistemas operacionais (quanto existirem). Caso a solução não faça uso de agentes, os dados devem ser obtidos por meio da coleta do tráfego de rede.	
2.19.1	De forma nativa (sem a necessidade de customização de parsers):	
2.19.1.1	Windows 7;	
2.19.1.2	Windows 8.1;	
2.19.1.3	Windows 10;	
2.19.1.4	Windows 11;	
2.19.1.5	Windows Server 2008 R2;	
2.19.1.6	Windows Server 2012;	
2.19.1.7	Windows Server 2012 R2;	
2.19.1.8	Windows Server 2016;	
2.19.1.9	Windows Server 2019;	
2.19.1.10	Windows Server 2022;	
2.19.1.11	Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;	
2.19.1.12	Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;	
2.19.1.13	Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;	
2.19.1.14	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;	
2.19.1.15	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;	
2.19.1.16	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;	
2.19.1.17	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;	
2.19.1.18	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;	
2.19.1.19	Amazon Linux;	
2.19.1.20	Debian Linux;	
2.19.1.21	Ubuntu Linux.	
2.20	Para os itens 2.13, 2.17, 2.18 e 2.19, as listas de soluções são do tipo "não exaustivas", devendo ser considerada pela CONTRATADA, por meio de configuração da solução, a possibilidade de inclusão ou alteração de produtos em decorrência da evolução do parque tecnológico da CONTRATANTE.	
2.21	A solução deve ser capaz de detectar comportamentos caracterizados como maliciosos de acordo com o MITRE ATT&CK Framework levando-se em consideração os dados recebidos dos ativos monitorados e gerados pelo coletor de tráfego de rede.	
2.22	A solução deve cobrir detecções nativas de, ao menos, os grupos de atacantes categorizados pelo MITRE ATT&CK.	
2.23	A solução deverá informar com qual técnica e tática do MITRE ATT&CK Framework o ataque está relacionado, além de possuir link direto para o site da organização.	
2.24	A solução deve possuir de maneira nativa detecções de, no mínimo, os seguintes vetores de ataque:	
2.24.1	Requisição a domínio suspeito;	
2.24.2	Execução de processos suspeitos;	
2.24.3	Requisição de dados de registro do sistema de nome de domínio (DNS);	
2.24.4	Comunicação com servidores Command & Control;	
2.24.5	Tentativa de desabilitar recursos de Sysmon;	

Anexo B

2.24.6	Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;	
2.24.7	Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;	
2.24.8	Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;	
2.24.9	Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;	
2.24.10	Detecção de execução do Mimikatz e variações;	
2.24.11	Detecção de processos que utilizam resultados do comando wget via Bash, Perl e Python;	
2.24.12	Detecção de tentativas de criação de reverse shells para Command & Control.	
2.25	A solução deve possuir a capacidade de identificar e monitorar o comportamento de atacantes baseados em IoC's (Indicators of Compromise) do próprio fabricante e de terceiros (threat intelligence).	
2.26	A solução deve possuir listas de terceiros com informações de IoC's com, no mínimo, IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.	
2.27	A solução deve possuir a capacidade de integração e/ou ingestão de dados de outras ferramentas de threat intelligence, de maneira manual ou por API, importando arquivos com base CSV ou STIX (Structured Threat Information Expression), através de assinatura de feeds de inteligência de ameaças de terceiros, aceitando, no mínimo, os seguintes tipos: IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.	
2.28	A solução deve disponibilizar informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações.	
2.29	A solução deve permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence).	
2.30	A solução deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar na defesa proativa contra ameaças.	
2.30.1	A solução deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e de terceiros para ajudar na identificação de ameaças.	
2.30.2	Após análise dos relatórios de ameaças pela CONTRATADA, deverá ser feita uma investigação dentro do ambiente computacional da CONTRATANTE e registrado um incidente caso sejam identificadas atividades presentes nos relatórios.	
2.30.3	Cada relatório deve possuir, no mínimo, informações como: região/país alvo, plataforma alvo e campanhas de ataques relacionadas aos dados do relatório.	
2.31	A solução deve possuir nativamente a capacidade de "deception" ou permitir que se implemente capacidade similar por meio de ferramenta complementar e integrada a solução proposta, possibilitando a marcação de ativos, credenciais, usuários e arquivos específicos como sendo "iscas" a fim de, quando acessados, gerarem alertas, facilitando o monitoramento e auditoria contínuos.	
2.31.1	Honeypot: máquina projetada para capturar informações sobre tentativas de acesso e exploração. Deve permitir a instalação de, ao menos, 05 (cinco) máquinas no ambiente;	
2.31.1.1	Os honeypots devem ser fornecidos em formato OVA – virtual appliance.	
2.31.2	Honey Credential: configuração de um conjunto de credenciais falsas na memória de um ativo;	
2.31.3	Honey User: usuário falso que não está associado a uma pessoa real dentro da organização e, portanto, nunca deve ser acessado – monitoramento do Microsoft Active Directory;	
2.31.4	Honey File: arquivo falso localizado em um compartilhamento de arquivos de rede.	
2.31.5	A solução deve ser capaz de detectar o vetor de entrada da ameaça na rede, identificar o caminho utilizado pelo invasor até o ativo, credencial, usuário ou arquivo específico e apresentar as vulnerabilidades exploradas no ativo (quando for o caso).	

Anexo B

2.32	Quando a solução não possuir capacidade de “deception”, a capacidade de “Breach and Attack Simulation” (BAS) pode ser apresentada, com os seguintes critérios mínimos:	
2.32.1	Caso a funcionalidade seja oferecida como um serviço, as licenças necessárias para a sua execução devem ser baseadas em vetores ou agentes, sendo um para cada tipologia: infraestrutura, network e e-mail; os 03 (três) tipos de licenças devem estar incluídas sem custos adicionais para a CONTRATANTE;	
2.32.3	Deve ser executado de forma automatizada, simulando ataques reais, mas que não coloquem em risco o ambiente computacional da CONTRATANTE;	
2.32.4	As simulações devem utilizar diferentes vetores de ataque;	
2.32.5	O serviço deve gerar um relatório mensal que indique como corrigir os problemas que venham a ser encontrados.	
2.33	A solução que fizer uso de agentes deve permitir sua instalação de forma “silenciosa” nos ativos a serem monitorados.	
2.34	A solução deve possuir as funcionalidades de:	
2.34.1	Monitoramento de comportamento (behavior monitor);	
2.34.2	Controle de aplicação;	
2.34.3	Monitoramento de eventos;	
2.34.4	Auditoria de alterações no sistema;	
2.34.5	Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.62.	
2.35	A solução deve monitorar os ativos em tempo real, estando eles dentro ou fora do domínio.	
2.36	Os agentes devem poder coexistir com outras soluções de proteção, como antivírus, instaladas nos ativos monitorados sem que gerem conflito nem incompatibilidade entre os softwares.	
2.37	Os agentes devem executar de maneira que não haja impacto na performance ou disponibilidade dos ativos monitorados.	
2.38	Os agentes e os coletores devem, em caso de desconexão com o console, manter as informações sendo coletadas a fim de serem enviadas quando a conexão for restabelecida.	
2.39	Os agentes e coletores devem enviar os dados para o console de maneira:	
2.39.1	Segura e criptografada;	
2.39.2	Que não haja impacto na performance ou disponibilidade da rede da CONTRATANTE.	
2.40	Os agentes e coletores, ao enviarem os dados para o console, não devem degradar o tráfego de saída da rede da CONTRATANTE.	
2.41	A solução deve monitorar, no mínimo:	
2.41.1	Força bruta no ativo (brute force – asset);	
2.41.2	Força bruta em conta local (brute force – local account);	
2.41.3	Detecção de evasão - Deleção de log de evento (detection evasion – event log deletion);	
2.41.4	Detecção de evasão - Deleção de log de evento local (detection evasion – local event log deletion);	
2.41.5	Correspondência de Threat Intel (endpoint threat intelligence match);	
2.41.6	Exploração mitigada (exploit mitigated);	
2.41.7	Hash sinalizado no ativo (flagged hash on asset) - a solução deve permitir cadastrar um hash qualquer para gerar um alerta quando for acessado no ativo;	
2.41.8	Processo sinalizado no ativo (flagged process on asset);	
2.41.9	Exploração de elevação de privilégio Kerberos (kerberos privilege elevation exploit);	

Anexo B

2.41.10	Movimentação lateral com personificação de administrador local (lateral movement – local administrator impersonation);	
2.41.11	Movimentação lateral com credenciais locais (lateral movement – local credentials);	
2.41.12	Tentativa de escalação de privilégio em honey credential local (local honey credential privilege escalation attempt);	
2.41.13	Hash malicioso no ativo (malicious hash on asset) - a solução deve gerar um alerta quando um hash já conhecido como malicioso é acessado no ativo;	
2.41.14	Criação de nova conta de usuário local (new local user account created);	
2.42	A solução deve ser capaz de fornecer uma listagem dos ativos sendo monitorados.	
2.43	A solução deve ser capaz de fornecer uma listagem dos ativos que estejam se comunicando no ambiente computacional da CONTRATANTE e que não estejam sendo monitorados.	
2.44	A solução deve ser capaz de identificar acessos a URLs maliciosas além das portas padrão 80 e 443.	
2.44.1	A solução deverá permitir classificar alertas relacionados a URLs em exceção para redução de falsos-positivos.	
2.45	A solução deve correlacionar logs e/ou dados de telemetria/de rede dos ativos monitorados para:	
2.45.1	Identificar comportamentos anômalos que aconteçam localmente no ativo monitorado;	
2.45.2	Identificar quais eventos devem gerar alertas;	
2.45.3	A solução deverá permitir classificar alertas relacionados a usuários e ativos em exceção para redução de falsos-positivos.	
2.46	O console de correlacionamento deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.	
2.47	A solução deve fazer uso de inteligência de ameaças do fabricante para analisar e correlacionar os dados recebidos.	
2.48	A solução deve detectar ameaças conhecidas usando casos de uso de detecção constantemente atualizados, e desconhecidas por meio de conjuntos de dados aprendidos.	
2.49	A solução deve prover funcionalidade de detecção de padrões em eventos coletados:	
2.49.1	A solução deve prover detecção de padrões de ataque em todas as suas fases, com base no modelo Cyber Kill Chain, MITRE ou NIST;	
2.50	A solução deve permitir a criação de alertas customizados baseados em um comportamento específico ou em um contexto de combinação de eventos.	
2.51	Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:	
2.51.1	Crítico;	
2.51.2	Alto;	
2.51.3	Médio;	
2.51.4	Baixo.	
2.52	A solução deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.	
2.53	A solução deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque.	
2.54	A solução deve permitir a visualização da correlação entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque.	

Anexo B

2.55	A solução deve permitir o encerramento remoto de processos ativos executados nas estações de trabalho e servidores sob sua gestão.	
2.56	A solução deve ser capaz de isolar uma estação de trabalho, desconectando-a da rede e permitindo se comunicar exclusivamente com a central da solução.	
2.56.1	A solução deve ser capaz de restaurar a conectividade da estação de trabalho com a rede.	
2.57	A solução deve ser capaz de realizar as ações dos itens 2.55. e 2.56. sem a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente (caso a solução faça uso) não possa ser instalado com direitos administrativos.	
2.58	A solução deve possuir a capacidade de monitorar a integridade de arquivos (FIM – File Integrity Monitoring) nos servidores monitorados.	
2.58.1	Nativamente, para os seguintes formatos de arquivos, no mínimo:	
2.58.1.1	.bat	
2.58.1.2	.cfg	
2.58.1.3	.conf	
2.58.1.4	.config	
2.58.1.5	.dll	
2.58.1.6	.exe	
2.58.1.7	.ini	
2.58.1.8	.sys	
2.58.2	A solução deve permitir a inclusão de novos formatos de arquivos diferentes dos nativos.	
2.59	Para realizar o monitoramento do tráfego de rede, a solução deve ser do tipo passiva e ser instalada em modo off-line na rede, ou seja, não ser um ativo em linha ou permitir o envio de logs e/ou dados de telemetria/de rede através de integração.	
2.60	A solução deve ser capaz de inspecionar o tráfego de rede baseado no volume de tráfego em Gbps da CONTRATANTE e realizar a análise dos dados coletados.	
2.61	A solução deve, junto com o monitoramento do tráfego de rede (ou por meio de agentes), implementar regras de detecção de intrusão para correlacionar e trazer as informações sobre possíveis anomalias e ataques no nível de rede.	
2.61.1	A solução deve permitir a criação de regras e/ou fornecer um conjunto de regras pré-definidas.	
2.61.1.1	No caso da solução possuir regras pré-definidas, deve haver sua atualização periódica cobrindo as informações de novas ameaças.	
2.62	A solução deve possuir funcionalidade de automação na resposta de incidentes com playbooks de resposta já funcionais, devendo suportar, no mínimo, a automação das seguintes tarefas:	
2.62.1	Envio de e-mails.	
2.62.2	Com a utilização de agentes (não deve haver a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente não possa ser instalado com direitos administrativos) ou outro mecanismo que a solução utilize para a automação:	
2.62.2.1	Isolamento de uma máquina – caso seja detectado uma ameaça ou comportamento anômalo em uma máquina, deve ser possível isolá-la da rede;	
2.62.2.2	Encerrar um processo malicioso – caso o agente detecte algum processo malicioso na máquina, a solução deve ter a capacidade de finalizar esse processo;	
2.62.3	Com integrações para as soluções nativas indicadas no item 2.17.1:	
2.62.3.1	Alertas relacionados a usuários do Microsoft Active Directory – se um alerta for gerado associado a uma credencial de domínio, a solução deve desabilitar o usuário para conter a ameaça de maneira rápida;	

2.62.3.2	Sugerir e/ou criar regras no firewall – se um alerta for gerado associado a uma consulta DNS a um domínio considerado malicioso, a solução deve possibilitar a criação de regras de bloqueio no firewall ou sugerir qual regra deve ser criada para tal.	
2.62.4	A solução deve permitir que cada tarefa nos playbooks de resposta de incidentes possa ser configurada de forma a:	
2.62.4.1	Ser totalmente automática;	
2.62.4.2	Aguardar uma interação humana para ser realizada.	
2.63	Em casos de identificação de uma ameaça, a solução deve ter a capacidade de bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional ou demais aplicações instaladas no ativo.	
2.64	A solução deve conter regras pré-definidas para detecção de ransomware e as principais famílias deste tipo de malware.	
2.65	A solução deve possuir módulo de investigação e detecção integrados.	
2.66	A solução deve apresentar os alertas de ameaças consolidados e correlacionados para melhor investigação e resposta aos incidentes.	
2.67	A solução deve permitir configuração de notificações por e-mail (SMTP) e Webhooks (do Google Workspaces, no mínimo) para envio de alertas e notificações.	
2.67.1	As notificações podem ser nativas ou, caso necessário, serem desenvolvidas pela CONTRATADA, sem custo para a CONTRATANTE, para viabilizar sua integração.	
2.68	A solução deve permitir que as detecções sejam correlacionadas com dados recebidos dos ativos monitorados.	
2.69	A solução deve, através dos dados do alerta, permitir a criação de um incidente e vinculá-lo ao alerta, possibilitando a definição da gravidade do incidente com dados de gravidade da fonte do alerta.	
2.70	A solução deve permitir visualizar uma lista de incidentes e suas descrições, solicitar enriquecimentos e executar ações sobre os incidentes.	
2.71	A solução deve criar uma linha do tempo (timeline) do ataque detectado, incluindo as evidências sobre cada alerta gerado e informando qual ativo gerou aquela evidência.	
2.71.1	A solução deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho.	
2.72	A solução deve ser capaz de classificar a relevância dos eventos, minimamente, em “crítico”, “alto”, “médio” e “baixo”.	
2.73	A solução deve permitir a alteração do status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma.	
2.74	A solução deve permitir visualizar as atividades suspeitas de forma a sinalizar a causa raiz, seguindo as categorias do MITRE ATT&CK.	
2.75	A solução deve permitir investigar os alertas gerados pelos modelos de detecção por meio de análise de impacto e análise de causa raiz.	
2.75.1	Deve ser possível ativar ou desativar qualquer modelo de detecção.	
2.75.2	A solução deverá possuir todos os módulos de detecção completamente licenciados, sem custo para a CONTRATANTE, independentemente da quantidade de modelos de detecção que venham a ser disponibilizados futuramente.	
2.76	A solução deve permitir a criação de listas de exceção de objetos para redução de falsos-positivos.	
2.77	A solução deve adicionar os logs, dados de telemetria e/ou de rede coletados/correlacionados aos incidentes/alertas detectados.	
2.78	A solução deve permitir o registro de incidentes por demanda, sem a necessidade de a própria solução ter gerado um alerta.	
2.79	A solução deve possibilitar que, para cada incidente gerado, um analista seja vinculado ao incidente e que ele possa criar anotações sobre como está a evolução da resposta deste incidente;	

Anexo B

2.80	A solução deve permitir que incidentes possam ser fechados após atividades serem encerradas, permitir marcação como falsos positivos e, também, que possam ser reabertos.	
2.81	A solução deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, indicando criticidade e níveis de prioridade.	
2.81.1	A classificação quanto ao nível de criticidade deve ser baseada nas regras do MITRE.	
2.82	A solução deve ter a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções.	
2.83	A solução deve permitir realizar buscas e filtros de objetos para possibilitar pesquisas e análises avançadas.	
2.84	A solução deve possibilitar a interação com cada um dos objetos relacionados ao evento para análise avançada e resposta.	
2.84.1	Ao clicar em quaisquer dos objetos, a solução deve permitir a realização de buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.	
2.85	A solução deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar, categorizar e recuperar os resultados da pesquisa.	
2.86	A solução deve permitir a realização de buscas através de strings parciais, exatas, valores nulos, coringas (wildcards) e caracteres especiais.	
2.87	A solução deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.	
2.88	A solução deve permitir a criação de dashboards e relatórios baseados em bibliotecas prontas ou, também, criar do zero.	
2.88.1	Deve possuir dashboards pré-configurados e permitir sua customização ou mesmo a criação de novos para refletir necessidades específicas da CONTRATANTE.	
2.88.2	Deve fornecer a possibilidade de criação de relatórios e dashboards para dados de todas as fontes de dados ingeridas (endpoints, rede, e-mail, nuvem, etc.), seja por meio de criação de consultas (queries) ou a partir de cliques com o mouse.	
2.88.3	Deve possuir dashboards pré-configurados que permitam a visualização executiva dos principais incidentes e atividades no ambiente com base em usuários, aplicações acessadas e estações de trabalho/servidores.	
2.88.4	Deve possuir, ao menos, 15 (quinze) dashboards em sua biblioteca, incluindo dashboards de fácil visualização de:	
2.88.4.1	Alertas e incidentes mais frequentes;	
2.88.4.2	Nível de risco do ambiente;	
2.88.4.3	Relatório dos últimos 30 (trinta) dias da detecção de incidentes;	
2.88.4.4	Top 10 (dez) ativos com incidentes;	
2.88.4.5	Os ativos que mais sofreram incidentes em um determinado período;	
2.88.4.6	Os usuários que mais sofreram incidentes em um determinado período;	
2.88.4.7	Ativos e contas descobertas;	
2.88.4.8	Ameaças descobertas e classificadas conforme a cadeia de ataque.	
2.88.5	Deve permitir configuração de atualização do tempo de cada dashboard.	
2.88.6	Deve permitir exportação dos relatórios para os seguintes formatos:	
2.88.6.1	Planilha: CSV e/ou Excel;	
2.88.6.2	Texto: HTML e/ou PDF.	
2.89	A solução deve permitir o gerenciamento de usuários, funções e permissões.	
2.90	A solução deve permitir a criação de usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações.	

Anexo B

2.91	A solução deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo do console.	
2.92	A solução deve registrar todas as atividades efetuadas pelos seus usuários, permitindo auditoria das ações realizadas.	
2.93	A solução deve disponibilizar APIs, com documentação e sem custo adicional, para integração com outras soluções.	
	MONITORAMENTO DEEP/DARK WEB (MONITORAMENTO DE MARCA E AMEAÇAS GLOBAIS)	
2.94	A CONTRATADA deverá realizar serviços de monitoramento de Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar). Os serviços e a respectiva solução utilizada para a realização do monitoramento de Deep/Dark Web devem atender às seguintes especificações mínimas:	
2.94.1	A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas à CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis.	
2.94.2	A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 06 (seis) domínios DNS da CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.	
2.94.3	O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana).	
2.94.4	A solução de monitoramento de Deep/Dark Web deve realizar buscas, no mínimo:	
2.94.4.1	Na Darknet;	
2.94.4.2	Em plataformas de compartilhamento de documentos;	
2.94.4.3	Pelas seguintes categorias:	
2.94.4.3.1	Por Bucket: Darknet TOR, Whois, Usenet, Leaks, Bot Logs, Wikileaks, Public Leaks, Dumpster, Sci-Hub;	
2.94.4.3.2	Por Site Público: .com, .org, .net, .info, .eu.	
2.94.4.3.3	Por Geolocalização.	
2.94.5	A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos considerando, no mínimo, as seguintes categorias:	
2.94.5.1	Domínio DNS;	
2.94.5.2	Endereço de e-mail;	
2.94.5.3	Endereço Bitcoin;	
2.94.5.4	Endereço Ethereum;	
2.94.5.5	Endereço MAC;	
2.94.5.6	Hash IPFS;	
2.94.5.7	IBAN (Número de Conta Bancária Internacional);	
2.94.5.8	IP e CIDR;	
2.94.5.9	Número de telefone;	
2.94.5.10	Número do cartão de crédito;	
2.94.5.11	URL.	
2.94.6	Deve detectar resultados de itens pesquisa duplicados, apresentando-os de forma consolidada, otimizando a busca por informações relevantes.	
2.94.7	A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados pelo período mínimo de 1 ano.	
2.94.8	A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:	

Anexo B

2.94.8.1	Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);	
2.94.8.2	Com base nos domínios, e-mails e URLs encontrados;	
2.94.8.3	Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;	
2.94.8.4	Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.	
2.94.9	A solução de monitoramento de Deep/Dark Web deve ter a capacidade de manter históricos de resultados de busca.	
2.94.10	A solução de monitoramento de Deep/Dark Web deve contemplar os seguintes itens:	
2.94.10.1	Monitoramento de atividades na Deep/Dark Web relacionadas às informações sobre domínios, URLs, IPs, hashes, credenciais, e-mails e informações sensíveis da CONTRATANTE.	
2.94.10.2	Amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web como:	
2.94.10.2.1	Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;	
2.94.10.2.2	Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;	
2.94.10.2.3	Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;	
2.94.10.2.4	Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC's;	
2.94.10.2.5	Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.	
2.94.10.3	Deve ser possível encontrar marketplaces, fóruns e agentes de ameaças;	
2.94.10.4	Deve ser capaz de realizar avaliação da exposição da marca e vazamentos de informações na Deep/Dark Web;	
2.94.10.5	Investigação de origens de vazamentos de, no mínimo:	
2.94.10.5.1	Grupos de hackers;	
2.94.10.5.2	Ameaças em fóruns;	
2.94.10.5.3	Salas de chats reservadas;	
2.94.10.5.4	Carteira de bitcoins e endereços;	
2.94.10.5.5	Registros históricos.	
2.94.10.7	Geração e notificação de alertas acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.	
2.95	A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado neste documento.	