À SECRETARIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO

TERMO DE REFERÊNCIA

CAPÍTULO 1 – TERMOS GERAIS

1. DO OBJETO (ART. 6º, XXIII, A)

1.1. DEFINIÇÃO DO OBJETO

Solução de TI consistente em serviços gerenciados de Segurança da Informação e Cibernética (MSS), com prestação contínua e sob demanda, aplicados ao ambiente tecnológico do Tribunal de Justiça do Estado do Paraná, pelo período de 36 (trinta e seis) meses prorrogável até o limite legal.

1.2. GLOSSÁRIO

Para fins deste Termo de Referência será utilizado ANEXO I - GLOSSÁRIO DE TERMOS.

1.1. ESPECIFICAÇÃO DETALHADA DO OBJETO

	Item	Categoria	Descrição	Qtde	Tipo
Grupo 01	**1**	**Projeto e implantação**		01	Unitário
	2	**Serviços de Governança e Conformidade de Segurança**			
		2.1	Diagnóstico de Maturidade de Segurança da Informação	03	Unitário
		2.2	Política de Segurança da Informação (PSI)	33	Mês
		2.3	Plano de Continuidade de Serviços Essenciais de TIC	33	Mês
		2.4	Plano de Resposta a Incidentes (PRI)	33	Mês
	3	**Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança**			
		3.1	Serviço de Security Operations Center (SOC)	825.000	Ativos protegidos
		3.2	Proteção contra Riscos Digitais (Threat Intelligence)	33	Mês
		3.3	Serviço de Takedown	60	Takedown executado
	4	**Sustentação de Operações de Soluções e Resposta a Requisições de Segurança**			
		4.1	Solução de Firewall	198	Ativos protegidos
		4.2	Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)	660.000	Ativos protegidos
	5	**Gestão de Vulnerabilidades e Testes de Segurança**			
		5.1	Gerenciamento Contínuo de Vulnerabilidades	33	Mês
		5.2	Testes de Segurança Automatizados (BAS)	990	Baterias realizadas
	6	**Gestão de Identidade**			
		6.1	Gerenciamento de Acesso Privilegiado (PAM)	2.640	Usuários administrativos protegidos
	7	**Serviços Técnicos Especializados por Demanda**		1.200	Horas sob demanda
Item Avulso	**8**	**Serviço de Teste de Invasão (Pentest)**		360	Horas sob demanda

Tabela 1 - Quadro de Especificação Detalhada do Objeto

É vedada a contratação de uma mesma empresa para o Grupo 01 e o item 8, devido à natureza dos serviços a serem contratados, que exige independência e autonomia entre os prestadores, sendo necessária a participação de empresas distintas que não tenham qualquer relação ou subordinação entre si, para garantir integridade e confiabilidade dos resultados pretendidos.

A CONTRATADA deverá possuir certificação ISO/IEC 27.001 vigente na contratação, emitida em nome da CONTRATADA por organização independente acreditada pelo Inmetro ou por autoridade equivalente globalmente reconhecida.

1.2. NATUREZA DO OBJETO

Trata-se da contratação de empresa especializada em serviços gerenciados de Segurança da Informação e Cibernética, usuais no mercado, oferecidos por fornecedores e empresas especializadas e passíveis de serem definidos de forma objetiva. Portanto, o objeto em questão se enquadra na definição de bens e serviços comuns, conforme a Decreto Estadual nº 10.086/2022.

Esta contratação tem natureza de serviço comum, de caráter continuado e sem fornecimento de mão-de-obra em regime de dedicação exclusiva.

2. FUNDAMENTOS DA CONTRATAÇÃO (ART. 6º, XXXIII, B)

2.1. NECESSIDADE DA CONTRATAÇÃO

O Poder Judiciário vem avançando tecnologicamente a cada ano, trazendo mais agilidade aos serviços prestados à sociedade e ampliando o acesso à Justiça. À medida que este avanço ocorre, o ambiente tecnológico do TRIBUNAL torna-se maior e mais complexo, necessitando também aprimorar os seus mecanismos e controles de segurança da informação para proteção da Confidencialidade, Disponibilidade e Integridade dos dados e informações sob sua responsabilidade.

O TRIBUNAL utiliza o método de proteção em camadas de segurança, criando várias camadas de proteção distintas e complementares, como por exemplo, segmentação de rede, Firewalls, IPS (*Intrusion Prevention System*), Filtro de conteúdo Web, Análise de Malware, WAF (*Web Application Firewall*), além de políticas, normas e procedimentos de segurança da informação.

A função de proteção exige o investimento contínuo em tecnologias, processos e pessoas, além de conhecimento altamente especializado, devido à atualização constante de métodos e técnicas de ataque utilizados pelos atacantes.

Além disso, o monitoramento constante e ininterrupto de 24 horas por dia, 7 dias na semana, e 365 dias por ano, e a rápida resposta à incidentes de segurança são necessidades fundamentais para identificação tempestiva de ameaças e resposta imediata, buscando minimizar o impacto da indisponibilidade dos serviços e sistemas, danos financeiros e danos à imagem do TRIBUNAL.

O modelo atual de segurança do TRIBUNAL está baseado em contratações de soluções de segurança como tecnologia. No entanto, a simples contratação de soluções não exime à necessidade de profissionais especializados para operação, sustentação, monitoramento das ferramentas e o co-relacionamento de informações de eventos de segurança, entre outros. Não é razoável que as soluções apresentem diversos alarmes, indicadores e recomendações sem que haja servidores suficientes na Secretaria de Tecnologia de Informação e Comunicação (SETI) para observar os indicadores de ameaças no ambiente do TRIBUNAL e tratar os alarmes e incidentes.

Verifica-se que o atual modelo de contratações, por meio da compra de produtos e contratação de serviços de operação não é suficiente para fazer frente à velocidade com que surgem novos tipos de ameaças, tentativas de ataques cibernéticos, além da necessidade de monitoramento ininterrupto.

No momento atual, a Divisão de Infraestrutura - DINFRA e a Divisão de Gestão de Segurança da Informação de TIC - DSEG não dispõem de quantitativos de servidores e nem de perfis profissionais suficientes para fornecer um serviço de segurança em regime de 24x7x365 dias, além da capacidade técnica necessária para enfrentamento aos desafios dos ataques cibernéticos atuais.

Aliado a isso, há enorme dificuldade de formação de profissionais qualificados em segurança da informação e cibernética, devido a demanda aquecida do mercado de trabalho, alto investimento em capacitação e a elevada curva de aprendizado. No serviço público, verifica-se a dificuldade de obter pessoas, do ponto de vista normativo e operacional, para a utilização de servidores públicos em regime de escala de trabalho 24x7x365 contínuos e ininterruptos, sem o prejuízo das atividades do dia a dia.

A solução viável encontrada é a soma de esforços entre empresas especializadas para prestação de serviço remoto junto ao TRIBUNAL, a fim de ampliar os mecanismos de segurança, aumentar a capacidade de monitoramento e diminuir o tempo de resposta a incidentes.

Partindo dessa percepção, a presente contratação se baseia em 03 pilares principais, tais como Governança de Segurança, MDR (*Managed Detection and Response*) e MSS (*Managed Security Services*). Onde a Governança prestará apoio a fim de avaliar, propor, revisar políticas, normas e procedimentos de segurança, além de verificar as regras de segurança da informação estabelecidas no TRIBUNAL. A equipe de MDR prestará um serviço gerenciado de segurança, por meio de um SOC (*Security Operations Center),* que fornece inteligência contra-ataques, caça de ameaças, monitoramento e resposta a incidente 24x7x365, simulação de ataques automatizados e testes de invasão (*Pentest*), de forma contínua e proativa. Além disso, o MSS será responsável pela operacionalização e sustentação de soluções de segurança alinhadas com as equipes de MDR.

A contratação também está alinhada à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída por meio da Resolução CNJ Nº 396/2021 de 7 de junho de 2021, por meio das ações para:

> *Fortalecer as ações de governança cibernética.*
>
> *Elevar o nível de segurança das infraestruturas críticas.*
>
> *Estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança.*
>
> *Elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa.*
>
> *Utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança.*
>
> *Utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação, especialmente em fóruns, inclusive da iniciativa.*
>
> *Realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo.*

Isso posto, as principais motivações da contratação são:

a) Aperfeiçoamento da Governança e Conformidade de Segurança da Informação e Cibernética, onde a CONTRATADA prestará apoio a fim de avaliar, propor, revisar políticas, normas e procedimentos de segurança, além de verificar as regras de segurança da informação e cibernéticas estabelecidas no TRIBUNAL;
b) Ampliação da capacidade de monitoramento e resposta a incidentes cibernéticos, através da contratação de um SOC (*Security Operations Center*) com a implementação do serviço de monitoramento e resposta a incidentes de segurança cibernética 24h por dia e 7 dias por semana e 365 dias por ano (24x7x365), por meio de equipe dedicada de modo remoto, para que se possa monitorar, analisar, detectar e responder à incidentes de segurança no ambiente do TRIBUNAL, buscando garantir a Confidencialidade, Integridade e Disponibilidade. Além da proteção contra riscos digitais e derrubada (*takedown*) de sites suspeitos e maliciosos;
c) Contratação de serviço contínuo de Sustentação de Operações de Soluções e Resposta a Requisições de Segurança para gerenciar, sustentar e operar soluções de segurança do parque tecnológico do TRIBUNAL, administrando e gerenciando ferramentas e soluções de Firewall Palo Alto Networks, 02 (dois) Firewalls PA-5220, 02 (dois) Firewalls PA-5420 e 02 (duas) gerencias centralizadas, totalizando 06 (seis) ativos de Firewall, desafogando as equipes de Infraestrutura do TRIBUNAL. Além da sustentação de soluções Microsoft 365 E3 com Add-on E5 Security, contendo licenciamento da solução Defender for Office Plan 1 e 2, Entra ID Plan 1 e 2, Defender for Endpoint Plan 2. Para o licenciamento de soluções de segurança Microsoft o TRIBUNAL possui 18.018 (dezoito mil e dezoito) ativos/licenças;
d) Contratação de serviço de Vulnerabilidades e Testes automatizados de segurança proativo para identificação de possíveis vulnerabilidades na rede, infraestrutura, serviços e aplicações do TJPR, a fim de evitar que ataques cibernéticos direcionados tenham sucesso, com sustentação e operação de solução fornecida pelo TRIBUNAL, incluindo a execução de testes de invasão;
e) Contratação de Serviço contínuo de Gestão de Acesso Privilegiado - PAM aos ativos e serviços de TIC do TRIBUNAL, visando garantir a proteção de identidade de credenciais administrativas utilizadas pela SETI para gerenciamento de ativos críticos;
f) Serviços técnicos especializados para atividades aderentes à contratação relacionadas aos temas de Segurança da Informação e cibersegurança, a serem demandados, aprovados e executados sob demanda.

2.2. REFERÊNCIA AOS ESTUDOS TÉCNICOS PRELIMINARES

Este termo de referência foi elaborado considerando o documento de oficialização de demanda Oficialização da Demanda de Soluções de TIC 9275949 e o Estudos Preliminares de STIC 9744428.

2.3. ANÁLISE DE MERCADO DE TIC

A análise de mercado para esta contratação foi realizada por metodologia estruturada e multidimensional, incluindo: pesquisa documental, consulta a relatórios especializados do setor (Gartner), análise de contratações similares de outros órgãos do Poder Judiciário, reuniões técnicas com especialistas e fabricantes, e avaliação crítica de soluções atualmente em operação no Tribunal. Estas diligências identificaram os serviços e tecnologias mais adequadas às necessidades institucionais específicas, considerando o cenário tecnológico atual e tendências evolutivas, garantindo alinhamento às demandas reais e melhores práticas do mercado de TIC.

2.4. ALTERNATIVAS ANALISADAS

Solução 1	
Solução:	Serviços prestados SOC por servidores internos da SETI

Descrição:	Esta solução considera a utilização do corpo de servidores da SETI para desempenhar as atividades de cibersegurança, aquisição e integração de soluções de mercado para as ferramentas e tecnologias necessárias, incluindo hardware (equipamentos) e software (licenças ou subscrições), serviços de implantação, garantia, atualização e suporte técnico, incluindo monitoramento 24x7, Blue Team e Red Team, sustentação de novos soluções de segurança e aplicação de Pentest.
Vantagem:	Sem necessidade de contratação
Desvantagem:	Insuficiência de servidores para prestar os serviços de SOC. Incapacidade técnica das equipes ou falta da expertise na matéria de cibersegurança. Necessidade de treinamento robusto de segurança da informação. Curva de aprendizado elevada para apresentação de resultados, sendo uma formação adequada em torno de 03 anos. Custos para pagamento ou diária de plantão de servidores, a fim de manter o monitoramento de 24 horas podia, 7 dias por semana e 365 dias por ano. Visão amplamente conhecida da infraestrutura do Tribunal, dificultando a execução de pentest. Falta de servidores para implementar e operacionalizar a solução de Privileged Access Management - PAM. Falta de servidores para operacionalizar a ferramenta de Gestão de Vulnerabilidades (Tenable).
Solução 2	
Solução:	Contratação de empresa especializada para prestação de serviços de segurança da informação
Descrição	Contratação de empresa especializada para prover os serviços de segurança da informação
Vantagem:	Monitoramento contínuo e análise, predizendo, prevendo, detectando e respondendo efetivamente as ameaças de todos os incidentes de segurança. Número de membros da equipe contratada suficiente para atender ao TJPR, frente aos desafios atuais. Equipe altamente capacitada e com expertise em segurança cibernética. Agregação de novas ferramentas e soluções trazidas ao ambiente do TJPR. Equipe para operacionalizar as ferramentas de segurança do Tribunal, realizando a sustentação contínua. Elevação do nível de segurança do Tribunal. Maximizar a disponibilidade dos serviços de TIC oferecidos pelo TJPR.
Desvantagem:	Necessidade e Custo de Contratação. Tempo de adequação. Transição entre empresas contratadas, após o término ou rompimento do contrato.

A SETI não dispõe de quantitativos e nem de perfis profissionais suficientes para fornecer um serviço de segurança em regime de 24x7x365 dias, nem tem expectativa de contratação a curto prazo, inviabilizando a solução 1.

O modelo atual de segurança do TJPR, baseado apenas na contratação de soluções tecnológicas, mostrou-se insuficiente diante da crescente complexidade e velocidade das ameaças cibernéticas. A falta de profissionais especializados para operar, monitorar e integrar essas ferramentas limita a capacidade de resposta do Tribunal, tornando essencial a expansão dos mecanismos de proteção.

A contratação de uma empresa especializada para serviços de gerenciamento, operação, monitoramento e resposta a incidentes de segurança, gestão de vulnerabilidades, conformidade e testes de intrusão (pentest) é considerada a alternativa mais viável. Essa abordagem permite ao Tribunal contar com uma equipe técnica dedicada, capaz de atuar 24x7, elevando o grau de detecção, prevenção e resposta a incidentes, além de agilizar a percepção de segurança entre os usuários.

Entre as principais vantagens estão a flexibilidade na aquisição de soluções, maior velocidade de implantação, acesso a profissionais altamente capacitados, monitoramento contínuo e maximização da disponibilidade dos serviços de TIC. Para que todo o ecossistema funcione adequadamente, é necessário um time de 8 a 12 especialistas, conforme recomendações do Gartner, além do alinhamento com as diretrizes do CNJ para garantir a segurança cibernética do Poder Judiciário.

3. DESCRIÇÃO DA SOLUÇÃO (ART. 6º, XXIII, C)

3.1. ESPECIFICAÇÃO

A solução que melhor atende a demanda do TRIBUNAL está descrita na Tabela 1.

O código CATSER é indicado na tabela a seguir:

Item	Código CATSER	Descrição
1.1	27022	Projeto e implantação
1.2	27340	Serviços de Governança e Conformidade de Segurança
1.3	27022	Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança
1.4	27022	Sustentação de Operações de Soluções e Resposta a Requisições de Segurança
1.5	27022	Gestão de Vulnerabilidades e Testes de Segurança
1.6	27022	Gestão de Identidade
1.7	27332	Serviços Técnicos Especializados por Demanda
2.1	27022	Serviço de Teste de Invasão (Pentest)

Tabela 2 – Tabela CATSER

3.2. DEMANDA PREVISTA PARA ATENDER AS NECESSIDADES DO TRIBUNAL

A demanda prevista contém o conjunto de serviços e soluções de segurança que melhor atendem as demandas do projeto e foram divididos em 7 itens do Grupo 01: **1 - Projeto e implantação**; **2 - Serviços de Governança e Conformidade de Segurança**; **3 - Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança**; **4 - Sustentação de Operações de Soluções e Resposta a Requisições de Segurança**; **5 - Gestão de Vulnerabilidades e Testes de Segurança**; **6 - Gestão de Identidade**; e **7 - Serviços Técnicos Especializados por Demanda;** e item **8 - Serviço de Teste de Invasão (Pentest)**. A vigência contratual de 36 (trinta e seis) meses será dividida em 03 etapas de execução: a primeira fase compreende o **Projeto e implantação** com duração de 03 (três) meses, iniciada a partir da assinatura do

contrato, seguida pela fase de **Operação**, que abrangerá os 33 (trinta e três) meses subsequentes do contrato. Os últimos 03 meses são denominados fase de **Transição do contrato**.

GRUPO 01:

Item 1 - Projeto e implantação

Devido à complexidade do projeto de contratação, composta de serviços e soluções informatizadas, entende-se a necessidade de uma fase de **Projeto e implantação** em que a CONTRATADA deverá realizar as atividades de planejamento, instalação, adoção tecnológica, configuração, implantação do serviço e elaboração de documentação técnica em conformidade com este Termo de Referência. A execução será de apenas 01 (uma) vez, iniciando a partir da assinatura de contrato e com término máximo de até 90 (noventa) dias corridos.

Item 2 - Serviços de Governança e Conformidade de Segurança

A contratação do serviço de Governança de Segurança da Informação é de atuação contínua e proativa, objetivando apoiar na avaliação, proposição, revisão políticas, normas e procedimentos de segurança, além de auxiliar para a conformidade (compliance) com as melhores práticas de mercado nos temas de segurança da informação e cibernética, normas do CNJ e requisitos internos ao TRIBUNAL.

Para este item estão previstas as demandas:

- 03 (três) avaliações de **Diagnóstico de Maturidade de Segurança da Informação**, com objetivo de realizar uma avaliação por ano de contrato vigente, a fim de avaliar o aumento da maturidade e progresso nos temas de segurança da informação e cibernética do TRIBUNAL;
- 01 (uma) demanda de um serviço mensal de apoio de aprimoramento e acompanhamento da **Política de Segurança da Informação - PSI**, para aperfeiçoamento, adequação e monitoramento da política pelo período de 33 (trinta e três) meses durante a fase de **Operação;**
- 01 (um) serviço mensal de apoio de aprimoramento e acompanhamento de **Plano de Continuidade de Serviços Essenciais de TIC com foco no SOC,** pelo período de 33 (trinta e três) meses durante a fase de **Operação;**
- 01 (um) serviço mensal de apoio de aprimoramento e acompanhamento de **Plano de Resposta a Incidentes - PRI** e planos de mitigação e recuperação, pelo período de 33 (trinta e três) meses durante a fase de **Operação**, aderente as necessidades estabelecidas pela Portaria Nº 162 e seus anexos do CNJ.

Item 3 - Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança

01 (uma) prestação mensal de serviço contínuo e ininterrupto de **Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança**, por meio de um Security Operations Center (SOC), contemplando: equipe, processos, documentação, gestão de eventos, incidentes e crises, incluindo solução informatizada para gerenciamento, monitoramento, detecção e resposta de informações, eventos e incidentes de segurança, licenciado pela CONTRATADA. A unidade de contratação é de periodicidade mensal por ativo protegido, sendo necessária a comprovação ao final de cada mês do serviço prestado para o efetivo pagamento. A quantidade estimada de ativos do TRIBUNAL é de 25.000 (vinte e cinco mil) ativos, conforme tabela de estimativa de ativos **ANEXO IV** - **ESTIMATIVAS DE ATIVOS PARA DIMENSIONAMENTO DOS SERVIÇOS**. Como a vigência do contrato é 36 (trinta e seis) meses, reduzindo 03 (três) meses do Projeto e implantação, a demanda prevista é de 825.000 ativos (oitocentos e vinte e cinco mil), durante a vigência do contrato.

01 (uma) prestação mensal de serviços contínuos e ininterruptos de **Proteção contra Riscos Digitais (Threat Intelligence)** pelo período de 33 (trinta e três) meses. A demanda de proteção atuará sobre o monitoramento dos perfis oficiais de redes sociais do TRIBUNAL, no mínimo os indicados na tabela abaixo.

Rede Social	Nome do Perfil	@
Instagram	Tribunal de Justiça do Paraná	@TJPRoficial
Youtube	Tribunal de Justiça do Paraná	@TJPRoficial
Facebook	Tribunal de Justiça do Paraná	@TJPRoficial
X (Twitter)	Tribunal de Justiça do Paraná	@TJPRoficial
Threads	Tribunal de Justiça do Paraná	@TJPRoficial
Bluesky	Tribunal de Justiça do Paraná	@TJPRoficial
Instagram	Escola Judicial do Paraná	@ejud.tjpr
Instagram	Adoção-Encontro Online TJPR	@adocao_encontroonlinetjpr
Instagram	2ª Vice-Presidência do TJPR	@2vicetjpr
Instagram	CEVID TJPR	@cevidtjpr
Instagram	1ª Vice-Presidência do TJPR	@tjpr1vice
Instagram	CONSIJ/CIJ do TJPR	@consij_cij.tjpr
Instagram	GMF - TJPR	@gmf_tjpr
Instagram	Corregedoria da Justiça do Paraná – TJPR	@corregedoria_tjpr
Instagram	Ouvidoria da Justiça Paraná	@ouvidoria_justica_pr
Youtube	2a Vice-Presidência do TJPR	@2vicetjpr
Youtube	Tribunal do Júri TJPR	@TribunaldoJuriTJPR
Youtube	TJPR - Sessões	@TJPRsessoes
Youtube	EJUD TJPR	@EJUDTJPR
Youtube	CEVID TJPR	@cevidtjpr7240
Facebook	2ª Vice-Presidência TJPR	@2vicetjpr
Facebook	CEVID	@cevidparana

Tabela 3 - Perfis oficiais de redes sociais do TRIBUNAL

Prestação de **Serviço de Takedown** de 60 (sessenta) unidades, considerando uma média de 20 (vinte) por ano, totalizando 60 (sessenta) durante a vigência do contrato, sendo o pagamento realizado por Takedown executado.

Item 4 - Sustentação de Operações de Soluções e Resposta a Requisições de Segurança

01 (uma) prestação mensal de serviço contínuo de **Sustentação de Operações de Soluções e Resposta a Requisições de Segurança** para gerenciar, sustentar e operar soluções de segurança do parque tecnológico do TRIBUNAL, administrando e gerenciando ferramentas e soluções de Firewall Palo Alto Networks, 02 (dois) Firewalls PA-5220, 02 (dois) Firewalls PA-5420 e 02 (duas) gerencias centralizadas Panorama, totalizando 06 (seis) ativos de Firewall pelo período de 33 (trinta e três) meses durante a **fase de Operação**, com uma quantidade total prevista de 198 ativos, sendo necessária a comprovação ao final de cada mês do serviço prestado para o efetivo pagamento.

01 (uma) prestação mensal de serviço contínuo e proativo para gerenciar, sustentar e operar soluções de segurança Microsoft do parque tecnológico do TRIBUNAL, administrando, sustentando e gerenciando ferramentas e soluções Microsoft 365 E3 com Add-on E5 Security, incluindo os recursos da solução Defender for Office Plan 1 e 2, Entra ID Plan 1 e 2, Defender for Endpoint Plan 2. Para o licenciamento de soluções de segurança Microsoft o TRIBUNAL possui 18.018 (dezoito mil e dezoito) ativos/licenças, totalizando para os 33 (trinta e três) meses 594.594 (quinhentos e noventa

e quatro mil e quinhentos e noventa e quatro) ativos/licenças. Por questões de oscilação no crescimento, onde ativos são inseridos e removidos da infraestrutura de TIC do TRIBUNAL e arredondamento, foram estimados a quantidade de 660.000 (seiscentos e sessenta mil) ativos, sendo pagos efetivamente por aferição mensal através de comprovação pela CONTRATADA.

Item 5 - Gestão de Vulnerabilidades e Testes de Segurança

01 (uma) prestação mensal de **Gerenciamento Contínuo de Vulnerabilidades** para identificação de possíveis vulnerabilidades nos ativos da rede, infraestrutura e aplicações do TRINUNAL, com a sustentação e operação da solução fornecida pelo TRIBUNAL, a fim de antecipar correções e evitar que ataques cibernéticos direcionados tenham sucesso. Esta demanda é com pagamento mensal, após comprovação do serviço prestado pelo prazo de 33 (trinta e três) meses durante a fase de **Operação**.

01 (uma) prestação de serviços de **Testes de Segurança Automatizados (BAS),** com solução fornecida pela CONTRATADA, para 30 (trinta) baterias de testes por mês, prestado pelo prazo de 33 (trinta e três) meses durante a fase de **Operação**, totalizando 990 (novecentos e noventa) baterias de testes.

Item 6 - Gestão de Identidade

01 (uma) prestação mensal de serviço contínuo de **Gestão de Acesso Privilegiado – PAM,** com solução fornecida pela CONTRATADA para dar suporte aos ativos e serviços de TIC do TRIBUNAL, licenciados para 80 (oitenta) usuários administrativos, contemplando os usuários administrativos da SETI que realizam o gerenciamento de ativos Data Center e Nuvem de responsabilidade do TRIBUNAL, totalizando 2.640 (dois mil e seiscentos e quarenta) usuários protegidos considerando 33 (trinta e três) meses durante a fase de **Operação**.

Item 7 - Serviços Técnicos Especializados por demanda

Serviços técnicos especializados por demanda para atividades aderentes à contratação não previstas no escopo anteriormente definido relacionadas ao tema de segurança da informação e cibernética, a serem demandados, aprovados e executados sob demanda, mediante Ordem de Serviço (OS), na forma de um banco de horas técnicas. Estão sendo estimadas a contratação eventual de até 400 (quatrocentos) horas por ano de vigência do contrato, podendo totalizar até 1.200 (um mil e duzentos) horas durante a vigência do contrato.

Item 8 - Serviço de Teste de Invasão (Pentest)

01 (uma) prestação de serviços de **Teste de Invasão (Pentest)** sob demanda, sendo previsto 01 (um) teste a cada 06 (seis) meses com um consumo médio de 60 (sessenta) horas por teste, totalizando 360 (trezentos e sessenta) horas durante a vigência do contrato. Conforme aderência ao Art.11, item X, da Resolução Nº 396 do CNJ.

3.3. OBJETIVOS

Os principais objetivos para a contratação são:

a) Obter apoio, através de empresas especializadas em segurança da informação e cibernética, nos temas de Governança de Segurança da Informação e Conformidade, por meio Identificação de Gaps (Gap Analysis), diagnóstico e avaliação da maturidade de segurança da informação, analisando processos, normas, políticas, procedimentos, planos, indicadores, métricas, pessoas, papéis, responsabilidades e soluções de segurança existente no TRIBUNAL;
b) Contratação de um SOC (*Security Operations Center*) para monitoramento, detecção, análise, investigação e resposta à incidentes de segurança cibernética em regime 24x7x365 dias por ano,

permitindo o aumento da capacidade de monitoramento, detecção e resposta à incidentes de segurança cibernética no ambiente do TRIBUNAL;

c) Implementação de serviço contínuo proativo para sustentação, administração, operação, suporte técnicos especializado das soluções de segurança do TRIBUNAL;
d) Gerir e operacionalizar o serviço de Gestão de Vulnerabilidades através de técnicos especializados, de forma contínua e proativa para identificação de possíveis vulnerabilidades com exposição a ameaças baseada em riscos, na rede, infraestrutura e aplicações do TRIBUNAL, a fim de evitar que ataques cibernéticos direcionados tenham sucesso;
e) Aumentar a capacidade de bateria de testes de vulnerabilidades de forma automatizada e manual, identificando vulnerabilidades para diminuir a superfície de ataques cibernéticos;
f) Ampliar o portfólio de soluções e controles de segurança por meio da contratação de serviços;
g) Aprimorar a Gestão de Segurança da Informação e Cibernética e a expansão dos serviços de MDR (Threat Intelligence) e MSS (Managed Security Services);
h) Aderir aos objetivos estabelecidos na ENSEC-PJ, por meio da Resolução Nº 396 de 07/06/2021 do CNJ;
i) Aderir aos objetivos estabelecidos na Portaria Nº 162 do CNJ.

3.4. BENEFÍCIOS

Os benefícios esperados com a contratação são:

a) Aumentar exponencialmente a capacidade de monitoramento, detecção e resposta à incidentes de segurança cibernética no ambiente do TRIBUNAL de modo contínuo e ininterrupto;
b) Agregar a expertise de mão de obra altamente capacitada e especializada em segurança da informação e cibernética as equipes do TRIBUNAL;
c) Manter uma equipe especializada ininterrupta de resposta rápida e efetiva a ataques e incidentes, visando minimizar o tempo de atuação e possíveis danos causos por ataques cibernéticos, mesmo fora do horário regimental do TRIBUNAL;
d) Aumentar o nível de segurança dos principais sistemas do TRIBUNAL, através da realização de testes automatizados e de invasão sob demanda, antecipando a identificação de vulnerabilidade de modo proativo;
e) Implantação de um SOC (*Security Operations Center*) com a capacidade de identificar, proteger, detectar, responder e recuperar, atuando na segurança defensiva e reativa. Prestando apoio direto às diversas áreas da SETI na investigação, remediação e melhorias de cibersegurança;
f) Prover a melhoria contínua em segurança da informação e cibersegurança de acordo com indicadores e relatórios de acompanhamento;
g) Redução de superfície de ataque através da ampliação de soluções de segurança e os mecanismos de proteção cibernética no TRIBUNAL com as soluções de SIEM, BAS e PAM;
h) Estar em conformidade com as recomendações e exigências do CNJ contidas nas Resoluções Nº 396 e Portaria Nº 162 e anexos.

3.5. ADEQUAÇÃO DO AMBIENTE

A CONTRATANTE disponibilizará, nos casos de instalação de hardware, tão somente a estrutura física básica de data center ou sala de dados: espaço físico, fornecimento de energia elétrica, refrigeração e conectividade com a rede do Tribunal.

Compete à CONTRATADA todos os serviços e equipamentos para instalação, manutenção (preventiva e corretiva) e gerenciamento do enlace de dados dedicado e de sua infraestrutura, garantindo sua disponibilidade e seu adequado funcionamento de forma segura.

Os serviços contratados serão realizados predominantemente de forma remota. Para este caso, o TRIBUNAL dispõe de recursos como Internet, rede de comunicação e Datacenter para comportar os serviços prestados.

Caso a equipe CONTRATADA preste serviços de forma presencial nas dependências da SETI, será necessária a infraestrutura de ponto de rede habilitado para acesso à rede corporativa e Internet.

O acesso ao ambiente do CONTRATANTE, do Grupo 01, deverá ser realizado através de link de comunicação dedicado, com acesso restrito e criptografado, no qual deverá ser provido e mantido pela CONTRATADA:

a) A utilização deste link de comunicação não deverá ultrapassar 80% (oitenta por cento) de sua capacidade, podendo ser utilizado VPN via internet como redundância;
b) Caso a capacidade do link, dimensionada pela CONTRATADA, seja considerada insuficiente para a prestação dos serviços a CONTRATADA deverá providenciar o seu aumento, sem custos para o CONTRATANTE;
c) Devido a limitação para adicionar novas operadoras à infraestrutura de tecnologia do TRIBUNAL, a CONTRATADA deve consultar o CONTRATANTE antes de contratar o serviço.

3.6. PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

O objeto da licitação, embora divisível em termos técnicos, apresenta características que tornam a contratação por item individual complexa e prejudicial à qualidade dos serviços a serem prestados. A fragmentação da contratação dificultaria a integração das soluções de proteção com os serviços de cibersegurança e a implementação de uma estratégia de segurança holística. Com um único fornecedor, a responsabilidade pela integração, operação e suporte das soluções MSS e Proteção recai sobre uma única empresa. Isso facilita a cobrança de resultados, a resolução de problemas e a garantia do cumprimento das obrigações contratuais.

O agrupamento também permite o aumento da eficiência administrativa por meio da otimização do gerenciamento do serviço, pois neste caso, não seria conveniente e oportuno a prestação desses serviços por partes distintas, considerando que lidar com um único ou poucos prestadores diminui o custo administrativo de gerenciamento de todo o processo de contratação (Acórdão 861/2013-TCU Plenário).

Destaca-se que o agrupamento não implica prejuízo à ampla competitividade, pois existem, no mercado, diversas empresas com capacidade de fornecer os produtos e serviços na forma estabelecida neste Termo de Referência.

Considerando as características dos itens, buscando garantir a qualidade dos serviços e otimizar a gestão da contratação, entende-se que há possibilidade em particionar o objeto da licitação em dois agrupamentos, um composto dos serviços essenciais e outro para o Serviço de Teste de Invasão (PenTest).

É vedada a contratação de uma mesma empresa para os itens do Grupo 01 e item 8 devido sua natureza, pois estes serviços exigem a segregação de funções. Esta separação de funções assegura que os testes de invasão sejam conduzidos de forma independente e rigorosa, proporcionando uma avaliação honesta e precisa das defesas de segurança.

A contratação será composta por 07 (sete) itens agrupados e 01 (um) item não agrupado, possibilitando a adjudicação do objeto por mais de uma empresa participante da licitação, conforme detalhado na tabela abaixo:

Grupo	Item	Descrição
1	1	Projeto e implantação

Grupo	Item	Descrição
	2	Serviços de Governança e Conformidade de Segurança
	3	Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança
	4	Sustentação de Operações de Soluções e Resposta a Requisições de Segurança
	5	Gestão de Vulnerabilidades e Testes de Segurança
	6	Gestão de Identidade
	7	Serviços Técnicos Especializados por Demanda
Item	8	Serviço de Teste de Invasão (PenTest)

Tabela 4 - Tabela de Adjudicação

3.7. ALINHAMENTO ESTRATÉGICO

A presente contração visa contemplar os seguintes objetivos do Planejamento Estratégico do Poder Judiciário (PEI 2021/2026) e Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC 2024):

PEI - Planejamento Estratégico do Poder Judiciário (PEI 2021 – 2026)

Objetivos Estratégicos Institucionais

02 – Fortalecimento da Relação Institucional do Judiciário com a Sociedade.

04 – Agilidade e Produtividade na Prestação Jurisdicional.

12 – Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados.

PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)

Objetivos Estratégicos de Tecnologia da Informação e Comunicação

OETIC.1 - Aprimorar a entrega de serviços e o valor para os clientes internos e externos.

OETIC.2 - Ampliar mecanismos de Infraestrutura e Segurança da Informação de TIC.

4. REQUISITOS DA CONTRATAÇÃO (ART. 6º, XXIII, D)

4.1. PRINCIPAIS REQUISITOS DO NEGÓCIO

Governança e Conformidade de Segurança - Grupo 01

Devido à complexidade do ambiente tecnológico do TRIBUNAL existe a necessidade de apoio na identificação de Gaps (lacunas), diagnóstico e avaliação da maturidade de segurança da informação do TRIBUNAL. Esta identificação de Gaps é importante para analisar processos existentes, normas, políticas, procedimentos, planos, indicadores, métricas, pessoas, papéis, responsabilidades e soluções de segurança do TRIBUNAL, considerando o alinhamento com normas ISO relacionadas à segurança da informação, frameworks NIST e CIS Control, leis e normativos do CNJ, propondo adequação, melhoria e aperfeiçoamento contínuo durante a vigência da contratação.

Uma vez identificada a necessidade de adequação, melhoria e aperfeiçoamento, o TRIBUNAL encontra respaldo na contratação para fazer os ajustes oportunos com objetivo de aumentar o seu nível de maturidade em segurança da informação e proteção cibernética.

Necessidade de apoio no alinhamento e aprimoramento do Plano de Continuidade de Serviços Essenciais, Plano de Administração de Crise - PAC, Plano de Recuperação de Desastres - PRD.

Necessidade de apoio no alinhamento e aprimoramento da Política de Segurança da Informação - PSI, adequando às necessidades do Tribunal, resoluções do CNJ, normas ISO, conformidade com as melhores práticas de Segurança da Informação.

Apoio na elaboração, implantação, execução e melhoria contínua de um Plano de Resposta a Incidentes e Processo de Tratamento e Resposta a Incidentes de segurança cibernética, incluindo um plano específico para o gerenciamento de crises cibernéticas, conforme Portaria 162 do CNJ e seus anexos.

Elaboração, documentação e melhoria contínua de métricas, indicadores chave de desempenho (KPI), painéis (dashboards) técnico-operacional (foco em tecnologia) e estratégico-gerencial (foco no negócio) e lições aprendidas, com relatórios mensais de situação e desempenho.

Análise, elaboração, documentação, acompanhamento e avaliação de um plano de ação de controles e salvaguardas de segurança cibernética, medidas de remediação e mitigação, planejando ações para aplicação de atualizações de segurança, regras, barreiras e hardening de ativos de TIC, a partir dos resultados dos diagnósticos, análises, testes, eventos e incidentes de segurança, tanto proativos/preventivos com base na gestão de vulnerabilidades e melhores práticas internacionais quanto reativos com base no tratamento de ameaças e incidentes.

Apoio na execução e acompanhamento de plano de ação com relatórios de progresso e situação. Repasse detalhados das ações executadas, acompanhamento do andamento e prestado todo esclarecimento de dúvidas e apoio consultivo necessário.

Monitoramento, detecção e resposta a incidentes - Grupo 01

Necessidade de estrutura de um SOC (Security Operations Center) para monitoramento, detecção, análise, investigação e resposta a incidentes de segurança cibernética em regime de 24 horas por dia, 07 dias na semana e 365 dias por ano.

Apoio, remotamente, a equipe de tratamento e resposta a incidentes de segurança (ETIR) da SETI, incluindo o Nível 1 (fase inicial), Nível 2 (fase avançada e em crises) e Nível 3 (fase especialista).

A CONTRATADA deverá fornecer e adotar Solução Informatizada para Gerenciamento, Monitoramento, Detecção e Resposta de Informações, Eventos e Incidentes de Segurança e ataques, devendo ser projetada como uma plataforma completa que atenda funcionalidades de monitoramento, inspeção e análise, detecção contínua de ameaças e ataques, investigação e defesa cibernética.

A Solução Informatizada de gerenciamento e seus serviços devem abranger não só o monitoramento, mas a detecção contínua de ameaças e ataques, agregando inteligência de segurança, incluindo análise comportamental de usuários e entidades (*User and Entity Behavioral Analysis – UEBA*) com inteligência artificial e aprendizado de máquina, identificação autônoma de táticas, técnicas e procedimentos (TTPs).

Gerenciamento de eventos de segurança, através de solução SIEM (Security Information Event Management – SIEM), incluindo serviços de coleta, consolidação, correlação e análise de logs.

Triagem, análise, investigação, Threat Hunting, Threat Research e inteligência de ameaças (*Threat Intelligence*) estratégica, tática e operacional, e validação, identificando atividades anômalas e, dentre essas, candidatos a incidentes, além da triagem, tratamento, priorização e categorização de incidentes de segurança.

Monitoramento e Detecção de Resposta de Rede (*Network Detection and Response - NDR*).

Orquestração, Automação e Resposta, através de solução SOAR (*Security Orchestration, Automation and Response*), licenciada pela empresa CONTRATADA, sendo do mesmo fabricante do SIEM ou com homologação comprovada pelo fabricante, quando houver. Além da capacidade de integrar, consolidar, agregar e correlacionar informações provenientes de outras fontes de telemetria a ativos de TIC e soluções de segurança do TRIBUNAL.

Elaboração, análise e melhoria e expansão dos casos de uso de monitoramento e detecção, playbooks de tratamento, resposta e automação.

Realização dos procedimentos cabíveis de análise e investigação forense pós-incidentes, aderentes com Portaria 162 do CNJ de 10/06/2021 e seus anexos.

Apoio na coordenação das ações de investigação e de comunicação, interna e externa, através do responsável/gerente do SOC.

Documentar os incidentes de segurança, registrar os procedimentos e as soluções encontradas para mitigação, lições aprendidas e possíveis necessidades de aperfeiçoamento.

Monitoramento de proteção da marca e da reputação institucional na internet, na Deep Web e na Dark web, incluindo redes sociais, repositórios de informação e lojas de aplicativos, identificando fraudes e golpes, operações se passando como legítimas em nome do TRIBUNAL, conteúdo malicioso, vazamentos de dados e ameaças externas, com capacidade de realizar takedown em nome do TRIBUNAL mediante procuração e autorização.

Monitoramento de Marca: Tribunal de Justiça do Estado do Paraná, Tribunal de Justiça do Paraná, Poder Judiciário do Paraná, TJPR, TJ-PR, TJ/PR.

- Domínios: tjpr.jus.br, tjpr.net, incluindo subdomínios (www, projudi, sei (protocolo), mail, webmail, entre outros);
- Perfis: Youtube @TJPRoficial | @TJPR - Sessões, Instagram: @tjproficial | @2vicetjpr | @tjpr1vice e X (antigo Twitter):@TJPRoficial.

As fontes de monitoramento devem incluir:

- Registros de domínios nacionais e internacionais, incluindo TLDs e gTLDs;
- Sites na internet, Deep Web e na Dark Web;
- Grupos, canais e comunidades em serviços de comunicação por mensagens e fóruns: WhatsApp (se aplicável), Telegram, Signal, Discord, Reddit;
- Repositórios e serviços de conteúdo e informação de grande abrangência: Github, Scribd e Reclame Aqui;
- Lojas de aplicativos (catálogo ou repositório de distribuição de software instalável para determinada plataforma de sistema operacional): Microsoft Store (Windows), Google Play (Android), Apple App Store (iOS/iPadOS), Samsung Galaxy Store (Android), Amazon Appstore (Android) e F-Droid (Android).

O serviço de monitoramento deve identificar:

- Fraudes, phishing, leilões, engenharia social e outros tipos de golpes, conteúdos maliciosos e ameaças relacionadas, réplicas, conteúdos ilegítimos, abusos e violações aos serviços utilizando nome, marca e/ou identidade visual institucionais do TRIBUNAL;
- Identificação de variação de nomes ou domínio, incluindo permutação de caracteres;

- Vazamento de dados e informações sensíveis da instituição;
- Monitoramento de ameaças globais e com foco em Brasil, Governo e Judiciário.

Sustentação de Operações de Soluções e Resposta a Requisições de Segurança - Grupo 01

Serviço contínuo e proativo para sustentação, administração, operação, suporte técnicos das soluções de segurança do TRIBUNAL, sendo eles:

- Cluster de Firewall Palo Alto - PA 5220;
- Cluster de Firewall Palo Alto - PA 5420;
- Solução de Gerência Centralizada Panorama;
- Microsoft Defender - Soluções de Segurança Microsoft licenciadas com: Microsoft 365 E3 com Add-on E5 Security;
- Microsoft Defender - Soluções de Segurança Microsoft licenciadas com: Microsoft 365 F3 com Add-on F5 Security;
- Solução de Gestão de Vulnerabilidades Tenable, licenciada para 2.000 ativos.

Gestão de Vulnerabilidades e testes de segurança - Grupo 01

Gestão contínua e proativa para identificação de possíveis vulnerabilidades com exposição a ameaças baseada em riscos, dos ativos na rede da infraestrutura e aplicações do TJPR, a fim de evitar que ataques cibernéticos direcionados tenham sucesso. A execução deverá ser realizada através de SCAN contínuo de ativos de TIC e monitoramento das aplicações indicadas pela equipe de segurança do TJPR, identificando, avaliando, categorizando, priorizando e tratando vulnerabilidades, avaliando configurações e conformidade com o devido apontamento para mitigação ou resolução.

A solução de Gestão de Vulnerabilidades será disponibilizada pelo TRIBUNAL, através da solução da fabricante Tenable licenciada para 2.000 ativos. Sendo 1.800 licenças para servidores/IPs e 200 licenças para uso de FQDN.

Deve realizar varreduras automatizadas de vulnerabilidade completas em ativos de TIC e reteste após aplicação de atualizações, patches e mitigação, incluindo varreduras autenticadas e não autenticadas, com compatibilidade no mínimo com o protocolo Security Content Automation Protocol – SCAP.

Agregação de recursos de inteligência de ameaças (*Threat Intelligence*) para rastreamento do uso ativo de TIC e priorização de vulnerabilidades, incluindo fontes estratégicas (relatórios, bases de conhecimento, feeds, fóruns e comunidades abertos, da Deep e da Dark Web etc.), táticas (correlação com táticas, técnicas e procedimentos – TTPs) e operacionais (correlação com indicadores de comprometimento – IOCs), do fabricante da ferramenta combinada com fontes abertas e da CONTRATADA.

Acompanhamento de comunicados, alertas de segurança, atualizações, Zero Day, referenciais de vulnerabilidades e melhores práticas de higienização de segurança e de hardening para ativos de TIC, incluindo: NIST, MITRE, OWASP Top 10, CIS Control, Cert.BR, fornecedores/fabricantes de tecnologia aplicáveis aos ativos de TIC do TRIBUNAL como Microsoft, Palo Alto, VMWare, Cisco, Google, Red Hat, Trend Micro, entre outros.

Testes de Segurança automatizados - Grupo 01

Planejamento, execução, análise e relatório de testes automatizados continuados de segurança com solução de simulação de brechas e ataques (*Breach and Attack Simulation - BAS*):

Deve ser capaz de realizar baterias de testes de simulação de ataques baseados em bibliotecas atualizadas de ameaças e exploits, com execução imediata ou agendamentos, abrangendo infiltração de rede e aplicações web, ambos com o fluxo de ator malicioso externo para ativo-alvo interno, e endpoint, com comprometimento e exfiltração em ativo-alvo interno, estação de trabalho ou servidor, cobrindo no mínimo o sistema operacional Microsoft Windows e Linux.

As simulações devem garantir ambiente controlado e não podem causar impacto nocivo real.

Para o atendimento do serviço a empresa CONTRATADA deverá disponibilizar ferramenta de simulação de brechas e ataques (*Breach and Attack Simulation – BAS)*, devidamente licenciado.

Os resultados devem validar e indicar controles de prevenção e proteção ineficazes e/ou suplantados, vulnerabilidades exploradas, caminhos de ataque e TTPs (táticas, técnicas e procedimentos) envolvidos.

Teste de invasão (Pentest) - item 8

Planejamento, execução e relatório com resultados de testes de invasão com atuação nos modelos black box, gray box, ou white box.

Os alvos dos testes de invasão devem ser aprovados pela equipe técnica do TRIBUNAL.

A equipe responsável pela execução do teste de penetração deve estar preparada para trabalhar em conjunto com a equipe de Monitoramento, detecção e resposta à incidentes.

Gestão de identidade - Grupo 01

Serviço contínuo na Gestão de Acesso Privilegiado - PAM no acesso ao gerenciamento de ativos críticos do TRIBUNAL, licenciado para 80 (oitenta) usuários administrativos.

Para o atendimento do serviço a empresa CONTRATADA deverá disponibilizar ferramenta de Gestão de Acesso Privilegiado - PAM, devidamente licenciado.

Serviços técnicos especializados por demanda - Grupo 01

Execução de serviços técnicos especializados para atividades não previstas no escopo anteriormente definido, a serem demandados, aprovados e executados sob demanda, mediante ordem de serviço (OS), na forma de um banco de horas técnicas anual.

4.2. REQUISITOS DE GARANTIA E SUPORTE - Grupo 01

A CONTRATADA deverá prover o serviço de sustentação, garantia, suporte, manutenção, atualização de todas as soluções informatizada e todos os softwares, hardwares e infraestrutura necessária para o pleno funcionamento dos itens contratados neste Edital.

A sustentação deverá ser realizada em regime 24 x 7 (24 horas por dia e 7 dias da semana), por profissionais especializados.

A sustentação, administração, operação das Soluções informatizadas fornecidas pela CONTRATADA e disponibilizadas pelo TRIBUNAL, serão serviços de natureza continuada de responsabilidade da CONTRATADA.

Todas as Soluções Informatizadas disponibilizadas pela CONTRATADA devem possuir os serviços de licenciamento ou subscrição, garantia, suporte técnico e atualização oficiais do fabricante, com níveis de serviço adequados e compatíveis com os dos serviços exigidos, que devem estar contratados e disponíveis a partir da implantação da respectiva solução.

As Soluções Informatizadas não podem constar, no momento da apresentação da proposta comercial, em listas de *End-of-Sale, End-of-Support, End-of-Life* ou similares do fabricante, e não podem ter previsão de descontinuidade de fornecimento, suporte ou vida pelo menos até o fim da vigência prevista para o contrato.

As Soluções Informatizadas devem ser instaladas em sua versão mais estável e atualizada.

Devem ser fornecidas a CONTRATANTE no mínimo 10 (dez) credenciais de acesso ao console das Soluções Informatizadas para que seja possível o acompanhamento, auditoria e direcionamento de ações.

A CONTRATADA deverá cumprir todos os termos e condições do contrato de licenciamento dos respectivos fabricantes das Soluções Informatizadas, cuidando do adequado dimensionamento quantitativo e qualitativo das licenças necessárias para a prestação dos serviços e aderência ao ambiente da CONTRATANTE, mantendo a conformidade com os direitos de propriedade intelectual.

Para todas as soluções ofertadas a CONTRATADA deve comprovar acesso aos recursos e serviços de apoio técnico, bem como à plenitude de capacidades e efetividade da ferramenta, prestados diretamente pelo fabricante, como centros e laboratórios de inteligência, investigação, diagnóstico, análise e automação, dentre outros aplicáveis.

A CONTRATADA deverá garantir, adicionalmente à garantia do fabricante:

- Suporte técnico 24x7 em português via telefone, e-mail e portal online;
- Orientações sobre uso, configuração e instalação da solução;
- Questões sobre compatibilidade e interoperabilidade da solução ofertada;
- Interpretação da documentação da solução ofertada;
- Orientação quanto às melhores práticas para implementação do serviço contratado;
- Apoio na recuperação de ambientes em caso de panes ou perda de dados.

4.3. REQUISITOS DE QUALIFICAÇÃO DE EQUIPE TÉCNICA - Grupo 01 e item 8

A CONTRATADA deverá dimensionar adequadamente a sua equipe de profissionais de forma a atingir os níveis de serviço estabelecidos no contrato, devendo prever e substituir imediatamente qualquer profissional por outro de mesmo perfil no caso de falta, impedimentos, férias, licenças e outras questões.

Não será exigida a dedicação exclusiva de profissionais na gestão e execução dos serviços demandados pela CONTRATANTE.

Todos os profissionais deverão possuir qualificação plena e conhecimento técnico compatível com a complexidade das demandas a serem atendidas.

A formação da equipe de profissionais é de exclusiva responsabilidade da CONTRATADA e serão gerenciados exclusivamente pelo PREPOSTO da empresa.

A CONTRATADA deve informar tempestivamente ao CONTRATANTE quando da substituição ou designação de novo PREPOSTO.

Todos os documentos para comprovação dos requisitos estarão sujeitos à diligência do TRIBUNAL para fins de confirmação das informações prestadas.

Durante a execução do contrato, a CONTRATADA se obriga a manter todos os profissionais com as qualificações especificadas.

Deverão ser afastados e substituídos pela CONTRATADA em até 05 (cinco) dias úteis, independentemente de justificativa, os profissionais alocados e/ou envolvidos no contrato que se enquadrem em quaisquer das situações abaixo:

a) Não atendam às qualificações exigidas para o perfil em que deve atuar;
b) Não apresentem nível de serviço compatível com o esperado;
c) Apresentem atuação e/ou prontidão considerada insatisfatória ou inadequada de acordo com o TRIBUNAL, ou que seja contrária ou conflitante ao interesse do serviço público;
d) Apresentem comportamento com problemas de má conduta e/ou postura inconveniente nos atendimentos efetuados ao TRIBUNAL;
e) Utilizem inadequadamente os procedimentos, fluxos de trabalho e ferramentas informatizadas.

A CONTRATADA, do Grupo 01, deverá dimensionar, alocar e manter equipe para execução adequada dos serviços contratados organizada no mínimo em grupos distintos para:

a) Governança e Gestão de Segurança da informação e Cibersegurança;
b) Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança;
c) Sustentação de Operações de Soluções e Resposta a Requisições de Segurança;
d) Gestão de Vulnerabilidades e Testes de Cibersegurança;
e) Gerenciamento de Acesso Privilegiado (PAM).

Para a implantação dos serviços, a CONTRATADA do Grupo 01 deverá disponibilizar profissional com o perfil de GERENTE DE PROJETOS.

A formação acadêmica mínima exigida para todo profissional de cada perfil é: curso superior completo de graduação na área de tecnologia da informação ou graduação em qualquer curso superior acrescido de curso de pós-graduação completo em área de tecnologia da informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

Para todos os itens solicitados na listagem de perfis por grupo de serviços a comprovação dos requisitos deverá ser composta de documentos como certificados ou diplomas de conclusão dos cursos exigidos. No caso dos cursos de nível superior deverão ser apresentados os diplomas.

A equipe técnica da CONTRATADA deverá possuir, no mínimo, os perfis e experiência dos profissionais alocados na prestação de cada um dos serviços, conforme quadro abaixo.

Perfil Profissional	**Quantidade Mínima**	**Formação Conhecimento**	**Certificações**	**Experiência**
Gerente Técnico do Contrato (Technical Account Manager - TAM)	Grupo 1: 1 Item 8: 1	Graduação em áreas de TI ou Segurança da Informação, com pós-graduação desejável. Contendo as seguintes habilidades: • Liderança e gerenciamento de equipe e conflitos.	O perfil deve possuir pelo menos 02 certificações, sendo uma delas CISSP ou CISM considerada obrigatória. • Certified Information Systems Security Professional (CISSP).	Mínimo de 03 (três) anos de experiência em gestão de segurança da informação.

Perfil Profissional	Quantidade Mínima	Formação Conhecimento	Certificações	Experiência
		• Responsável pela Qualidade do Serviço/Plataforma. • Apresentação Executiva / Técnica. • Especialista em Cibersegurança com ênfase em SOC.	• ISACA - Certified Information Security Manager (CISM). • EXIN - Information Security Foundation based on ISO/IEC 27001 (ISFS) ou similar • EXIN - Cyber and IT Security Foundation ou similar • ISC2 - Certified in Cybersecurity (CC) • EC-Council - Certified Security Specialist (E|CSS) • GIAC - Security Essentials (GSEC) • CompTIA - Security+ (SYO-601) ou superior • ISACA - CSX Cybersecurity Practitioner Certification (CSX-P)	
Governança e Gestão de Cibersegurança	Grupo 1: 1	• Conhecimento em Normas ISO (27005, 27002, 27001). • Conhecer os frameworks do CIS Control v8, Mitre ATT&CK, NIST Cybersecurity Framework. • Aplicação de avaliações e consultoria. • Realização de Assessments. • Criação de planos de governança corporativa e segurança da informação. • Gestão de Risco. • Análise de impacto no negócio.	O perfil deve possuir pelo menos 02 das certificações abaixo: • EXIN - Information Security Management Professional based on ISO/IEC 27001 (ISMP) ou similar • CompTIA - Security+ (SYO-601) ou superior • ISACA - Certified Information Security Manager (CISM) • ISACA - Certified in Risk and Information Systems Control (CRISC) • ISACA - Certified in Governance of Enterprise IT (CGEIT) • ISACA - Certified Information Systems Auditor (CISA)	Experiência mínima de 03 (três) anos em acompanhamento, auditoria e controles de conformidade, normas e riscos de TI.

Perfil Profissional	Quantidade Mínima	Formação Conhecimento	Certificações	Experiência
Monitoramento, Detecção e Resposta Gerenciados de Cibersegurança	Grupo 1: 3	• Triagem de eventos. • Categorização de ameaças. • Análise de impacto de incidentes. • Execução de Playbooks. • Contenção de Ameaças. • Atendimento de chamados dentro do SLA. • Execução de Checklist e Rotinas Operacionais. • Conhecimento em NIST 800-61 Rev2. • Runbook. • Automação de processos. • Desenvolvimento de Scripts.	O perfil deve possuir pelo menos 02 das certificações abaixo: • ISC2 - Certified Information Systems Security Professional (CISSP) • EC-Council - Certified Incident Handle (C|CIH) • EC-Council - Certified Ethical Hacker (C|EH) • EC-Council - Certified SOC Analyst (C|SA) • CompTIA - Security+ (SYO-601) ou superior • CompTIA - Cybersecurity Analyst (CySA+) • GIAC - Continuous Monitoring Certification (GMON) • GIAC - Certified Intrusion Analyst (GCIA) • GIAC - Certified Incident Handler (GCIH)	• Experiência na prestação de serviços de administração de solução de Gerenciamento e Correlação de Eventos de Segurança da Informação - SIEM, em ambientes com, no mínimo, 5.000 (cinco) mil ativos. • Mínimo de 03 (três) anos de experiência no monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e resposta a incidentes.
Analista de Inteligência de Ameaças (Threat Intelligence) e Caçada Contínua a Ameaças (Threat Hunting)	Grupo 1: 2	• Criação de Regras de Baseline. • Técnicas de OSINT. • Gerenciamento do ciclo de vida da inteligência de ameaças. • Criação de personas e interação com fraudadores. • Conhecimento de agentes de risco e grupos de ataque. • Detecção de novas fontes de ameaças e de monitoramento. • Prover Inteligência operacional e estratégica das ameaças. • Compartilhando informações de	O perfil deve possuir pelo menos 02 das certificações abaixo: • ISC2 - Certified Information Systems Security Professional (CISSP) • EC-Council - Certified Ethical Hacker (C|EH) • EC-Council - Certified Threat Intelligence Analyst (C|TIA) • CompTIA - Security+ (SYO-601) ou superior • CompTIA - Cybersecurity Analyst (CySA+) • GIAC - Continuous Monitoring Certification (GMON) • GIAC - Certified Intrusion Analyst (GCIA)	• Conhecimento avançado em segurança da informação, com experiência em investigação e identificação de possíveis ameaças à segurança da informação da organização, trabalhando com grande variedade de fontes, incluindo dados de rede, registros de segurança e inteligência de ameaças, para identificar atividades suspeitas. • Experiência comprovada de no mínimo 12 (doze)

Perfil Profissional	Quantidade Mínima	Formação Conhecimento	Certificações	Experiência
		inteligência através do MISP. • Caçada de ameaças. • Conhecimento em metodologias como Tahiti, Magma e HMM. • Descobrir novas ameaças e TTPs. • Busca ativa e proativa de indicadores de comprometimento (IOCs). • Análise de log e correlação de eventos. • Colaboração com Threat Intelligence. • Criação de casos de uso de SIEM. • Criação de novos playbooks.	• GIAC - Certified Incident Handler (GCIH)	meses em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e Advanced threat detection (ATD).
Analista de Resposta a Incidentes e Forense Digital (DFIR)	Grupo 1: 1	• Condução de WarRoom de Incidentes. • Condução de Resposta a Incidentes Cibernéticos (CIR). • Condução de Análises Forenses (DFIR). • Análise de Malware, Rede e Sistemas. • Confecção de Relatório de Causa Raiz e Recomendações. • Conhecimento em NIST 800-61 Rev2.	O perfil deve possuir pelo menos 02 das certificações abaixo: • ISC2 - Certified Information Systems Security Professional (CISSP) • EC-Council - Certified Ethical Hacker (C|EH) • EC-Council - Computer Hacking Forensic Investigator (C|HFI) • CompTIA - Security+ (SYO-601) ou superior • CompTIA - Cybersecurity Analyst (CySA+) • GIAC - Continuous Monitoring Certification (GMON) • GIAC - Certified Intrusion Analyst (GCIA) • GIAC - Certified Incident Handler (GCIH)	• Experiência na prestação de serviços de identificação, investigação e resposta a incidentes de segurança cibernética. • Deve ainda possuir experiência na investigação, coleta, análise e preservação de evidências digitais independente da fonte, incluindo computadores, dispositivos móveis, redes e dados em nuvem, para identificar e reconstruir atividades suspeitas. • Experiência comprovada de no mínimo 12 (doze) meses em monitoramento de ataques cibernéticos

Perfil Profissional	Quantidade Mínima	Formação Conhecimento	Certificações	Experiência
				utilizando ferramentas e soluções de SIEM e Advanced threat detection (ATD).
Analista de Gestão de Vulnerabilidades e Testes de Segurança	Grupo 1: 1 Item 8: 1	• Execução de varreduras de rede e de vulnerabilidades. • Conhecimento em Teste de invasão e exploração de vulnerabilidades. • Fazer parte do planejamento e estratégia de gestão vulnerabilidades. • Aplicar a política de gestão de vulnerabilidades. • Acompanhar plano de ação das vulnerabilidades. • Tenable: Conhecimento avançado em sustentação e operação de solução Tenable.	O perfil deve possuir pelo menos 02 das certificações abaixo: • EC-Council - Certified Ethical Hacker (C|EH) • EC-Council - Certified Penetration Testing Professional (C|PENT) • Offensive Security Certified Professional (OSCP) • CompTIA Security+ (SYO-601) ou superior • CompTIA - Cybersecurity Analyst (CySA+) • CompTIA - PenTest+ • GIAC - Penetration Tester Certification (GPEN)	• Experiência na prestação de serviços de gestão de vulnerabilidades, incluindo o monitoramento e o tratamento das vulnerabilidades. • Experiência em testes de invasão de segurança da informação em ambientes com, no mínimo, 1.000 (um mil) ativos. • Experiência comprovada de no mínimo 2 (dois) anos.
Analista de Segurança	Grupo 1: 3, sendo pelo menos 01 de cada especialidade (Palo Alto, Microsoft, PAM)	• Palo Alto: Conhecimento avançado na sustentação e operação de Solução de Firewall Palo Alto Networks • Microsoft: Conhecimento avançado na sustentação e operação de soluções de segurança Microsoft. • PAM: Conhecimento avançado na solução informatizada PAM.	O perfil deve possuir respectivamente as certificações abaixo: • Palo Alto: Palo Alto Networks Certified Network Security Administrator (PCNSA). • Microsoft: SC-200 Secure IT systems with threat management, monitoring, and response solutions. • Certificação de nível avançado da Solução Informatizada de PAM (Privileged Access Management), ofertada pela CONTRATADA.	• Experiência na prestação de serviços de sustentação e operação de solução de firewall Palo Alto Networks. • Experiência na prestação de serviços de sustentação e operação de solução Microsoft como Microsoft 365 E3 com Add-on E5 Security, contendo os recursos de Defender for Office Plan 1 e 2, Entra ID Plan 1 e 2, Defender for Endpoint Plan 2.

Perfil Profissional	Quantidade Mínima	Formação Conhecimento	Certificações	Experiência
				• Experiência na prestação de serviços de sustentação e operação de solução informatizada de PAM (Privileged Access Management), ofertada como serviço pela CONTRATADA. • Experiência comprovada de no mínimo 24 meses para cada solução.

Tabela 5 - Perfis e experiência profissional dos profissionais

4.4. METODOLOGIA DO TRABALHO

4.4.1. ATENDIMENTO – Grupo 01

A modalidade principal de atendimento e execução dos serviços será do tipo remota, realizada nas dependências da CONTRATADA, obedecendo, obrigatoriamente, os critérios estabelecidos para a sua execução, conforme previstos neste Termo de Referência e seus anexos.

As solicitações de atendimento poderão ser registradas a qualquer tempo.

Todos os atendimentos deverão ser iniciados no Brasil e no idioma português do Brasil.

Os serviços gerenciados de Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança devem obrigatoriamente serem executados, ofertados, e estarem acessíveis à CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, após a implementação do serviço.

As seguintes atividades devem ser realizadas obrigatoriamente em modalidade presencial nas dependências do TRIBUNAL, sendo elas:

a) Atividades de implantação, atualização e manutenção de equipamentos fornecidos e gerenciados pela CONTRATADA, planejadas ou emergenciais;
b) Atuação em casos de inacessibilidade de soluções, equipamentos e recursos gerenciados;
c) Atuação em incidentes massivos, incidentes críticos, crises e desastres, quando as equipes remotas e profissionais envolvidos esgotarem tempo considerado razoável para tratamento e resposta do incidente;
d) Em situações urgentes e estratégicas em que seja indispensável e altamente recomendada a atuação presencial, sendo devidamente comunicadas pelo TRIBUNAL.

Não havendo a solução do incidente de forma remota, a CONTRATADA deverá fazer o atendimento de forma presencial, a fim de solucionar o problema sem que acarrete qualquer ônus ao TRIBUNAL.

Para os casos de incidentes cibernéticos com impacto crítico que impossibilitem a prestação de serviço remoto, o TRIBUNAL determinará à CONTRATADA, que os perfis profissionais se apresentem, no prazo de 12 horas, na sede da SETI do TRIBUNAL, em Curitiba-PR, para a continuidade da prestação dos serviços. Essa condição deverá permanecer até que

seja restabelecida a situação de normalidade para o atendimento na modalidade remota, situação que será sinalizada pelo TRIBUNAL.

A decisão de acionamento da CONTRATADA para tratar os Incidentes Cibernéticos de impacto crítico, bem como o seu desacionamento cabe, única e exclusivamente ao CONTRATANTE.

Os serviços realizados pela CONTRATADA, deverão ser efetuadas de forma a não comprometer o perfeito funcionamento dos sistemas, recursos ou equipamentos da CONTRATANTE, devendo a CONTRATADA seguir o Processo de Mudança e janelas de manutenção estabelecidos no TRIBUNAL.

Caso haja a necessidade de interrupção dos sistemas, recursos, equipamentos ou da rotina dos trabalhos de qualquer setor funcional, em decorrência dos serviços realizados pela CONTRATADA, estes deverão estar devidamente planejados e serem necessariamente aprovados pela CONTRATANTE.

Quaisquer alegações por parte da CONTRATADA contra infraestrutura (ambiente inadequado, baixo desempenho dos servidores de processamento de dados, storage ou rede logica etc.) ou mau uso dos usuários da CONTRATANTE, devem ser comprovadas tecnicamente através de laudos detalhados e conclusivos. Não serão admitidas conclusões baseadas em suposições técnicas sem fundamentação, “experiência” dos técnicos ou alegações baseadas em exemplos de terceiros. Enquanto não for efetuado o laudo, e esse não demonstrar claramente os problemas alegados, a CONTRATADA deve prosseguir com o atendimento aos chamados.

A CONTRATADA deve prever nos processos de gestão de serviços, incluindo o processo de tratamento e resposta à incidentes de segurança cibernética, a matriz RACI, o momento e a forma de escalar e demandar para o TRIBUNAL requisições, incidentes e mudanças de segurança, quando envolver equipes internas de sustentação e operação de infraestrutura e sistemas, contratos de apoio e outros serviços específicos existentes para os ativos e serviços de TIC envolvidos que não sejam cobertos pelo objeto contratado, e deve executar tais escalonamentos conforme previsto.

Os chamados deverão ser registrados no sistema de atendimento, contendo no mínimo as seguintes informações:

a) Número do registro da solicitação;
b) Data e hora de abertura;
c) Nome do solicitante (usuário);
d) Motivo da abertura do chamado;
e) Estado da solicitação (em aberto, pendente ou concluído);
f) Descrição da resolução do chamado;
g) Data e hora do fechamento.

4.4.2. CANAIS DE COMUNICAÇÃO E ATENDIMENTO – Grupo 01

A CONTRATADA deve prover no mínimo os seguintes canais de comunicação para atendimento aos chamados e solicitações para os todos os serviços gerenciados de segurança da informação e cibernética, que devem estar disponíveis 24x7x365 (vinte e quatro horas por dia, sete dias da semana, todos os dias do ano):

1. Linha ou central telefônica gratuita ou com custo de ligação local com cobertura nacional (0800, 0300, 400x), acessível a partir de telefones fixos e celulares;
2. Portal de serviços via web, com tráfego criptografado utilizando protocolo SSL/TLS compatível com os principais navegadores web e plataformas desktop;
3. Correio eletrônico (e-mail), com domínio registrado e de propriedade da CONTRATADA.

Para os atendimentos urgentes, incluindo a incidentes massivos e de alta severidade, serviços de sustentação indisponíveis e em cenário de crise ou desastre, devem ser previstos canais de comunicação prioritários, incluindo no mínimo:

a) Linha telefônica com a opção de contato direto com atendente humano com no máximo 01 nível de atendimento automático via URA;
b) Sala de videoconferência segura, acessível via web e aplicativos desktop e móvel, permitindo reuniões de no mínimo 10 (dez) pessoas.

Todo o atendimento deve ser iniciado por profissionais da CONTRATADA, que estejam em horário de trabalho no momento do atendimento, vedado o uso do chamado “regime de plantão”, “sobreaviso” e/ou sistemas similares, onde o funcionário passa a trabalhar apenas quando acionado.

Os atendimentos referentes aos serviços continuados do objeto contratado são ilimitados durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas e/ou quantidade de atendimentos realizados, se limitando apenas ao escopo, com exceção dos serviços que são sob demanda ou unitários.

A CONTRATADA, do Grupo 01, deve realizar a condução de análises regulares da eficácia das regras, políticas e configurações implementadas nas ferramentas de segurança, sugerindo e implementando melhorias para fortalecer a postura de segurança do CONTRATANTE.

O compartilhamento interno das informações do SOC deve manter aderência, no que couber, ao padrão Traffic Light Protocol (TLP) e, ainda, com futuros normativos relacionados à governança da informação do TRIBUNAL.

4.4.3. GESTÃO DOS SERVIÇOS - Grupo 01

A gestão e operação dos serviços pela CONTRATADA deve seguir os padrões e melhores práticas internacionais de gestão de serviços de tecnologia (ITSM) do framework Axelos ITIL e/ou normas ISO 20000 - Gestão de serviços de tecnologia da informação.

A CONTRATADA, do Grupo 01, deverá estruturar no seu sistema ITSM e em seus canais de atendimento um catálogo de serviços, fluxos de atendimento, tratamento e escalonamento, e base de conhecimento que reflitam adequadamente todas as necessidades do objeto, cabendo também à CONTRATADA realizar ajustes e melhoria contínua sempre que necessário.

Solicitações de atendimento e de serviços, junto com os incidentes identificados, devem ser convergidos, registrados, mantidos, atualizados e resolvidos em um único sistema de gerenciamento de serviços de tecnologia da CONTRATADA, de forma a garantir que todas as informações estejam sempre consolidadas e atualizadas, independente do canal de comunicação utilizado.

Na gestão e operação de serviços, a CONTRATADA deve:

a) Integrar, seja via APIs ou serviços web, com a plataforma ServiceNow, incluindo no mínimo os módulos ITSM e SecOps, licenciado pelo TRIBUNAL;
b) Realizar a comunicação bilateral imediata ou no menor tempo possível;
c) Replicar os dados, alinhados com a equipe técnica do tribunal, das solicitações e incidentes para o acompanhamento e gestão pela equipe interna do TRIBUNAL.

As solicitações de atendimento poderão ser registradas a qualquer dia e horário, tanto em dias úteis como finais de semana, feriados e pontos facultativos, e devem ser atendidos de acordo com os níveis mínimos de serviço.

As solicitações de atendimento podem ser abertas automaticamente por soluções informatizadas da CONTRATADA e do TRIBUNAL, de acordo com integrações definidas.

Não deverá haver fechamento de uma solicitação de atendimento sem a anuência do TRIBUNAL, seja em processo aprovado ou em caráter excepcional, de forma que caso uma solicitação seja indevidamente fechada por profissional da CONTRATADA, poderá será reaberta pelo TRIBUNAL no prazo de até 30 (trinta) dias corridos, voltando a contar o prazo a partir da abertura original da solicitação de atendimento, inclusive para efeitos de aplicação das glosas e sanções.

Uma solicitação de atendimento somente poderá ser cancelada com a anuência do TRIBUNAL, que deverá analisar a situação para possível readequação de prazos e outras providências que se fizerem necessárias.

Enquanto requisições e incidentes estiverem escalados e/ou atribuídos ao TRIBUNAL, continua sendo responsabilidade da CONTRATADA o acompanhamento do andamento, o esclarecimento de dúvidas e a prestação do apoio técnico e consultivo necessário.

Nas requisições, incidentes e mudanças escaladas e demandas para o TRIBUNAL, a CONTRATADA deve observar e obedecer aos processos específicos de gestão de serviços de tecnologia do TRIBUNAL.

Sempre que aplicável, a CONTRATADA deve prever a integração e a comunicação bilateral com unidades, processos e, caso existam, ferramentas institucionais de governança e conformidade, de segurança institucional, de segurança da informação e de privacidade e proteção de dados pessoais, incluindo no mínimo:

a) Comitê de Governança de Segurança da Informação - CGSI e Unidade de Segurança da Informação;
b) Comitê de Crises Cibernéticas - CCC;
c) Núcleo de Segurança Institucional - NISI, em especial quando necessário articular ações junto às autoridades de polícia (civil e/ou militar) ou de inteligência e segurança institucional, incluindo notificação e investigação de incidentes penalmente relevantes e de ilícitos cibernéticos;
d) Comitê Gestor de Proteção de Dados Pessoais (CGPD) - em especial quando incidentes cibernéticos envolverem vazamento de dados pessoais e outras violações dos direitos fundamentais de liberdade e de privacidade da pessoa natural, nos termos da Lei Geral de Proteção de Dados Pessoais - LGPD (Lei federal Nº 13.709, de 14/08/2018) e demais legislação e normativos aplicáveis.

4.4.4. PORTAL DE INDICADORES DE SERVIÇO - Grupo 01

A CONTRATADA deverá disponibilizar ao TRIBUNAL um portal de indicadores de serviço, para consolidação dos dados, indicadores e métricas gerados das soluções informatizadas que compõem o objeto.

O portal deverá ser disponibilizado em modelo de software como serviço (SaaS) e estar acessível ao TRIBUNAL via Internet, em regime 24x7x365 (vinte e quatro horas por dia, sete dias da semana, todos os dias do ano), com mecanismos seguros adequados de comunicação e de autenticação.

O TRIBUNAL terá direito a criação de no mínimo 10 (dez) usuários com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.

Os usuários devem ser capazes de consultar, visualizar as informações em diferentes visões aplicáveis, incluindo gráficos diversos (tipo pizza, barra, linha etc.) e tabelas/listagens, bem como gerar relatórios.

Os dados e as informações disponibilizadas devem incluir, no mínimo, os insumos para apuração dos níveis mínimos de serviços aplicáveis, conforme instrumentos de medição de resultado constantes nos INDICADORES DE MEDIÇÃO DE RESULTADO (IMR).

Os dados e as informações exibidas pelo portal devem representar o ambiente em tempo de execução e de forma automática (real time).

Todos os indicadores exibidos pelo portal devem possuir a funcionalidade de detalhamento (drilldown).

Todos os indicadores exibidos pelo portal devem ainda possuir funcionalidade de exibição dos dados de origem de um gráfico de maneira tabular, a fim de que seja possível aferir os dados.

O portal deverá possibilitar customizar limiares dos serviços e eventos para gerar alarmes de acordo com o acordo os níveis mínimos de serviços definido no presente termo de referência.

O portal deve armazenar os dados durante o período mínimo de 1 (um) ano e deverá permitir a criação de filtros por períodos.

Dos indicadores de Risco - KRI:

a) Deverá ser exibido no portal a quantidade de Vulnerabilidades que estavam presentes na última auditoria realizada através de gráfico(s) com separação dos tipos/quantidades com a opção de "Drill Down", possibilitando assim visualização de forma mais detalhada das vulnerabilidades listadas.

b) O portal deverá possuir recurso para apresentar:

- **Total de vulnerabilidades no parque (categorizadas por risco);**
- **Novas vulnerabilidades identificadas;**
- **Indicador de compliance;**
- **Indicadores de saúde dos serviços gerenciados;**
- **Eventuais ameaças na Darkweb.**

Dos indicadores de meta e performance - KGI e KPI:

a) O portal de indicadores deverá possuir relatório gráfico indicando tempo médio dos atendimentos dos incidentes por fase de Análise, Contenção, Erradicação e Recuperação, possibilitando a filtragem por período: Últimos 15 dias; Últimos 30 dias; Últimos 45 dias;

b) Deverá possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro de período filtrado, exibindo uma linha de tempo que apresente qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio;

c) Deverá ser possível a consulta deste gráfico para cada uma das fases de atendimento (Análise, contenção, erradicação e recuperação);

d) Indicadores de saúde das soluções informatizadas ofertadas e sustentadas pela CONTRATADA.

Dos indicadores por categoria Mitre ATT&CK:

a) O Portal de indicadores deverá possuir gráfico que separe e classifique os incidentes de acordo com as categorias (táticas/técnicas) existentes na base de conhecimento do MITRE ATT&CK, sendo elas no mínimo:

- Initial Access;
- Execution;
- Persistence;

- Privilege Escalation;
- Defense Evasion;
- Credencial Access/brute force;
- Lateral Movement;
- Collection;
- Command and Control;
- Exfiltration;
- Impact.

4.4.5. RELATÓRIOS E REUNIÕES DE ACOMPANHAMENTO - Grupo 01

A CONTRATADA deverá entregar durante a vigência do contrato os seguintes relatórios e reuniões de acompanhamento:

Entregável	Periodicidade	Responsável	Prazo
Relatório de Indicadores de Medição de Resultados **- RIMR**	Mensal	CONTRATADA	até o 5º dia útil do mês.
Reunião técnica informativa - RTI, conforme **Tabela 7 - Relatório técnico de acompanhamento mensal.**	Mensal	CONTRATADA com a presença do Gerente Técnico	até o 3º dia útil do mês.
Reunião de alinhamento semanal **e acompanhamento de atividades,** possíveis apontados problemas recorrentes ou pontuais que estejam impactando a qualidade da execução do contrato. Após essas reuniões deverão ser formulados planos de ações corretivos para cada área/serviço que não esteja cumprindo os padrões de qualidade exigidos no contrato.	Semanal	CONTRATATA com participação da equipe técnica do TRIBUNAL	01 encontro semanal a ser definido pela equipe técnica do Tribunal.
Portal de indicadores de serviço, **conforme especificação do item 4.4.4.**	Diário	CONTRATADA	Diariamente até às 13h

Tabela 6 - Relatórios e reuniões de acompanhamento

Itens que devem ser contemplados na Reunião técnica informativa - RTI de acompanhamento mensal com entrega da ata da reunião:

Relatório técnico de acompanhamento		
ID	**Título**	**Descrição**
1	Introdução	a. Confidencialidade: quem pode acessar o documento b. Quadro de versões (versão, autor/revisor, data etc.) c. Índice analítico (sumário)
2	Resumo Executivo	a. Período de referência b. Quadro resumo e indicadores dos serviços executados no período

Relatório técnico de acompanhamento		
ID	**Título**	**Descrição**
		c. Ocorrência ou não de ataques bem-sucedidos ao TRIBUNAL no período d. Quantitativo de incidentes de segurança no período e. Quantitativo de eventos de segurança no período f. Quantitativo e estado de chamados no período g. Quantitativo e estado das vulnerabilidades e da superfície de ataque no período
3	Implantação, Melhoria Contínua e Transferência de Conhecimento	a. Progresso da fase de implantação inicial e pontos de atenção b. Melhorias nos serviços realizadas no período (pós-implantação inicial) c. Descritivo de relatórios, documentações e ações de transferência de conhecimento realizados no período
4	Serviços de Governança e Conformidade	a. Gráficos, métricas e indicadores consolidados estratégico-gerenciais e técnico-operacionais do período b. Lições aprendidas no período c. Análise de pontos de atenção d. Quadro-resumo das atividades e ocorrências no período e. Diagnósticos e avaliações realizados no período, seus principais resultados e indicadores de conformidade e de progresso f. Normas, políticas, planos, processos e procedimentos elaborados e/ou revisados no período, com suas principais considerações g. Aspectos abordados ou revisados na Política de Segurança da Informação, Plano de Continuidade de Serviços Essenciais de TIC, Plano de Resposta a Incidentes no período h. Oportunidades pontuais de melhoria do serviço
5	Monitoramento, Detecção e Resposta de Cibersegurança	a. Gráficos e indicadores do serviço b. Análise de pontos de atenção c. Quadro-resumo das atividades e ocorrências no período d. Visão consolidada dos playbooks e casos de uso de monitoramento, tratamento e resposta implementados, revisados e executados no período e. Hipóteses, atividades e evidências da caçada contínua de ameaças (threat hunting) no período f. Oportunidades pontuais de melhoria do serviço
5.1	Ataques (quando houver)	a. Detalhamento de ataques bem-sucedidos, ações realizadas, impacto
5.2	Incidentes de Segurança	a. Quadro resumo dos TOP 10 incidentes do período b. Descrição dos incidentes do período (detalhamentos dos ativos, origem e destino envolvidos etc.) c. Gráfico de histórico do quantitativo de eventos (últimos 6 meses) d. Ações tomadas para tratamento e resposta dos incidentes
5.3	Eventos de Segurança	a. Quadro-resumo dos TOP 10 eventos de segurança correlacionados do período b. Visão consolidada das triagens, investigações e caças de ameaças realizadas no período

Relatório técnico de acompanhamento		
ID	**Título**	**Descrição**
		c. Gráfico de histórico do quantitativo de eventos por categoria (últimos 6 meses) d. Quadro-resumo da situação dos chamados
5.4	Proteção contra Riscos Digitais (DRP)	a. Ocorrências identificadas no período e seu tratamento b. Takedowns comunicados e seu andamento c. Gráfico histórico do quantitativo e tipos de ocorrências (últimos 6 meses)
6	Sustentação de Operações de Soluções e Resposta a Requisições	a. Gráficos de indicadores do serviço b. Análise de pontos de atenção c. Quadro-resumo das requisições recebidas no período d. Oportunidades pontuais de melhoria do serviço
7	Gestão de Vulnerabilidades e Testes de Segurança	a. Gráficos e indicadores do serviço b. Análise de pontos de atenção c. Quadro-resumo das atividades e ocorrências no período d. Oportunidades pontuais de melhoria do serviço
7.1	Gestão Contínua de Vulnerabilidades	a. Quadro resumo das TOP 10 vulnerabilidades no período b. Segregação de informações por nível de severidade da vulnerabilidade c. Quadro resumo das vulnerabilidades identificadas e remediadas no período d. Varreduras automatizadas de vulnerabilidade em ativos internos realizadas no período e. Varreduras automatizadas de vulnerabilidade em ativos expostos externamente realizadas no período f. Gráfico de histórico dos quantitativos de vulnerabilidades (últimos 6 meses)
8	Serviços Técnicos Especializados	a. Descrição, progresso e quantitativo de horas técnicas das ordens de serviço abertas, em andamento e concluídas no período b. Análise de pontos de atenção

Tabela 7 - Relatório técnico de acompanhamento

4.5. REQUISITO DE SEGURANÇA - Grupo 01 e Item 8

A CONTRATADA e seus profissionais devem estar alinhadas com a Política de Segurança de Informação - PSI deste TRIBUNAL.

A fim de garantir a segurança entre CONTRATANTE e a CONTRATADA não será permitido SOC terceirizado ou consórcio de empresas.

A CONTRATADA deve assinar e entregar a CONTRATANTE no início da vigência do contrato o Termo de Sigilo e Confidencialidade, conforme ANEXO II - TERMO DE SIGILO E CONFIDENCIALIDADE (CONTRATADA) modelo contido neste Termo de Referência.

O termo de confidencialidade e sigilo deve ser reconhecido e assinado por todos os funcionários que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato, sendo que o CONTRATANTE pode solicitar, a qualquer momento, a comprovação dessa obrigação.

As exigências do termo de sigilo e confidencialidade visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TIC.

A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais informações, dados, mídias, documentos ou meios de armazenamento.

4.6. CONFORMIDADE TÉCNICA E LEGAL – Grupo 01 e Item 8

A CONTRATADA deverá estar alinhada com as premissas, políticas e especificações técnicas que regulamentam a Secretaria de Tecnologia da Informação - SETI do TRIBUNAL, quando aplicáveis. Deverão ser observados os seguintes preceitos legais na contratação:

a) Lei Geral de Proteção de Dados Nº 13.709/2018;
b) Lei Estadual Nº 15.608/2007;
c) Lei Federal Nº 8.666/1993;
d) Resolução Nº 182/2013 do CNJ;
e) Lei Federal Nº 14.133/2021;
f) Decreto Estadual Nº 10.086/202;
g) Resolução Nº 468/2022 do CNJ;
h) Lei Federal Nº 9.609/1998 (Lei de Proteção da Propriedade Intelectual de Programa de Computador);
i) Resolução Nº 370 de 28/01/2021 do CNJ;
j) Resolução Nº 396 de 07/06/2021 do CNJ;
k) Portaria Nº 162 de 10/06/2021 do CNJ.

A CONTRATADA deverá atender aos dispositivos da Lei Federal n° 13.709/2018 - Lei Geral de Proteção de Dados, em específico no compromisso de:

a) abster-se de qualquer atividade que constitua uma violação das disposições da Lei;
b) admitir o tratamento de seus dados pessoais nos termos da Lei;
c) vedar o tratamento de dados pessoais sensíveis com objetivo de qualquer espécie, com exceção daquelas hipóteses previstas no parágrafo 4° do art. 11 da Lei Federal no 13.709/18;
d) dar ciência prévia ao CONTRATANTE para fazer uso dos dados privados, sempre zelando pelos princípios da minimização da coleta, necessidade de exposição específica da finalidade, sem prejuízo da mera correção dos dados.

5. MODELO DE EXECUÇÃO DO OBJETO (ART. 6º, XXIII, E)

5.1. FASES DO CONTRATO

Devido à complexidade e criticidade dos serviços contratados será implementado, para a execução do contrato, o método de trabalho baseado no conceito de delegação de responsabilidade. Esse conceito define o CONTRATANTE como responsável pela gestão do contrato e pela atestação da aderência aos padrões de qualidade exigidos dos serviços entregues, e a CONTRATADA como responsável pela execução dos serviços e gestão dos recursos humanos e soluções de segurança necessárias.

Para o Grupo 01, em razão da natureza da contratação, este objeto prevê 03 (três) fases de execução:

Fases do contrato	Descrição
Projeto e implantação	Iniciando a partir do 1º dia de vigência do contrato até o início da fase de Operação
Operação	Iniciando a partir do 91º dia de contrato até o término do contrato
Transição do Serviço	Iniciando em até 90 dias antes da data de término do contrato, ocorrendo em paralelo com fase de Operação

Tabela 8 - Fases do contrato

I) Fase de Projeto e implantação

Os primeiros 90 (noventa) dias de contrato serão considerados como período de **Projeto e implantação** para ajuste dos serviços, durante os quais os **Indicadores de Medição de Resultado (IMR)** não serão medidos e os itens de serviço mensais contínuos não serão pagos, devendo a CONTRATADA considerar todos os custos necessários para a execução dos serviços durante este período no valor do item 1 "Projeto e implantação", do Grupo 01.

A CONTRATADA deve executar no prazo máximo de 90 (noventa) dias, a contar da assinatura do contrato, a fase de **Projeto e implantação** com as atividades de planejamento, instalação, adoção tecnológica, implantação do serviço, configuração e elaboração de documentação técnica, em conformidade especificação técnica deste Termo de Referência.

II) Fase de Operação

Na **fase de Operação** todos os serviços continuados devem operar de forma integral, devendo todos os recursos e soluções previstos estarem disponibilizados pela CONTRATADA, com a aplicação dos indicadores e metas de desempenho e qualidade, estando sujeita as penalidades e glosas pelo não cumprimento dos níveis de serviço estabelecidos.

Nesta fase, os **Indicadores de Medição de Resultado (IMR)** serão medidos e os itens de serviço mensais contínuos serão pagos mensalmente, mediante efetiva comprovação.

III) Fase de Transição do Serviço

A Fase de Transição do Serviço está relacionada ao processo de finalização pela CONTRATADA da prestação dos serviços contratados, visando estabelecer critérios de **Transição do Serviço**, pelo tempo necessário e de forma a garantir a transferência de conhecimento e adaptação de eventual nova(s) empresa(s) contratada(s) e equipes do TRIBUNAL que vierem a absorver os serviços.

A CONTRATADA deve elaborar planejamento e realizar o repasse integral e irrestrito de informações, dados, documentos e conhecimentos necessários e suficientes para promover a continuidade dos serviços.

A CONTRATADA deverá envidar esforços para a correta e tempestiva transferência de informações, conhecimentos e dados para a nova CONTRATADA para prestação dos serviços, inclusive mediante participação efetiva das equipes técnicas no planejamento.

A CONTRATADA deve exportar e fornecer, em formato completo, aberto e interoperável:

- Uma consolidação completa de todas as políticas, estratégias, planos, processos, procedimentos, métricas, indicadores e painéis elaborados, revisados e/ou propostos pela CONTRATADA;
- Todos os dados, informações, registros, relatórios e configurações relevantes da solução Informatizada para Gerenciamento, Monitoramento, Detecção e Resposta de Informações, Eventos e Incidentes de Segurança,

incluindo os registros (logs) consolidados e repositórios de dados e metadados de eventos e incidentes, casos de uso de monitoramento, playbooks, regras e scripts de resposta, orquestração e automação, dentre outros relevantes;

- Todos os dados, informações, registros, relatórios e configurações relevantes da solução Informatizada de Gestão de Acesso Privilegiado - PAM, incluindo os registros (logs) consolidados e repositórios de dados e metadados de eventos, políticas, estratégias, planos, processos, procedimentos, métricas, dentre outros relevantes;
- Consolidação completa de todas as políticas, estratégias, planos, topologias, processos, procedimentos, métricas, indicadores e painéis elaborados, metodologia de trabalho e configurações relevantes relacionados aos serviços de sustentação e operação;
- Todos os dados, informações, registros, relatórios e configurações relevantes do serviço de Proteção contra Riscos Digitais;
- Todos os dados, informações, registros, relatórios e configurações relevantes da solução informatizada de testes de segurança, incluindo catálogo atualizado de ativos de software identificados e suas configurações, vulnerabilidades identificadas, remediações aplicadas, regras e exceções adotadas, critérios e métricas de priorização de riscos, dentre outros relevantes;
- Todos os dados, informações, registros, relatórios e configurações relevantes da Solução informatizada de simulação de violações e ataques.

A CONTRATADA deverá elaborar e atualizar toda a documentação que porventura não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato.

Durante a fase de **Transição do Serviço**, caso um ou mais serviços sejam substituídos por novos serviços contratados aptos a iniciar operação imediata, o TRIBUNAL pode definir escala gradativa de respectivos serviços da CONTRATADA que serão interrompidos até o término da transição.

Ao término da vigência do contrato, deve haver:

- A revogação de todas as credenciais e autorizações de acesso da CONTRATADA aos serviços e soluções informatizadas;
- A suspensão ou eliminação de caixas postais e outros recursos de tecnologia que eventualmente tenham sido criados ou destinados para a CONTRATADA;
- A devolução de recursos materiais que eventualmente tenham sido destinados para a CONTRATADA.

5.2. DINÂMICA DA EXECUÇÃO

A execução do contrato será sob o regime de empreitada por preço global, com exceção aos itens 2.1 - Diagnóstico de Maturidade de Segurança da Informação e item 7 - Serviços Técnicos Especializados por Demanda, bem como do item 8 - Serviço de Teste de Invasão (Pentest), aos quais o regime será de empreitada por preço unitário (sob demanda).

A tabela a seguir apresenta a dinâmica e os prazos máximos que devem ser executados para o Grupo 01, com exceção ao ID 11 da Tabela 9.

ID	Evento	Prazo	Medição	Responsável
1	Assinatura do Contrato	D	-	CONTRATADA e CONTRATANTE
2	Reunião de iniciação (kick-off) do contrato, incluindo alinhamento sobre os itens 3 e 4	D + 5	Úteis	CONTRATADA e CONTRATANTE

ID	Evento	Prazo	Medição	Responsável
3	Emissão de OS para execução do primeiro Diagnóstico de Maturidade de Segurança da Informação	D + 5	Úteis	CONTRATANTE
4	Apresentação do Projeto e implementação pela CONTRATADA, contendo o detalhamento das ações necessárias para a absorção dos conhecimentos e ativação dos serviços	D + 10 = P	Úteis	CONTRATADA
5	Alocação do Gerente Técnico do Contrato (TAM)	P	Marco	CONTRATADA
6	Aprovação do Projeto e implementação pelo TRIBUNAL com emissão do Termo de Recebimento Provisório	P + 3	Úteis	CONTRATANTE
7	Reunião de alinhamento dos serviços continuados "Política de Segurança da Informação (PSI)", "Plano de Continuidade de Serviços Essenciais de TIC" e "Plano de Resposta a Incidentes (PRI)"	D + 45	Corridos	CONTRATADA
8	Finalização do Projeto e implantação e entrega da Declaração final de implantação e documentação dos serviços, conforme especificação técnica	D + 90 = E	Corridos	CONTRATADA
9	Emissão pela CONTRATANTE do Termo de Recebimento Definitivo, após a conclusão do ID 8	E + 5	Corridos	CONTRATANTE
10	Entrega do primeiro Diagnóstico de Maturidade de Segurança da Informação	D + 90	Corridos	CONTRATADA
11	Início da fase de Operação	D + 91 = O	Corridos	CONTRATADA
12	Aprovação da entrega do primeiro Diagnóstico de Maturidade de Segurança da Informação	05 dias após a conclusão do item 10	Corridos	CONTRATANTE

Tabela 9 - Dinâmica de execução da implantação

ID	Evento	Prazo	Medição	Responsável
1	Primeiro dia do mês	M	Marco	-
2	Reunião técnica informativa - RTI	M + 3	Úteis	CONTRATADA
3	Entrega do Relatório Indicadores de Medição de Resultado - RIMR e Emissão da Nota Fiscal / Fatura definitiva do serviço mensal	M + 5 = N	Úteis	CONTRATADA
4	Pagamento Mensal	N + [Fluxo de pagamento]	Úteis	CONTRATANTE

Tabela 10 - Dinâmica de execução da operação

A execução dos itens de quantitativos unitários deverão ser controlados por fluxo de trabalho acordado entre a CONTRADATA e CONTRATANTE para que não excedam o valor máximo contratado.

A tabela a seguir apresenta a dinâmica e os prazos máximos que devem ser executados para os serviços sob demanda (itens 2.1, 7 e 8).

ID	Evento	Prazo	Medição	Responsável
1	O TRIBUNAL emite demanda de Ordem de Serviço (OS)	D	-	CONTRATANTE
2	Confirmação de recebimento de Ordem de Serviço (OS) pela CONTRATADA	D + 3	Úteis	CONTRATADA
3	O prazo máximo para CONTRATADA analisar a demanda e apresentar uma proposta, com prazo/cronograma de execução e quantidade de horas técnicas necessárias (Prazo R)	D + 10 = P	Úteis	CONTRATADA
4	Aprovação/Rejeição da proposta pelo TRIBUNAL e autorização da Ordem de Serviço (OS)	P + 5 = O	Úteis	CONTRATANTE
5	Início da execução da Ordem de Serviço (OS)	O + 5	Úteis	CONTRATADA
6	CONTRATADA conclui a execução da Ordem de Serviço (OS) com entrega dos relatórios	R	Úteis	CONTRATADA
7	Emissão do termo de Recebimento Provisório	R + 3	Úteis	CONTRATANTE
8	Aprovação/Rejeição da entrega pelo TRIBUNAL	R + 5 = S/N*	Corridos	CONTRATANTE
9	TRIBUNAL realiza solicitação revisões, adequações ou correções na entrega, caso rejeitada	N + 10 = M	Corridos	CONTRATANTE
10	Prazo máximo para CONTRATADA realizar os ajustes solicitados (retorna item 7)	M + 5 = R	Corridos	CONTRATADA
11	Aprovada a entrega da Ordem de Serviço (OS), o TRIBUNAL emitirá o termo de Recebimento Definitivo	S + 10	Corridos	CONTRATANTE

Tabela 11 - Dinâmica de execução serviços sob demanda (itens 2.1, 7 e 8)

* Aprovação ou não do relatório de execução da OS.

A CONTRATADA poderá solicitar a ampliação do prazo máximo apresentando justificativa. A ampliação do prazo máximo somente poderá ocorrer por decisão exclusiva do CONTRATANTE, devendo ser adequados os demais prazos.

No caso de descumprimento dos prazos estabelecidos a CONTRATADA estará sujeita as penalidades descritas no CADERNO DE PENALIDADES - Grupo 01 e item 8 .

Haverá suspensão de contagem dos prazos para as Ordens de Serviço (OS) que necessitarem de providência por parte do CONTRATANTE.

Considerando que o valor do Grupo 1 ultrapassa a quantia de R$ 5.000.000,00 (cinco milhões de reais), a CONTRATADA deverá entregar o Formulário de Análise de Perfil das Contratadas do Tribunal de Justiça do Estado do Paraná no prazo de até 30 (trinta) dias corridos contados após a assinatura do contrato, sob pena de aplicação das sanções previstas neste Termo de Referência, conforme previsto no Decreto Judiciário nº 62/2026. A solicitação de preenchimento do formulário será enviada à contratada pelo gestor do contrato, por meio de link, em até 5 (cinco) dias úteis após a assinatura do instrumento contratual.

5.3. INSTRUMENTOS DE SOLICITAÇÃO DO (S) SERVIÇO(S)

Os instrumentos de solicitação dos serviços deverão atender a todos os critérios técnicos especificados neste Termo de Referência.

5.4. MONITORAMENTO DA EXECUÇÃO

5.4.1. ACOMPANHAMENTO DA CONTRATAÇÃO - Grupo 01 e item 8

O representante do TRIBUNAL registrará todas as ocorrências relacionadas com o fornecimento e a execução dos serviços especificados neste Termo de Referência, determinando o que for necessário à regularização das faltas ou defeitos observados.

As decisões e providências que ultrapassarem a competência dos representantes deverão ser solicitadas aos seus superiores em tempo hábil para adoção das medidas convenientes.

A CONTRATADA deverá manter preposto para representá-la durante o fornecimento e a execução dos serviços ora tratados, desde que aceito pelo TRIBUNAL.

Ao TRIBUNAL é reservado o direito de efetuar diligência, a qualquer tempo, quanto aos documentos exigidos neste Termo de Referência e em seus anexos.

A existência e a atuação da fiscalização em nada restringem a responsabilidade, única, integral e exclusiva da CONTRATADA, no que concerne à execução do objeto contratado.

O acompanhamento da contratação deverá atender a todos os requisitos técnicos especificados neste Termo de Referência.

5.4.2. MECANISMOS FORMAIS DE COMUNICAÇÃO - Grupo 01 e item 8

Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

A comunicação se dará por e-mail, reuniões virtuais (gravadas), ofícios, telefonemas, e outros correlatos que possam ficar registrados.

Os emissores de comunicações formais, por parte do CONTRATANTE, serão os membros da equipe de fiscalização.

O destinatário de comunicações formais será o preposto da CONTRATADA.

5.5. TRANSFERÊNCIA DE CONHECIMENTO – Grupo 01

A CONTRATADA deve promover a transferência de conhecimento aos indicados pelo TRIBUNAL, de forma a permitir a plena gestão, entendimento, operação, monitoramento e otimização dos serviços e soluções objeto do contrato, na forma de reuniões, apresentações, documentação, relatórios e outros meios que se façam adequados.

A transferência de conhecimento deverá ser ministrada de forma a cobrir toda estrutura e topologia projetada para atendimento aos requisitos da contratação, e deve estar contemplada nas fases de Projeto e implantação, Operação e Transição.

A CONTRATADA deverá encaminhar à CONTRATANTE os documentos comprobatórios de realização da transferência do conhecimento.

A transferência de conhecimento pode ser realizada em formato presencial ou online, conforme determinado pelo CONTRATANTE.

Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida, mediante formalização entre as partes, ao término ou rompimento do contrato ou por solicitação do TRIBUNAL.

A CONTRATADA deverá, seja proativamente ou quando identificada a necessidade, ou sob demanda mediante a formalização da solicitação pelo TRIBUNAL, elaborar e apresentar pareceres técnicos de análise, esclarecimento, orientação, estudos e recomendações sobre demandas e assuntos especializados relacionados a quaisquer dos serviços prestados.

A CONTRATADA deverá consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades.

5.6. NÍVEIS DE SERVIÇOS EXIGIDOS (NSE)

Os níveis de serviços exigidos deverão atender a todos os critérios especificados neste Termo de Referência.

5.7. DIREITOS DE PROPRIEDADE INTELECTUAL - Grupo 01 e item 8

A CONTRATADA cederá ao TRIBUNAL o direito patrimonial e a propriedade intelectual, em caráter definitivo, de todos e quaisquer produtos e resultados gerados em consequência do cumprimento deste contrato, podendo o CONTRATANTE proceder às modificações necessárias à continuidade do serviço e/ou contratar terceiros para fazê-lo.

Entendem-se por resultados os relatórios, análises, estudos e pareceres técnicos, normativos (políticas, estratégias, planos, processos, procedimentos), métricas, indicadores e painéis definidos, documentação, casos de uso, playbooks e runbooks, controles e salvaguardas propostos e implantados, scripts, códigos fonte, protótipos, registros, modelos e bases de dados e qualquer outro conteúdo ou informação produzido exclusivamente em decorrência da execução dos serviços.

A CONTRATADA cederá também ao TRIBUNAL os direitos autorais vinculados à prestação dos serviços, nos termos do artigo 4º da Lei Nº 9.609/1998, referentes a todos e quaisquer produtos e resultados gerados em consequência do cumprimento deste contrato.

Caberá à CONTRATADA arcar com quaisquer valores decorrentes de imputação judicial ao CONTRATANTE, relativos a esses direitos.

Ficam resguardados os direitos autorais de resultados ou produtos decorrentes da execução dos serviços que tenham prévia restrição de direitos de propriedade patrimonial e intelectual ou autorais da CONTRATADA ou de terceiros, devendo nestes casos ser concedido o direito de uso mais amplo possível ao CONTRATANTE, visando sua continuidade e independência.

5.8. SUBCONTRATAÇÃO

Fica vedada a subcontratação total ou parcial do objeto contratual, uma vez que a sua prestação não pode ser dividida em frações de execução sem prejudicar a solução como um todo. Assim, a proibição de subcontratação atua como uma salvaguarda para a integridade e o bom desempenho dos serviços, prevenindo os efeitos negativos do compartilhamento de responsabilidades entre a CONTRATADA e a subcontratada durante a execução contratual.

5.9. DA PARTICIPAÇÃO DE CONSÓRCIOS

Não será permitida a participação de consórcios nesta licitação. A exigência de consórcios usualmente é aplicada a objetos complexos que nenhuma empresa, individualmente, conseguiria fornecer, o que não se aplica a este caso.

5.10. PARTICIPAÇÃO DE COOPERATIVAS

As cooperativas também não poderão participar deste certame, pois a natureza dos serviços a serem executados apresenta características incompatíveis com a organização do trabalho em forma de cooperativa, tais como: demandas com mecanismos de gestão e controle continuados visando assegurar a adoção de métodos e padrões que são rotineiramente verificados; relação de hierarquia técnica e funcional entre os profissionais; níveis diferenciados de responsabilização técnica; empresas cujo objeto social não seja pertinente e compatível com o objeto deste termo de referência e seus anexos.

6. MODELO DE GESTÃO DO CONTRATO (ART. 6º, XXIII, F)

6.1. FISCALIZAÇÃO

A CONTRATADA deve fiscalizar o cumprimento do objeto do contrato, cabendo-lhe integralmente os ônus decorrentes de má fiscalização. Esta dar-se-á independentemente daquela será exercida pelo CONTRATANTE.

O CONTRATANTE se reserva ao direito de acompanhar e fiscalizar os serviços realizados pela CONTRATADA, verificando a aderência às especificações técnicas definidas, zelando pelo cumprimento dos prazos e monitorando a qualidade dos serviços.

A fiscalização realizada por parte do CONTRATANTE não diminui ou atenua a responsabilidade da CONTRATADA pela execução de qualquer serviço.

6.2. PRINCIPAIS PAPÉIS

A Equipe de Gestão da Contratação, designada no documento 10169470, é definida na tabela a seguir.

Gestor do Contrato Titular - Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas a coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente do órgão.	**Maria Aparecida Levis Costa** Analista de Sistemas
Gestor Suplente do Contrato Suplente - Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas a coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente do órgão.	**Paulo Alfredo Ribas Toledo** Técnico em Computação
Fiscal Administrativo Titular - Servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.	**Simone Sampaio Ribeiro** Técnico Judiciária
Fiscal Administrativo Suplente - Servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.	**Stephanie Wakabayashi** Técnico Judiciária
Fiscal Demandante - Servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.	**Lauro Andrey de Souza Bueno** Analista de Sistemas
Fiscal Técnico - Servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.	**Adriano Witkovski** Técnico em Computação

Fiscal Técnico - Servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.	**Eder Sibirkin** Técnico em Computação

Tabela 12 - Equipe de Gestão da Contratação

Seus papéis e responsabilidades são definidas no artigo 22, § 3 da Resolução nº 468/2022 do CNJ e descritas no guia de contratações de STIC do poder judiciário (páginas 9/12), anexo à referida resolução. Segue abaixo as definições:

Caberá aos Gestores do Contrato todas as ações necessárias ao fiel cumprimento das condições estipuladas no contrato e ainda:

a) analisar a documentação que antecede o pagamento;
b) analisar os pedidos de reequilíbrio econômico-financeiro do contrato;
c) analisar eventuais alterações contratuais, após ouvido o fiscal do contrato;
d) analisar os documentos referentes ao recebimento do objeto contratado;
e) acompanhar o desenvolvimento da execução através de relatórios e demais documentos relativos ao objeto contratado;
f) decidir provisoriamente a suspensão da entrega de bens ou a realização de serviços;
g) efetuar a digitalização e armazenamento dos documentos fiscais e trabalhistas da CONTRATADA no sistema GMS, quando couber, bem como no Portal Nacional de Contratações Públicas (PNCP);
h) preencher o termo de avaliação de contratos administrativos disponibilizado pelo setor responsável pelo sistema de gestão de materiais, obras e serviços;
i) inserir os dados referentes aos contratos administrativos no Portal Nacional de Contratações Públicas (PNCP);
j) iniciar e instruir o procedimento para aplicação das penalidades previstas neste Contrato e na legislação, no caso de constatar irregularidade cometida pela CONTRATADA, encaminhando à comissão competente;
k) manter controles adequados e efetivos do presente Contrato, do qual constarão todas as ocorrências relacionadas com a execução, inclusive o controle do saldo contratual, com base nas informações e relatórios apresentados pelo fiscal;
l) tomar as providências relativas à retenção da garantia contratual eventualmente prestada, com a notificação da seguradora da abertura de procedimento administrativo em face da empresa CONTRATADA, mantendo-a atualizada sobre o andamento quando solicitado;
m) verificar a manutenção da necessidade, economicidade e oportunidade da contratação;
n) propor medidas que melhorem a execução do Contrato;
o) outras atividades compatíveis com a função.

Caberá aos Fiscais do Contrato o acompanhamento da execução do objeto da presente contratação, informando ao gestor as ocorrências que possam prejudicar o bom andamento de sua execução e ainda:

a) anotar, em registro próprio, todas as ocorrências relacionadas com a execução e determinar o que for necessário à regularização de falhas ou defeitos observados;
b) esclarecer prontamente as dúvidas administrativas e técnicas e divergências surgidas na execução do objeto contratado;
c) expedir, através de notificações e/ou relatório de vistoria, as ocorrências e fazer as determinações e comunicações necessárias à perfeita execução dos serviços;
d) proceder, conforme cronograma físico-financeiro, as medições dos serviços executados e aprovar a planilha de medição emitida pela CONTRATADA ou conforme disposto em contrato;
e) adotar as medidas preventivas de controle dos contratos, inclusive manifestar-se a respeito da suspensão da entrega de bens, a realização de serviços ou a execução de obras;

f) conferir e certificar as faturas relativas às aquisições, serviços ou obras;
g) proceder as avaliações dos serviços executados pela CONTRATADA;
h) determinar por todos os meios adequados a observância das normas técnicas e legais, especificações e métodos de execução dos serviços exigíveis para a perfeita execução do objeto;
i) exigir o uso correto dos equipamentos de proteção individual e coletiva de segurança do trabalho;
j) determinar a retirada de qualquer empregado subordinado direta ou indiretamente à CONTRATADA, inclusive empregados de eventuais subcontratadas, ou as próprias subcontratadas, que, a seu critério, comprometam o bom andamento dos serviços;
k) receber designação e manter contato com o preposto da CONTRATADA e, se for necessário, promover reuniões periódicas ou especiais para a resolução de problemas na entrega dos bens ou na execução dos serviços ou das obras;
l) dar parecer técnico nos pedidos de alterações contratuais;
m) verificar a correta aplicação dos materiais;
n) requerer das empresas testes, exames e ensaios quando necessários, no sentido de promoção de controle de qualidade da execução das obras e serviços ou dos bens a serem adquiridos;
o) realizar, na forma do art. 140 da Lei Federal nº 14.133/2021, o recebimento do objeto contratado, quando for o caso;
p) propor à autoridade competente a abertura de procedimento administrativo para apuração de responsabilidade;
q) atestar, em documento hábil, o fornecimento, a entrega, a prestação de serviço ou a execução da obra, após conferência prévia do objeto contratado encaminhar os documentos pertinentes ao gestor;
r) confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no Contrato;
s) verificar se o prazo de entrega, especificações e quantidades encontram- se de acordo com o estabelecido no instrumento contratual;
t) informar, em prazo hábil no caso de haver necessidade de acréscimos ou supressões no objeto do Contrato ao gestor do Contrato;
u) outras atividades compatíveis com a função.

6.3. GARANTIA CONTRATUAL

Não se verifica a necessidade de exigir garantia de execução, uma vez que os serviços serão pagos mensalmente após a conclusão dos serviços ou da respectiva ordem de serviço (sob demanda) mediante verificação e atesto, de forma que os riscos de inexecução contratual se mostram minorados.

No mais, caso haja a aplicação de penalidade de multa, esta pode vir a ser descontada de futuros pagamentos que ocorrerão ao longo da vigência contratual.

6.4. OBRIGAÇÕES DA CONTRATADA

6.4.1. SEGURANÇA INSTITUCIONAL - Grupo 01 e item 8

A CONTRATADA deverá cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas, processos, padrões e regulamentos estabelecidos na Política de Segurança da Informação do TRIBUNAL e demais documentações.

A CONTRATADA não poderá divulgar, mesmo em caráter estatístico, quaisquer informações originadas no TRIBUNAL sem prévia autorização formal.

A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo sobre quaisquer dados, informações, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos, sob pena de lei e sanção na forma prevista no item 6.8 CADERNO DE PENALIDADES - Grupo 01 e item 8 .

A CONTRATADA deverá respeitar as normas e procedimentos de controle e acesso às dependências do TRIBUNAL, caso eventualmente realize atendimentos presenciais.

Quando nas dependências do TRIBUNAL, os técnicos da empresa CONTRATADA ficarão sujeitos a todas as normas internas de segurança do TRIBUNAL, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.

A CONTRATADA deverá substituir imediatamente qualquer um de seus profissionais caso sejam considerados inconvenientes à boa ordem e às normas disciplinares do TRIBUNAL.

6.4.2. DEVERES E RESPONSABILIDADES DA CONTRATADA - Grupo 01 e item 8

A CONTRATADA deverá:

Fornecer os bens e prestar serviços conforme especificações, quantidades, prazos e demais condições estabelecidas no termo de referência, no edital, no contrato e em todos os seus anexos.

Prestar os serviços que deverão atender a todos os critérios técnicos especificados neste termo de referência.

Responsabilizar-se integralmente pela execução dos serviços, primando pela qualidade, desempenho, eficiência e produtividade na execução dos trabalhos dentro dos prazos estipulados e cujo descumprimento será considerado infração passível de aplicação das penalidades previstas.

Autorizar e assegurar a CONTRATANTE o direito de fiscalizar, sustar e/ou recusar os serviços que não estejam de acordo com as especificações estabelecidas no termo de referência, no edital, no contrato e em todos os seus anexos.

Disponibilizar um funcionário representante legal para exercer o papel de preposto, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

Comunicar formal e imediatamente ao gestor ou fiscal técnico da CONTRATANTE, sobre mudanças nos dados para acionamento dos atendimentos técnicos, requisições de serviço, manutenção e garantia.

Fornecer mão de obra qualificada e suficiente para execução das tarefas pertinentes ao serviço contratado.

Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da CONTRATANTE, referentes a qualquer problema detectado ou ao andamento dos serviços contratados.

Comunicar ao TRIBUNAL qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários.

Comunicar ao CONTRATANTE, de imediato e por escrito, qualquer irregularidade verificada durante a execução do contrato, para a adoção das medidas necessárias à sua regularização.

Arcar com despesa decorrente de qualquer infração seja qual for, desde que praticada por seus funcionários no recinto do TRIBUNAL ou através de acesso remoto.

Responder pelos danos causados diretamente à administração do TRIBUNAL ou a terceiros, decorrentes de sua culpa ou dolo, durante o fornecimento e a execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou o acompanhamento pelo TRIBUNAL, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente.

Responder, ainda, por quaisquer danos causados diretamente aos equipamentos ou a outros bens de propriedade do TJPR, quando esses tenham sido ocasionados por seus funcionários durante o fornecimento e a prestação dos serviços, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente.

Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir.

Manter, durante toda a execução do contrato, todas as condições de habilitação exigidas para a contratação.

Manter em compatibilidade com as obrigações a serem assumidas, durante toda a execução do contrato, todas as condições de habilitação e de qualificação na licitação.

Responder por todas as despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias, passagens, diárias, hospedagem, alimentação, hora extra e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que eles não têm nenhum vínculo empregatício com o CONTRATANTE.

Colaborar com a equipe técnica de segurança cibernética do TRIBUNAL para a análise de incidentes e o desenvolvimento de estratégias de mitigação.

Manter registros detalhados de todas as atividades realizadas.

Assegurar a confidencialidade, integridade e disponibilidade das informações do TRIBUNAL durante a execução dos serviços.

Assinar o Termo de Sigilo e Confidencialidade, conforme ANEXO II - TERMO DE SIGILO E CONFIDENCIALIDADE (CONTRATADA), quando da assinatura do contrato.

Declarar ciência da Política de Relacionamento entre o Tribunal de Justiça do Estado Paraná e os seus Agentes com as Contratadas e as Potenciais Contratadas (Decreto Judiciário nº 62/2026 disponível em: https://www.tjpr.jus.br/legislacao-atos-normativos/-/atos/documento/4760362) e do Código de Ética e Conduta do Poder Judiciário do Estado do Paraná (disponível em: https://www.tjpr.jus.br/web/comissao-de-etica-e-de-conduta/código-de-ética-e-conduta)

6.5. OBRIGAÇÕES DA CONTRATANTE - Grupo 01 e item 8

A CONTRATANTE deverá:

Proporcionar à CONTRATADA as facilidades necessárias ao cumprimento do contrato, inclusive acesso remoto ao software objeto do contrato, quando devidamente justificado e sob as condições de segurança e sigilo pactuadas.

Designar responsáveis para o acompanhamento e fiscalização da execução do objeto contratual.

Estabelecer normas e procedimentos de acesso às suas instalações para a execução de serviços.

Informar à CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados.

Comunicar formalmente qualquer anormalidade ocorrida na execução do objeto deste termo de referência.

Verificar minuciosamente, no prazo fixado, a conformidade dos serviços executados para fins de aceite na ocasião dos faturamentos mensais e dos serviços sob demanda.

Receber os serviços provisoriamente e definitivamente, mediante termo de recebimento e em conformidade com a legislação.

Atestar as faturas de serviço apresentadas mensalmente pela CONTRATADA, informando imediatamente e por escrito sobre a eventuais glosas a serem aplicadas, justificando seus motivos.

Efetuar o pagamento à CONTRATADA, após o recebimento e aprovação dos serviços executados.

Permitir o acesso às dependências do TRIBUNAL, dos técnicos da CONTRATADA, responsáveis pela execução dos serviços.

Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da CONTRATADA.

Aplicar as sanções conforme previsto no presente termo de referência.

Emitir atestados de capacidade técnica quando solicitado, desde que atendidas as obrigações contratuais.

6.6. VIGÊNCIA CONTRATUAL - Grupo 01 e item 8

A vigência da contratação será de 36 (trinta e seis) meses contados da assinatura do contrato, podendo ser prorrogado sucessivamente, respeitada a vigência máxima decenal.

6.7. TRANSIÇÃO CONTRATUAL - Grupo 01

O prazo inicial para a fase de **Transição do Serviço** será de até 90 (noventa) dias, iniciando mediante comunicação prévia do TRIBUNAL.

Durante a fase de **Transição do Serviço**, caso um ou mais serviços sejam substituídos por novos serviços contratados aptos a iniciar operação imediata, o TRIBUNAL pode definir escala gradativa de respectivos serviços da CONTRATADA que serão interrompidos até o término da transição.

O Termo de Referência da presente contratação e da nova contratação devem prever os critérios das Fase de Transição Inicial e Transição Final de prestação de serviços, de modo a garantir o pleno repasse de conhecimento, de dados e de operações de forma ininterrupta, com a gradativa desativação dos serviços que finalizam, alinhado a gradativa ativação do novo contrato.

Considerando entendimento referendado pelo Tribunal de Contas da União, é possível prever uma pequena sobreposição entre dois contratos para fins de transição contratual desde que prevista e justificada no planejamento de ambas as contratações (a que expira e a que se inicia), mas que não gere pagamentos em duplicidade.

A CONTRATADA deverá efetuar o repasse de conhecimentos para a nova CONTRATADA por meio de reuniões e documentos técnicos e/ou manuais específicos.

O plano de transição contratual e sua execução deverão ser viabilizados sem ônus adicionais à CONTRATANTE.

6.8. CADERNO DE PENALIDADES - Grupo 01 e item 8

6.8.1. Penalizações

6.8.1.1. A CONTRATADA será responsabilizada administrativamente pelas seguintes infrações, conforme previsto na Lei Federal nº 14.133/2021, no Decreto Estadual nº 10.086/2022 e no Decreto Judiciário nº 269/2022-TJ/PR:

a) dar causa à inexecução parcial do contrato;
b) dar causa à inexecução parcial do contrato que cause grave dano ao CONTRATANTE, ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) dar causa à inexecução total do contrato;
d) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
e) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
f) praticar ato fraudulento na execução do contrato;
g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
i) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

6.8.1.1.1. Considera-se inexecução total do contrato a recusa injustificada de cumprimento integral da obrigação contratualmente determinada.

6.8.1.2. A CONTRATADA que incorrer nas infrações administrativas previstas no item 6.8.1.1 sujeitar-se-á às seguintes sanções:

a) **advertência**: exclusivamente pelas infrações administrativas na letra “a” do item 6.8.1.1 e no caso de descumprimento, de pequena relevância, de obrigação legal ou infração à Lei quando não se justificar aplicação de sanção mais grave;
b) **multa** com relação a quaisquer das infrações previstas no item 6.8.1, que será calculada na forma prevista neste Contrato;
c) **impedimento**: pelas infrações administrativas previstas nas letras "b" a "d" do item 6.8.1.1, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos;
d) **inidoneidade**: pelas infrações administrativas previstas nas letras "e" a "i" do item 6.8.1.1, bem como pelas infrações administrativas previstas nas letras "b" a "d" do referido item que justifiquem a imposição de penalidade mais grave de impedimento, e impedirá o responsável de licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

6.8.1.3. Para fins de aplicação da advertência, considera-se pequena relevância o descumprimento de obrigações ou deveres instrumentais ou formais que não impactam objetivamente na execução do contrato, bem como não cause prejuízos ao CONTRATANTE.

6.8.1.4. A sanção de advertência, impedimento e inidoneidade poderão ser aplicadas cumulativamente com a multa.

6.8.1.5. As sanções de impedimento e inidoneidade serão aplicadas de modo independente em relação a cada infração diversa cometida.

6.8.1.5.1. Para o cômputo dessas sanções deverão ser observadas as demais regras dos arts. 224 a 225 do Decreto Estadual nº 10.086/2022.

6.8.1.6. A aplicação das sanções previstas nas alíneas do item 6.8.1.2 não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE.

6.8.1.7. Na aplicação das penalidades serão consideradas as circunstâncias do art. 156, §1º, da Lei Federal nº 14.133/2021, quais sejam:

a) a natureza e a gravidade da infração cometida;
b) as peculiaridades do caso concreto;
c) as circunstâncias agravantes ou atenuantes;
d) os danos que dela provierem para ao CONTRATANTE;
e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

6.8.1.7.1. Deverão ser consideradas como agravantes e atenuantes as circunstâncias previstas nos arts. 211 a 212 do Decreto Estadual nº 10.086/2022.

6.8.1.7.2. O cometimento de mais de uma infração em uma relação contratual sujeitará o infrator à sanção cabível para a mais grave entre elas, ou se iguais, somente uma delas, sopesando-se, em qualquer caso, as demais infrações como circunstância agravante, observando-se, ainda o previsto nos parágrafos do art. 198 do Decreto Estadual nº 10.086/2022.

6.8.1.8. A mora no cumprimento de obrigações contratuais independe de notificação da CONTRATADA (dies interpellat pro homine), salvo previsão expressa.

6.8.1.8.1. O cumprimento parcial da parcela em atraso reduzirá proporcionalmente a base de cálculo da penalidade de multa.

6.8.1.9. As sanções de multa moratória não serão cumuladas com a pena de multa prevista para o caso de rescisão contratual, quando a rescisão decorrer da própria mora.

6.8.1.10. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

6.8.1.11. Além do previsto no item 6.8.1.1.1 poderá configurar a inexecução total da obrigação e a aplicação da penalidade prevista no item 6 da Tabela 15 - Tabela de conduta 03, sem prejuízo de eventual indenização pela CONTRATADA derivada de perdas e danos causados ao CONTRATANTE (decorrente das infrações cometidas), quando:

a) a execução do objeto contratado for inferior a 50% (cinquenta por cento) do total;
b) houver reiterado descumprimento das obrigações assumidas;
c) o atraso na execução ultrapassar o prazo limite de 30 (trinta) dias corridos e não houver o interesse do CONTRATANTE em manter a contratação;
d) o descumprimento parcial prejudicar a solução como um todo.

6.8.1.11.1. A rescisão do contrato dependerá de análise de oportunidade e conveniência do CONTRATANTE.

6.8.1.12. A personalidade jurídica poderá ser desconsiderada administrativamente, conforme previsto no art. 160 da Lei Federal nº 14.133/21, devendo ser observados os procedimentos previstos nos arts. 215 a 223 do Decreto Estadual nº 10.086/2022.

6.8.1.13. Após a regular tramitação do procedimento administrativo para apuração da irregularidade e a aplicação de sanções, incidindo a aplicação da penalidade de multa, a CONTRATADA será notificada para o pagamento.

6.8.1.13.1. Transcorrido o prazo para o pagamento da multa sem o seu adimplemento o CONTRATANTE poderá compensar o valor devido com qualquer crédito existente nesta ou em outra contratação.

6.8.1.13.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pelo CONTRATANTE ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

6.8.1.13.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

6.8.1.14. Qualquer multa ou encargo imputado à CONTRATADA, não pago no prazo concedido pela CONTRATANTE, será inscrito no CADIN Estadual e em Dívida Ativa do Estado e cobrado com base na Lei Federal nº 6.830/1980, sem prejuízo da correção monetária.

6.8.1.15. As disposições desta cláusula de penalidades não excluem a responsabilização da licitante por eventuais atos lesivos previstos na Lei Federal nº 12.846/2013 e demais legislações, bem como a responsabilidade de indenização suplementar em caso de perdas e danos decorrente da conduta.

6.8.1.15.1. Nesses casos, os atos lesivos serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na Lei Federal nº 12.846/2013.

6.8.1.16. Sem prejuízo das demais penalidades, as de multa serão aplicadas conforme detalhamento constante das tabelas abaixo.

6.8.1.16.1. Para a verificação e enquadramento da conduta nas tabelas de penalidades, será considerada em primeiro lugar a conduta específica e somente será aplicada a genérica na falta daquela.

6.9. TABELA DE CONDUTAS 1 - Grupo 01:

ID	CONDUTAS	PENALIDADES
1	Deixar de realizar o atendimento (TMIA) no prazo estabelecido na tabela de Nível Mínimo de Serviços no item 11.5 para eventos categorizados como CRÍTICO.	Aplicar-se-á multa de R$ 1000,00 (mil reais) por hora que exceder o prazo máximo para início de atendimento (TMIA). Observando o máximo de 10% (dez por cento) do valor da categoria do item correspondente aos serviços e produtos da tabela 1.
2	Deixar de realizar a solução operacional (TMSO) no prazo estabelecido na tabela de Nível Mínimo de Serviços no item 11.5 para eventos categorizados como CRÍTICO.	Aplicar-se-á multa de R$ 1000,00 (mil reais) por hora que exceder o prazo máximo para início de atendimento (TMIA). Observando o máximo de 10% (dez por cento) do valor da categoria do item correspondente aos serviços e produtos da tabela 1.

3	Deixar de realizar a solução definitiva (TMSDC) no prazo estabelecido na tabela de Nível Mínimo de Serviços no item 11.5 para eventos categorizados como CRÍTICO.	Aplicar-se-á multa de R$ 600,00 (seiscentos reais) por hora que exceder o prazo máximo para início de atendimento (TMIA). Observando o máximo de 10% (dez por cento) do valor da categoria do item correspondente aos serviços e produtos da tabela 1.
4	Deixar de realizar o atendimento (TMIA) no prazo estabelecido na tabela de Nível Mínimo de Serviços no item 11.5 para eventos categorizados como ALTO.	Aplicar-se-á multa de R$ 800,00 (oitocentos reais) por hora que exceder o prazo máximo para início de atendimento (TMIA). Observando o máximo de 10% (dez por cento) do valor da categoria do item correspondente aos serviços e produtos da tabela 1.
5	Deixar de realizar a solução operacional (TMSO) no prazo estabelecido na tabela de Nível Mínimo de Serviços no item 11.5 para eventos categorizados como ALTO.	Aplicar-se-á multa de R$ 800,00 (oitocentos reais) por hora que exceder o prazo máximo para início de atendimento (TMIA). Observando o máximo de 10% (dez por cento) do valor da categoria do item correspondente aos serviços e produtos da tabela 1.
6	Deixar de realizar a solução definitiva (TMSDC) no prazo estabelecido na tabela de Nível Mínimo de Serviços no item 11.5 para eventos categorizados como ALTO.	Aplicar-se-á multa de R$ 500,00 (quinhentos reais) por hora que exceder o prazo máximo para início de atendimento (TMIA). Observando o máximo de 10% (dez por cento) do valor da categoria do item correspondente aos serviços e produtos da tabela 1.
7	O atraso injustificado na entrega dos bens ou na prestação do serviço no início da execução do contrato de acordo com os prazos estabelecidos.	Multa de 1% (um por cento) a 2% (dois por cento) do valor do item 1 Projeto e implantação, do Grupo 01, por dia de atraso.

Tabela 13 - Tabela de conduta 01

O **prazo máximo de atendimento** consiste no tempo entre a abertura de um chamado pela CONTRATANTE e o seu primeiro atendimento pela CONTRATADA.

O **prazo máximo para solução** consiste no tempo entre a abertura de um chamado pela CONTRATANTE e a sua solução definitiva pela CONTRATADA, **com a CONTRATANTE sendo informada.**

Haverá suspensão de contagem dos prazos para o **chamado** ou **ordem de serviço** que, **realmente** for comprovado que houve alguma pendência por parte da CONTRATANTE.

6.10. TABELA DE CONDUTAS 2 – Grupo 01 e item 8:

ID	CONDUTAS	PENALIDADES
1	O descumprimento de prazos de entrega de documentação solicitados pela CONTRATANTE estipulados no Termo de Referência, conforme previsão no edital ou em contrato; ou Inobservância do prazo fixado para entrega do Formulário de Análise de Perfil das Contratadas do Tribunal de Justiça do Estado do Paraná.	Multa no valor fixo de R$ 1000,00 (mil reais) por dia corrido de atraso.
2	Deixar de realizar os repasses de conhecimento ou capacitações inerentes à prestação dos serviços,	Multa no valor fixo de R$ 200,00 (duzentos reais) por evento.

	de acordo com as características previstas no contrato.	
3	Deixar de manter, na vigência do contrato, as condições originais de habilitação.	Multa de 2% (dois por cento), por evento, calculada sobre o valor mensal do contrato.
4	Deixar de disponibilizar serviços contratados, caracterizando a inexecução parcial.	Multa de 10 a 20% sobre o valor da parcela inadimplida, sem prejuízo de eventual indenização pela CONTRATADA, derivada de perdas e danos causados ao Tribunal de Justiça decorrente das infrações cometidas.
5	Deixar de realizar a correção da causa raiz das glosas causando reincidência delas.	Multa de 2x o valor estipulado na glosa por mês de reincidência.
6	Causar indisponibilidade dos serviços do CONTRATANTE por paralização ou instabilidade dos serviços contratados, sem justa causa ou por motivo de imperícia na execução das atividades contratuais.	Multa de 1% (um por cento) a 10% (dez por cento) do valor global.

Tabela 14 - Tabela de conduta 02

6.11. TABELA DE CONDUTAS 3 - Grupo 01 e item 8:

ID	CONDUTAS	PENALIDADES
1	O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos quando não haja previsão de conduta específica ou Quando o preposto ou responsável técnico não se apresentar em reunião pré-agendada.	Primeira vez: Advertência Segunda vez e seguintes: Multa de 0,5% (zero vírgula cinco por cento) a 1% (um por cento) do valor mensal do contrato por dia de inadimplência e/ou fato gerador ensejador da multa, conforme a natureza da obrigação, limitado ao máximo de 10% (dez por cento) do valor mensal estimado da contratação.
2	O não cumprimento de cláusulas contratuais, quando não haja previsão de conduta específica ou O desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores ou Quando deixar de substituir prestador de serviço que se portar ou realizar condutas de modo inconveniente ou não atenda às necessidades.	Multa de 0,5% (zero vírgula cinco por cento) a 2% (dois por cento) do valor mensal do contrato por dia de inadimplência e/ou fato gerador ensejador da multa, conforme a natureza da obrigação, limitado ao máximo de 20% (vinte por cento) do valor mensal estimado da contratação.
3	A paralisação do serviço ou do fornecimento, sem justa causa e prévia comunicação à Administração, quando não haja previsão de conduta específica.	Multa de 0,5% (zero vírgula cinco por cento) a 3% (três por cento) do valor global do contrato por dia de inadimplência e/ou fato gerador ensejador da multa, conforme a natureza da obrigação, limitado ao máximo de 20% (vinte por cento) do valor mensal estimado da contratação.
4	Quando for evidenciado que o prestador de serviço da CONTRATADA realizou atividade de quebra ou ameaça de	Multa de 10% (dez por cento) a 20% (vinte por cento) do valor global estimado da contratação.

ID	CONDUTAS	PENALIDADES
	segurança das informações do TRIBUNAL, inseriu código malicioso em sistema, inseriu intencionalmente praga digital na rede do TRIBUNAL, obteve acesso não autorizado à informação ou sistema ou Apresentar documento falso ou fazer declaração falsa ou Agir de má-fé na relação contratual ou Frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o contrato. ou Deixar de notificar irregularidades ou não conformidades identificadas durante a vigência do contrato.	
5	Abandonar a execução do contrato ou Incorrer em inexecução total contratual quando não haja previsão de conduta específica ou Tenha sofrido condenação judicial definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos ou Demonstrar não possuir idoneidade para contratar com a Administração, em virtude de atos ilícitos praticados, em especial, infrações à ordem econômica definidas na Lei Federal no 8.158/1991 ou Tenha sofrido condenação definitiva por ato de improbidade administrativa, na forma da lei ou A subcontratação total ou parcial do seu objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital e no contrato ou A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato.	Multa de 10% a 20% (vinte por cento) sobre o valor global do contrato, sem prejuízo de eventual indenização pela CONTRATADA, derivada de perdas e danos causados ao Tribunal de Justiça decorrente.
6	Descumprimento ou inexecução total do contrato/obrigações que gere a rescisão contratual.	Multa de 10% (dez por cento) sobre o valor global do contrato, sem prejuízo de eventual indenização pela CONTRATADA, derivada de perdas e danos causados ao Tribunal de Justiça decorrente das infrações cometidas.
7	Descumprimento da obrigação de zelo no tratamento dos dados pessoais da pessoa natural vinculada ao CONTRATANTE, ou em caso de tratamento de dados sem o	Multa de 10% (dez por cento) sobre o valor total do Contrato.

ID	CONDUTAS	PENALIDADES
	consentimento específico e destacado por termo de compromisso, ou outra irregularidade havida no cumprimento do Contrato, por culpa da CONTRATADA.	
8	Tratar dados pessoais sensíveis com o objetivo de obter vantagem econômica, ou outra irregularidade havida no cumprimento do Contrato, por culpa da CONTRATADA.	Multa de até 10% (vinte por cento) sobre o valor total do Contrato.

Tabela 15 - Tabela de conduta 03

7. CRITÉRIOS DE RECEBIMENTO E DE PAGAMENTO (ART. 6º, XXIII, G)

7.1. RECEBIMENTO

O recebimento provisório é o recebimento das entregas, parciais ou completas dos serviços pelo TRIBUNAL para posterior análise e conferência das informações prestadas, conforme exigências do objeto.

O recebimento definitivo é dado pelo TRIBUNAL após verificar e atesto que as informações prestadas estão completas, em conformidade com as exigências do objeto.

O Termo de Recebimento Definitivo não exclui a responsabilidade civil da empresa vencedora por vícios qualitativos, quantitativos ou técnicos dos materiais ou por desacordo com as especificações estabelecidas neste Termo de Referência, verificadas posteriormente.

7.1.1. RECEBIMENTO DE PROJETO E IMPLANTAÇÃO

O objeto do Item 1, do Grupo 01 da **Tabela 1 - Quadro de Especificação Detalhada do Objeto,** denominado **Projeto e implantação**, será recebido provisoriamente após apresentação e aprovação do Projeto e implantação pelo TRIBUNAL e recebido definitivamente no término da execução da fase **Projeto e implantação,** conforme requisitos especificados no item 2.2 PROJETO E IMPLANTAÇÃO do ANEXO A – ESPECIFICAÇÕES TÉCNICAS DO OBJETO DE STIC.

7.1.2. RECEBIMENTO DE NATUREZA MENSAL

Serão recebidos mensalmente nas entregas dos serviços e nas quantidades especificadas, após validação e atesto, no prazo de até 5 (dias) úteis, o objeto dos seguintes itens Grupo 01, **2.2, "Política de Segurança da Informação (PSI)", 2.3, "Plano de Continuidade de Serviços Essenciais de TIC" e 2.4, "Plano de Resposta a Incidentes (PRI)", 3.1, "Serviço de Security Operations Center (SOC)", 3.2, "Proteção contra Riscos Digitais (Threat Intelligence)", 3.3 Serviço de Takedown, 4.1, "Solução de Firewall", 4.2", "Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)", 5.1, "Gerenciamento Contínuo de Vulnerabilidades", 5.2, "Testes de Segurança Automatizados (BAS)" e 6.1, "Gerenciamento de Acesso Privilegiado (PAM)"**Tabela **1** - Quadro de Especificação Detalhada do Objeto**.**

7.1.3. RECEBIMENTO DE NATUREZA SOB DEMANDA

Serão recebidos provisoriamente nas entregas dos relatórios e Ordem de Serviços (OS) executadas, e em definitivo após a validação e ratificação pelos Gestores deste Contrato, os seguintes itens do Grupo 01, **2.1 "Diagnóstico de Maturidade de Segurança da Informação** e **7 "Serviços Técnicos Especializados por Demanda"** e, item 8 **"Serviço de Teste de Invasão (Pentest)"** Tabela **1** - Quadro de Especificação Detalhada do Objeto.

7.2. PAGAMENTO

O pagamento relativo ao **Item 1**, do Grupo 01 da **Tabela 1 - Quadro de Especificação Detalhada do Objeto**, denominado **Projeto e implantação**, será executado e pago uma única vez, faturado em duas parcelas, sendo:

a) 50% (cinquenta por cento) do valor total do item 1 **Projeto e implementação**, após aprovação pelo TRIBUNAL, considerado o recebimento provisório do item.

b) 50% (cinquenta por cento) do valor total do item 1 **Projeto e implantação** ao término da execução do item, após a assinatura do **Termo de Recebimento Definitivo** do serviço **Projeto e implantação**.

Os itens, do Grupo 01, **2.2 "Política de Segurança da Informação (PSI)"**, **2.3 "Plano de Continuidade de Serviços Essenciais de TIC"** e **2.4 "Plano de Resposta a Incidentes (PRI)"**, **3.1 "Serviço de Security Operations Center (SOC)"**, **3.2,"Proteção contra Riscos Digitais (Threat Intelligence)"**, **3.3 "Serviço de Takedown"**, **4.1 "Solução de Firewall"**, **4.2" "Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)"**, **5.1 "Gerenciamento Contínuo de Vulnerabilidades de infraestrutura"**, **5.2 "Testes de Segurança Automatizados (BAS)"** e **6.1 "Gerenciamento de Acesso Privilegiado (PAM)"**, da **Tabela 1 - Quadro de Especificação Detalhada do Objeto** serão pagos **mensalmente**, baseado em relatórios enviados pela CONTRATADA.

Os itens, do Grupo 01, **2.1 "Diagnóstico de Maturidade de Segurança da Informação"** e **7 "Serviços Técnicos Especializados por Demanda"**, do item 8 "Serviço de Teste de Invasão (Pentest)" da **Tabela 1 - Quadro de Especificação Detalhada do Objeto** serão pagos **conforme execução**, autorizada mediante **Ordem de Serviço (OS)**, após o aceite definitivo da entrega.

O TRIBUNAL se reserva ao direito de descontar do pagamento os eventuais débitos da CONTRATADA, inclusive os relacionados com multas, sansões, danos e prejuízos contra terceiros.

Glosas poderão ser aplicadas pelo CONTRATANTE em caso de descumprimento das obrigações contratuais pela CONTRATADA.

As glosas serão deduzidas do valor da nota fiscal do mês corrente.

Os pagamentos dos itens com natureza mensal serão realizados após o atesto de atendimento aos requisitos desta contratação, no prazo máximo de 30 (trinta) dias corridos a contar do protocolo da solicitação, mediante requerimento subscrito contendo a respectiva nota fiscal/fatura, depois de atestado pelo fiscal do Contrato.

A CONTRATADA deverá formular pedido de pagamento através de formulário eletrônico disponível no endereço https://www.tjpr.jus.br/protocolo-admin (opção "contratados"), acompanhado da nota fiscal/fatura com o CNPJ do CONTRATANTE no 77.821.841/0001-94, bem como carta/requerimento em papel timbrado da empresa, indicando a modalidade, número de licitação e itens, número do Contrato, dados bancários para depósito, devidamente instruído com os demais documentos de regularidade fiscal atualizados.

Para fins de liberação do pagamento, a Administração efetuará consulta ao Cadastro Informativo Estadual - Cadin Estadual. As pessoas físicas e jurídicas com registro no Cadin Estadual estarão impedidas de receber pagamentos referentes a contratação, na forma do art. 3 da Lei 18.466/2015.

Na hipótese de atraso do pagamento da Nota Fiscal/Fatura devidamente atestada, e desde que para tal não tenha concorrido de alguma forma a CONTRATADA, o valor devido pelo CONTRATANTE será atualizado financeiramente, se assim solicitado pela CONTRATADA, obedecendo à legislação vigente.

No caso de incorreção nos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão eles restituídos à CONTRATADA para as correções necessárias, não respondendo o CONTRATANTE por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes, haja vista que o prazo para pagamento será interrompido, e terá sua contagem iniciada novamente somente após a apresentação dos documentos corretos.

Nenhum pagamento será efetuado ao fornecedor enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

A contestação de glosas deverá ser formalizada por escrito e enviada à equipe de fiscalização do CONTRATANTE, apresentando justificativas e anexando evidências.

O CONTRATANTE analisará a contestação e emitirá parecer técnico no prazo de 5 dias úteis.

7.3. REAJUSTE

Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado. Após o interregno de um ano e desde que haja requerimento da CONTRATADA, o preço inicialmente contratado poderá ser reajustado mediante prévia negociação entre as partes, observados os preços praticados no mercado, tendo como limite máximo a variação do Índice de Custo de Tecnologia da Informação - ICTI (ou, na impossibilidade de uso deste, do Índice de Preços ao Consumidor Amplo - IPCA), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

A proposta da empresa deve levar em conta todos os custos operacionais para o período de vigência da contratação, inclusive quanto à reoneração gradual prevista para os anos de 2025 e 2026. Assim, a reoneração gradual, por ser previamente de conhecimento dos licitantes, não será fato ensejador de reequilíbrio econômico-financeiro.

As demais condições para o reajuste serão previstas no instrumento contratual.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR (ART. 6º, XXIII, H)

8.1. MODALIDADE, TIPO DE LICITAÇÃO E CRITÉRIOS DE HABILITAÇÃO

8.1.1. MODALIDADE, TIPO DE LICITAÇÃO

Por se tratar de serviços gerenciados de segurança da informação e cibernética diante da existência no mercado de diversos fornecedores para atender as necessidades deste TJPR, os serviços pretendidos apresentam características padronizadas e usuais.

Assim, pode-se concluir, a princípio, que são de natureza “comum” e, portanto, poderá ser utilizada a modalidade “Pregão”, menor preço, com modo de disputa ABERTO e considerado o PREÇO TOTAL/GLOBAL para o respectivo lote, sendo que a diferença entre os lances enviados não poderá ser inferior aos indicados na tabela abaixo e incidirão tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

Para fins de disputa será utilizada a tabela a seguir, com os intervalos mínimos entre lances, que engloba todos os serviços/quantitativos descritos no item 1.3 deste Termo de Referência.

Grupo	Item	Descrição	Intervalo mínimo entre lances
1	**1**	**Projeto e implantação**	R$ 5.000,00
	2	**Serviços de Governança e Conformidade de Segurança**	R$ 1.000,00
	3	**Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança**	R$ 5.000,00
	4	**Sustentação de Operações de Soluções e Resposta a Requisições de Segurança**	R$ 1.000,00
	5	**Gestão de Vulnerabilidades e Testes de Segurança**	R$ 1.000,00
	6	**Gestão de Identidade**	R$ 1.000,00
	7	**Serviços Técnicos Especializados por Demanda**	R$ 500,00
Item Avulso	**8**	**PenTest**	R$ 200,00

Tabela 16 - Intervalo mínimo entre lances

É vedada a contratação de uma mesma empresa para o Grupo 01 e o item 8, devido à natureza dos serviços a serem contratados, que exige independência e autonomia entre os prestadores, sendo necessária a participação de empresas distintas que não tenham qualquer relação ou subordinação entre si, para garantir integridade e confiabilidade dos resultados pretendidos.

Cada licitante poderá ofertar lances para o Grupo 01 e o item 8, no entanto somente se sagrará vencedora de um deles. Assim, caso a licitante seja declarada vencedora do Grupo 01 será automaticamente desclassificada quanto ao item 8, ou seja, o item 8 deverá ser analisado posteriormente ao Grupo 01.

8.2. PROPOSTA DE PREÇOS

A proposta de preços deverá ser redigida, conforme o **ANEXO VII - Modelo de Proposta Comercial**, em língua portuguesa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, e dela deverá constar:

a) Identificação social, número do CNPJ, assinatura do representante legal da proponente, referência a esta licitação, número de telefone, endereço, dados bancários, número de fax e indicação de endereço eletrônico (email);
b) O prazo de validade da proposta é de 60 (sessenta) dias, a contar da data de abertura da sessão pública estabelecida no preâmbulo deste Edital;
c) Indicação única de preço (R$), com exibição dos valores unitário, em algarismos, e total/global, em algarismos e por extenso, conforme o lance final respectivo;
d) Declaração de que não se beneficiará, junto ao fabricante, de vantagens decorrentes do registro de oportunidade para parceiros comerciais ou prática semelhantes em detrimento dos demais concorrentes;
e) Para os itens 3, 5 e 6, do grupo 1, declaração da licitante de que é fabricante ou parceira autorizada para comercializar e prestar os serviços previstos na contratação;
f) Para o grupo 1, declaração de que atenderá integralmente aos seguintes itens, cuja documentação comprobatória deverá ser apresentada oportunamente como condição para a assinatura do contrato, sendo:
   "Ao menos um SOC da CONTRATADA deverá **possuir certificação ISO/IEC 27.001** vigente na contratação, emitida em nome da CONTRATADA por organização independente acreditada pelo Inmetro ou por autoridade equivalente globalmente reconhecida".

Todos os equipamentos, soluções informatizadas, softwares utilizados pela CONTRATADA para a entrega deste serviço, devem ser declarados de forma clara e objetiva na proposta cadastrada para a fase de lances deste processo, incluindo, minimamente, fabricante, modelo, versão, conforme ANEXO VI - Modelo Planilha de Custos - Solução Informatizada.

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

Justificativa para o item "f": A presente contratação é um marco para os objetivos e necessidades de Segurança da Informação e Cibernética para o TRIBUNAL.

Os objetivos contemplam desde apoio à Governança de Segurança, avanço nos níveis de maturidades e diagnósticos, apoio a construção de planos, monitoramento 24x7 e resposta a incidente e a sustentação de controles de segurança da informação extremamente importantes para a operação.

Dessa forma, a CONTRATADA será responsável pela sustentação e operação dos controles de segurança do Firewall, Antispam, Antivirus, Scan de vulnerabilidade e Testes de Penetração, em ambiente complexo e heterogêneo de soluções em infraestrutura crítica, tendo como consequência a responsabilidade por administrar soluções tecnológicas de segurança altamente críticas para o TRIBUNAL e acesso a informações sensíveis.

Além de toda complexidade mencionada, este TRIBUNAL, através da expertise da sua equipe de contratação, apoiada por relatórios da consultoria Gartner, e do acompanhamento do mercado de Cibersegurança, entende que o risco cibernético na cadeia de fornecedores é universalmente reconhecido como crítico para qualquer contratante, conforme destacado pelos principais estudos e relatórios globais de 2024 e 2025.

O Fórum Econômico Mundial, em seu "Global Cybersecurity Outlook 2025", aponta que 54% das grandes organizações consideram os desafios na cadeia de suprimentos como o maior obstáculo para alcançar a resiliência cibernética.

A crescente interdependência entre empresas e fornecedores amplia a exposição a ataques, tornando a cadeia de suprimentos um vetor de risco sistêmico, exacerbado por tensões geopolíticas e o uso crescente de inteligência artificial.

Além disso, o relatório "Retrospectiva de Cibersegurança 2024" da VaultOne reitera que ataques à cadeia de suprimentos, incluindo o comprometimento de fornecedores de software e hardware e a exploração de vulnerabilidades em dispositivos IoT, foram as principais ameaças do ano.

O "Global Risks Report 2025" do Fórum Econômico Mundial ainda posiciona os ataques cibernéticos e falhas de infraestrutura de TI entre os 10 principais riscos globais em termos de probabilidade e impacto, citando a cadeia de suprimentos como um dos pontos mais vulneráveis em setores críticos.

Esses estudos convergem para a mesma avaliação: o risco cibernético na cadeia de fornecedores possui alta probabilidade de ocorrência e um potencial impacto severo, recomendando ações robustas para minimizá-lo ou mitigá-lo.

Baseado nesse contexto, a equipe de contratação entende que a certificação ISO 27.001 se torna um requisito indispensável para esta contratação. Pois, a certificação representa a avaliação e o monitoramento contínuo de fornecedores, garantindo que a empresa possui uma estrutura robusta, requisitos mínimos de segurança implementados e validados, processos documentados de segurança da informação, continuidade de negócio e auditorias, além de uma abrangente avaliação de riscos e a implementação de controles para o tratamento desses riscos.

Entendemos que a ISO 27.001 assegura conformidade com normas reconhecidas, histórico de incidentes e práticas de segurança adotadas, permitindo que a empresa esteja alinha a CONTRATADA com princípios essenciais de gestão de acesso e privilégios, como o menor privilégio, autenticação multifator (aderente a Portaria do CNJ 140/2024) e monitoramento/auditoria de acessos de terceiros.

A necessidade de validação externa por organizações independentes e competentes é um pilar central desta justificativa. A equipe de contratação do TRIBUNAL não possui a expertise avançada em segurança da informação e nem a capacidade de volume de trabalho adequada para realizar checagens e auditorias complexas, a fim de verificar integralmente a aderência da CONTRATADA a boas práticas e controles de segurança. A certificação ISO 27.001 serve precisamente para suprir essa lacuna, delegando essa validação a especialistas externos credenciados.

Além disso, a escolha da ISO 27.001 para esta contratação segue a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ - Resolução CNJ 392/2021).

Embora existam outras certificações que garantam avaliação e monitoramento contínuo de controles e boas práticas em segurança da informação, como FedRAMP e CMMC, apenas a ISO 27.001 é emitida no Brasil, o que atende plenamente às necessidades da contratação e aos requisitos pretendidos.

Por fim, a história recente do próprio TRIBUNAL serve como um alerta crucial: o maior incidente de segurança sofrido foi decorrente da falha no processo de emissão de certificado digital em uma fornecedora de serviço terceirizada, a qual, segundo pesquisas, falhou nos controles mínimos de segurança sobre seus processos de trabalho. Este exemplo real sublinha a vulnerabilidade inerente à contratação de serviços sem uma validação rigorosa de suas práticas de segurança.

Em suma, exigir a certificação ISO 27.001 para a empresa que irá operar e sustentar os serviços de tecnologias de segurança não é apenas uma formalidade, mas uma medida proativa e essencial para mitigar riscos cibernéticos na cadeia de suprimentos, garantir a proteção dos controles críticos de segurança e dados altamente sensíveis do TRIBUNAL e assegurar que a CONTRATADA implementa às melhores práticas internacionais de segurança da informação, com validação independente e pertinente ao contexto nacional. É uma salvaguarda indispensável para a resiliência e integridade das atividades finalísticas do TRIBUNAL.

Portanto, esta equipe de contratação entende e reforça que **"Ao menos um SOC da CONTRATADA deverá estar instalado no Brasil e possuir certificação ISO/IEC 27.001 vigente na contratação, emitida em nome da CONTRATADA por organização independente acreditada pelo Inmetro ou por autoridade equivalente globalmente reconhecida"**.

8.3. QUALIFICAÇÃO TÉCNICA

A comprovação da qualificação técnica na habilitação da licitação será por meio de atestado(s) de capacidade técnico-operacional emitido(s) por pessoa jurídica de direito público ou privado em nome da LICITANTE, que comprove experiência que executou ou executa, de forma satisfatória, Serviços Gerenciados de Cibersegurança e/ou Segurança da Informação similares aos especificados neste Termo de Referência.

Serão considerados compatíveis os atestados que comprovem a prestação de Serviços Gerenciados de Segurança (MSS), por pelo menos 12 (doze) meses, das seguintes parcelas de maior relevância:

Para o grupo 1:

1) Serviços prestados de governança e conformidade de segurança da informação ou cibersegurança, para instituição com no mínimo 2.000 (dois mil) usuários de tecnologia e contemplando no mínimo:

a) Elaboração de diagnósticos e avaliações de análise de Gap (situação e lacunas), maturidade e conformidade (com leis, normas e melhores práticas);
b) Elaboração e implantação de Plano de Continuidade de Negócios (PCN/BCP) e realização de Análise de Impacto nos Negócios (AIN/BIA);
c) Elaboração e revisão de políticas e normas, planos, procedimentos, indicadores e métricas de cibersegurança e/ou segurança da informação.

2) Serviços gerenciados prestados de monitoramento, detecção e resposta de eventos e incidentes de cibersegurança e/ou segurança da informação, em ambiente com no mínimo 3.000 (três mil) ativos ou 2.500 (dois mil e quinhentos) EPS (eventos por segundo), contemplando no mínimo:

a) Serviço de SOC (Security Operations Center) próprio da CONTRATADA;
b) Equipes de profissionais especializados em segurança da informação e cibersegurança, atuando em níveis 1, 2 e 3 de atendimento, operando em regime contínuo e ininterrupto 24x7x365;

c) Capacidade de inteligência de ameaças (*Threat Intelligence*), caçada contínua de ameaças (*Threat Hunting)* e gerenciamento de crises;
d) Operação de solução tecnológica especializada e atuação no gerenciamento, análise, triagem, automação e resposta de informações, eventos e incidentes de segurança.

3) Serviços de sustentação e operação de soluções de segurança contemplando no mínimo:
a) Solução de Next Generation Firewall Enterprise;
b) Soluções de Segurança de proteção de endpoint;
c) Solução de Gestão de Vulnerabilidade Tenable ou Qualys.

4) Serviços de gestão contínua de vulnerabilidades em ambientes com ao menos 1.000 (um mil) ativos e contemplando no mínimo:
a) Execução de varreduras de descoberta e conformidade em rede externa e interna para identificação, mapeamento e análise de vulnerabilidades em ativos corporativos de TIC;
b) Priorização de riscos cibernéticos de vulnerabilidades e ativos de TIC;
c) Operação de solução tecnológica especializada para gestão, varredura, avaliação e remediação de vulnerabilidades e de configuração segura, com análise e priorização do risco cibernético.

5) Serviços de gerenciamento de acesso privilegiado (PAM) em ambiente com no mínimo 25 (vinte e cinco) usuários administrativos ou 1.000 (um mil) ativos de TIC gerenciados.

Para o item 8:

1) Serviço de Teste de Invasão (Pentest), com no mínimo 150 horas, para exploração de vulnerabilidades de segurança da informação, que contenham pelo menos:
a) 1.000 (mil) usuários;
b) 1.000 (mil) ativos computacionais;

Será admitido o somatório de atestados para 50% do quantitativo exigido para a qualificação técnica, desde que demostrada a prestação do serviço de forma concomitante, o que pode ser comprovada por um único atestado ou por atestados distintos executados no mesmo período, demostrando a simultaneidade e a compatibilidade técnica entre os objetos.

Além disso, para os outros 50% do quantitativo exigido para qualificação técnica deverá ser apresentado atestado único, não sendo admitido somatório.

Nos atestados deverão estar expressos, no mínimo, as seguintes informações:

a) Dados da empresa licitante: nome e CNPJ;
b) Dados da empresa cliente: nome e CNPJ;
c) Descrição dos serviços/fornecimento com dados que permitam o amplo entendimento dos trabalhos realizados e identifiquem a compatibilidade e semelhança com objeto da licitação;
d) Dados do emissor do atestado: nome e contato;
e) Data de emissão e assinatura do emissor.

O TRIBUNAL poderá promover diligências para dirimir quaisquer dúvidas, esclarecer ou complementar informações prestadas e aferir a veracidade das informações constantes nos atestados e documentos apresentados, incluindo visita presencial ao ambiente da CONTRATADA se julgar necessário, sob pena de desclassificação em caso de negação de diligências.

A licitante poderá disponibilizar todas as informações que entender necessárias à comprovação da legitimidade do atestado. Em caso de dúvidas, com relação ao conteúdo do atestado, poderá ser solicitado da licitante a apresentação de documentos como, por exemplo, contratos, notas de empenho ou notas fiscais etc.

Não será admitido atestado emitido por empresas pertencentes ao mesmo grupo econômico da proponente. Consideram-se pertencentes ao mesmo grupo econômico as entidades que embora tendo, cada uma delas, personalidades jurídicas próprias, mantiverem, entre si, direta ou indiretamente, relação de controle (art. 1.098 do Código Civil), ou estiverem sob o controle, direção ou administração, direta ou indireta, de outra pessoa física ou jurídica em comum.

A empresa licitante deverá apresentar comprovação ponto a ponto, contemplando os requisitos funcionais estabelecidos neste termo de referência, para cada uma das tecnologias e serviços exigidos e utilizados para a prestação do serviço contratado.

O pregoeiro poderá, subsidiado pelo apoio técnico do CONTRATANTE e como condição de aceitação da proposta, solicitar à empresa classificada como a primeira colocada na disputa, que se submeta à realização de Prova de Conceito (POC) para comprovar o pleno atendimento de requisitos para os quais restem eventuais dúvidas, a serem enumerados pela CONTRATANTE.

a) O pregoeiro irá agendar data e horário, com antecedência de até 10 (dez) dias úteis, para que a LICITANTE apresente os itens duvidosos através de Prova de Conceito (POC);
b) A POC será realizada em ambiente preparado pela empresa classificada e apresentada de forma on-line, para que a LICITANTE demonstre a comprovação do atendimento dos requisitos enumerados, conforme as especificações exigidas no edital e seus anexos;
c) As despesas de preparação e apresentação da POC serão de responsabilidade da LICITANTE.

A LICITANTE que não apresentar a POC na data estabelecida, ou que apresentar POC que não atenda às exigências do edital, terá sua proposta desclassificada.

Justificativas para exigência do atestado: A exigência de que um dos atestados comprove, no mínimo, 50% do quantitativo total dos atestados de cada item justifica-se pela necessidade de demonstrar experiência significativa e concreta na execução de parcela relevante do objeto, sem, contudo, inviabilizar a participação de empresas que, embora não tenham executado integralmente o objeto em um único contrato, possuam experiência acumulada e capacidade técnica comprovada.

O Tribunal de Justiça do Estado do Paraná (TJPR) é uma instituição de grande porte, responsável pela prestação jurisdicional de milhões de jurisdicionados em mais de cem comarcas, operando um ecossistema tecnológico de elevada complexidade que abrange mais de 25.000 ativos, 75 contas de acesso privilegiado, 6 ativos de firewall e sistemas judiciais de missão crítica que processam diariamente dados pessoais, sensíveis e protegidos por sigilo de justiça.

Diante dessa dimensão e criticidade, a exigência de que ao menos um atestado de capacidade técnico-operacional comprove, no mínimo, 50% dos quantitativos de cada parcela de maior relevância é medida imprescindível para assegurar que a licitante já operou, de forma concreta e em um único contrato, serviços de segurança da informação em escala compatível com o porte do Tribunal, uma vez que a gestão de ambientes com milhares de ativos, a correlação massiva de eventos em tempo real, o controle de dezenas de credenciais privilegiadas e a sustentação de múltiplas camadas de defesa simultâneas impõem desafios operacionais, de governança e de dimensionamento de equipe que não podem ser adequadamente inferidos a partir do mero somatório de contratos de pequena escala.

As quantidades mínimas exigidas nos atestados têm por objetivo avaliar a capacidade da CONTRATADA em prestar os serviços de segurança da informação e cibernética de complexidade similar ao requerido pelo TRIBUNAL neste Edital. Os itens e seus quantitativos não superam a 50% das quantidades solicitadas, metodologia aceita pelo Tribunal de Contas da União (TCU) para qualificar empresas contratadas.

8.4. QUALIFICAÇÃO ECONÔMICA E FINANCEIRA

As exigências de qualificação econômica e financeira serão aquelas previstas no Edital.

8.5. CRITÉRIOS DE HABILITAÇÃO JURÍDICA, FISCAL e SICAF

8.5.1. HABILITAÇÃO SICAF

A habilitação da arrematante cadastrada no SICAF será verificada por consulta on-line ao sistema, quanto aos documentos por ele abrangidos, e por meio da documentação complementar especificada neste edital.

Os documentos abrangidos pelo SICAF são os relativos à:

a) habilitação jurídica, exceto comprovação de legitimidade para assinatura;
b) de propostas e contratos de seu representante legal ou procurador;
c) regularidade fiscal e trabalhista;
d) qualificação econômico-financeira;
e) qualificação técnica.

A arrematante não cadastrada no SICAF, ou com a documentação vencida/ausente no referido sistema, deverá apresentar o(s) documento(s) de habilitação nos prazos de envio da proposta recomposta.

8.5.2. HABILITAÇÃO JURÍDICA

Documentos relativos à habilitação jurídica:

- Cópia do contrato social (ou instrumento equivalente - tais como estatuto social ou requerimento de empresário) com alterações e consolidação em vigor, bem como documento comprobatório de seus administradores e representantes;

8.5.3. HABILITAÇÕES FISCAL, SOCIAL E TRABALHISTA

Documentos relativos à habilitação fiscal, social e trabalhista:

- prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) do Ministério da Fazenda (comprovante emitido pela Receita Federal ou Certificado de Registro Cadastral – CRC, emitido pelo SICAF);
- inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- provas de regularidade fiscal perante a Fazenda Municipal/Distrital do domicílio ou sede da arrematante;
- provas de regularidade fiscal perante a Fazenda Estadual/Distrital do domicílio ou sede da arrematante;
- provas de regularidade com a Fazenda Nacional, mediante a apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (SRFB) e Procuradoria Geral da Fazenda Nacional (PGFN);

- provas de regularidade perante o Fundo de Garantia por Tempo de Serviço - FGTS, fornecido pela Caixa Econômica Federal – CEF;
- provas de regularidade perante a Justiça do Trabalho;
- demonstrações de cumprimento do disposto no art. 7º, inc. XXXIII, da Constituição Federal.

8.6. SUSTENTABILIDADE

O objeto ora contratado não apresenta riscos identificados de impactos ambientais.

8.7. VISITA TÉCNICA

Não há obrigatoriedade de visita técnica para a contratação.

8.8. AMOSTRA

Não há obrigatoriedade de amostra para a contratação.

8.9. FORMALIZAÇÃO DA CONTRATAÇÃO

As obrigações decorrentes desta contratação a serem firmadas entre o CONTRATANTE e a CONTRATADA serão formalizadas através de contrato, observando-se as condições estabelecidas neste Termo de Referência, da legislação vigente e da proposta apresentada.

A empresa vencedora do certame será regularmente convocada para assinar o contrato ou receber/retirar instrumento equivalente, dentro do prazo de (05) cinco dias úteis, sob pena de decair do direito à contratação, sem prejuízo das penalidades previstas em lei, neste termo, no instrumento convocatório e no contrato.

O prazo da convocação poderá ser prorrogado uma vez, por igual período, quando solicitado durante o seu transcurso pela parte e desde que ocorra motivo justificado aceito pelo CONTRATANTE.

A recusa injustificada da empresa vencedora em assinar o contrato ou receber/retirar instrumento equivalente, dentro do prazo estabelecido neste Termo de Referência, caracteriza o descumprimento total da obrigação assumida, sujeitando-se às penalidades legalmente estabelecidas.

A empresa vencedora e/ou a empresa remanescente, se convocada, deverá comprovar as mesmas condições de habilitação consignadas no edital convocatório, como condição para celebração do contrato.

A assinatura de contratos e termos eletrônicos pode ser realizada também por meio eletrônico, nos termos do Decreto Judiciário nº 269/22 deste Tribunal de Justiça.

9. ESTIMATIVA DO VALOR DA CONTRATAÇÃO (Art. 6º, XXIII, i)

O estudo para estabelecer a estimativa do valor da contratação encontra-se no documento de Estudos Técnicos Preliminares (SEI 9744428).

10. ADEQUAÇÃO ORÇAMENTÁRIA (Art. 6º, XXIII, j)

A presente contratação está prevista no Plano de Contratações de Soluções de TIC para o exercício financeiro de 2025 versão 1.2, devidamente apresentado no expediente administrativo SEI nº 0039457-26.2024.8.16.6000, o qual, foi aprovado pelo Comitê Gestor de Tecnologia da Informação e Comunicação (SEI nº 0033045-60.2016.8.16.6000, Ata 11449185 item 2) e pelo Comitê de Governança de Tecnologia da Informação e Comunicação na 1ª reunião de 2025 (SEI nº 0017736-81.2025.8.16.6000, Ata 11671204 item 6).

A demanda está registrada na categoria licitações no item "SETI-23.2025 SOC - Security Operations Center", sob o valor estimado de R$ 4.000.000,00 (quatro milhões reais) para 2025.

Ainda, relativamente à Resolução n.º 195/2014 do CNJ, a distribuição orçamentária para o objeto em questão constará no Plano de Contratações na proporção de 50% para o 1.º Grau e 50% para o 2.º Grau.

11. NIVEIS MÍNIMOS DE SERVIÇOS - NMS

11.1. CONSIDERAÇÕES GERAIS

Os níveis mínimos de serviço são critérios mínimos aceitáveis pelo TRIBUNAL de modo a aferir e avaliar diversos fatores relacionados ao cumprimento dos serviços contratados. Os principais critérios a serem considerados são:

- Prazos e quantidades de entrega e execução de serviços compatíveis com os resultados esperados
- Disponibilidade dos serviços continuados e de suas soluções;
- Alocação de equipe em conformidade com os requisitos;
- Qualidade da entrega e execução de serviços compatível com o objeto.

Para mensurar esses fatores, deverão ser utilizados indicadores com metas quantificáveis e objetivos a serem cumpridas pela CONTRATADA.

Os indicadores devem ser utilizados para medir o resultado da prestação de serviços e, consequentemente, servir de base para cálculo mensal do valor de remuneração da CONTRATADA.

Os **Indicadores de Medição de Resultado (IMR)** serão apurados mensalmente, conforme critérios indicados nas tabelas aplicáveis no item 11. NIVEIS MÍNIMOS DE SERVIÇOS - NMS.

Os indicadores devem ser medidos do primeiro ao último dia de cada mês.

Os níveis de serviço deverão ser mensurados preferencialmente de forma automatizada e não poderão ser manipulados pela CONTRATADA.

Será adotado como regra de arredondamento no cálculo dos indicadores uma casa decimal, quando aplicável.

Os níveis mínimos de serviço e seus instrumentos de medição serão apurados e as glosas serão passíveis de aplicação **a partir início da fase de Operação,** conforme descrição da Dinâmica da Execução.

11.2. DAS ALTERAÇÕES DOS NÍVEIS MÍNIMOS DE SERVIÇO

Para cálculo dos indicadores de disponibilidade, serão computados como Tempo de Indisponibilidade:

- Tempo em que o respectivo serviço esteja indisponível ou com desempenho severamente degradado, impossibilitando sua eficácia;
- Será computado o intervalo de tempo decorrente entre o início da indisponibilidade do serviço e a sua total recuperação;
- Em caso de ocorrências sucessivas de indisponibilidade dentro de um intervalo inferior a 24 (vinte e quatro) horas do surgimento da primeira, tais períodos devem ser considerados de recorrência desde a primeira ocorrência de indisponibilidade. Neste caso, o tempo de indisponibilidade deve ser contado a partir do surgimento da indisponibilidade inicial até a recuperação da última indisponibilidade no intervalo.

Não serão computados como Tempo de Indisponibilidade, nem no cálculo de prazos que dependam da disponibilidade de ativos, as situações de:

- Indisponibilidade das instalações físicas, da rede ou dos links de internet do TRIBUNAL utilizados para comunicação com os serviços remotos da CONTRATADA, quando a responsabilidade for exclusiva do TRIBUNAL;
- Indisponibilidade do ambiente computacional do TRIBUNAL, quando a responsabilidade for exclusiva do TRIBUNAL;
- Manutenções programadas do ambiente computacional do TRIBUNAL;
- Manutenções programadas pela CONTRATADA, desde que previamente comunicadas ao TRIBUNAL;
- Tempo decorrido em chamados escalados para o fabricante de um componente de solução informatizada, enquanto estiverem em tratamento e cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução.

Os indicadores e metas podem ser revisados e alterados em comum acordo entre a CONTRATADA e a CONTRATANTE durante a vigência do contrato.

11.3. GLOSAS

A CONTRATADA estará sujeita à aplicação de glosas de valores correspondentes aos serviços ou produtos não conformes ou irregulares, conforme apurações do **Indicadores de Medição de Resultados (IMR)**.

- Os percentuais e valores de glosas apurados serão descontados no faturamento referente ao mês de competência de apuração ou subsequentes, se aplicável.

O somatório de todas as glosas aplicáveis (percentuais) incide sobre o valor total da fatura mensal do item de serviço de natureza continuada afetado, ou do valor total da fatura de entrega do serviço por empreitada, ou do valor total da Ordem de Serviço (OS), no mês de ocorrência, limitado a 10% (dez por cento) do respectivo item do serviço. Ultrapassado o limite de glosa, e sem prejuízo da aplicação desta, será aberto procedimento administrativo para aplicação das sanções cabíveis previstas no ID 1 da Tabela 15 - Tabela de Conduta 03.

A aplicação de glosa pelo não atendimento de metas dos **Indicadores de Mediação de Resultado (IMR)**, onde se aplicar, poderá ser objeto de contestação, por meio do oferecimento de elementos que visem comprovar a não responsabilidade, por parte da CONTRATADA.

11.4. O ACORDO DE NÍVEL DE SERVIÇO (SLA / ANS) DE ATENDIMENTO

Os prazos estabelecidos no acordo de nível de serviço serão contados a partir da abertura de ticket de atendimento e serão classificados conforme as severidades especificadas na tabela abaixo, caso a demanda que gerou os tickets de atendimentos já tenha sido previamente classificado.

Nível de Severidade	Impacto/ Descrição
CRÍTICO	problema que causa ou possa causar comprometimento ou possa interromper ou interrompa funcionalidades essenciais para a operação do TRIBUNAL, com perda ou paralisação total de serviços, sistemas, ativos de TIC em produção ou que impactem significativamente a confidencialidade, disponibilidade e integridade dos dados e informações do TRIBUNAL, como por exemplo: • Algum tipo de incidente que gerou indisponibilidade em servidores essenciais e sistemas, afetando um ou mais usuários;

	• Infecção ou paralisação generalizada devido a ransomware ou algum outro tipo de malware; • Roubo ou vazamento de dados devido a falha humana ou técnica; • Algum tipo de impacto ou risco grave a empresa ou a equipe de Segurança da Informação; • Quando o problema/incidente/requisição é definido com o nível de criticidade “CRÍTICO”.
ALTA	problema que interrompe operações funcionais com a manutenção da operação do ambiente, ainda que com restrições de desempenho ou de funcionalidades não essenciais, como por exemplo: • Servidor de produção ou sistema crítico está apresentando instabilidade, degradação ou sofrendo ataques recorrentes que podem acarretar uma exploração ou vazamento de dados; • Alarmes de nível ALTA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; • Ocorrências/Incidentes/requisições relacionados a usuários definidos como VIP pelo CONTRATANTE; • Quando o problema/incidente/requisição é definido com o nível de criticidade “ALTA”.
MÉDIA	problema que não causa nenhuma perda de funcionalidade e não impede a operação dos serviços essenciais do TRIBUNAL, como por exemplo: • Nenhum serviço crítico está envolvido e não existe risco de perda de dados; • Alarmes de nível MÉDIO identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; • Quando o problema/incidente/requisição é definido com o nível de criticidade “MÉDIA”.
BAIXA	esclarecimento de dúvidas ou consultas técnicas, como por exemplo: • Dúvidas ou apoio à implementação; • Novas implementações; • Sugestões de novos recursos ou aprimoramento do Software; • Alarmes de nível BAIXA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; • Evidências de um bloqueio ou tratativa automatizada; e • Quando o problema/incidente/requisição é definido com o nível de criticidade “BAIXA".

Tabela 17 - Tabela de níveis de criticidade e impacto

Um atendimento pode, a depender da evolução da gravidade do problema, ser escalado de graduação de severidade, com os prazos de solução do problema sendo considerados o do novo nível de severidade e começando a ser contabilizados a partir do momento da escalação do chamado ao novo nível.

11.5. INDICADORES DE MEDIÇÃO DE RESULTADO (IMR)

O IMR deverá ser utilizado como base para construção do Relatório de Indicadores de Medição de Resultados - RIRM do Contrato e evidências de comprovação dos serviços efetivamente prestados pela CONTRATADA.

Os prazos para atendimento devem obedecer, no mínimo, aos parâmetros da tabela abaixo, contabilizados a partir da abertura do chamado e serão medidos e apurados mensalmente, de modo a alcançar as respectivas metas exigidas:

Item	Tipo de Incidente	Severidade	TMIA	TMSO	TMSDC	Métricas de Desempenho *	Glosa As glosas incidem sobre o valor mensal do item afetado.
1	Tratamento de Incidente de segurança	Crítica	30min	4 horas	24 horas	≥ 99%	N/A

Item	Tipo de Incidente	Severidade	TMIA	TMSO	TMSDC	Métricas de Desempenho *	Glosa As glosas incidem sobre o valor mensal do item afetado.
2	Tratamento de Incidente de segurança	Alta	60 min	8 horas	48 horas	≥ 99%	N/A
3	Tratamento de Incidente de segurança	Média	2 horas	24 horas	60 horas	≥ 95%	1% (um por cento) por descumprimento da meta, e; 0,1% (um décimo por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta.
4	Tratamento de Incidente de segurança	Baixa	8 horas	48 horas	72 horas	≥ 95%	1% (um por cento) por descumprimento da meta, e; 0,1% (um décimo por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta.
5	Solicitação de serviço	Crítico	60 min	2 horas	N/A	≥ 99.7%	3% (um por cento) por descumprimento da meta, e; 0,1% (um décimo por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta.
6	Solicitação de serviço	Alta	2 horas	6 horas	N/A	≥ 95%	3% (um por cento) por descumprimento da meta, e; 0,1% (um décimo por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta.
7	Solicitação de serviço	Média	4 horas	24 horas	N/A	≥ 95%	1% (um por cento) por descumprimento da meta, e; 0,1% (um décimo por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta.
8	Solicitação de serviço	Baixa	8 horas	48 horas	N/A	≥ 95%	1% (um por cento) por descumprimento da meta, e; 0,1% (um décimo por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta.

Item	Tipo de Incidente	Severidade	TMIA	TMSO	TMSDC	Métricas de Desempenho *	Glosa As glosas incidem sobre o valor mensal do item afetado.
9	Solicitação de serviço planejado	N/A	24 horas	Não se aplica	Conforme planejado	= 100%	1% (um por cento) por descumprimento da meta, e; 0,1% (um décimo por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta.
10	Tratamento ou controle de vulnerabilidade crítica ou ameaça emergente	Crítica	6 horas	48 horas	Conforme planejado	≥ 95,0%	1% (um por cento) por descumprimento da meta, e; 0,1% (um décimo por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta.

Tabela 18 - Indicadores de Medição de Resultado baseado em tempo de resposta

* O cálculo da métrica de desempenho é realizado através dos eventos que atenderam os prazos divido pelo total de eventos registrados multiplicado por 100.

TMIA – Tempo Máximo para Início do Atendimento.

TMSO – Tempo Máximo para Solução Operacional, requerido para que o serviço ou o sistema impactado volte a funcionar, independentemente de ter sido resolvida a causa raiz do problema.

TMSDC – Tempo Máximo para a Solução Definitiva do Chamado, situação em que o serviço esteja plenamente funcional e a causa raiz do problema é eliminada.

Serão medidos resultados para um acompanhamento geral dos serviços prestados de modo a alcançar as respectivas metas exigidas:

Item	Tipo de Solicitação/ Incidente	Métricas de desempenho	Glosa As glosas incidem sobre o valor mensal do item afetado.
1	Descumprimento dos prazos dos entregáveis do item 2	Zero ocorrências	1% / dia corrido de atraso
2	Disponibilidade mensal de cada serviço continuado, aferido individualmente	Total de tempo de disponibilidade do serviço / Total de tempo no mês x 100 ≥ 99,7% Fonte: Portal de indicadores de serviço da CONTRATADA	5% (um por cento) por descumprimento da meta, e; 0,5% (cinco décimos por cento) adicional a cada 0,1% (um décimo por cento) abaixo da meta,

Item	Tipo de Solicitação/ Incidente	Métricas de desempenho	Glosa As glosas incidem sobre o valor mensal do item afetado.
3	Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução	Zero ocorrências	0.25% (vinte e cinco décimos por cento) por ocorrência
4	Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação	Zero ocorrências	0.25% (vinte e cinco décimos por cento) por ocorrência
5	Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução	Zero ocorrências	0.25% (vinte e cinco décimos por cento) por ocorrência
6	Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada	Zero ocorrências	0.25% (vinte e cinco décimos por cento) por ocorrência
7	Comunicar aos administradores do anfitrião (host) o Takedown em menos de 120 min. do horário de detecção do incidente ou aprovação da comunicação pelo Tribunal	Zero ocorrências	0.25% (vinte e cinco décimos por cento) por ocorrência
8	Entrega de dashboard de acompanhamento diário	Zero ocorrências	0.1% (um décimo por cento) por ocorrência

Tabela 19 - Indicadores de Medição de Resultado Geral

ANEXO A – ESPECIFICAÇÕES TÉCNICAS DO OBJETO DE STIC

1. OBJETO

Solução de TI consistente em serviços gerenciados de Segurança da Informação e Cibernética (MSS), com prestação contínua e sob demanda, aplicados ao ambiente tecnológico do Tribunal de Justiça do Estado do Paraná, pelo período de 36 (trinta e seis) meses prorrogável até o limite legal.

2. ITENS DO OBJETO

	Item	Categoria	Descrição	Qtde	Tipo
Grupo 1	1	**Projeto e implantação**		01	Unitário
	2	**Serviços de Governança e Conformidade de Segurança**			
		2.1	Diagnóstico de Maturidade de Segurança da Informação	03	Unitário
		2.2	Política de Segurança da Informação (PSI)	33	Mês
		2.3	Plano de Continuidade de Serviços Essenciais de TIC	33	Mês
		2.4	Plano de Resposta a Incidentes (PRI)	33	Mês
	3	**Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança**			
		3.1	Serviço de Security Operations Center (SOC)	825.000	Ativos protegidos
		3.2	Proteção contra Riscos Digitais (Threat Intelligence)	33	Mês
		3.3	Serviço de Takedown	60	Takedown executado
	4	**Sustentação de Operações de Soluções e Resposta a Requisições de Segurança**			
		4.1	Solução de Firewall	198	Ativos protegidos
		4.2	Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)	660.000	Ativos protegidos
	5	**Gestão de Vulnerabilidades e Testes de Segurança**			
		5.1	Gerenciamento Contínuo de Vulnerabilidades	33	Mês
		5.2	Testes de Segurança Automatizados (BAS)	990	Baterias realizadas
	6	**Gestão de Identidade**			
		6.1	Gerenciamento de Acesso Privilegiado (PAM)	2.640	Usuários administrativos protegidos
	7	**Serviços Técnicos Especializados por Demanda**		1.200	Horas sob demanda
Item Avulso	8	**Serviço de Teste de Invasão (Pentest)**		360	Horas sob demanda

Tabela 1 - Itens do Objeto

2.1. CONSIDERAÇÕES GERAIS

Os serviços prestados devem ser providos de modo a gerenciar remotamente e administrar equipamentos e softwares componentes dos Serviços Gerenciados de Segurança (MSS), bem como identificar e investigar eventos que possam comprometer a segurança dos serviços de Tribunal, manter a infraestrutura de segurança atualizada, mapear e executar processos de resposta a incidentes de segurança, avaliar periodicamente as configurações implementadas, abrangendo também o enfrentamento de emergências, crises, ataques cibernéticos, vazamentos de informações e eventos relacionados, sob um regime de 24x7 (vinte e quatro horas por dia, sete dias por semana).

A CONTRATADA é responsável por prover todos os softwares, hardwares e infraestrutura necessária para o funcionamento das soluções exigidas neste processo, salvo as soluções descritas explicitamente, que serão disponibilizados pela CONTRATANTE para hospedar os serviços inerentes ao atendimento do contrato.

Se houver a necessidade de implantação de controladores, concentradores, coletores, sensores, agentes, conectores, equipamentos dedicados (appliances) e qualquer outro recurso de hardware e software local na infraestrutura interna do TRIBUNAL, a CONTRATADA deve fornecer e sustentar todos os recursos necessários e ser responsável pelo seu fornecimento, implantação, instalação, configuração, sustentação, atualização, administração e operação, sem custo adicional.

A CONTRATADA deve garantir que a prestação do serviço não impacte negativamente a performance dos sistemas, ativos e rede corporativa do TRIBUNAL.

Todos os pontos funcionais exigidos e especificados neste termo de referência são requerimentos obrigatórios, devendo ser considerados nas diferentes fases de implementação e, por conseguinte, na operação dos serviços.

2.2. PROJETO E IMPLANTAÇÃO

A CONTRATADA deve executar no prazo máximo de 90 (noventa) dias, a contar da assinatura do contrato, o Projeto e implantação com atividades de planejamento, instalação, adoção tecnológica, implantação do serviço, configuração e elaboração de documentação técnica.

A CONTRATADA deve convocar reunião inicial para apresentação do preposto do contrato e do gerente de projetos desta fase, contendo no mínimo os seguintes itens:

a) Alinhamento do projeto, marcos e prazos específico de cada etapa, prioridades, regras de negócios, requisitos, serviços e aspectos de infraestrutura para implementação dos serviços;
b) Definição do canal de atendimento para reporte de incidentes, problemas e solicitações de serviço;
c) Definição de papéis e responsabilidades.

Todas as atividades e documentação apresentadas deverão ser previamente aprovadas pela CONTRATANTE.

É responsabilidade da CONTRATADA o levantamento, junto à CONTRATANTE, de todas as informações necessárias para implantação/adoção dos itens de serviço, incluindo topologia e configuração atual, processos de trabalho em execução e locais de execução dos serviços.

A implantação, configuração e manutenção das soluções deverá ser realizada por profissional certificado pelo fabricante.

No término do Projeto e Implantação a CONTRATADA deve entregar uma Declaração de Implantação e um Relatório final de Implantação contendo documentação de cada serviço implementado com no mínimo as seguintes informações:

- Descrição dos serviços implantados;
- Descrição da topologia física e lógica, após a ativação dos serviços, dos ambientes onde estão hospedados os equipamentos, softwares e soluções entregues pela CONTRATADA;
- Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;
- Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;
- Definição de responsabilidades;
- Recursos de alta disponibilidade;
- Credenciais de acesso para acompanhamento da parte técnica do TRIBUNAL;
- Procedimentos para abertura e atendimento a chamados;
- Procedimentos de recuperação de equipamentos;
- Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;
- Rotinas periódicas configuradas;
- Documentação dos processos de trabalho associados ao item;
- Desenho dos racks onde estão instalados os equipamentos, se aplicável;
- Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos);
- A CONTRATADA deverá seguir o processo de mudança estabelecido pela CONTRATANTE;
- Todos os serviços previstos neste processo deverão ser implantados, documentados e revisados pela CONTRATADA, seguindo a metodologia ITIL;
- 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.

2.3. SERVIÇOS DE GOVERNANÇA E CONFORMIDADE DE SEGURANÇA

A CONTRATADA deverá prestar Serviços de Governança e Conformidade de Segurança com amplo apoio e suporte técnico e metodológico ao TRIBUNAL em segurança da informação e cibersegurança, visando alcançar metas e objetivos da organização, incluindo conformidade com a legislação, normativos e melhores práticas, elevação da maturidade e melhoria contínua, além disso, deve estruturar, planejar, implementar, controlar, monitorar e evoluir arcabouços e instrumentos do sistema de gestão de segurança da informação (SGSI), considerando os objetivos gerais definidos na norma ABNT ISO/IEC 27014:2021 - Governança da segurança da informação a seguir:

- Apoio para estabelecer segurança da informação e cibernética abrangente e integrada ao TRIBUNAL;
- Estabelecer arcabouço para auxiliar na tomada de decisões usando uma abordagem baseada em risco;
- Apoiar na definição do direcionamento de iniciativas e aquisições;
- Assegurar a conformidade com os requisitos internos e externos;
- Apoiar na promoção de uma cultura positiva de segurança;
- Assegurar que o desempenho da segurança atenda aos requisitos atuais e futuros da entidade;
- Apoiar de forma consultiva, em todos os serviços prestados, a melhoria contínua da segurança do ambiente.

A CONTRATADA deverá realizar, documentar e apresentar diagnósticos e avaliações, com análises de GAPs (situação e lacunas), maturidade, progresso e melhoria contínua, conformidade com leis, normas, melhores práticas, políticas, processos, planos e procedimentos, controles e atividades, papéis e responsabilidades, com periodicidade mínima anual, tendo como base os seguintes referenciais:

- Nível global (arcabouço de governança e gestão): NIST Cybersecurity Framework (CSF) incluindo seus quatro Níveis (Tiers) de Implementação da Estrutura, normas ABNT NBR ISO/IEC 27001:2022 - Requisitos de Sistemas de gestão da segurança da informação, ABNT NBR ISO/IEC 27032:2015 - Diretrizes para segurança cibernética, ABNT NBR ISO/IEC 27004:2017 - Sistemas de gestão da segurança da informação - Monitoramento, medição, análise e avaliação, Resolução CNJ Nº 396/2021 - Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e seus Anexos na Portaria CNJ nº 162/2021;
- Nível conceitual de controles: norma ABNT NBR ISO/IEC 27002:2022 - Controles de segurança da informação;
- Nível de catálogo de controles de segurança e privacidade nas camadas lógica e física: CIS Critical Security Controls, complementado por linha de base personalizada do NIST Special Publication (SP) 800-53 - Security and Privacy Controls for Information Systems and Organizations;
- CSA Cloud Controls Matrix (CCM);
- Common Criteria for Information Technology Security Evaluation (CC:2022 ou série ISO/IEC 15408:2022) e Common Methodology for Information Technology Security Evaluation (CEM:2022 ou ISO/IEC 18045:2022);
- Podem ser adotados referenciais atualizados que venham a estar disponíveis e sejam aprovados pelo TRIBUNAL, devendo ser feito o mapeamento entre o referencial anterior e o novo para que se tenha uma visão de progresso.

Deve-se adotar como referência a experiência e a metodologia da CONTRATADA, bem como a conformidade às seguintes normas e boas práticas:

- CNJ. Resolução Nº 370 de 28/01/2021 - Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- CNJ. Resolução Nº 396 de 07/06/2021 - Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- CNJ. Portaria Nº 162 de 10/06/2021 - Aprova Protocolos e Manuais criados pela Resolução CNJ Nº 396/2021;
- TJPR. Decreto Judiciário Nº 560/2022 - P-GP Política de Segurança da Informação - PSI, no âmbito do Poder Judiciário do Estado do Paraná.

Deve haver um ciclo de revisão e melhoria contínua para métricas e indicadores, objetivos, visando o aperfeiçoamento de políticas e normas, planos, processos, procedimentos de segurança da informação da CONTRATADA.

A CONTRATADA deverá executar o estabelecimento online da apuração, documentação e melhoria contínua de métricas, indicadores chave de desempenho (KPI), painéis (dashboards) técnico-operacional (foco em tecnologia) e estratégico-gerencial (foco no negócio) e lições aprendidas, com relatórios mensais de situação e desempenho, tendo como referência: Gartner Cybersecurity Business Value Benchmark: métricas de níveis de proteção orientados a resultados.

2.3.1. DIAGNÓSTICO DE MATURIDADE DE SEGURANÇA DA INFORMAÇÃO

A CONTRATADA deverá realizar, nos primeiros 90 (noventa) dias de cada ciclo anual a execução deste serviço, sendo avaliação de Diagnóstico de Maturidade de Segurança da Informação e Cibernética no ambiente do CONTRATANTE com o objetivo de identificar lacunas ou oportunidades de melhoria (*Gap Analysis*), avaliando políticas, normas, processos, procedimentos, papéis e responsabilidades e os controles de segurança na CONTRATANTE.

A CONTRATADA, após o levantamento inicial das lacunas ou falhas de segurança da informação no ambiente da CONTRATANTE, deverá elaborar, apresentar e apoiar na execução de um plano de ação em conjunto com a CONTRATANTE, priorizando as falhas ou lacunas de maior risco e falhas mais críticas para o ambiente do TRIBUNAL.

Para o diagnóstico de maturidade, a CONTRATADA deverá entregar no mínimo:

a) Relatório de diagnóstico e avaliação, contendo uma análise detalhada dos resultados obtidos, com recomendações para melhorias e dashboards;
b) Nível de maturidade dos controles de segurança da informação;
c) Importância dos controles de segurança para o TRIBUNAL;
d) Análise de Gaps dos controles de segurança, conforme maturidade coletada nos questionários e na análise técnica de segurança dos ativos, e o cenário de ameaças;
e) Relatórios executivos, técnicos, por detalhe dos controles, por comparação com frameworks de segurança, completos e detalhados;
f) Comparação e possível maturidade e aderência a frameworks de segurança.
g) Plano de ação para implementação das melhorias recomendadas;
h) Apresentação executiva dos resultados e planos de ação para a alta administração da organização, contendo os seguintes tópicos:
    - Informações da equipe de trabalho;
    - Resumo;
    - Categorização dos controles;
    - Resultados da avaliação;
    - Status de implementação (não implementado, parcialmente implementado e implementado) para os controles/domínios;
    - Matriz de priorização;
    - Road-map de implementação;
    - Comparativo entre os diagnósticos, demonstrando a evolução da maturidade de segurança obtida pelo TRIBUNAL.

2.3.2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

A CONTRATADA deverá apoiar na proposta de elaboração, análise, revisão e melhoria contínua da Política de Segurança da Informação (PSI) da CONTRATADA, considerando processos e procedimentos de segurança da informação, com base nas necessidades, na legislação e nos normativos vigentes aplicáveis, bem como nas melhores práticas de mercado, visando orientar e sustentar, em termos normativos e regulatórios, a efetividade e eficácia das operações e práticas de segurança da informação e cibernética no TRIBUNAL.

2.3.3. PLANO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DE TIC COM FOCO NO SOC

A CONTRATADA deverá apoiar no aprimoramento, execução, adequação as melhores práticas, plano de testes e melhoria contínua do Plano de Continuidade de Serviços Essenciais de TIC com foco no SOC durante a vigência do contrato, priorizando os serviços essenciais de TIC do TRIBUNAL. O apoio também deve incluir construção e validação dos planos de Plano de Administração de Crise (PAC), Plano de Continuidade Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

Deve dotar como referência a experiência e a metodologia da CONTRATADA de normas como:

a) ABNT NBR ISO 22301:2020 - Sistema de gestão de continuidade de negócios — Requisitos;
b) ABNT NBR ISO 22313:2020 - Orientações para o uso da ABNT NBR ISO 22301;

c) ABNT NBR ISO 27005:2023 - Gestão de riscos de segurança da informação;
d) ABNT ISO/TS 22317:2023 - Diretrizes para análise de impacto nos negócios (BIA);
e) ISO/TS 22332:2021 - Guidelines for Developing Business Continuity Plans and Procedures;
f) ISO 22398:2013 - Societal Security - Guidelines for Exercises.

Apoiar na realização da análise de impacto com foco nos Serviços Essenciais de TIC do TRIBUNAL e na quantificação do impacto que a indisponibilidade do serviço de essencial causa no negócio do CONTRATANTE.

Apoiar no planejamento, elaboração e execução de testes e em exercícios na gestão de continuidade com foco em Serviços Essenciais de TIC.

Apoiar na análise de risco, identificando potenciais ameaças para a continuidade e a probabilidade que porventura venham acontecer, bem como, precisará incluir medidas para gerenciar as ameaças identificadas, quando o custo se justificar.

Apoiar na análise de impacto no negócio (AIN), considerando:

a) A identificação dos Serviços Essenciais de TIC do CONTRATANTE;
b) Determinar os efeitos da indisponibilidade;
c) Avaliação do cenário que será impactado;
d) Análise das obrigações legais junto ao cumprimento pela CONTRATADA e CONTRATANTE;
e) Análise do tempo que o CONTRATANTE se manterá em caso de indisponibilidade total da TIC;
f) Avaliação dos requisitos mínimos de restabelecimento (pessoal, infraestrutura e serviços de TIC) para assegurar os processos críticos para o CONTRATANTE;
g) Determinar o tempo mínimo e máximo dos níveis de serviços a serem recuperados;
h) Determinar quais processos do CONTRATANTE devem ser recuperados por completo.

Apoiar e orientar o CONTRATANTE para lidar com os riscos. Além da estrutura de decisão, quatro tipos de risco que requerem diferentes planos de gerenciamento de risco: Riscos de rotina, Riscos complexos, Riscos incertos e Riscos ambíguos.

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.

Apoiar em estabelecer o processo de gerenciamento de risco envolvendo a revisão das informações coletadas como parte das avaliações de risco, passando pelas etapas de identificação, análise e avaliação dos riscos. Essas informações devem constituir a base das decisões que levam ao resultado para cada risco percebido, que será estabelecido em conjunto com o CONTRATANTE.

Apoiar na operacionalização da Gestão de Riscos de segurança da informação e cibernética, 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.

Apoiar no gerenciamento de riscos, devendo a CONTRATADA:

a) Utilizar a matriz de riscos existente no TRIBUNAL e juntamente com a SETI para propor ações de tratamento dos riscos (evitar, aceitar, mitigar, eliminar ou transferir);

b) Realizar ações de análise de riscos, visando a criação de uma matriz em conformidade com as diretrizes da administração da CONTRATADA;
c) Acompanhar e realizar ações de orientação junto aos responsáveis para cada ação definida nos processos de mitigação e tratamento.

Avaliação de riscos:

a) Apoiar no entendimento para a probabilidade de 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;
b) A CONTRATADA deve apoiar na avaliação de riscos, identificando os riscos a processos ou serviços em particular, níveis de ameaças e vulnerabilidades, níveis de risco e medidas de redução de riscos.

2.3.4. PLANO DE RESPOSTA A INCIDENTES (PRI)

A CONTRATADA deverá apoiar na elaboração, implantação, execução e melhoria contínua de um Plano de Resposta a Incidentes (PRI) de Segurança cibernética, contemplando o processo e visando maximizar a eficácia e minimizar os tempos de detecção e de resposta aos incidentes de segurança cibernética, observando também a integração e a ampla visibilidade.

Deve contemplar as fases de planejamento e preparação, detecção e notificação, triagem e análise, contenção, erradicação e recuperação, documentação e lições aprendidas.

Deve contemplar as comunicações internas e externas e as correlações com incidentes de segurança da informação e incidentes de privacidade e proteção de dados pessoais.

Deve incluir um plano específico para o gerenciamento de crises cibernéticas, buscando a continuidade dos serviços de TIC afetados e seu restabelecimento.

Deve contemplar planos de mitigação e recuperação de serviços e ativos de TIC.

Deve contemplar análise forense de fatos penalmente relevantes.

Deve adotar como referência experiência e metodologia da CONTRATADA e as seguintes normas e boas práticas:

- CNJ. Portaria Nº 162 de 10/06/2021, em especial os protocolos de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ); Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ); e Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ);
- ABNT NBR ISO 22320:2020 Diretrizes para gestão de incidentes;
- ISO/IEC 27035-1:2023 Information Security Incident Management - Part 1: Principles of Incident Management;
- ISO/IEC 27035-2:2023 Information Security Incident Management - Part 2: Guidelines to Plan and Prepare for Incident Response;
- ABNT NBR ISO/IEC 27035-3:2021 Gestão de Incidentes de Segurança da Informação Parte 3: Diretrizes para Operações de Resposta a Incidentes de TIC;
- ABNT NBR ISO/IEC 27037:2013 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital;
- NIST SP 800-61 - Computer Security Incident Handling Guide, Rev. 2;
- NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations, Rev. 5.1, Incident Response - IR;

- FIRST.Org Computer Security Incident Response Team (CSIRT) Services Framework, versão 2.1.0, em especial as áreas de serviço “Information Security Event Management” e “Information Security Incident Management”;
- CIS Controle 17 - Gestão de Respostas a Incidentes;
- CREST Cyber Security Incident Response Guide, Version 1.

2.4. MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTAS A INCIDENTES DE SEGURANÇA

2.4.1. SERVIÇOS DE SECURITY OPERATIONS CENTER (SOC)

A CONTRATADA prestará o serviço de monitoramento, detecção, triagem, investigação e resposta, gerenciamento de eventos e incidentes de segurança da informação e cibernética, por meio de um Serviços de Security Operations Center ou Centro de Operações de Segurança próprio da CONTRATADA, contemplando equipe, processos, gestão de eventos, incidentes e crises. A prestação deverá incluir solução informatizada para gerenciamento, monitoramento, detecção e resposta de informações, eventos e incidentes de segurança, licenciado pela CONTRATADA, devendo utilizar processos, planos integrados e especializados de Nível 0 (automação), Nível 1 (atuação inicial), Nível 2 (atuação avançada) e Nível 3 (especialistas).

O funcionamento do SOC deve ser em regime ininterrupto 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano (úteis e não úteis).

A CONTRATADA deve atender uma das opções abaixo:

a) possuir no mínimo 02 (dois) Centros de Operação de Segurança, sendo um em território nacional, redundantes e que devem estar em pleno funcionamento (infraestrutura física, lógica, equipe e processos) na contratação e durante toda a vigência do contrato, de modo que a indisponibilidade não afete a prestação dos serviços. O SOC principal e o redundante utilizados no serviço devem estar situados em regiões distintas, e estar no mínimo a 50 km (cinquenta quilômetros) de distância geodésica um do outro, como redundância geográfica para mitigar os riscos de interrupção dos serviços e de perda total dos dados em caso de desastres naturais, falhas de energia, entre outros eventos adversos;
b) deve possuir 01 (um) Centro De Operações de Segurança (SOC) em território nacional, em pleno funcionamento (infraestrutura física, lógica, equipe e processos), na contratação e durante toda a vigência do contrato. A operação deve ser garantida de forma que a continuidade dos serviços não seja interrompida por tempestividades de qualquer natureza através da apresentação de um plano de continuidade.

Ao menos um SOC da CONTRATADA deverá possuir certificação ISO/IEC 27.001 vigente na contratação e durante a vigência do contrato, emitida em nome da CONTRATADA por organização independente acreditada pelo Inmetro ou por autoridade equivalente globalmente reconhecida, garantindo que a CONTRATADA siga as principais diretrizes e controles de segurança da informação e de privacidade de dados.

Deve possuir estrutura central para visualização dos painéis de monitoramento (video-wall) que permita que todos os profissionais visualizem informações e eventos relevantes simultaneamente.

Deve utilizar sistema de gerenciamento de circuito fechado de televisão (CFTV), que viabilize o rastreamento de pessoas dentro do ambiente da CONTRATADA, e cujas imagens possam ser recuperadas e mantidas armazenadas por, no mínimo, 90 (noventa) dias.

Deve possuir controle de acesso físico seguro de funcionários, com pelo menos um dos seguintes fatores de autenticação: cartão de identificação magnético ou de proximidade, biometria de leitura de digital, face ou retina, e

registro de entrada e saída de visitantes, com registro de entrada e saída de todas as pessoas mantido por, pelo menos, 90 (noventa) dias.

Deve possuir perímetro físico equipado com sensor de intrusão e alarmes contra acesso indevido.

Deve possuir estrutura de armazenamento de dados que permita a manutenção dos registros das requisições e dos incidentes relacionados aos serviços contratados por, no mínimo, o prazo do contrato.

Deve possuir sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPS (*Uninterruptible Power Supply*), garantindo a transição entre o fornecimento normal da energia e o grupo gerador.

Deve possuir componentes de segurança e plano de recuperação necessários para garantir a preservação dos dados em casos de incêndio e catástrofes.

Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores estejam inacessíveis a leituras e a capturas externas desautorizadas.

Os recursos físicos da CONTRATADA (prédio, salas, mesas e outros) poderão ser compartilhados com outros clientes, desde que a infraestrutura lógica que atende o TRIBUNAL seja separada dos demais clientes, segregada e segmentada por mecanismos como multilocação (multitenancy), VLANs e controles compensatórios de segurança.

Deve possuir ambiente dedicado único e exclusivamente para laboratório, onde seja possível reproduzir os incidentes e problemas do TRIBUNAL, sem que haja impacto na operação dos SOCs e/ou do próprio TRIBUNAL.

Deve garantir capacitação e treinamento inicial e contínuo dos profissionais que executam os serviços.

Deve gerenciar a alocação de turnos e substituições temporárias e definitivas dos profissionais de sua equipe, de forma a garantir a prestação de serviços de forma contínua, ininterrupta e eficaz.

A CONTRATADA deverá fornecer link, às suas custas, de comunicação dedicado cuja utilização não deverá ultrapassar 80% (oitenta por cento) de sua capacidade, podendo ser utilizado VPN via Internet como redundância.

A CONTRATADA deverá dimensionar as soluções informatizadas capaz de suportar, sem perda de performance, usuários simultâneos e ativos (incluindo desktops, servidores, impressoras, switchs roteadores e todo equipamento que tenha a ele atribuído, um endereço IP, conforme estimativa de ativos apresentadas no **ANEXO IV - ESTIMATIVAS DE ATIVOS PARA DIMENSIONAMENTO DOS SERVIÇOS**.

Todos os equipamentos e softwares utilizados pela CONTRATADA para a entrega deste serviço, quando for o caso e se necessário à consecução das atividades de segurança, devem atender às especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado, adotando como referência de mercado estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC e ISG Group.

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

O TRIBUNAL poderá a qualquer tempo registrar (abrir) um incidente de segurança, seja oriundo do seu corpo técnico ou dos usuários internos.

O início do processo de tratamento e resposta a incidente de segurança se dará sempre que um evento ou série de eventos adversos for submetido pelo monitoramento, bem como sempre que um incidente de segurança for registrado pelo TRIBUNAL.

A CONTRATADA deverá envidar seus melhores esforços para que quaisquer ataques, invasões ou incidentes sofridos pelo TRIBUNAL em seu ambiente tecnológico sejam identificados, controlados e prontamente reportados para atuação técnica da SETI orientando e fornecendo informações para que equipes internas possam interromper ou mitigar estas situações, em caráter provisório ou definitivo, mantendo as ações registradas para o fornecimento de relatórios e recomendações ao TRIBUNAL.

O SOC deve orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer.

Para o monitoramento, Tratamento de Resposta a Incidentes, a CONTRATADA:

a) Deve orientar e apoiar na geração e encaminhamento de logs úteis dos ativos de infraestrutura de TIC do TRIBUNAL para o SOC;
b) Se necessário, implementar e gerenciar estrutura de logs centralizadas, contendo recursos de alta disponibilidade no ambiente do TRIBUNAL com capacidade de coletar e filtrar logs úteis de diferentes fontes internas para prestação dos serviços, para o envio ao SOC, visando economia de espaço, desempenho e performance de rede;
c) Os mecanismos de envio de log ou estrutura implementada deve ser aprovada pela equipe técnica da SETI, se houver;
d) Os mecanismos de envio de log ou estrutura deve prever o envio de logs para mais um destino, conforme definição da equipe técnica do TRIBUNAL.

Deve supervisionar sua equipe na execução dos serviços, inclusive nas ações conjuntas com a área de TIC do TRIBUNAL, garantindo a observância e cumprimentos das políticas, normas, procedimentos e melhores práticas e dos níveis de serviço estabelecidos.

Deve atuar diligentemente quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TIC do TRIBUNAL.

Deve receber as demandas dos serviços relativas à área de segurança da informação e cibernética e providenciar a execução e alocação de recursos de trabalho.

Deve realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo TRIBUNAL.

Deve priorizar os atendimentos críticos, conforme definição do TRIBUNAL.

Deve fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação do TRIBUNAL, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas.

Deve manter em manuais e scripts atualizados todos os serviços e soluções adotados, sejam eles novos ou já implantados no TRIBUNAL.

Realizar a definição, análise, atualização, melhoria e expansão dos casos de uso de monitoramento e detecção, bem como dos playbooks de tratamento, resposta e automação.

Deverão ser realizadas mensalmente análises dos eventos para a sugestão de novos casos de uso, **sem restrição de quantidade**. A CONTRATADA deverá conduzir as análises dos eventos, sugerir novos casos de uso, bem como implementar as regras de correlação. Além disso, deverá ser possível que a CONTRATANTE solicite a criação de novos casos de uso conforme suas necessidades.

Deve entregar mensalmente relatórios gerenciais, incluindo níveis de serviço, atualizações de versões, principais incidentes e vulnerabilidades, estatísticas sobre desempenho e melhorias propostas, entre outras recomendações.

Deve entregar relatórios mensais dos resultados dos serviços prestados, com análise crítica clara elaborada pelos times técnicos da CONTRATADA.

Deve confeccionar relatórios técnicos pontuais sob demanda.

Deve agendar reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE.

O TRIBUNAL pode, a qualquer momento, solicitar a inclusão ou a exclusão de fonte de dados, de campos personalizados em eventos, regras de co-relacionamento de eventos, geração de alertas e de incidentes de segurança cibernética.

Rever periodicamente às políticas e processos do SOC, a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL.

2.4.2. FORENSE DIGITAL

Realizar os procedimentos cabíveis de análise e investigação forense pós-incidentes para fatos penalmente relevantes, observando o Protocolo de investigação de ilícitos da Portaria Nº 162 do CNJ e anexos, a saber:

Durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar, sempre que possível:

a) As mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;
b) Os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM);
c) Todos os registros de eventos aplicáveis.

Nos casos de inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado, deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os “metadados” desses arquivos, como data, hora de criação e permissões.

Documentar todos os eventos de segurança, sua investigação e as medidas tomadas, bem como todas as informações, procedimentos e históricos relevantes.

Todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da solução. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

Coordenar as ações de investigação e de comunicação, interna e externa, de forma centralizada.

A CONTRATADA deve dimensionar um quantitativo de no mínimo 400 (quatrocentas) horas anuais e cumulativas, dedicadas ao TRIBUNAL para tratar incidentes de severidade alta, intensivos e/ou complexos e crises, onde exigir ação altamente especializada e urgente, incluindo gestão de crises e investigação avançada e forense digital (DFIR), podendo ser realizadas presencial ou remotamente de acordo com a necessidade, quando as equipes remotas de monitoramento de ataque exauriram as possibilidades para a tratamento e resposta do incidente.

2.4.3. EQUIPE, PROCESSOS E ATIVIDADES DE GESTÃO DE EVENTOS, INCIDENTES E CRISES

A CONTRATADA deverá operar e acompanhar o ciclo completo de tratamento e resposta a eventos e incidentes cibernéticos e de gestão de crises cibernéticas, seguindo os processos definidos, conforme **Serviço de Governança e Conformidade de Segurança**, incluindo:

- Planejamento e preparação;
- Monitoramento, detecção e triagem contínuos de eventos;
- Caçada contínua a ameaças (Threat Hunting);
- Registro, análise, avaliação e investigação de incidentes;
- Resposta a incidentes, incluindo contenção, erradicação e recuperação;
- Gestão de crises;
- Avaliação e escalonamento de incidentes;
- Acompanhamento e orientação de ações;
- Documentação, geração de relatórios e consolidação de lições aprendidas.

A CONTRATADA deve implantar, operar e sustentar integralmente a solução informatizada para gerenciamento, análise, automação e resposta de informações, eventos e incidentes de segurança, de forma a tirar seu máximo proveito no tratamento e resposta a eventos e incidentes, contemplando minimamente as seguintes atividades:

- Planejar a implantação da solução;
- Verificar os pré-requisitos de instalação e compatibilidade da solução com o ambiente computacional on-premises e de nuvem do TRIBUNAL;
- Configurar as integrações da solução entre o ambiente da CONTRATADA e o ambiente do CONTRATANTE;
- Configurar a console de gerenciamento da solução;
- Criar e manter atualizadas as políticas e regras da solução, conforme as recomendações do fabricante e melhores práticas para o ambiente computacional da CONTRATANTE;
- Instalar, reinstalar e desinstalar os agentes/sensores e demais componentes da solução;
- Realizar Health Checks;
- Configurar alertas, dashboards e relatórios;
- Configurar, alterar e calibrar quaisquer funcionalidades da solução;
- Realizar troubleshooting em caso de problema;
- Atualizar a versão e aplicar patches e hotfixes da solução.

A CONTRATADA deverá dimensionar, alocar e manter equipe de tratamento e resposta a incidentes atuando em Nível 1 (atuação inicial), Nível 2 (atuação avançada) e Nível 3 (especialistas), organizada no mínimo em grupos distintos para:

- Monitoramento e detecção de eventos, incidentes e ataques;
- Caçada contínua a ameaças (*Threat Hunting*);
- Inteligência de ameaças (*Threat Intelligence);*

- Gestão de crises e investigação avançada de incidentes.

Avaliar se todos os ativos/datasources de logs e telemetria, para a adequada e correta geração e correlação de eventos, estão sendo gerados e enviados corretamente, observando se há ausências ou inadequações, e tomar as providencias necessárias, seja executando as adequações nos ativos de soluções introduzidas pela CONTRATADA ou, em caso de ativos cuja sustentação esteja fora do objeto contratado, solicitar, orientar (prestar apoio técnico e consultivo) e acompanhar a habilitação e configuração do ativo junto ao TRIBUNAL.

Assegurar a correta triagem e classificação inicial dos eventos e os respectivos tipos de ações decorrentes, bem como a identificação e minimização de falsos positivos.

Assegurar que todo evento seja registrado na solução informatizada e garantir a segurança da informação destes, independentemente de sua classificação e fase de tratamento.

Os times da CONTRATADA para segurança defensiva (*Blue Team*), ofensiva (*Red Team*) e mista (*Purple Team*) devem funcionar, interagir e atuar de maneira integrada, compartilhando conhecimento sobre táticas, técnicas e procedimentos de ataque, soluções para vulnerabilidades encontradas dentre outros, para que, por meio da atuação conjunta, aumente-se a efetividade da proteção do ambiente.

Para a caçada contínua a ameaças (*Threat Hunting*), a CONTRATADA, por meio de processos contínuos, estruturados e proativos, deve realizar, no mínimo, as seguintes atividades:

- Definir hipóteses de possibilidades de ameaças e de como encontrá-las, elaboradas utilizando como referência vetores de ameaças novos e ativos e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, indicadores de comprometimento (IoC) de casos relevantes, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e procedimentos (TTP), podendo ser utilizados Framework do MITRE ATT&CK, entre outros;
- Planejar e realizar a coleta dos eventos dentro das plataformas relevantes de acordo com cada hipótese definida;
- Avaliar a massa de eventos para buscar anomalias associadas à hipótese definida e registrar evidências encontradas;
- Caso sejam encontrados eventos maliciosos e/ou incidentes, incluí-los no processo de tratamento e resposta a incidentes de segurança.

Para o tratamento dos incidentes de segurança, a CONTRATADA deve, alinhado com o Processo de Tratamento de Incidentes, realizar as seguintes ações:

- Efetuar a resposta, investigação e encerramento dos incidentes de segurança, incluindo o acionamento do seu Nível 2 e, nos casos de incidentes massivos e de severidade alta, seus especialistas de Nível 3;
- Fazer a análise inicial dos incidentes confirmados e identificar os principais vetores de ataque e/ou exploração utilizados;
- Classificar os incidentes em níveis de severidade, priorizar e escalar conforme o processo vigente;
- Notificar o TRIBUNAL com os detalhes do incidente detectado e ativos de TIC envolvidos, de acordo com a severidade do incidente e a matriz de escalonamento no processo vigente;
- Elaborar, executar e manter atualizados os roteiros de investigação e os playbooks de resposta a incidentes com a devida aprovação final do TRIBUNAL;
- Automatizar playbooks por meio de ferramenta de orquestração e automação.;

- Prover a proposta de contenção, erradicação e recuperação, em articulação com as equipes do TRIBUNAL, executar os procedimentos sob sua responsabilidade com a devida autorização do TRIBUNAL e observado o processo de Gestão de Mudanças do TRIBUNAL, e controlar as ações, notificações e escalonamento dos incidentes, de acordo com os roteiros de resposta pré-definidos;
- Efetuar investigações relacionadas aos incidentes, com o objetivo de identificar a causa-raiz, coletar todas e quaisquer evidências e identificar os ativos de TIC afetados.

Uma vez instaurada crise cibernética e iniciado seu gerenciamento, cabe à CONTRATADA:

- Instaurar seu grupo de gestão de crises, incluindo nome, título, telefones, e-mail etc., além da sequência a ser seguida no acionamento dos profissionais;
- Definir notificações a serem enviadas aos envolvidos, compostas pelo iniciador, pessoas envolvidas (incluindo nome, telefone e e-mail) e a mensagem, mantendo um histórico de envio de notificações na solução informatizada;
- Ativar e acompanhar as atividades do Plano de Continuidade, quando existir, ou proposição de um plano de retorno à normalidade;
- Registrar a crise na solução informatizada e associá-la ao(s) incidente gerador;
- Criar e acompanhar eventos de crises, documentando as características fundamentais, como: sumário, status, categoria, data/horário de início e término, severidade, detalhes sobre o cenário;
- Identificar localização do evento de crise, impacto à infraestrutura, necessidade do envolvimento de departamento jurídico e/ou de seguro e estimativas de custos;
- Realizar análises pós-crises, a partir de questionários de avaliação dos procedimentos e gerenciamento de crise, identificando e documentando as lições aprendidas;
- Fornecer um dashboard específico para crises que permita visualizar e acompanhar indicadores, eventos e andamentos relevantes.

A CONTRATADA deve monitorar a atividade de ameaças e ocorrência de incidentes globais, através de feeds de inteligência de ameaças, identificados a partir de análises e pesquisas na DarkWeb e outras fontes de informação, de modo a antever eventuais ameaças e ataques ao TRIBUNAL e aprimorar os controles dos serviços contratados.

Ameaças e ataques direcionados ao mesmo segmento de atuação do TRIBUNAL devem ser imediatamente sinalizados para que seja tomada uma decisão em relação à atuação dos serviços contratados.

A CONTRATADA deve prestar, sob demanda e proativamente, apoio técnico e consultivo sobre assuntos correlatos ao ambiente de segurança cibernética do TRIBUNAL e monitoramento, detecção e resposta de incidentes e ataques, incluindo pareceres técnicos, recomendações, estudos e avaliações afins.

2.4.4. SOLUÇÃO INFORMATIZADA PARA GERENCIAMENTO, MONITORAMENTO, DETECÇÃO E RESPOSTA DE INFORMAÇÕES, EVENTOS E INCIDENTES DE SEGURANÇA

A CONTRATADA deve fornecer e adotar Solução Informatizada para Gerenciamento, Monitoramento, Detecção e Resposta de Informações, Eventos e Incidentes de Segurança e ataques, devendo ser projetada como uma plataforma completa e para atender funcionalidades de monitoramento, inspeção e análise, detecção contínua de ameaças e ataques, investigação e defesa cibernética.

A solução poderá ser ofertada em ambiente de nuvem, em appliance virtual ou appliance físico composto de hardware e software devidamente licenciado pela CONTRATADA. Quando necessário para o adequado funcionamento da solução, será admitida a instalação de coletores, agentes, conectores ou componentes auxiliares na infraestrutura do

CONTRATANTE, ficando sob responsabilidade exclusiva da CONTRATADA o seu fornecimento, implantação, configuração, sustentação e operação, sem qualquer ônus adicional.

Deve possuir arquitetura distribuída, com no mínimo as seguintes funcionalidades, módulos ou componentes nativamente integrados:

- Gerenciamento de informações e eventos de segurança (*Security Information and Event Management - SIEM*) de nova geração;
- Inteligência de ameaças (*Threat Intelligence Platform - TIP*);
    - A CONTRATADA deverá dispor de serviço de Threat Intelligence ou Inteligência de Ameaças (Threat Intelligence Platform - TIP), integrado diretamente ao SIEM, fornecendo Indicadores de Comprometimento (IOCs) e/ou feeds de inteligência provenientes de Inteligência Cibernética.
- Orquestração, automação e resposta (*Security Orchestration, Automation and Response - SOAR*);
- Análise de comportamento de usuários e entidades (*User and Entity Behavior Analytics - UEBA*);
- Detecção e Resposta de Rede (*Network Detection and Response - NDR*);
- Malware Sandbox.

Excepciona-se da obrigatoriedade de integração nativa, no parágrafo anterior, os componentes de Detecção e Resposta de Rede (NDR) e Malware Sandbox, os quais poderão ser providos por meio de integração via APIs (Application Programming Interface) ou conectores específicos homologados pelo fabricante, desde que assegurada a total interoperabilidade e a capacidade de resposta orquestrada e automatizada dentro da plataforma principal.

O gerenciamento de informações, eventos, alertas e incidentes deve possuir os seguintes recursos e capacidades:

- Ingestão de dados, coleta de registros (logs) e telemetria e geração de metadados;
- Indexação, agregação e enriquecimento dos metadados;
- Retenção de dados e metadados e armazenamento de eventos e registros processados;
- Correlacionamento, triagem e análises avançadas de eventos, alertas, detecção e tratamento de incidentes.

Durante toda a vigência da contratação, não deve existir para a solução ofertada limitação quanto a quantidade de consultas de usuário nem de consultas programáticas (queries) às informações, quantidade de parses no tratamento de eventos, quantidade de conectores para ingestão, quantidade de envio de registros por ativo e quantidade de casos de uso.

Ser extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período, preferencialmente adotando repositório em arquitetura “data lake”.

Ter recursos de segregação lógica multilocação ("*multitenancy*") em uma arquitetura adequada para funcionar em ambiente multilocatário (“*multitenant*”).

Ser dimensionada e licenciada para coletar, processar, correlacionar e armazenar eventos das fontes de dados do ambiente computacional on-premise e em nuvem do TRIBUNAL.

Coletar, interpretar, normalizar e correlacionar eventos de segurança em tempo real, provenientes de logs de diferentes fontes do ambiente computacional do TRIBUNAL, com o objetivo de detectar incidentes e permitir a ação imediata da equipe de resposta a incidentes.

Ser capaz de tratar, no mínimo, os seguintes formatos, protocolos e fontes:

- Syslog, Simple Network Management Protocol (SNMP);
- Microsoft Windows Event Log;
- Common Event Format - CEF, estruturado (ex: JSON, Regex etc.) ou não estruturado.

Deve permitir a retenção do histórico de segurança da CONTRATADA, contemplando, minimamente, os seguintes dados:

- Dados de eventos de segurança;
- Dados das aplicações;
- Dados dos sistemas operacionais;
- Dados das nuvens públicas e privadas;
- Dados do tráfego de rede;
- Tráfego de registro (syslog).

Ser capaz de coletar registros (logs) e informações de telemetria em serviços em nuvem pública de software (SaaS), plataforma (PaaS) e infraestrutura (IaaS), via integração por interfaces de programação (APIs), protocolos e agentes que sejam providos e homologados no mínimo pelos seguintes provedores:

- Amazon Web Services (AWS);
- Google Cloud Platform (GCP);
- Microsoft Azure, Oracle Cloud.

Ser capaz de inspecionar registros de plataformas de colaboração corporativa como Google Workspace e Microsoft/Office 365.

Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) e soluções de gestão de identidade.

Possuir API restful para integração com vários serviços para ingestão de registros, telemetria e tráfego para detecção e resposta a eventos de segurança.

Prover mecanismo de coleta de logs de dispositivos e fontes não suportados nativamente, por meio de personalização de coletores.

Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta.

Possuir mecanismos de compressão e controle de fluxo para a transmissão de dados entre os coletores e os servidores de gerenciamento, através de um dos componentes da solução (aplicação, sistema operacional, etc).

Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume de eventos.

Armazenar os alertas, incidentes e os eventos, inclusive os normalizados, de forma indexada.

Toda a comunicação entre os componentes deve ser criptografada.

Possuir política de retenção configurável para o tempo de armazenamento de eventos em formato bruto (raw), preservando evidências para fins de conformidade e eventuais ações forenses, com retenção de dados brutos pelo período mínimo de 30 (trinta) dias.

Reter os dados processados e metadados de eventos, como alertas e registro de incidentes gerados, em registros no banco de dados e/ou data lake da solução pelo período mínimo de 12 (doze) meses, salvo para consultas e pesquisas on-line, devendo, no mínimo, os últimos 30 (trinta) dias de registros serem armazenados a quente (hot-storage).

Proteger os registros contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada.

Permitir o expurgo dos dados de forma automática, com a personalização do prazo de expurgo, sendo que somente será permitida a exclusão de eventos conforme a política de retenção de dados definida, ou seja, todos os eventos mais antigos que extrapolem o tempo de retenção definido.

Permitir a correlação de eventos, devidamente estruturados em metadados.

Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas também deve ser capaz de criar analisadores personalizados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis.

Permitir filtrar e selecionar os eventos que serão inseridos na solução e a criação e alteração de filtros.

Tratar eventos e alertas em um fluxo de refinamento, através de categorização e priorização, análise crítica, investigação, enriquecimento de informações e análises, inteligência de ameaças (*Threat Intelligence*) incluindo fontes estratégicas (relatórios, bases de conhecimento, feeds, fóruns e comunidades abertas, da Deep Web e da Dark Web etc.), táticas (correlação com táticas, técnicas e procedimentos - TTPs) e operacionais (correlação com indicadores de comprometimento - IOCs), e validação, identificando atividades anômalas e, dentre essas, candidatos a incidentes.

Deve realizar análise comportamental de usuários e entidades (User and Entity Behavioral Analysis - UEBA) com aprendizado de máquina para detectar ameaças.

Deve ser capaz de detectar padrões de ataques, através da elaboração de baseline comportamental dos usuários e entidades.

Deve possuir técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal.

Deve possuir a capacidade de identificar anomalias nos comportamentos individuais dos usuários e entidades, tais como:

- Horário atípico do acesso;
- Número atípico de sessões de uso nos sistemas operacionais;
- Volume de conexões atípico;
- Volume de transferências de dados atípico;
- Localização geográfica atípica da origem do acesso;
- Endereço IP de origem atípico do acesso;
- Acesso atípico a dados armazenados;
- Criação e uso de processos (executáveis em memória) atípicos pelo usuário/entidade;
- Mudança na postura de risco do usuário/entidade.

Deve enriquecer os eventos em tempo real com o contexto do usuário e da entidade. Os dados enriquecidos devem fornecer atributos de contexto que podem ser usados para a elaboração de perfis de comportamento, comparações entre pares, pesquisas e investigações.

Implementar regras avançadas que conectem eventos sem correlação direta e gerem incidentes caso seja constatado algum desvio.

Possuir capacidade de contextualização, utilizando dados de diferentes origens (servidores, aplicações etc.) em uma única console, otimizando o processo de análise e resposta a incidentes.

Agregar eventos semelhantes que ocorrerem dentro de um limite de tempo ou quantidade de eventos específicos.

Possuir identificação autônoma de táticas, técnicas e procedimentos (TTPs) mapeando automaticamente com o *framework MITRE ATT&CK*.

Deve incluir capacidades de integração nativa com ferramentas de proteção, detecção e resposta de endpoints (*Endpoint Protection Platforms - EPP* e *Endpoint Detection and Response - EDR*), incluindo obrigatoriamente a atual do TRIBUNAL - Microsoft Defender.

Deve permitir modelagem de ameaças com a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco.

Deve possuir tecnologia para análise automatizada de artefatos maliciosos (“malware sandbox”) que minimamente contemple as funcionalidades a seguir:

- Analisar indicadores comportamentais de um artefato;
- Realizar análise estatística e dinâmica para validar se o artefato é malicioso ou não;
- Suportar a análise de artefatos BAT, CHM, DLL, EXE, ISO, HTA, JAR, JS, JSE, LNK, MSI, MHTML, documentos do Microsoft Office, PE32, PDF, VBE, VBS, WSF, XML, ZIP.

Permitir a caçada rápida de ameaças por meio da pesquisa em linguagem natural.

Deve ser eficaz na detecção de ameaças e ataques de Ransomware.

Deve ser capaz de detectar, no mínimo, as seguintes ameaças de identidade:

- Password spray;
- Brute force;
- Varredura de credenciais;
- Golden ticket;
- Pass-the-hash;
- Atividade não usual/atípica de usuário;
- Elevação de privilégios;
- Movimentação lateral.

Apresentar as informações sobre os eventos que compõem um alerta ou incidente identificado pelas regras de correlação da solução, referenciando tais eventos básicos a partir do evento alerta/incidente.

Possuir um sistema de alertas personalizável pelo administrador da solução, com a possibilidade de geração de alertas via dashboard automatizados ou e-mail quando um incidente for detectado.

Permitir a criação e o gerenciamento de detecção de ameaças e conformidade na forma de regras, análises, relatórios e dashboards.

Deve suportar controle de acesso baseado em função (RBAC) granular com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações.

Possuir workflow automatizado para a resposta e gerenciamento de incidentes, de modo que ações de criação, alteração, escalonamento, documentação e fechamento de incidentes possam ser realizadas automaticamente pela solução.

Prover acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redesenvolvimento.

Possuir funcionalidades de atualização, gerenciamento e configuração centralizadas de todos os agentes ou conectores distribuídos da solução.

Permitir a categorização manual de eventos inéditos não categorizados por padrão e sua aplicação em eventos futuros de mesma natureza.

Permitir pesquisas no histórico de eventos, fornecendo capacidade de visualizar os detalhes dos eventos (drill down), inclusive no formato bruto, quando aplicável, para análise forense e investigação de incidentes.

A partir de um evento ou conjunto de eventos, apresentar seus relacionamentos de forma gráfica e possibilitar fazer drill down para efetiva investigação e identificação de causa raiz.

Gerenciamento, análise, orquestração e automação de políticas, posturas, casos de uso, playbooks e integrações, com capacidade de resposta autônoma e aplicação próxima a tempo real, com componente de Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation and Response - SOAR), totalmente e nativamente integrado à solução, com o objetivo de automatizar os processos e fluxos de trabalho, a execução de atividades repetitivas ou de difícil execução e a orquestração das diversas ferramentas de segurança, com necessidade mínima de atuação humana.

Deve possuir integração nativa com os diversos ativos e recursos de infraestrutura e segurança de TIC e capacidade de integrar, consolidar, agregar e correlacionar também todas as informações oriundas de outras fontes de telemetria disponíveis.

Deve prover plataforma para gerenciamento e documentação de eventos/incidentes/casos de uso de ponta a ponta, automação de resposta a incidentes, investigação, automação de playbooks e repositório único de evidências.

Não deve ter restrições com limitações de licença sobre o número de casos, número de playbooks criados ou número de ações realizadas pelos usuários do sistema.

O recurso de gerenciamento de incidentes deve permitir a definição de um processo abrangente desde o registro e triagem inicial de um incidente até a sua resolução e prevenção, gerenciando eficazmente incidentes.

A CONTRATADA deverá promover a automação de processos e fluxos de trabalho em solução interativa, prática e de fácil implementação, sem a necessidade de customização ou alteração do código-fonte.

Os Dashboards (painéis), gráficos e relatórios, devem:

- Fornecer dashboards e relatórios pré-configurados e permitir a criação de dashboards e relatórios personalizados de forma flexível, ágil e intuitiva, incluindo gráficos como tipo pizza, linha, colunas, barras e tabelas dinâmicas, contemplando as diversas necessidades de visão gerencial;
- Possuir dashboards de monitoramento em tempo real e de dados históricos;

- Permitir a emissão de relatórios de forma tempestiva ou agendada, permitindo configurar o envio automático e agendado para grupos de usuários ou usuários específicos;
- Permitir a sobreposição e o cruzamento de informações, e agrupamentos por critérios comuns;
- Permitir ao usuário organizar os gráficos e informações, em seus painéis e dashboards, ajustando o layout e conteúdo do painel de acordo com suas necessidades.

Permitir que a partir de qualquer gráfico de gestão, contido em painéis e dashboards, o usuário possa, de forma gráfica e interativa:

- Clicar e listar os registros relacionados com os dados contidos no gráfico (drill down);
- Realizar alterações dinâmicas de atributos, como a alteração de eixos, título, legenda, escala, rótulos de dados, tamanho;
- Permitir o gerenciamento de permissões por usuários e grupos para acesso aos dashboards e relatórios e para compartilhamento;
- Permitir a geração de relatórios, impressão e exportação para arquivos em formatos como .csv e .pdf.

Permitir integração com a Solução Informatizada para Gestão de Vulnerabilidades, adquirida pelo TRIBUNAL.

Quanto ao mecanismo de detecção e resposta na rede (NDR):

- Ser capaz de analisar o tráfego TCP/UDP na rede da CONTRATANTE para detectar comportamentos e possíveis ameaças, gerando eventos de alerta de acordo com o tipo de tráfego;
- Ser capaz de produzir e coletar informações de telemetria em tempo real de tráfego de rede, tomando como base, no mínimo, as conexões de rede principais do data center do TRIBUNAL;
- Suportar a análise de no mínimo 08 (oito) Gbps de tráfego total devendo ser fornecidos equipamentos capazes de realizar espelhamento de tráfego (seja incluso em Appliance ou por meio de derivação de rede - Network Tap) com no mínimo duas interfaces fibra óptica de 10 (dez) Gbps cada, com especificações de SFP a serem oportunamente fornecidas pelo TRIBUNAL;
- Ser capaz de funcionar em modo de monitoramento, sem bloquear comunicações maliciosas de entrada ou saída;
- Ser capaz de inspecionar cada pacote individualmente e detectar e extrair adequadamente o protocolo e serviço, contornando de forma confiável eventuais medidas de evasão.

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

- Utilização da largura de banda;
- Tentativas de invasão e varreduras de IPs e portas;
- Autenticações recusadas ou com falhas;
- Análise de arquivos benignos e maliciosos e suas respectivas categorias;
- Ataques de negação de serviço;
- Conexões de comando e controle presentes, internamente ou para a Internet;
- Dispositivos que representam o maior risco;
- Tempos de resposta, tráfego de entrada e saída (inbytes/outbytes);
- Aplicações que consomem mais recursos de rede;
- Análise de DNS (tempos de resposta, comunicação, time-out, erros e desempenho);
- Identificação de aplicações da Camada 7;
- Principais eventos críticos de segurança;
- Monitoramento de certificado SSL;

- Ataques de adivinhação de credenciais (força bruta, password spraying).

Suportar o protocolo HTTP/2.

Ser capaz de detectar tráfego de rede potencialmente malicioso, como *ransomware*, movimentação lateral, consultas e conexões de comando e controle (C&C), mineração de criptomoedas (crypojacking), Mimikatz e outros, incluindo as que se aproveitam do tráfego RPC e SMB.

Ser capaz de exportar ou importar índices de dados em formato legível.

Ser capaz de ativar monitoramento personalizado e prover extensibilidade de detecção por meio de padrões abertos.

Ser capaz de identificar táticas e técnicas adversárias segundo o modelo MITRE ATT&CK.

2.4.5. PROTEÇÃO CONTRA RISCOS DIGITAIS (THREAT INTELLIGENCE)

A CONTRATADA deve realizar **Proteção contra Riscos Digitais (Threat Intelligence)** com o monitoramento da marca e da reputação institucional na Internet, na Deep Web e na Dark Web, incluindo redes sociais, serviços de comunicação, repositórios de informação e lojas de aplicativos, identificando fraudes e golpes, conteúdo malicioso, vazamentos de dados e ameaças externas globais e com foco em Brasil, Governo e Judiciário, e providenciar Takedown em nome do TRIBUNAL mediante procuração e autorização.

O objeto de monitoramento deve incluir, no mínimo:

- **Marca**: Tribunal de Justiça do Estado do Paraná, Tribunal de Justiça do Paraná, Poder Judiciário do Paraná, TJPR, TJ-PR, TJ/PR;
- **Domínios:** tjpr.jus.br, tjpr.net, incluindo subdomínios (www, projudi, sei, mail, webmail, entre outros);
- **Perfis:** Conforme lista de perfis oficiais do TJPR, conforme **Tabela - Perfis oficiais de redes sociais do TRIBUNAL.**

As fontes de monitoramento devem incluir, no mínimo:

- Sites e serviços na internet (aberta ou superficial), na deep web (internet profunda) e na dark web (internet obscura);
- Registros de domínios nacionais e internacionais, incluindo TLDs e gTLDs;
- Perfis e comunidades em redes sociais e plataformas de mídias sociais, contemplando no mínimo Facebook, Instagram, Twitter, YouTube e LinkedIn, e desejável também Flickr;
- Grupos, canais e comunidades em serviços de comunicação por mensagens e fóruns, contemplando no mínimo Telegram e Discord, e desejável também WhatsApp;
- Repositórios e serviços de conteúdo e informação de grande abrangência, como Github e Gitlab;
- Lojas de aplicativos (catálogo ou repositório de distribuição de software instalável para determinada plataforma de sistema operacional), contemplando no mínimo Google Play (Android), Apple App Store (iOS/iPadOS) e Microsoft Store (Windows), e desejável também Samsung Galaxy Store (Android) e F-Droid (Android).

O monitoramento deve abranger conteúdo e informações em texto, mídias de imagem, áudio e vídeo, incluindo o reconhecimento e análise de texto em arquivos e bases de dados, e desejável, também, em imagens (Optical Character Recognition - OCR).

O serviço deve identificar, no mínimo:

- Fraudes, phishing e outros tipos de golpes, conteúdo malicioso e ameaças relacionadas;
- Réplicas, conteúdos ilegítimos, abusos e violações aos serviços utilizando nome, marca e/ou logomarca institucionais do TRIBUNAL;
- Typosquatting (variações de nome, permutações de caracteres e outras variantes visando erros comuns de digitação) e variações ilegítimas ou maliciosas de domínio, certificado SSL/TLS, marca institucional e outros nomes objeto do monitoramento;
- Vazamento de dados, credenciais e informações de segurança e institucionais sensíveis e confidenciais;
- Violação de direitos de uso do TRIBUNAL ou a tentativa de burlar os meios de proteção desses direitos.

Em caso de suspeita ou identificação de ocorrências monitoradas, a CONTRATADA deve realizar no mínimo as seguintes atividades:

- Registrar e gerenciar o incidente em todo o seu ciclo de vida;
- Notificar e emitir alertas, bem como confirmar eventuais suspeitas junto ao TRIBUNAL;
- Comunicar a obrigação de Takedown (desativação administrativa e retirada do ar) do objeto do incidente aos administradores do seu anfitrião (host);
- Acompanhar o andamento e efetivação do Takedown;
- Analisar e investigar a rastreabilidade da ocorrência, visando identificar informações relevantes como autoria, linha do tempo, técnicas, meios e caminho de obtenção, exfiltração, propagação e veiculação;
- Elaborar e apresentar relatórios de andamento e análise;
- Monitorar a possibilidade de reincidência da ocorrência por, no mínimo, 30 (trinta) dias corridos a partir da efetivação do Takedown;
- Tomar providências cabíveis em seu âmbito de atuação visando garantir a eficácia do Takedown, incluindo reiterar e obter esclarecimentos junto aos administradores do anfitrião;
- Subsidiar informações ao TRIBUNAL para a criação e melhoria de controles de segurança aplicáveis para evitar ocorrências similares futuras.

Orientar a equipe do TRIBUNAL sobre eventuais ações complementares cabíveis.

2.5. SUSTENTAÇÃO DE OPERAÇÕES DE SOLUÇÕES E RESPOSTA A REQUISIÇÕES DE SEGURANÇA

A CONTRATADA será responsável pela Sustentação de Operações e Resposta a Requisições de Segurança, operação, suporte técnico, monitoramento, melhoria contínua dos ativos tecnológicos de segurança do TRIBUNAL especificadas no "**ANEXO IV - ESTIMATIVAS DE ATIVOS PARA DIMENSIONAMENTO DOS SERVIÇOS**", bem como reduzir ou mitigar riscos, custos e impactos de eventuais incidentes de segurança na área de tecnologia da informação de forma a garantir os três pilares da segurança - CID (confidencialidade, integridade, disponibilidade).

A CONTRATADA será responsável pelo gerenciamento, sustentação, operação, monitoramento, melhoria contínua das soluções informatizadas ou produtos contratados como serviços e fornecidas pelas CONTRATADA.

Monitorar o ambiente 24x7x365, quanto à disponibilidade e desempenho dos equipamentos que compõe a solução a ser gerenciada.

A CONTRATADA deverá empregar especialistas com experiência comprovada na gestão de ferramentas de segurança especificadas e em práticas de segurança cibernética.

A CONTRATADA será responsável pelo monitoramento contínuo do desempenho e da capacidade das soluções de segurança, identificando proativamente quaisquer questões que possam impactar a eficiência ou a segurança dos sistemas e serviços providos pela Secretaria de Tecnologia da Informação (SETI).

Fazer a gestão dos incidentes (criação de alertas, detecção e abertura de chamados).

Acompanhamento completo dos incidentes de segurança, performance e disponibilidade.

Realizar a monitoração de performance e disponibilidade dos ativos.

Realizar o acionamento por matriz de escalação hierárquica e funcional, para eventos de segurança, performance e disponibilidade.

Faz parte da prestação o gerenciamento dos serviços de manutenção preventiva e corretiva das soluções de segurança (equipamentos, ferramentas, softwares etc.) nos quais a CONTRATADA gerencia, administra e sustenta.

Quanto ao suporte especializado a CONTRATADA deve:

- Permitir a abertura, acompanhamento e validação de chamados através de e-mail, web site (portal do cliente) e telefone (0800) no regime 24x7x365 com atendimento em português do Brasil;
- Possuir processo de escalação funcional, mapeamento e documentado, com os seguintes níveis de atendimento: N1, N2 e N3, conforme melhores práticas descritas pelo ITIL;
- Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos;
- Possuir análise técnica documentada pelo N3 do SOC antes do envolvimento dos fabricantes, a fim de garantir o processo de escalação funcional;
- Possuir os processos de gerenciamento de incidente, requisição, eventos, problemas, mudanças, incidentes críticos, documentados de acordo com as melhores práticas descritas pelo ITIL.

Os administradores de soluções do CONTRATANTE terão total acesso à plataforma para fins de auditoria, porém a responsabilidade pela operação diária da solução será da CONTRATADA.

Cabe a CONTRATADA realizar de forma proativa as ações necessárias para manter o ambiente de segurança da CONTRATANTE adequado às melhores práticas do mercado, devendo:

- Atualizar os firmwares e/ou softwares das soluções que compõe a solução e das respectivas consoles de gerenciamento;
- Documentar as soluções informatizadas, contendo matriz de responsabilidades;
- Elaborar relatório de Health Check;
- Fortalecer a postura de segurança do CONTRATANTE.

Propor ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes, as mantendo documentadas, devendo:

- Sugerir tais ajustes e melhorias nas tecnologias de segurança sob operação da CONTRATANTE;
- Após aprovação da CONTRATANTE, executar tais ajustes e melhorias nas soluções entregues como parte do objeto deste edital, as mantendo documentadas e acessíveis no portal do cliente.

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.

Manter uma rotina mensal de análise de indicadores internos e pesquisa de mercado com o objetivo de apresentar à CONTRATANTE um relatório com as inovações tecnológicas e solução que possam aumentar a qualidade e o grau de maturidade da segurança da informação do ambiente tecnológico.

Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TIC.

Monitorar permanentemente e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE.

Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades.

Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração.

Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços.

Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação e cibernética.

Monitorar e propor soluções aos projetos/atividades em andamento otimizando-os quanto aos requisitos de Segurança da Informação.

Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento.

Participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede.

Elaborar relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, destinados à segurança da informação.

Seguir o processo de mudança estabelecido pelo CONTRATANTE. Sempre que solicitado, a CONTRATADA deverá estar disponível a participar das reuniões para prestar informações sobre os ambientes e serviços por elas executados. Mudanças que impliquem em um conjunto de procedimentos complexos, que envolvam várias equipes ou empresas contratadas e que implicarem em riscos de paralisação de quaisquer serviços considerados prioritários, deverão ser tratadas como um Projeto.

A CONTRATADA deverá apresentar proposta de todas as mudanças no ambiente, conforme níveis de controle estabelecidos. Para todas as mudanças apresentadas, será necessário acompanhar dentre outras informações, as análises de risco relativas às mudanças, descrevendo o impacto da sua realização.

Monitorar permanente e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média de acessos e identificando comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços.

Agendar e realizar as manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), fora do horário regular, salvo quando expressamente autorizado:

- As manutenções programadas, que impliquem em extensiva parada do ambiente serão realizadas, conforme autorização do TRIBUNAL. Tais atividades realizadas fora do horário regular não ensejarão

qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos;

- A todos os serviços de manutenção corretiva e preventiva que são considerados de natureza contínua e que devam ser minimizadas a sua necessidade de parada em ambiente de produção;
- Testar todos os serviços após a realização de manutenções preventivas e/ou corretivas, ficando sua aceitação final dependente da área demandante e/ou de fiscalização do CONTRATANTE, que avaliará as características esperadas para o serviço.

Elaborar e manter atualizados os Planos de Capacidade, de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres para os serviços objeto deste Termo.

Fornecer ao CONTRATANTE acesso à console dos produtos ofertados para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente.

Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos.

Priorizar os atendimentos críticos, conforme definição da CONTRATANTE.

Reagir aos eventos de segurança da informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE.

Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TIC.

Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados.

Elaborar e propor plano de execução dos serviços.

Organizar a alocação de turnos e de profissionais de sua equipe.

Definir plano de treinamento inicial e contínuo dos profissionais que executam os serviços.

Executar outros serviços correlatos à supervisão dos profissionais na execução dos Serviços Gerenciados de Segurança.

Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer.

Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação do TRIBUNAL, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas.

Receber as demandas dos serviços relativas à área de segurança da informação e providenciar a execução e alocação de recursos de trabalho.

Supervisionar sua equipe de profissionais na execução das ações conjuntas com a área de infraestrutura, cumprindo a política de segurança da informação do TRIBUNAL e aplicando as melhores práticas de segurança.

Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TIC.

Realizar as atividades em observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE.

Apoiar na análise e definição das regras de uso dos recursos computacionais do CONTRATANTE.

Implantar e configurar regras de firewall, IDS, IPS, antivírus, Antispam, proteção de identidade.

Realizar análise de tentativas de invasão a sistemas e equipamentos.

Propor processos e procedimentos de Segurança da Informação.

Monitorar e analisar os logs dos serviços de segurança (equipamentos, sistemas operacionais de servidores e clientes, conexões, programas utilizados etc.), propondo ações corretivas e de melhorias.

Executar periodicamente testes de alta disponibilidade na infraestrutura do CONTRATANTE com o objetivo de validar o seu funcionamento.

Apoiar o CONTRATANTE em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura.

Realizar a configuração das ferramentas que compõem as soluções, a fim de garantir o uso eficiente delas.

Acionar o fabricante das ferramentas sempre que necessário, sem nenhum custo adicional para o CONTRATANTE.

Emitir e customizar relatórios das soluções gerenciadas.

2.6. GESTÃO DE VULNERABILIDADES E TESTES DE SEGURANÇA

2.6.1. GERENCIAMENTO CONTINUO DE VULNERABILIDADES

Um serviço de Gerenciamento Contínuo de Vulnerabilidades remoto e terá como objetivo principal a análise do ambiente da CONTRATANTE quanto a segurança da informação para identificar, mapear, documentar, controlar e reportar possíveis vulnerabilidades em seus sistemas, serviços e ativos de infraestrutura tecnológica, bem como apresentar recomendações de melhorias e/ou correções das vulnerabilidades identificadas durante os testes.

Fazem parte do processo de gestão de vulnerabilidades as fases de Varredura de vulnerabilidades, Alerta de Vulnerabilidades, Priorização da Vulnerabilidades e Controle das vulnerabilidades (nos equipamentos fornecidos pela CONTRATADA e fornecimento do plano de remediação nos demais equipamentos do ambiente). Estas fases devem atuar de forma integrada com o objetivo de proverem informações suficientes para uma proteção mais eficaz do ambiente da CONTRATADA.

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

Os testes devem acontecer mediante alinhamento com a CONTRATANTE, com anuência da área técnica responsável pela sustentação em produção do sistema ou ativo.

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

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

Deverá ser realizada, com periodicidade mínima semanal, uma varredura interna de vulnerabilidades.

Deverá ser considerado um total de 2.000 ativos para o monitoramento de vulnerabilidades, sendo 1.800 para IPs e 200 para FQDNs.

As varreduras de vulnerabilidades deverão considerar até 2.000 endereços IPs e definidos pela CONTRATANTE, devendo considerar as seguintes etapas:

- Levantamento de todos os ativos da infraestrutura de TIC que deverão ser alvo da varredura. Para cada ativo, deverão ser levantados além das informações básicas, as informações de criticidade do ativo no ambiente, a matriz de responsáveis e as informações das janelas de manutenção e mudanças;
- Execução da varredura de vulnerabilidades;
- Análise dos resultados e priorização das vulnerabilidades;
- Elaboração e entrega de um Plano de Remediação considerando a criticidade da vulnerabilidade identificada e, também, os critérios definidos na fase de Levantamento de Ativos;
- Para toda vulnerabilidade encontrada, a CONTRATADA deverá descrever as ações para correção. Caso precise ter acesso as configurações dos ativos de tecnologia, a CONTRATADA deverá justificar a necessidade, ficando a cargo do CONTRATANTE decidir pela liberação;
- Para realização das varreduras de vulnerabilidades deve ser utilizada a ferramenta de propriedade da CONTRATANTE.

Gestão contínua de vulnerabilidades e de exposição a ameaças de forma proativa e recorrente, baseada na identificação, avaliação, categorização, priorização, tratamento e análise crítica de vulnerabilidades e riscos de segurança de ativos corporativos de TIC, gerenciamento e análise de exposição a ameaças e da superfície de ataque interna e externa, com utilização de ferramenta especializada;

A CONTRATADA deve realizar de forma continuada o processo de gestão de vulnerabilidades e de exposição a ameaças, baseada em riscos e em priorização, com a realização de varreduras, análises e remediações periódicas, utilizando solução/ferramenta(s) especializada indicada pelo TRIBUNAL.

O processo de gestão contínua de vulnerabilidades deve ser definido e revisado no contexto dos serviços de governança e gestão de cibersegurança, contemplando no mínimo as seguintes atividades a serem executadas pela CONTRATADA:

- Planejamento de ciclos e escopos;
- Identificação, avaliação e atualização do ambiente computacional, ativos e recursos do TRIBUNAL, mantendo uma base de dados de dispositivos, dos softwares neles instalados e da priorização quando da remediação;
- Execução de varreduras de descoberta, identificação e conformidade;
- Identificação e mapeamento de vulnerabilidades de segurança em ativos e recursos;
- Identificação, análise e recomendação de correções e, na impossibilidade destas, de medidas de contorno;
- Sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades e aplicação das melhores práticas de segurança;
- Trabalhar integrado com o SOC, sugerindo a ativação ou alteração de regras quando surgirem novas vulnerabilidades no ambiente do TRIBUNAL;
- Seguir as normas ISO/ABNT relativas à segurança da informação cabíveis;
- Fornecer lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

- Executar a análise de vulnerabilidades de forma a abranger novos equipamentos e aplicações instaladas;
- Apontar necessidade de atualização de controles, salvaguardas e indicadores no âmbito dos serviços de governança e gestão de cibersegurança.

Devem ser realizadas varreduras automatizadas de vulnerabilidade completas em ativos corporativos internos e externos, em ciclos completos com periodicidade mínima trimestral e repetição das varreduras após aplicação de atualizações, patches e outras remediações e salvaguardas.

Após um período de calibração e ajustes, as varreduras automatizadas por agentes e da rede externa devem objetivar a periodicidade mínima semanal, e as varreduras da rede interna devem objetivar a periodicidade mínima mensal, levando em consideração os ciclos de gestão de patches e atualizações e impactos no desempenho, disponibilidade e tráfego dos ativos.

Acompanhamento de alertas de segurança, atualizações de segurança, referenciais de vulnerabilidades e melhores práticas de higienização de segurança e de hardening para ativos de TIC, incluindo, mas não se limitando a:

- CIS Benchmarks;
- NIST Official Common Platform Enumeration (CPE);
- MITRE Common Weakness Enumeration (CWE);
- OWASP Top 10.

Repositórios e centros de segurança dos principais fornecedores/fabricantes de tecnologia aplicáveis aos ativos de TIC do TRIBUNAL, contemplando no mínimo:

- Microsoft;
- Oracle;
- Google;
- Red Hat;
- Dell/EMC;
- HP/Aruba;
- Palo Alto Networks;
- VMware;
- Broadcom/Symantec;
- Trend Micro;
- Cisco;
- Tenable.

A CONTRATADA deve sustentar, administrar e operacionalizar integralmente a solução da Tenable, licenciada pelo TRIBUNAL para 2.000 ativos, sendo 1.800 IPs e 200 licenças de FQDN, incluindo minimamente:

- Detecção e identificação de ativos;
- Realização de scans;
- Atualização de base de vulnerabilidades;
- Realização de configurações e melhorias;
- Interação com os fabricantes das soluções;
- Backup e restore;
- Resolução de problemas;
- Suporte proativo e corretivo;

- Instalação de serviços adicionais;
- Atualização, de acordo com as recomendações do fabricante.

A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o modelo da mesma.

2.6.2. TESTES DE SEGURANÇA AUTOMATIZADOS (BAS)

Implantação, planejamento, execução, análise e relatório de **Testes de Segurança Automatizados (BAS)**, repetíveis e continuados de segurança com ferramenta de simulação de violações e ataques (*breach and attack simulation - BAS*), visando:

- Avaliar e validar a eficácia operacional dos controles de segurança e identificar as lacunas na cadeia e postura de segurança;
- Avaliar e validar se as fontes de registros e telemetria e as regras de monitoramento, detecção e resposta estão sendo capturadas pela ferramenta de monitoramento, buscando também reduzir falsos positivos e negativos;
- Executar simulações de ataque que compõem hipóteses a serem validadas no processo de caçada contínua de ameaças e gerar registros (logs) e evidências para a busca nas ferramentas envolvidas no processo.

A CONTRATADA deve, de forma continuada e periódica:

- Identificar e entender os ativos-alvo mais críticos e representativos para aplicação dos testes de segurança automatizados;
- Criar e configurar os casos de uso, processos, ciclos e cobertura de testes;
- Administrar e monitorar a execução dos testes, analisar e reportar os resultados e recomendações decorrentes.

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

- Devem ser realizadas mensalmente no mínimo 30 (trinta) execuções de baterias de simulações em ativos do TRIBUNAL.
- Criar e melhorar painéis (dashboards) e relatórios personalizados para apresentar resultados objetivos e abrangentes.

2.6.2.1. SOLUÇÃO INFORMATIZADA DE SIMULAÇÃO DE VIOLAÇÕES E ATAQUES

Fornecimento e sustentação de solução informatizada de Simulação de violações e ataques (Breach and Attack Simulation - BAS), composta por agentes (softwares) ou atores (simuladores virtuais), conforme exigências descritas neste documento.

A solução poderá ser ofertada em ambiente de nuvem, em appliance virtual (para a plataforma VMware poderá ser alocado na infraestrutura da CONTRATANTE) ou appliance físico composto de hardware e software devidamente licenciado pela CONTRATADA.

Os itens que compõem a Solução de BAS e seu sistema de gerenciamento devem ser produzidos pelo mesmo fabricante.

Não serão aceitas ferramentas gratuitas, desenvolvidas pela, ou para, própria LICITANTE e/ou baseadas em softwares projetados para uso genérico, devendo estas serem providas por fabricantes amplamente consolidados no mercado.

Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado, adotando como referência de mercado estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC, ISG Group.

A solução deve contemplar a versão de software e/ou firmware mais estável e recomendado pelo fabricante.

O fabricante deve possuir rede de inteligência (threat inteligence) própria da solução para atualização constante de ameaças (threat feed) de forma automática.

Deve ser capaz de realizar baterias de testes de simulação de ataques baseados em bibliotecas atualizadas de ameaças e exploits, com execução imediata ou agendamentos, abrangendo infiltração de rede e aplicações web, ambos com o fluxo de ator malicioso externo para ativo-alvo interno, e endpoint, com comprometimento e exfiltração em ativo-alvo interno, estação de trabalho ou servidor, cobrindo no mínimo o sistema operacional Microsoft Windows.

As simulações devem garantir ambiente controlado e sem impacto nocivo real, ou seja, não deverá trazer qualquer risco real de infectar a rede do TRIBUNAL em suas atividades.

Os resultados devem validar e indicar controles de prevenção e proteção ineficazes e/ou suplantados, vulnerabilidades exploradas, caminhos de ataque e TTPs (táticas, técnicas e procedimentos) envolvidos de acordo com o framework MITRE ATT&CK.

Permitir o gerenciamento centralizado da ferramenta, por meio de interface gráfica (GUI), nos formatos web segura (https) ou em formato de aplicativo cliente compatível com Windows 10 e superior, podendo ser em nuvem (cloud), appliance virtual ou por meio da própria solução.

A solução deve possuir agentes (softwares) que possam ser instalados em máquinas, ou em ambientes virtuais (servidores), confeccionadas para simulação de ataques, ou apresentar atores (simuladores) virtuais, podendo ser arquivos em formato Open Virtualization Appliance (OVA), com a capacidade de criar um local próprio capaz de permitir a reprodução de ataques, além disso:

- Os agentes devem ser compatíveis com sistemas operacionais Linux e Windows (Server e Professional);
- Possibilitar a instalação de agentes ou máquinas OVA/ISO em ambientes de nuvem (cloud);
- Permitir que os agentes possam ser removidos (desinstalados) de uma máquina ou ambiente e instalados em outro local reaproveitando uma mesma licença.

Ser capaz de criar contas de usuários de forma local ou a autenticação e autorização de usuários por meio dos protocolos TACACS ou LDAP ou AD (Active Directory) ou mecanismos de autenticação e autorização utilizando credenciais corporativas no modelo de federação, usando o protocolo SAML.

Ser capaz de simular ataques e validar as capacidades de prevenção e detecção para invasões em rede, gateways de web e e-mail, web application firewall (WAF), endpoints (EPP/EDR, antivírus) e Microsoft Active Directory, simular ataques em toda a cadeia de destruição cibernética (Cyber Kill Chain), incluindo infiltração, movimento lateral e exfiltração de dados, phishing, ransomwares, violações de segurança e ataques persistentes avançados (APTs).

O portfólio de ameaças e ataques da solução deve ser baseado em frameworks de segurança cibernética, tais como MITRE ATT&CK, OWASP, CVSS ou NIST, e abranger todo o ciclo de ataque.

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

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

Permitir a criação de novas simulações de ataques e a customização destas a partir dos existentes em sua base de ameaças, de forma a permitir adaptações no comportamento e na ação dos ataques.

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

Possuir a instrumentação de indicadores de comprometimento (IOCs) provenientes de provedores de Threat Intelligence e/ou laboratório de inteligência de ameaça do fabricante da solução.

Disponibilizar APIs (interfaces de programação de aplicações) que permitam sua integração com demais soluções de segurança do TRIBUNAL.

Possuir integração com solução de monitoramento, detecção e resposta.

Possuir dashboard com visualização dos resultados das simulações que retratem o nível de risco para cada fase da “Cyber Kill Chain”, baseado no MITRE ATT&CK com a possibilidade de customizar as visões apresentadas.

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

Possuir visualização por no mínimo:

- Tipo de ataque simulado;
- O que o artefato executou;
- Data em que a simulação do ataque aconteceu;
- Taxa de penetração.

Permitir a realização de backup ou a opção de recuperação da solução, em caso de desastre, para no mínimo as configurações da solução de BAS.

Podendo ser funcionalidade não disponível para o cliente, realizado sob demanda junto ao fabricante.

Possuir registros que identifiquem o histórico completo de acessos (logins) e ações, por cada usuário ou grupo de usuários, incluindo as contas administrativas e com privilégios, podendo ser apresentado por meio de relatórios ou através de APIs ou scripts.

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

Permitir exportar relatórios para formatos PDF e CSV.

Apresentar relatório detalhando a ação do ataque simulado.

Possuir capacidade de entregar relatório ou disponibilizar por meio de interface gráfica informações da sequência de execução do artefato malicioso, baseado na matriz do MITRE ATT&CK, bem como detalhar as alterações na máquina local e conexões externas executadas durante a simulação.

Permitir exportar os logs da solução BAS, via API ou conectores, para a solução de SIEM.

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

Possuir base ampla de recomendação de remediação possibilitando visualizar ações de correção, redução do impacto da vulnerabilidade/ataque e prevenção alinhados com as recomendações específicas dos fabricantes de elementos de segurança.

A solução deve possuir atualização diária da base de malwares.

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

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

Possuir as seguintes opções para o formato do registro da hora dos eventos gerados com a integração do EDR: ISO 8601, UTC segundos, UTC milisegundos e UTC nanosegundos.

Permitir customização de simulação de campanhas de ameaças, utilizando no mínimo os seguintes IOCs: hash de arquivos, nome do host, URLs e endereços IPv4.

2.7. GESTÃO DE IDENTIDADE

2.7.1. GERENCIAMENTO DE ACESSO PRIVILEGIADO (PAM)

Tem por finalidade fornecer serviço de Gerenciamento de Acesso Privilegiado (PAM) de forma centralizada para controle dos acessos de contas privilegiadas e genéricas, promovendo a rastreabilidade dos responsáveis por ações executadas com essas credenciais. Deve incluir ainda o monitoramento do período em que uma conta está sob posse de um usuário, a disponibilização de senhas temporárias e o registro detalhado de todas as atividades realizadas durante o uso da conta. Essa abordagem visa a preservar evidências, assegurando a rastreabilidade das ações executadas e prevenindo acessos não autorizados a sistemas e servidores críticos para o negócio.

Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado, adotando como referência de mercado estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC e ISG Group.

Como parte integrante desse serviço, deve ser contemplada a solução informatizada de PAM licenciada para 80 (oitenta) usuários administrativos, independentemente da quantidade de credenciais que serão gerenciadas.

A CONTRATADA deverá realizar todas as operações de implantação, administração, gerenciamento e monitoração da solução de Serviço de PAM fornecida, incluindo, mas não se limitando a:

- Realização de configurações;
- Interação com os fabricantes das soluções;
- Backup e restore;
- Resolução de problemas;
- Suporte;
- Instalação de serviços adicionais e melhoria contínua;
- Atualização, de acordo com as recomendações do fabricante, e licenças a serem disponibilizadas pela CONTRATADA.

A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o modelo da mesma.

A CONTRATADA documentará a configuração do sistema PAM fornecido, e será a única responsável pela manutenção e atualização do mesmo, até o final do contrato.

A solução deverá possibilitar a proteção e gerenciamento de usuários administrativos que possuem acessos privilegiados na infraestrutura de TIC do Tribunal de Justiça do Estado do Paraná.

A solução não deverá possuir EOL (*End-of-life)* e EOS (*End-of-support*) anunciados para um prazo superior a 36 meses.

Cada pacote de software ofertado deve ser instalado em sua última versão estável e estar coberto por contrato de suporte e atualização de versão pelo fabricante durante a vigência do contrato.

A solução poderá ser ofertada em ambiente de nuvem, em appliance virtual (para a plataforma VMware poderá ser alocado na infraestrutura da CONTRATANTE) ou appliance físico composto de hardware e software devidamente licenciado pela CONTRATADA.

Empregando recurso de appliance físico, estes deverão estar dimensionado de forma a atender esta demanda de retenção de logs solicitada.

Caso o banco de dados e/ou sistema operacional, utilizado pela solução, seja de terceiros, a solução deverá ser entregue com licenças de software e garantia que a compatibilize com a solução.

A solução não deve utilizar ferramentas de terceiros para completar a solução excetuando-se a camada de sistema operacional e banco de dados.

A solução deve possuir ferramenta de monitoração própria para que seja possível especificar limiares (thresholds) referente ao uso de memória, CPU, disco e banco de dados, e demais interações por meio do protocolo proprietário ou aberto (SNMP).

Independente do modelo adotado, será necessário proporcionar uma retenção dos logs de até 180 dias, com gravações na ordem de 8 horas/dia, 5 dias por semana, no mínimo.

A solução deve apoiar, no mínimo, os requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como:

- Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento;
- Proteger o acesso a dados pessoais sensíveis;
- Responsabilizar pessoal e responder a incidentes;
- Aplicar boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados.

Apoiando os requisitos da LGPD, a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a

sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas-alvo diversos do ambiente.

A solução deverá monitorar sessões, gravar, detectar, correlacionar e mitigar todos os comportamentos anormais de, pelo menos, 80 (oitenta) usuários administrativos simultâneos, acessando todos os sistemas-alvo do ambiente tecnológico, dentre eles Servidores Linux/Unix e Windows, banco de dados, appliances e demais ativos de rede e sistemas computacionais diversos.

A solução deve atender, no mínimo, os sistemas-alvo baseados nas seguintes tecnologias:

- Sistemas Operacionais Linux/Unix e Microsoft Windows;
- Microsoft Hyper-V e VMWare;
- Contas de usuários de sistemas e de serviço;
- Credenciais do Microsoft COM+, IIS;
- Apache TomCat, RedHat Jboss, Wildfly, Nginx;
- Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP;
- Contas de usuários e administradores de bancos de dados Microsoft SQL Server, PostgreSQL, MySQL;
- Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) - switches, roteadores, balanceadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage);
- Contas de usuários e administradores de consoles de gerenciamento de servidores;
- Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo;
- Credenciais de nuvem em VMWare ESXi, Azure, AWS, GCP e Microsoft 365.

A solução deverá realizar a gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, com monitoramento e gravação de sessões privilegiadas.

A solução deverá conceder acesso aos sistemas utilizando “Remote Desktop” e “SSH”, disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no S.O. do servidor de destino, possibilitando habilitar gravação da sessão, caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino.

A solução deve permitir integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando, no mínimo, as seguintes funcionalidades:

- Integração e gestão de acessos privilegiados em contas de serviços em nuvem;
- Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem.

A solução deve possuir as sessões administrativas acessadas e monitoradas em tempo real, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação

de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada e possibilitando pesquisar ações específicas na sessão gravada.

A solução deve proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios.

A solução deve ser capaz de descobrir e alterar credenciais Microsoft Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, exibindo em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento.

A solução deve gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado.

A solução deve possuir funcionalidades de “AD Bridge” para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD.

A solução deve provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente.

A solução deve permitir a definição de Fluxos de Aprovação (*Workflows*) para obtenção de acesso às Contas Privilegiadas, com as seguintes características:

- Permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável;
- Permitir a aprovação perante um agendamento de ações administrativas.

Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução.

Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas.

A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP.

A solução deve oferecer em sua console de gerenciamento diferentes visões e opções de acordo com as permissões dos usuários.

A solução deve suportar métodos para registrar e relatar qualquer ação realizada, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail e integração com SIEM.

Permitir o envio automático de logs para servidores syslog, de forma aderente ao disposto em RFC 5424 - The Syslog Protocol (IETF).

A solução deve registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkouts, mudanças de delegação, relatórios e outras atividades, incluindo:

- Registros de acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas;
- Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários;
- Alterações nas funções de delegação;
- Adições, deleções e alterações de senhas gerenciadas pela solução;
- Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas;
- Relatórios filtrados por período, tipo de operação, sistema, gerente e outros critérios.

A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como:

- Lista de sistemas gerenciados;
- Senhas armazenadas/Contas gerenciadas;
- Eventos de alteração de senha;
- Permissões de acesso web;
- Auditoria de contas, sistemas e usuários.

A solução deve realizar análise comportamental e mitigação de risco no ambiente crítico para Identidades Privilegiadas.

A solução deverá realizar a identificação e o correlacionamento de ações, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros) do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução.

A solução deve identificar e combinar ações que caracterizam abusos, montando perfis de comportamento anormal e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas, tais como, nova autenticação, suspensão e encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo:

- Acesso privilegiado à solução durante dias/horários irregulares. Detectado quando um usuário recuperar uma senha de conta privilegiada em um dia/horário irregular de acordo com seu perfil comportamental;
- Acesso excessivo a contas privilegiadas. Detectado quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental;
- Acesso privilegiado à solução através de IP irregular ou desconhecido. Detectado quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental;
- Acesso privilegiado não gerenciado. Detectado quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução;
- Máquina acessada a partir de endereços IP incomuns;
- Máquina acessada durante horários irregulares. Detectado quando uma máquina é acessada em um horário irregular, de acordo com seu padrão de utilização;
- Acessos excessivos a uma máquina;
- Acesso anômalo a várias máquinas. Detectado quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto;
- Máquina incomum originando acesso;
- Usuário incomum logando de uma máquina de origem conhecida;
- Suspeita de roubo de credenciais. Detectado quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução;

- Alteração de senha suspeita. Detectado quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução;
- Atividades suspeitas detectadas durante uma sessão privilegiada. Detectado quando é identificada uma sessão privilegiada com atividades (comandos e anomalias na solução) definidas como suspeitas.

Para atendimento do item acima, poderão ser utilizados recursos integrados às soluções do Item 2.4 MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTAS A INCIDENTES DE SEGURANÇA.

A solução deverá permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador.

Ser capaz de, durante o processo de definição da política de composição de senha:

- Gerar senhas aleatórias com extensão de 127 (cento e vinte e sete) caracteres ou mais;
- Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos;
- Especificar qual o tipo de caractere na composição das senhas a serem geradas;
- Implementar controle de acesso baseado em papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada;
- Deve permitir a formação de grupos de usuários e dispositivos, bem como a atribuição de privilégios de acesso a esses grupos, onde esses privilégios de acesso possam ser atribuídos por critérios como tipo de dispositivo, sistemas operacionais, banco de dados e aplicativos de virtualização;
- Garantir que a senha gerada seja diferente do nome da conta correspondente. Exemplo: se a credencial ou conta tem o nome “Administrador” a senha gerada jamais pode ser composta da mesma forma;
- Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha.

Realizar automaticamente a descoberta, detecção, importação e armazenamento no repositório seguro de chaves SSH em sistemas Linux, implementando:

- Suporte a chaves criptográficas nos tamanhos 1024, 2048, 4096;
- Auditoria e controle dos acessos às chaves por sistema de aprovações;
- Reconciliação de chaves, renovando-as e armazenando-as novamente;
- Conexão transparente a ativos da rede utilizando as chaves armazenadas;
- Gerenciamento em grupos, permitindo que múltiplas máquinas herdem a mesma chave SSH.

Possibilitar colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador.

Permitir o encerramento automatizado da sessão em caso de detecção de atividade suspeita de alta criticidade.

Fornecer meio de integração para que soluções de terceiros também possam encerrar sessões suspeitas (ex: SIEM executa terminação de sessão).

Criar relatórios que podem ser exportados em pelo menos um dos formatos editáveis: HTML, CSV, XLSX ou XLS.

A solução deverá disponibilizar:

- Mecanismo de retirada e devolução de contas e senhas compartilhadas;
- Definição de tempo de validade, permitindo o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;

- Troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido;
- Troca de senhas por demanda, permitindo a troca de senhas nos sistemas gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (grupo de todos os sistemas operacionais UNIX, por exemplo).

Suportar, através da interface Web para acesso e recuperação das senhas, de forma nativa, a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução.

A solução deve fornecer dados ad-hoc agendados, relatórios em tempo real dos usuários, contas, configuração da solução e informações sobre os processos da solução.

Permitir que os comandos executados em sistemas Linux monitorados sejam gravados em modo texto.

Permitir, através de interface gráfica, que administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.

Suportar em sua interface web e de administração métodos autenticação de duplo fator, compatíveis com os métodos a seguir:

- Algoritmo de One-time Password, com pelo menos um dos aplicativos: Google Authenticator, Oauth, Authy, YubioAth, RSA SecureID, SAASPASS e 1Password;
- Smart cards;
- Tokens em geral;
- Certificados Digitais.

Possuir interface única, na mesma solução, para o gerenciamento de senhas e sessões.

A solução deverá prover mecanismos de atualização de segurança sob demanda e com rastreabilidade dos pacotes instalados por meio de interface gráfica intuitiva (desejável).

A solução não deve depender da instalação de agentes para realizar a troca de senhas e gravação de sessão.

A solução deve ter uma console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas.

2.7.2. A ARQUITETURA E SEGURANÇA DA SOLUÇÃO

A solução deverá possuir mecanismo de segurança que mantenha a entrega de credenciais em caso de queda da rede ou parada total do cofre digital, evitando assim a parada de aplicações críticas.

Utilizar banco de dados em alta disponibilidade, para armazenamento de credenciais, com as melhores práticas de segurança e mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução.

Todos os elementos que compõem a solução, devem ser instalados em regime de alta disponibilidade.

Caso a solução seja na mobilidade on-premisse, ela deve replicar as configurações em 02 (duas) localidades, de modo que, no evento de falha total de seus elementos instalados em uma localidade, continue disponível via uso dos elementos da outra localidade, com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação.

Todos os sistemas e recursos necessários para operação do módulo de cofre de senhas, deverão ser passíveis de plena utilização a partir de uma única localidade (site), em caso de contingência.

Em caso de utilização de ambiente on-premisse, tanto os appliances virtuais quanto sistemas operacionais da solução devem ser “hardenizados” e protegidos com firewall interno.

Deve permitir o backup e restore de seu banco de dados, bem como das configurações de software estabelecidas.

Deve permitir a execução de tarefas de backup e criptografia sem a necessidade de agentes de terceiros ou parada do ambiente ou comprometimento de qualquer funcionalidade, provendo assim o maior nível possível de segurança e integridade dos dados a serem copiados.

Deve permitir a execução de backups automatizados, possibilitando a programação/agendamento de horários e configuração de locais para seu armazenamento local e remoto.

Deve ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (cofre), por meio de backup ou método análogo, para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas e dados gerenciados pela solução.

Ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos.

Ainda que as gravações estejam armazenadas em locais diferentes, a solução deve permitir que essas evidências sejam consultadas a partir de qualquer console web instalada, de maneira centralizada.

A solução deve ser disponibilizada com um SDK (*Software Development Kit*) que pode ser configurado para permitir que aplicações possam:

- Atualizar informações de contas automaticamente no banco de dados de senhas;
- Alterar senhas em texto-claro incorporados em aplicações de uma forma segura no banco de dados de senhas;
- Solicitar as credenciais sob demanda via REST ou SOAP ao invés de utilizar credenciais estáticas;
- Deverá integrar-se nativamente ao cofre digital da solução, utilizando sua mesma interface web.

Deve possuir REST APIs detalhadamente documentadas no website do fabricante, estas APIs devem fornecer minimamente as funcionalidades de gestão das identidades, grupos e perfis, gestão de métodos de MFA, gestão de aplicações web, gestão de senhas, gestão do portal dos usuários finais e autenticação de usuários finais utilizando os métodos de MFA oferecidos.

A solução deverá fornecer credenciais tanto por meio de acesso interativo via interface da solução na rede quanto por integração programática via APIs (Webservice).

O uso de agente deve permitir instalação em múltiplos servidores web dos sistemas gerenciados pela solução, sem necessidade de aquisição de licenças, visando fornecer a melhor adaptação à arquitetura do CONTRATANTE.

Deverá manter um cache atualizado das credenciais utilizadas localmente no servidor da aplicação, a fim de prevenir falhas na comunicação com o cofre digital e trazer velocidade às consultas.

Deverá suportar a utilização de executável para scripts e aplicações nativas em plataforma Windows.

Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em comandos Linux, comandos, janelas e aplicações Windows, Expressões regulares para comandos em geral e Eventos configurados manualmente, permitindo a atribuição de nível de risco customizado.

Caso a solução fornecida faça uso das funcionalidades disponibilizadas pelas CALs (Client Access License) do serviço Microsoft Remote Desktop Services (RDS) para acessos através da mesma, a CONTRATANTE irá disponibilizar tal Infraestrutura, para que não seja afetada a experiência dos usuários.

Permitir a opção de implementar o gerenciamento de troca de senhas em redes segregadas e remotas a fim de acomodar links de alta latência, redes isoladas (DMZ) e outras restrições semelhantes.

A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, WMI, SSH e HTTP/HTTPS.

Integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas.

Permitir o agrupamento lógico de credenciais, obedecendo uma hierarquia, a fim de simplificar a configuração e aplicação de políticas apropriadas para diferentes tipos de sistemas alvo, além de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas.

Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e realizar verificações agendadas e automáticas, a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino correspondam às mesmas senhas armazenadas no banco de dados da solução. Caso a senha da conta gerenciada pela solução seja diferente daquela armazenada no banco de dados, a solução deve ser capaz de gerar relatórios e alertas notificando este evento.

A solução deve conter meios de acessar os vídeos de gravações, incluindo:

- Filtrar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado;
- A função de gravação de sessões, devendo realizar o isolamento de sessões de acesso, atuando como um proxy/servidor de salto entre a máquina do usuário e o ativo a ser acessado.

Permitir que os usuários solicitem acesso aos gestores através de interface web intuitiva.

Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma.

Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dasboards, filtros e gráficos configuráveis, sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos.

Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores.

Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo:

- E-mail com conteúdo do alerta
- Envio de alerta para solução SIEM.

Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:

- Comportamento dos usuários na utilização das aplicações;
- Visão sobre a segurança das aplicações;
- Mapa com a geolocalização das autenticações;
- Visão sobre o comportamento dos endpoints (Mobile e Computadores);
- Visão sobre o comportamento das Identidades.

A solução deve permitir a configuração de dashboards personalizados.

2.7.3. PROTEÇÃO PARA APLICAÇÕES CONTEINERIZADAS

A solução deve prover proteção e gerenciamento de secrets que atenda as demandas de segurança de credenciais e suas subcategorias, onde entende-se como secrets uma estrutura de dados que possa conter senhas, chaves privadas, tokens e chaves de APIs e ser entregue de maneira segura e criptografada para aplicações, contêineres e serviços.

Deve criptografar todas as chaves privadas SSL utilizadas por quaisquer serviços da solução, ou utilizadas na criptografia da base de dados evitando que sejam armazenadas em texto claro no sistema de arquivos. A criptografia deve ocorrer antes da escrita em armazenamento persistente, evitando que informações sejam comprometidas em caso de acesso aos dados. Deve permitir que a chave master de criptografia seja armazenada e provida por soluções de HSM.

A solução deverá atuar como gerador e intermediário (broker) de secrets para diversos clientes, como aplicações, contêineres e clientes de criptografia e ainda possibilitar o armazenamento de múltiplas versões de um mesmo secret. O fornecimento de secrets deve oferecer meios de controle de solicitante com múltiplos fatores, incluindo minimamente Tempo de vida (TTL) e restrições de IP/range.

Os secrets devem ser modificáveis, com base em critérios de tempo de uso (Lease time) ou expiração, sendo que após expiração, a rotação ocorre de acordo com políticas definidas no sistema. Todo secret deve conter por padrão, pelo menos duas listas de acesso com papéis/grupos que podem ler o secret e que podem alterar o secret.

Todos os registros de eventos de segurança como autenticação de clientes, solicitação de secrets, revogação de secrets, acesso de usuários, aplicações ou clientes a secrets, mudanças de permissão, deverão ser armazenados de maneira que impossibilite a sua alteração e se mantenha a correta integridade das evidências.

As operações com secrets devem gerar trilha de auditoria contendo, no mínimo, a identificação do cliente (usuário ou usuário sistêmico), a identificação do secret, horário (Timestamp completo), ação (leitura ou alteração) e se a ação foi permitida ou não.

Deve utilizar definição de papéis (RBAC) para autorização de identidades de usuários e de aplicações onde possam ser definidos e relacionados entre si quando possível para usuários, grupos de usuários, usuários sistêmicos (máquinas, serviços e processos) e grupos de usuários sistêmicos.

Todas as operações envolvendo usuários e grupos sistêmicos e não-sistêmicos, políticas e secrets, incluindo a criação, leitura e alteração, devem ser feitas via linguagem aberta de serialização YAML.

A obtenção de secrets deve ser permitida por diversos meios, incluindo, pelo menos, linha de comando (CLI) e RestAPI. Os secrets deverão ser disponibilizados unicamente para as aplicações ou serviços que os consomem, sendo que

em hipótese alguma, devem ser disponibilizados no nível do sistema operacional ou “namespaces” acessíveis por outras aplicações.

A solução deverá guardar e rotacionar os secrets no repositório central de credenciais da solução, sem necessidade de criação de novo ambiente de administração de credenciais, mantendo os requisitos de segurança já definidos para aquela solução.

Deve oferecer recursos de redundância, alta disponibilidade e suporte a balanceamento de carga se utilizando da infra-estrutura disponibilizada pela CONTRATANTE. A alta disponibilidade deve conter funcionalidade de replicação automática entre as bases da solução, oferecendo pelo menos 2 réplicas. O conjunto de réplicas deve oferecer funcionalidade de Failover automático, onde uma das réplicas assumirá a operação em caso de problemas. Deve haver funcionalidade de backup seguro do conteúdo armazenado e configurações do produto, possibilitando a prática de Disaster Recovery.

Para que não haja sobrecarga nem exposição do repositório central da solução e suas redundâncias, a solução deve oferecer componentes que absorvam a carga de requisições. Esses componentes devem agregar capacidade de requisições por segundo de maneira quantitativa ao total da solução.

2.8. SERVIÇOS TÉCNICOS ESPECIALIZADOS POR DEMANDA

A CONTRATADA deve disponibilizar um banco de horas técnicas anual para execução de Serviços Técnicos Especializados por demanda para atividades correlatas não previstas no escopo original, a serem demandados, aprovados e executados sob demanda, mediante Ordem de Serviço (OS).

Os serviços técnicos especializados **serão pagos sob demanda**, ficando a cargo da CONTRATANTE a fiscalização, homologação e aprovação.

Os serviços poderão ser executados conforme requisitos mínimos definidos a seguir:

- Serviços de consultoria e/ou mentoria para implementação de novas tecnologias, processos, normas, políticas de segurança da informação e cibernética;
- Serviços de consultoria e/ou mentoria para evoluções na infraestrutura do ambiente do TRIBUNAL;
- Produção de documentação e material técnico para passagem de conhecimento;
- Elaboração de workshops, webinários, palestras, entre outros, para desenvolvimento dos profissionais do TRIBUNAL.

A CONTRATADA não será eximida da responsabilidade de executar outros serviços relacionados à segurança da informação e cibernética, definidos anteriormente nos requisitos mínimos.

A CONTRATADA deverá analisar a solicitação e elaborar a proposta, a qual deverá conter, no mínimo, com as seguintes informações:

- Identificação da proposta;
- Nome do técnico responsável pelos serviços;
- Quantidade de horas técnicas necessárias para a execução dos serviços;
- Valor cobrado para a execução dos serviços;
- Descrição detalhada da execução dos serviços;
- Especificação dos artefatos da execução dos serviços;
- Cronograma da execução, que deverá conter, no mínimo:
    - Data de início;

    - Data de término.
- Dependendo do nível de complexidade da execução dos serviços, deverão ser definidos os marcos de entregas parciais e suas respectivas:
    - Data de início dos marcos de entregas parciais;
    - Data de término dos marcos de entregas parciais.
- Data da proposta;
- Assinatura do técnico responsável pela proposta.

Após o recebimento da proposta da CONTRATADA, cabe ao CONTRATANTE aprovar ou não a sua execução, emitindo a respectiva ordem de serviço.

Em caso de atraso no cronograma de execução a CONTRATADA deverá solicitar alteração prévia junto a CONTRATANTE.

Emitida a ordem de serviço a CONTRATADA terá o prazo de 05 (cinco) dias úteis para iniciar a execução das atividades, conforme item Dinâmica de execução dos serviços técnicos especializados e sob demanda.

Após a CONTRATADA executar a Ordem de Serviço (OS) deverá comunicar o encerramento das atividades para a homologação do serviço executado.

No caso de divergência com entrega parcial/incompleta/Incorreta da Ordem de Serviço a contratada deverá refazer as atividades para que seja possível homologação por parte do CONTRATANTE.

A CONTRATADA deverá encaminhar para a CONTRATANTE o relatório da Ordem de Serviço (OS).

A CONTRATANTE deverá homologar o relatório da Ordem de Serviço (OS) encaminhado pela CONTRATADA.

O faturamento somente será realizado mediante o encaminhamento do relatório da Ordem de Serviço (OS) pela CONTRATADA e aprovação da OS pela CONTRANTE.

A CONTRATADA deverá oferecer, por um período mínimo de 90 (noventa) dias corridos, a garantia dos serviços técnicos especializados.

2.9. SERVIÇO DE TESTE DE INVASÃO (PENTEST)

O Serviço de Teste de Invasão (Pentest) será realizado sob demanda, mediante Ordem de Serviço (OS), tendo como produto um relatório detalhado da atividade.

A CONTRATADA deve realizar a condução de análises regulares da eficácia das regras, políticas e configurações implementadas nas ferramentas de segurança, sugerindo e implementando melhorias para fortalecer a postura de segurança do CONTRATANTE.

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.

Caso a CONTRATANTE entenda haver algum risco na execução do Pentest que possa comprometer, em qualquer grau, o funcionamento de sistemas, ativos ou processos 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.

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.

Os sistemas, serviços e ativos de TI da CONTRATANTE a serem submetidos aos testes, serão definidos em alinhamento junto a CONTRATADA, sendo:

- As solicitações serão elaboradas pela CONTRATANTE, que ficará responsável pelo acompanhamento da execução do teste junto à CONTRATADA;
- Nas solicitações deverão ser contemplados, no mínimo, os seguintes tópicos (escopo):
    - O sistema ou ativo de tecnologia a ser testado;
    - A modalidade de Pentest a ser aplicada (Black Box, Grey Box, White Box);
    - Tipo de ambiente a ser realizado o Pentest (Interno ou Externo);
    - Todos os testes deverão ser acompanhados, homologados e supervisionados por setor competente e a critério do CONTRATANTE.

Durante os testes, não poderão ser executados quaisquer variações dos seguintes ataques sem explícita autorização prévia e monitoração pela equipe técnica responsável da CONTRATANTE:

- Ataques de negação de serviços e flooding;
- Engenharia social, por exemplo, phishing, vishing, pharming, personificação, roubo de identidade e outros;
- Ataques que possam causar danos físicos, por exemplo, arrombamentos, danos às fechaduras eletrônicas, ativação de sistemas de alarme;
- Ataques que envolvam vetores de infecção, tais como, ransomware, vírus, worms, trojan, rootkits e outros.

Cada teste de intrusão, necessariamente, deverá seguir as seguintes fases, nesta ordem:

PLANEJAMENTO - A partir da solicitação pela CONTRATANTE inicia-se a fase de Planejamento, quando serão apresentados e discutidos os itens constantes no teste.

- Na fase de planejamento serão definidos:
    - Pacote de invasão/Pentest ou a quantidade de horas necessárias;
    - Objetivo de “comprometer o ambiente” para ser alcançado como por exemplo. Caso o objetivo mude durante a tentativa, deve ser reportado em relatório posterior;
    - Processos e atividades permitidas ou proibidas (escopo);
    - O detalhamento do cronograma;
    - As informações e acessos necessários para a realização do Pentest (especialmente nos casos de Pentests Graybox e Whitebox).

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:

- Coleta passiva, caracterizada pela obtenção de informações utilizando-se, no mínimo, as seguintes técnicas/serviços/ferramentas, quando aplicáveis:
    - Whois e nslookup (consultas DNS;
    - Sites de busca;

        - Listas de discussão;
        - Blogs de colaboradores;
        - Dumpster diving ou trashing;
        - Informações livres;
        - Packet sniffing “passive eavesdropping”;
        - Captura de banner;
        - Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas, quando aplicáveis:
            - Port scanning (Mapeamento de rede);
            - Varredura de vulnerabilidade.

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 na CONTRATANTE, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável.

Além disso, deve-se atender os seguintes itens:

- A CONTRATADA deverá ser capaz de aplicar, no mínimo, os seguintes tipos de ataques, quando aplicáveis:
    - SQL Injection;
    - LDAP Injection;
    - Cookie Tampering;
    - Cross-Site Scripting (XSS);
    - Directory Transversal;
    - Buffer Overflow;
    - OS Command Execution;
    - Command Injection;
    - Remote Code Inclusion;
    - Server Side Includes (SSI) Injection;
    - File disclosure;
    - Information Leak;
    - Problemas com o SNMP;
    - DDos (Distribuited Denial of Service);
    - Dos (Denial of Service);
    - Contra protocolo TCP;
    - Violações do protocolo HTTP;
    - Ataque contra aplicação.

RELATÓRIO - Após a fase de Exploração, deve ser elaborado e entregue pela CONTRATADA um relatório técnico do teste de intrusão com visão técnica e um relatório sumário executivo em até 30 (dias) após a execução, exceto para o primeiro teste do contrato.

O relatório executivo deverá conter de forma sumarizada os resultados apresentados e a classificação dos riscos, probabilidade e impacto que as eventuais fragilidades (vulnerabilidades) identificadas possam causar ao CONTRATANTE em caso de sucesso de sua exploração.

- O relatório técnico deve conter ao menos:
    - Objetivo, escopo, tipo e modalidade do teste;

    - Metodologias, técnicas, fontes de pesquisa, referências, equipamentos e ferramentas utilizadas;
    - Atividades realizadas e em ordem cronológica;
    - Tempo do analista utilizado em cada atividade;
    - Informações acessadas e detalhes da infraestrutura descoberta, caso aplicável;
    - Confirmação ou refutação de existência das vulnerabilidades.
- Descrição de todas as vulnerabilidades e ameaças porventura encontradas, informando, no mínimo:
    - Nome;
    - Nível de Risco;
    - Intrusiva (sim / não);
    - Classificação de vulnerabilidade;
    - Descrição;
    - Observação;
    - Recomendação de Remediação;
    - Link do patch ou da correção;
    - Número CVE, se houver;
    - SANS / FBI referência Top 20;
    - IAVA (Information Assurance Vulnerability Alert) Referência;
    - Detalhamento do caminho utilizado e evidências da exploração das vulnerabilidades porventura encontradas;
    - Tipos de ataques realizados;
    - Avaliação de riscos e impacto da vulnerabilidade e consequente exploração;
    - Contra-medidas para correção ou mitigação dos riscos decorrentes das vulnerabilidades encontradas;
    - Anexos com os resultados dos testes automatizados e vídeos de realização dos ataques bem-sucedidos, quando assim solicitados.
- Prover informações sobre a efetividade da simulação, apresentando ao menos:
    - Quantidade de usuários testados;
    - Quantidade de usuários que somente visualizaram;
    - Quantidade de usuários que clicaram em algum link/anexo;
    - Quantidade de usuários enganados;
    - Tempo decorrido desde a última simulação;
    - Deve estar disponível, pelo menos, em português e inglês;
    - Alerta de Vulnerabilidades.

A CONTRATADA deverá apoiar no plano de ação para a correção das vulnerabilidades encontradas.

Após as correções das vulnerabilidades porventura encontradas (atividade sob responsabilidade do CONTRATANTE), a CONTRATADA realizará, através da mesma solicitação que gerou o primeiro teste, um novo conjunto de testes a fim de validar as correções, considerando os seguintes itens:

- Serão testados os mesmos ativos ou sistemas, seguindo as mesmas definições da fase de planejamento sem, no entanto, realizar a descoberta de novas informações relativas à superfície de ataque;
- O objetivo é verificar se todos os tratamentos foram aplicados para as vulnerabilidades anteriormente encontradas, a partir da confirmação de que estas não mais existem ou não podem mais ser exploradas;
- Ao final da fase de reteste também deverá ser obedecida a fase de apresentação dos resultados;

- Não será necessária a abertura de nova solicitação para que seja realizado o reteste, ele estará condicionado e vinculado a solicitação que gerou o teste inicial.

A janela de tempo para a execução da atividade de Pentest será acordada entre CONTRATANTE e CONTRATADA, preferencialmente em períodos e horários de menor pico de forma a não impactar na atividade jurisdicional.

ANEXO I - GLOSSÁRIO DE TERMOS

ABNT: Associação Brasileira de Normas Técnicas, organização brasileira para padronização.

BAS: Breach and Attack Simulation, simulação de violações e ataques.

CFTV: Circuito fechado de televisão.

CONTRATADA: a(s) empresa(s) vencedora(s) do processo licitatório e responsável(eis) pelo objeto será denominada simplesmente de “CONTRATADA”.

CSA: Cloud Security Alliance, notória organização internacional para melhores práticas de segurança em ambientes de computação em nuvem.

CSMA: Cybersecurity Mesh Architecture, arquitetura de malha de segurança cibernética.

CVE®: MITRE Common Vulnerabilities and Exposures , vulnerabilidades e exposições comuns, marca registrada da MITRE Corporation, se refere tanto ao programa (esforço internacional conduzido pela comunidade e patrocinado pelo Governo dos Estados Unidos) com a missão de identificar, definir e catalogar vulnerabilidades de segurança cibernética divulgadas publicamente (Programa CVE), quanto ao catálogo de todos os registros de vulnerabilidades e exposições identificados por ou reportados ao Programa CVE (CVE List).

DRP: Digital Risk Protection, Proteção contra Riscos Digitais.

DR: Disaster Recovery, recuperação de desastres.

DINFRA: Divisão de Infraestrutura da SETI.

DSEG: Divisão de Gestão de Segurança da Informação da SETI.

EDR: Endpoint Detection and Response, detecção e resposta em dispositivos de usuário final.

EPP: Endpoint Protection Platform, plataforma de proteção de dispositivos de usuário final.

ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética, variação brasileira do acrônimo internacional CSIRT, computer security incidente response team ou cyber security incidente response team.

FQDN: Fully Qualified Domain Name, nome de domínio totalmente qualificado.

HORÁRIO REGIMENTAL DO TRIBUNAL: período compreendido entre 12 (doze) e 19 (dezenove) horas, de segunda a sexta-feira, excluídos os feriados, será denominado simplesmente de "HORÁRIO REGIMENTAL DO TJPR".

ITIL: Information Technology Infrastructure Library, biblioteca de infraestrutura de tecnologia da informação, framework de melhores práticas para gerenciamento de serviços na era digital, marca registrada da AXELOS, Reino Unido.

ITSM: Information Technology Service Management, gestão de serviços de tecnologia da informação.

LGPD: Lei Geral de Proteção de Dados Pessoais, Lei Federal Nº 13.709, de 14 de agosto de 2018.

MDR: Managed Detection and Response, monitoramento, detecção, investigação e resposta gerenciados de eventos e incidentes.

MSS: Managed Security Services, serviços gerenciados de segurança cibernética.

NDR: Detecção e Resposta de Rede.

NIST: National Institute of Standards and Technology, organização do Governo dos Estados Unidos responsável por metrologia e padronização em tecnologias, com notoriedade internacional.

NMS: Níveis Mínimos de Serviço, critérios objetivos e mensuráveis estabelecidos com a finalidade de aferir e avaliar fatores como qualidade, prazo, eficácia, desempenho e disponibilidade dos serviços prestados, definindo o patamar limite para o qual o TRIBUNAL considera o serviço adequado e aceitável.

OVA: Open Virtualization Appliance.

OWASP: Open Worldwide Application Security Project, notória organização (fundação) internacional sem fins lucrativos para melhores práticas de segurança de software.

PAC: Plano de Administração de Crise.

PENTEST: teste de penetração, teste de intrusão e teste de invasão são sinônimos.

PENTEST EXTERNO: 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.

PENTEST INTERNO: 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.

PENTEST Black-box: Quando o executor do teste não possui informações acerca do ambiente tecnológico e arquitetura do alvo.

PENTEST Gray-box: Quando o executor do teste tem conhecimento limitado ou algumas informações acerca do ambiente tecnológico e arquitetura do alvo.

PENTEST White-box: Quando o executor tem pleno conhecimento e vasta informação acerca do ambiente tecnológico e arquitetura do alvo.

PRODUTO: Objeto do Termo de Referência, seja ele hardware, software, acessório, periférico ou consumível poderá será denominado simplesmente de "produto".

SANDBOX: Ambiente de computação isolado.

SETI: Secretaria de Tecnologia da Informação do TRIBUNAL será denominado simplesmente de “SETI” e seu endereço oficial é Rua Álvaro Ramos nº 157, 1º andar, Centro Cívico, Curitiba - Paraná.

SIEM: Security Information and Event Management, gestão de informações e eventos de segurança.

SOC: Security Operations Center ou Centro de Operações de Segurança.

SOAR: Security Orchestration, Automation and Response, orquestração, automação e resposta de segurança.

TAKEDOWN: Ação que visa derrubar ou retirar do ar domínios, sites e dados.

TIC: a Tecnologia da Informação e Comunicação será denominada simplesmente de "TIC".

TRIBUNAL: Tribunal de Justiça do Paraná será denominado simplesmente de “TRIBUNAL” ou TJPR.

ANEXO II - TERMO DE SIGILO E CONFIDENCIALIDADE (CONTRATADA)

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

PROCESSO ADMINISTRATIVO Nº _____

CONTRATO Nº _____

O Tribunal de Justiça do Estado do Paraná, com sede em Curitiba - PR, inscrito no CNPJ sob o nº 77.821.841/0001-94, doravante denominado TRIBUNAL, e a Empresa _____, estabelecida à _____, CEP: _____, inscrita no CNPJ sob o nº _____, doravante denominada CONTRATADA, representada neste ato pelo (a) Sr. (a). _____, (cargo) _____, (nacionalidade) _____, (estado civil) _____, (profissão) _____, portador (a) da Cédula de Identidade nº _____, e do CPF nº _____, residente e domiciliado (a) em _____, e, sempre que em conjunto referidas como PARTES.

CONSIDERANDO o atendimento à exigência do contrato supracitado, celebrado pelas PARTES, doravante denominado CONTRATO.

CONSIDERANDO a necessidade de manter o sigilo e a confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do TRIBUNAL de que a CONTRATADA tomar conhecimento em razão da execução do CONTRATO, respeitando todos os critérios aplicáveis.

CONSIDERANDO os aspectos de classificação e acesso à informação e de proteção de dados estabelecidos na legislação e normas vigentes, em especial: Lei Federal Nº 8.159, de 18 de novembro de 2011, “Lei de Acesso à Informação”. Lei Federal nº 13.709, de 14 de agosto de 2018, “Lei Geral de Proteção de Dados - LGPD”; Decreto Judiciário Nº 560/2022 - P-GP Política de Segurança da Informação - PSI, que institui a Política de Segurança da Informação no âmbito do TRIBUNAL.

Estabelecem o presente TERMO DE SIGILO CONFIDENCIALIDADE, doravante denominado TERMO, com vínculo indissociável ao CONTRATO, mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O objeto do presente TERMO é regular ao tratamento dos dados, regras de negócio, Testes de Invasão (Pentest), credenciais de acesso, documentos e informações produzidas ou custodiadas pelo TRIBUNAL, sejam elas escritas, digitais, verbais ou de qualquer outro modo apresentada, tangível ou intangível, doravante denominadas simplesmente INFORMAÇÕES, que a CONTRATADA tiver acesso em virtude da execução do CONTRATO, principalmente aquelas classificadas como CONFIDENCIAIS, provendo a necessária e adequada PROTEÇÃO ÀS INFORMAÇÕES.

1.2. O presente TERMO constitui acordo entre as PARTES, cujas estipulações e obrigações aplicam-se a todas e quaisquer INFORMAÇÕES reveladas pelo TRIBUNAL.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

2.1. A CONTRATADA se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer INFORMAÇÕES que venham a ser fornecidas pelo TRIBUNAL, a partir da data de assinatura deste TERMO, devendo ser tratadas como INFORMAÇÕES CONFIDENCIAIS, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pelo TRIBUNAL.

2.2. A CONTRATADA se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou prepostos faça uso das INFORMAÇÕES do TRIBUNAL.

2.3. O TRIBUNAL zelará para que as INFORMAÇÕES que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pela CONTRATADA.

CLÁUSULA TERCEIRA - DAS LIMITAÇÕES DA CONFIDENCIALIDADE

3.1. As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I. Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das PARTES.

II. Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO que não estejam sujeitos à obrigação de confidencialidade.

III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as PARTES tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a estas, na medida do possível, tempo hábil para pleitear medidas de proteção cabíveis.

3.2. Será permitido à CONTRATADA divulgar "Dados Agregados", aqui entendidos como informações anonimizadas que podem ser baseadas ou derivadas de Informações Confidenciais sem qualquer menção ao TRIBUNAL, exclusivamente no âmbito do curso regular dos seus negócios de fornecimento aos seus clientes dos mesmos tipos de produtos e serviços prestados ao TRIBUNAL.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES ADICIONAIS

4.1. A CONTRATADA se compromete a utilizar as INFORMAÇÕES reveladas exclusivamente para os propósitos da execução do CONTRATO.

4.2. A CONTRATADA se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste TERMO e da natureza confidencial das INFORMAÇÕES do TRIBUNAL.

4.3. A CONTRATADA firmará acordos por escrito com seus empregados e consultores ligados direta ou indiretamente ao CONTRATO, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento.

4.4. A CONTRATADA deve tomar todas as medidas necessárias à proteção das INFORMAÇÕES do TRIBUNAL, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo TRIBUNAL.

4.5. Cada PARTE permanecerá como única proprietária de todas e quaisquer INFORMAÇÕES eventualmente reveladas à outra parte em função da execução do CONTRATO.

4.6. O presente TERMO não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

4.7. A CONTRATADA obriga-se perante o TRIBUNAL a informar, tão logo tome conhecimento, qualquer violação das regras do presente TERMO por parte da CONTRATADA ou de quaisquer outras pessoas, inclusive nos casos de violação não intencional ou culposa.

4.8. Caso a revelação das informações seja determinada por ordem judicial, a PARTE notificada se compromete a avisar à outra, para que possa tomar todas as medidas preventivas para proteger as informações. Nesse caso, a parte deverá revelar apenas as informações exigidas por determinação judicial e deverá informar à outra quais as informações e em que extensão serão reveladas.

CLÁUSULA QUINTA - DO RETORNO DE INFORMAÇÕES

5.1. Todas as INFORMAÇÕES reveladas devem retornar à parte reveladora imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

5.1.1. A CONTRATADA deverá devolver, íntegros e integralmente, todos os documentos a ela fornecidos, inclusive eventuais cópias, na data estipulada pelo TRIBUNAL para entrega, ou quando não mais for necessária a manutenção das informações confidenciais, comprometendo-se a não reter quaisquer reproduções, totais ou parciais, cópias ou segundas vias, em qualquer meio ou suporte.

5.1.2. A CONTRATADA deverá destruir quaisquer documentos por ela produzidos que contenham informações confidenciais do TRIBUNAL, quando não mais for necessária a manutenção dessas, comprometendo-se a não reter quaisquer reproduções totais ou parciais, cópias ou segundas vias, em qualquer meio ou suporte, sob pena de incorrer nas penalidades previstas neste Termo.

CLÁUSULA SEXTA - DA VIGÊNCIA

6.1. O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até 5 (cinco) anos após o término do CONTRATO.

CLÁUSULA SÉTIMA - DAS PENALIDADES

7.1. A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo culminar inclusive na rescisão do CONTRATO firmado entre as PARTES.

7.1.1. Neste caso, a CONTRATADA estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo TRIBUNAL, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo e/ou judicial, sem prejuízo das demais sanções legais cabíveis.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES GERAIS

8.1. Surgindo divergências quanto à interpretação do pactuado neste TERMO ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as PARTES tais divergências, de acordo com os

princípios da legalidade, da equidade, da razoabilidade, da economicidade, da boa-fé, e, as preencherão com estipulações que deverão corresponder e resguardar as INFORMAÇÕES do TRIBUNAL.

8.2. O disposto no presente TERMO prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à CONFIDENCIALIDADE DE INFORMAÇÕES.

8.3. A omissão ou tolerância das PARTES em exigir o estrito cumprimento das condições estabelecidas neste instrumento não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA NONA - DO FORO

9.1. Fica eleito o foro de Curitiba - PR para dirimir quaisquer dúvidas oriundas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, a CONTRATADA assina o presente TERMO eletronicamente, no Sistema Eletrônico de Informações do Tribunal de Justiça do Paraná.

Curitiba, __ de _____ de _____.

_____

CONTRATADA

[Cargo]

CPF Nº _____ RG nº _____

_____

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

Gestor do Contrato

Testemunhas:

Nome:

RG:

CPF:

Nome:

RG:

CPF:

ANEXO III - TERMO DE COMPROMISSO DA PROTEÇÃO DE DADOS PESSOAIS

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

PROCESSO ADMINISTRATIVO Nº _____

CONTRATO Nº _____

O Tribunal de Justiça do Estado do Paraná, com sede em Curitiba - PR, inscrito no CNPJ sob o nº 77.821.841/0001-94, doravante denominado TRIBUNAL, e a Empresa _____, estabelecida à _____, CEP: _____, inscrita no CNPJ sob o nº _____, doravante denominada CONTRATADA, representada neste ato pelo (a) Sr. (a). _____, (cargo) _____, (nacionalidade) _____, (estado civil) _____, (profissão) _____, portador (a) da Cédula de Identidade nº _____, e do CPF nº _____, residente e domiciliado (a) em _____, e, sempre que em conjunto referidas como PARTES.

O TRIBUNAL e a CONTRATADA se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, realizando o tratamento de dados pessoais disponibilizados pelas partes, em meios físicos ou digitais, em consonância e em cumprimento das disposições preconizadas pela Lei Geral de Proteção de Dados Pessoais, a Lei Nº 13.709, de 14 de agosto de 2018, regulamentada no TRIBUNAL, assim como atenderão a suas respectivas atualizações e os padrões aplicáveis em seu segmento, vinculadas às seguintes disposições:

a) O tratamento de dados pessoais dar-se-á exclusivamente de acordo com as bases legais previstas nas hipóteses dos artigos 7º, 11 e/ou 14 da Lei Nº 13.709, de 2018, e para propósitos legítimos, específicos, explícitos e informados ao titular, limitado às atividades necessárias ao atingimento das finalidades de execução do CONTRATO, utilizando-os, quando seja o caso, em cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por requisição da Agência Nacional de Proteção de Dados.

b) A CONTRATADA compromete-se a tratar todos os dados pessoais como confidenciais, exceto se já eram de conhecimento público, devendo observar requisitos e práticas de segurança da informação para garantir a confidencialidade dos dados pessoais, inclusive no seu armazenamento, transmissão ou compartilhamento.

c) Caso seja necessário coletar dados pessoais não abrangidos pelo item 1 e não previamente informados pela CONTRATANTE, indispensáveis para o atendimento de eventual demanda específica decorrente do CONTRATO, a coleta deverá ser realizada mediante a prévia autorização do Encarregado de Proteção de Dados do Tribunal de Justiça do Paraná, responsabilizando-se a CONTRATADA pela obtenção do consentimento dos titulares.

d) Nas hipóteses em que a CONTRATADA (operadora), por força de suas atividades, tenha que repassar dados pessoais para tratamento de outra empresa/entidade (sub operadora), obtidos em razão deste contrato, deve obter autorização formal da CONTRATANTE, responsabilizando-se ambas (operadora e sub operadora) de forma solidária, na forma do art. 42, §1º, I da Lei Nº 13.709, de 2018.

e) As partes devem permitir aos titulares o acesso aos seus respectivos dados pessoais, bem como a promover alterações e cancelamentos e conceder informações quanto ao tratamento, quando solicitado expressamente.

f) Não ocorrerá transferência da propriedade ou controle dos dados pessoais pela CONTRATADA, sendo que os dados eventualmente gerados, obtidos ou coletados na execução contratual serão de propriedade dos respectivos titulares, sendo vedado o compartilhamento ou comercialização de quaisquer elementos de dados, produtos ou subprodutos que se originem ou sejam criados a partir do tratamento de dados pessoais.

g) As partes não fornecerão ou compartilharão, em qualquer hipótese, dados pessoais sensíveis de seus colaboradores, prestadores de serviços e/ou terceiros, salvo se expressamente solicitado por uma parte à outra, caso o objeto do CONTRATO justifique o recebimento de tais dados pessoais sensíveis, estritamente para fins de atendimento de legislação aplicável.

h) As partes informarão e instruirão os seus colaboradores, prestadores de serviços e/ou terceiros sobre o tratamento dos dados pessoais, observando todas as condições deste Termo, nunca cedendo ou divulgando tais dados a terceiros, salvo se expressamente autorizado pelo titular, por força de lei ou por determinação judicial; e garantindo a privacidade e a confidencialidade dos dados pessoais, mantendo controle rigoroso de acesso.

i) A CONTRATADA deve monitorar sua própria conformidade, de colaboradores, de prestadores de serviços e/ou de terceiros, com relação à proteção de dados pessoais, devendo apresentar relatórios sempre que solicitado pela CONTRATANTE com informações como o “status” dos sistemas de processamento de dados pessoais, as medidas de segurança, o tempo de inatividade registrado das medidas técnicas de segurança, a conformidade estabelecida com as medidas organizacionais, eventuais violações de dados e/ou incidentes de segurança, as ameaças percebidas à segurança e aos dados pessoais e as melhorias exigidas e/ou recomendadas.

j) A CONTRATANTE, ou representantes por ela indicados, poderá acompanhar, monitorar, auditar e fiscalizar a conformidade das obrigações de proteção de dados pessoais, sem que isso implique em qualquer diminuição de responsabilidade da CONTRATADA, podendo, ainda, notificar e fornecer informações, para atendimento em 48 (quarenta e oito) horas, sobre qualquer não cumprimento (ainda que suspeito) das disposições legais ou contratuais relativas à proteção de dados pessoais, de qualquer violação de segurança ou de exposições/ameaças em relação à conformidade com a proteção de dados pessoais, ou em período menor, se necessário, para atender a qualquer ordem judicial, de autoridade pública ou de regulador competente.

k) A CONTRATADA corrigirá, completará, excluirá e/ou bloqueará os dados pessoais, quando solicitado pela CONTRATANTE, devendo, ainda, comunicar sobre reclamações e solicitações dos titulares de dados pessoais.

l) A CONTRATADA manterá registro das operações de tratamento de dados pessoais que realizar, bem como implementará medidas técnicas e organizacionais necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação, transferência, difusão ou o acesso não autorizado, além de garantir que o ambiente utilizado por ela (seja ele físico ou lógico) seja estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios gerais previstos na Lei N. 13.709, de 2018, e às demais normas regulamentares aplicáveis, para garantir, além da segurança, a confidencialidade e a integridade dos dados pessoais.

m) A CONTRATADA deve informar à CONTRATANTE sobre qualquer incidente de segurança que implique violação ou risco de violação de dados pessoais, relacionado ao presente instrumento, em até 48 (quarenta e oito) horas, contadas do momento em que tomou conhecimento, por quaisquer meios, do respectivo incidente.

n) As partes excluirão, de forma irreversível, os dados pessoais retidos em seus registros, mediante solicitação da outra parte ou dos titulares dos dados, salvo conforme determinado por Lei ou ordem judicial.

o) Os peticionamentos relacionados ao tratamento de dados serão endereçados à XXXXX para apreciação do Encarregado de Proteção de Dados, através do correio eletrônico YYYY, e serão atendidos dentro de prazo razoável.

p) Encerrada a vigência do instrumento contratual ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a CONTRATADA interromperá o tratamento dos dados pessoais coletados no decorrer da execução contratual, bem como daqueles disponibilizados pela CONTRATANTE, e, em no máximo 30 (trinta) dias, eliminará completamente os dados pessoais e todas as cópias porventura existentes (seja em formato digital ou físico), salvo quando a CONTRATADA tenha que manter os dados para cumprimento de obrigação legal, ou outra hipótese determinada pela Lei Nº 13.709, de 2018.

q) O tratamento dos dados coletados, somente quando autorizado de uma parte à outra, poderão ser conservados pelo período de 05 (cinco) anos após o término do CONTRATO, com sua posterior eliminação, sendo autorizada sua conservação nas hipóteses descritas no artigo 16 da Lei Nº 13.709, de 2018.

r) Independentemente do disposto em qualquer outra cláusula deste Termo, a CONTRATADA é a única responsável por todo e qualquer dano decorrente do descumprimento da Lei Nº 13.709, de 2018, pela CONTRATADA, por seus colaboradores, prepostos, subcontratados, parceiros comerciais, empresas afiliadas ou qualquer agente ou terceiro a ela vinculado ou que atue em seu nome.

s) Eventuais responsabilidades das partes serão apuradas conforme estabelecido neste termo e de acordo com o que dispõe a Seção III, Capítulo VI, da Lei Nº 13.709, de 2018.

t) Fica eleito o foro de Curitiba - PR para dirimir quaisquer dúvidas oriundas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

ANEXO IV - ESTIMATIVAS DE ATIVOS PARA DIMENSIONAMENTO DOS SERVIÇOS

Para referência de dimensionamento dos serviços e das soluções informatizadas, devem ser consideradas as estimativas da infraestrutura de TIC do TRIBUNAL, conforme tabela a seguir:

Tabela com estimativa de ativos de Infraestrutura de TIC do TRIBUNAL

Item	Ativo	Quantidade
1	Servidores físicos	80
2	Servidores virtuais	700
3	Estação de trabalho	16.000
4	Notebooks	3.000
5	Impressoras	3.000
6	DNS	4
7	Links de Internet	3
8	Site WAN	215
9	Ativos de rede (switch, roteadores, etc)	1.200
10	VPN	4
11	Serviço de Diretório	6
12	Storages	4
13	Usuários internos	18.000

Tabela 1 - Estimativa de ativos de TIC do TRIBUNAL

Tabela de soluções de segurança do TRIBUNAL para Sustentação pela CONTRATADA

Item	Ativo	Descrição	Quantidade
1	Solução de Firewall 01	Palo Alto - PA 5220	02
2	Solução de Firewall 02	Palo Alto - PA 5420	02
3	Solução de Gerência Centralizada	Palo Alto Panorama	02

4	Microsoft Defender	Soluções de Segurança Microsoft licenciadas com: Microsoft 365 E3 com Add-on E5 Security	4.000
5	Microsoft Defender	Soluções de Segurança Microsoft licenciadas com: Microsoft 365 F3 com Add-on F5 Security	14.018
6	Solução de Gestão de Vulnerabilidades	Tenable, licenciado para 2.000 ativos	01

Tabela 2 - Soluções de segurança para Serviço de Sustentação

ANEXO V - MODELO TABELA MENSAL DE SERVIÇO PRESTADO

Item	Categoria	Descrição	Qtde	Unitário R$	Total R$
2	Serviços de Governança e Conformidade de Segurança				
	2.1	Diagnóstico de Maturidade de Segurança da Informação	01	x	1x
	2.2	Política de Segurança da Informação (PSI)	01	x	1x
	2.3	Plano de Continuidade de Serviços Essenciais de TIC	01	x	1x
	2.4	Plano de Resposta a Incidentes (PRI)	01	x	1x
3	Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança				
	3.1	Serviço de Security Operations Center (SOC)	x	x	x
	3.2	Proteção contra Riscos Digitais (Threat Intelligence)	X	x	x
	3.3	Serviço de Takedown	x	x	x
4	Sustentação de Operações de Soluções e Resposta a Requisições de Segurança				
	4.1	Solução de Firewall	x	x	x
	4.2	Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)	x	x	x
5	Gestão de Vulnerabilidades e Testes de Segurança				
	5.1	Gerenciamento Contínuo de Vulnerabilidades	x	x	x
	5.2	Testes de Segurança Automatizados (BAS)	x	x	x
6	Gestão de Identidade				
	5.1	Gerenciamento de Acesso Privilegiado (PAM)	x	x	x

Tabela 1 - Modelo Tabela Mensal de Serviço Prestado

ANEXO VI - MODELO PLANILHA DE CUSTOS - SOLUÇÃO INFORMATIZADA

Item de Serviço	**Grupo 01 - 3.1**						
Solução informatizada para gerenciamento, monitoramento, detecção e resposta de informações, eventos e incidentes de segurança							
Fabricante	Componente/Suíte	Descrição	Part Number	Versão	Qtde	Unitário mensal R$	Total Mensal R$
Total Global Mensal R$							

Tabela 1 - Planilha de custos Solução SOC

Item de Serviço	**Grupo 01 - 5.2**						
Testes de Segurança Automatizadas (BAS)							
Fabricante	Componente/ Suíte	Descrição	Part Number	Versão	Qtde	Unitário mensal R$	Total Mensal R$
Total Global Mensal R$							

Tabela 2 - Planilha de custos Solução BAS

Item de Serviço	**Grupo 01 - 6.1**						
Solução informatizada para Gerenciamento de Acesso Privilegiado (PAM)							
Fabricante	Componente/Suíte	Descrição	Part Number	Versão	Qtde	Unitário mensal R$	Total Mensal R$

Total Global Mensal R$	

Tabela 3 - Planilha de custos Solução PAM

ANEXO VII - MODELO DE PROPOSTA COMERCIAL

Tabela - Modelo Proposta Comercial

Grupo 01						
Item	**Categoria**	**Descrição do Item**	**Qtde**	**Tipo**	**Valor Unitário R$**	**Valor Total R$**
1	Projeto e implantação		01	Unitário		
2	Serviços de Governança e Conformidade de Segurança					
	2.1	Diagnóstico de Maturidade de Segurança da Informação	03	Unitário		
	2.2	Política de Segurança da Informação (PSI)	33	Mês		
	2.3	Plano de Continuidade de Serviços Essenciais de TIC	33	Mês		
	2.4	Plano de Resposta a Incidentes (PRI)	33	Mês		
3	Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança					
	3.1	Serviço de Security Operations Center (SOC)	825.000	Ativos protegidos		
	3.2	Proteção contra Riscos Digitais (Threat Intelligence)	33	Mês		
	3.3	Serviço de Takedown	60	Takedown executado		
4	Sustentação de Operações de Soluções e Resposta a Requisições de Segurança					
	4.1	Solução de Firewall	198	Ativos protegidos		
	4.2	Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)	660.000	Ativos protegidos		
5	Gestão de Vulnerabilidades e Testes de Segurança					

	5.1	Gerenciamento Contínuo de Vulnerabilidades	33	Mês		
	5.2	Testes de Segurança Automatizados (BAS)	990	Baterias realizadas		
6	Gestão de Identidade					
	6.1	Gerenciamento de Acesso Privilegiado (PAM)	2.640	Usuários administrativos protegidos		
7	Serviços Técnicos Especializados por Demanda		1.200	Horas sob demanda		
Total Global do Grupo R$ Preço Global do Grupo por extenso R$:						

Item Avulso					
Item	**Descrição do Item**	**Qtde**	**Tipo**	**Valor Unitário R$**	**Valor Total R$**
8	Serviço de Teste de Invasão (Pentest)	360	Horas sob demanda		
Total Global do Grupo R$ Preço Global do Grupo por extenso R$:					

ANEXO IX - MODELO DE DEMONSTRAÇÃO DE ATENDIMENTO AOS QUESITOS TÉCNICOS (PONTO A PONTO)

Grupo 01

Item 2.4	Serviço de Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança	Declaração/Comprovação (Documento, página, site etc.) de atendimento ao requisito.
2.4.1-1	O funcionamento do SOC deve ser em regime ininterrupto 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano (úteis e não úteis).	
2.4.1-2	A CONTRATADA deve atender uma das opções abaixo: a) possuir no mínimo 02 (dois) Centros de Operação de Segurança, sendo um em território nacional, redundantes e que devem estar em pleno funcionamento (infraestrutura física, lógica, equipe e processos) na contratação e durante toda a vigência do contrato, de modo que a indisponibilidade não afete a prestação dos serviços. O SOC principal e o redundante utilizados no serviço devem estar situados em regiões distintas, e estar no mínimo a 50 km (cinquenta quilômetros) de distância geodésica um do outro, como redundância geográfica para mitigar os riscos de interrupção dos serviços e de perda total dos dados em caso de desastres naturais, falhas de energia, entre outros eventos adversos. b) deve possuir 01 (um) Centro De Operações de Segurança (SOC) em território nacional, em pleno funcionamento (infraestrutura física, lógica, equipe e processos), na contratação e durante toda a vigência do contrato. A operação deve ser garantida de forma que a continuidade dos serviços não seja interrompida por tempestividades de qualquer natureza através da apresentação de um plano de continuidade.	
2.4.1-3	Deve possuir estrutura central para visualização dos painéis de monitoramento (video-wall) que permita que todos os profissionais visualizem informações e eventos relevantes simultaneamente.	
2.4.1-4	Deve utilizar sistema de gerenciamento de circuito fechado de televisão (CFTV), que viabilize o rastreamento de pessoas dentro do ambiente da CONTRATADA, e cujas imagens possam ser recuperadas, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias.	
2.4.1-5	Deve possuir controle de acesso físico seguro de funcionários, com pelo menos um dos seguintes fatores de autenticação: cartão de	

	identificação magnético ou de proximidade, biometria de leitura de digital, face ou retina, e registro de entrada e saída de visitantes, com registro de entrada e saída de todas as pessoas mantido por pelo menos 90 (noventa) dias.	
2.4.1-6	Deve possuir perímetro físico equipado com sensor de intrusão e alarmes contra acesso indevido.	
2.4.1-7	Deve possuir estrutura de armazenamento de dados que permita a manutenção dos registros das requisições e dos incidentes relacionados aos serviços contratados por, no mínimo, o prazo do contrato.	
2.4.1-8	Deve possuir sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPS (Uninterruptible Power Supply), garantindo a transição entre o fornecimento normal da energia e o grupo gerador.	
2.4.1-9	Deve possuir componentes de segurança e plano de recuperação necessários para garantir a preservação dos dados em casos de incêndio e catástrofes.	
2.4.1-10	Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores estejam inacessíveis a leituras e a capturas externa, desautorizadas.	
2.4.1-11	Deve possuir ambiente dedicado único e exclusivamente para laboratório, onde seja possível reproduzir os incidentes e problemas do TRIBUNAL, sem que haja impacto na operação dos SOCs e/ou do próprio TRIBUNAL.	
2.4.1-12	Deve garantir capacitação e treinamento inicial e contínuo dos profissionais que executam os serviços.	
2.4.1-13	Rever periodicamente as políticas e processos do SOC, a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL.	
2.4.3-1	Comprovar existência de equipe de tratamento e resposta a incidentes atuando em Nível 1 (atuação inicial), Nível 2 (atuação avançada) e Nível 3 (especialistas), organizada no mínimo em grupos distintos para: • Monitoramento e detecção de eventos, incidentes e ataques; • Caçada contínua a ameaças (Threat Hunting); • Inteligência de ameaças (Threat Intelligence); • Gestão de crises e investigação avançada de incidentes.	

2.4.3-2	Os times da CONTRATADA para segurança defensiva (Blue Team), ofensiva (Red Team) e mista (Purple Team) devem funcionar, interagir e atuar de maneira integrada, compartilhando conhecimento sobre táticas, técnicas e procedimentos de ataque, soluções para vulnerabilidades encontradas e outros, para que, por meio da atuação conjunta, aumente-se a efetividade da proteção do ambiente.	
2.4.3-3	A caçada contínua a ameaças (Threat Hunting) por meio de processos contínuos, estruturados e proativos, deve realizar, no mínimo, as seguintes atividades: • Definir hipóteses de possibilidades de ameaças e de como encontrá-las, elaboradas utilizando como referência vetores de ameaças novos e ativos e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, indicadores de comprometimento (IoC) de casos relevantes, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e procedimentos (TTP), podendo ser utilizados Framework do MITRE ATT&CK, entre outros; • Planejar e realizar a coleta dos eventos dentro das plataformas relevantes de acordo com cada hipótese definida; • Avaliar a massa de eventos para buscar anomalias associadas à hipótese definida e registrar evidências encontradas; • Caso sejam encontrados eventos maliciosos e/ou incidentes, incluí-los no processo de tratamento e resposta a incidentes de segurança.	
2.4.3-4	O tratamento dos incidentes de segurança deve, alinhado com o Processo de Tratamento de Incidentes, realizar as seguintes ações: • Efetuar a resposta, investigação e encerramento dos incidentes de segurança, incluindo o acionamento do seu Nível 2 e, nos casos de incidentes massivos e de severidade alta, seus especialistas de Nível 3; • Fazer a análise inicial dos incidentes confirmados e identificar os principais vetores de ataque e/ou exploração utilizados; • Classificar os incidentes em níveis de severidade, priorizar e escalar conforme o processo vigente; • Notificar o cliente, com os detalhes do incidente detectado e ativos de TIC envolvidos, de acordo com a severidade do incidente e a matriz de escalonamento no processo vigente; • Elaborar, executar e manter atualizados os roteiros de investigação e os playbooks de resposta a incidentes, com a devida aprovação final do cliente;	

	• Automatizar playbooks por meio de ferramenta de orquestração e automação; • Prover a proposta de contenção, erradicação e recuperação, em articulação com as equipes do cliente, executar os procedimentos sob sua responsabilidade com a devida autorização do cliente e observado o processo de Gestão de Mudanças do cliente, e controlar as ações, notificações e escalonamento dos incidentes, de acordo com os roteiros de resposta pré-definidos; • Efetuar investigações relacionadas aos incidentes, com o objetivo de identificar a causa-raiz, coletar todas e quaisquer evidências e identificar os ativos de TIC afetados.	
2.4.3-5	Deve monitorar a atividade de ameaças e ocorrência de incidentes globais, através de feeds de inteligência de ameaças, identificados a partir de análises e pesquisas na DarkWeb e outras fontes de informação, de modo a antever eventuais ameaças e ataques ao TRIBUNAL e aprimorar os controles dos serviços contratados.	
2.4.4-1	Deve fornecer e adotar Solução Informatizada para Gerenciamento, Monitoramento, Detecção e Resposta de Informações, Eventos e Incidentes de Segurança e ataques, devendo ser projetada como uma plataforma completa e para atender funcionalidades de monitoramento, inspeção e análise, detecção contínua de ameaças e ataques, investigação e defesa cibernética	
2.4.4-2	Deve possuir arquitetura distribuída, com no mínimo as seguintes funcionalidades, módulos ou componentes nativamente integrados: • Gerenciamento de informações e eventos de segurança (Security Information and Event Management - SIEM) de nova geração; • Inteligência de ameaças (Threat Intelligence Platform - TIP); • Orquestração, automação e resposta (Security Orchestration, Automation and Response - SOAR); • Análise de comportamento de usuários e entidades (User and Entity Behavior Analytics - UEBA); • Detecção e Resposta de Rede (Network Detection and Response - NDR); • Malware Sandbox. Excepciona-se da obrigatoriedade de integração nativa, no parágrafo anterior, os componentes de Detecção e Resposta de Rede (NDR) e Malware Sandbox, os quais poderão ser providos por	

	meio de integração via APIs (Application Programming Interface) ou conectores específicos homologados pelo fabricante, desde que assegurada a total interoperabilidade e a capacidade de resposta orquestrada e automatizada dentro da plataforma principal.	
2.4.4-3	O gerenciamento de informações, eventos, alertas e incidentes deve possuir os seguintes recursos e capacidades: • Ingestão de dados, coleta de registros (logs) e telemetria e geração de metadados; • Indexação, agregação e enriquecimento dos metadados; • Retenção de dados e metadados e armazenamento de eventos e registros processados; • Correlacionamento, triagem e análises avançadas de eventos, alertas, detecção e tratamento de incidentes;	
2.4.4-4	Durante toda a vigência da contratação, não deve existir para a solução ofertada limitação quanto a quantidade de consultas de usuário nem de consultas programáticas (queries) às informações, quantidade de parses no tratamento de eventos, quantidade de conectores para ingestão, quantidade de envio de registros por ativo e quantidade de casos de uso.	
2.4.4-5	Ser extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período, preferencialmente adotando repositório em arquitetura “data lake”.	
2.4.4-6	Ter recursos de segregação lógica multilocação ("multitenancy") em uma arquitetura adequada para funcionar em ambiente multilocatário (“multitenant”).	
2.4.4-7	Ser dimensionada e licenciada para coletar, processar, correlacionar e armazenar eventos das fontes de dados do ambiente computacional on-premise e em nuvem do TRIBUNAL.	
2.4.4-8	Coletar, interpretar, normalizar e correlacionar eventos de segurança em tempo real, provenientes de logs de diferentes fontes do ambiente computacional do TRIBUNAL, com o objetivo de detectar incidentes e permitir a ação imediata da equipe de resposta a incidentes.	
2.4.4-9	Ser capaz de tratar, no mínimo, os seguintes formatos, protocolos e fontes: • Syslog, Simple Network Management Protocol (SNMP); • Microsoft Windows Event Log;	

	• Logs em texto delimitado (como vírgula, tabulação, pipe); • Common Event Format - CEF, estruturado (ex: JSON, Regex etc.) ou não estruturado.	
2.4.4-10	Deve permitir a retenção do histórico de segurança da CONTRATADA, contemplando, minimamente, os seguintes dados: • Dados de eventos de segurança; • Dados das aplicações; • Dados dos sistemas operacionais; • Dados das nuvens públicas e privadas; • Dados do tráfego de rede; • Tráfego de registro (syslog).	
2.4.4-11	Ser capaz de coletar registros (logs) e informações de telemetria em serviços em nuvem pública de software (SaaS), plataforma (PaaS) e infraestrutura (IaaS), via integração por interfaces de programação (APIs), protocolos e agentes que sejam providos e homologados no mínimo pelos seguintes provedores: • Amazon Web Services (AWS); • Google Cloud Platform (GCP); • Microsoft Azure, Oracle Cloud.	
2.4.4-12	Ser capaz de inspecionar registros de plataformas de colaboração corporativa como Google Workspace e Microsoft/Office 365.	
2.4.4-13	Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) e soluções de gestão de identidade.	
2.4.4-14	Possuir API restful para integração com vários serviços para ingestão de registros, telemetria e tráfego para detecção e resposta a eventos de segurança.	
2.4.4-15	Prover mecanismo de coleta de logs de dispositivos e fontes não suportados nativamente, por meio de personalização de coletores.	
2.4.4-16	Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta.	
2.4.4-17	Possuir mecanismos de compressão e controle de fluxo para a transmissão de dados entre os coletores e os servidores de gerenciamento, através de um dos componentes da solução (aplicação, sistema operacional, etc).	
2.4.4-18	Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume de eventos.	

2.4.4-19	Armazenar os alertas, incidentes e os eventos, inclusive os normalizados, de forma indexada.	
2.4.4-20	Toda a comunicação entre os componentes deve ser criptografada.	
2.4.4-21	Possuir política de retenção configurável para o tempo de armazenamento de eventos em formato bruto (raw), preservando evidências para fins de conformidade e eventuais ações forenses, com retenção de dados brutos pelo período mínimo de 30 (trinta) dias.	
2.4.4-22	Reter os dados processados e metadados de eventos, como alertas e registro de incidentes gerados, em registros no banco de dados e/ou data lake da solução pelo período mínimo de 12 (doze) meses, meses, salvo para consultas e pesquisas on-line, devendo, no mínimo, os últimos 30 (trinta) dias de registros serem armazenados a quente (hot-storage).	
2.4.4-23	Proteger os registros contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada.	
2.4.4-24	Permitir o expurgo dos dados de forma automática, com a personalização do prazo de expurgo, sendo que somente será permitida a exclusão de eventos conforme a política de retenção de dados definida, ou seja, todos os eventos mais antigos que extrapolem o tempo de retenção definido.	
2.4.4-25	Permitir a correlação de eventos, devidamente estruturados em metadados.	
2.4.4-26	Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas também deve ser capaz de criar novos analisadores personalizados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis.	
2.4.4-27	Permitir filtrar e selecionar os eventos que serão inseridos na solução e a criação e alteração de filtros.	
2.4.4-28	Tratar eventos e alertas em um fluxo de refinamento, através de categorização e priorização, análise crítica, investigação, enriquecimento de informações e análises, inteligência de ameaças (Threat Intelligence) incluindo fontes estratégicas (relatórios, bases de conhecimento, feeds, fóruns e comunidades abertas, da Deep Web e da Dark Web etc.), táticas (correlação com táticas, técnicas e procedimentos - TTPs) e operacionais (correlação com indicadores de comprometimento - IOCs), e validação,	

	identificando atividades anômalas e, dentre essas, candidatos a incidentes.	
2.4.4-29	Deve realizar análise comportamental de usuários e entidades (User and Entity Behavioral Analysis - UEBA) com aprendizado de máquina para detectar ameaças.	
2.4.4-30	Deve ser capaz de detectar padrões de ataques, através da elaboração de baseline comportamental dos usuários e entidades.	
2.4.4-31	Deve possuir técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal.	
2.4.4-32	Deve possuir a capacidade de identificar anomalias nos comportamentos individuais dos usuários e entidades: • Horário atípico do acesso; • Número atípico de sessões de uso nos sistemas operacionais; • Volume de conexões atípico; • Volume de transferências de dados atípico; • Localização geográfica atípica da origem do acesso; • Endereço IP de origem atípico do acesso; • Acesso atípico a dados armazenados; • Criação e uso de processos (executáveis em memória) atípicos pelo usuário/entidade; • Mudança na postura de risco do usuário/entidade.	
2.4.4-33	Deve enriquecer os eventos em tempo real com o contexto do usuário e da entidade. Os dados enriquecidos devem fornecer atributos de contexto que podem ser usados para a elaboração de perfis de comportamento, comparações entre pares, pesquisas e investigações.	
2.4.4-34	Implementar regras avançadas que conectem eventos sem correlação direta e gerem incidentes caso seja constatado algum desvio.	
2.4.4-35	Possuir capacidade de contextualização, utilizando dados de diferentes origens (servidores, aplicações etc.) em uma única console, otimizando o processo de análise e resposta a incidentes.	
2.4.4-36	Agregar eventos semelhantes que ocorrerem dentro de um limite de tempo ou quantidade de eventos específicos.	
2.4.4-37	Possuir identificação autônoma de táticas, técnicas e procedimentos (TTPs) mapeando automaticamente com o framework MITRE ATT&CK.	

2.4.4-38	Deve incluir capacidades de integração nativa com ferramentas de proteção, detecção e resposta de endpoints (Endpoint Protection Platforms - EPP e Endpoint Detection and Response - EDR), incluindo obrigatoriamente a atual do TRIBUNAL - Microsoft Defender.	
2.4.4-39	Deve permitir modelagem de ameaças com a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco.	
2.4.4-40	Deve possuir tecnologia para análise automatizada de artefatos maliciosos (“malware sandbox”) que minimamente contemple as funcionalidades a seguir: • Analisar indicadores comportamentais de um artefato; • Realizar análise estatística e dinâmica para validar se o artefato é malicioso ou não; • Suportar a análise de artefatos BAT, CHM, DLL, EXE, ISO, HTA, JAR, JS, JSE, LNK, MSI, MHTML, documentos do Microsoft Office, PE32, PDF, VBE, VBS, WSF, XML, ZIP.	
2.4.4-41	Permitir a caçada rápida de ameaças por meio da pesquisa em linguagem natural.	
2.4.4-42	Deve ser eficaz na detecção de ameaças e ataques de Ransomware.	
2.4.4-43	Deve ser capaz de detectar no mínimo as seguintes ameaças de identidade: • Password spray; • Brute force; • Varredura de credenciais; • Golden ticket; • Pass-the-hash; • Atividade não usual/atípica de usuário; • Elevação de privilégios; • Movimentação lateral.	
2.4.4-44	Apresentar as informações sobre os eventos que compõem um alerta ou incidente identificado pelas regras de correlação da solução, referenciando tais eventos básicos a partir do evento alerta/incidente.	
2.4.4-45	Possuir um sistema de alertas personalizável pelo administrador da solução, com a possibilidade de geração de alertas via dashboard automatizados ou e-mail quando um incidente for detectado.	

2.4.4-46	Permitir a criação e o gerenciamento de detecção de ameaças e conformidade na forma de regras, análises, relatórios e dashboards.	
2.4.4-47	Deve suportar controle de acesso baseado em função (RBAC) granular com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações.	
2.4.4-48	Possuir workflow automatizado para a resposta e gerenciamento de incidentes, de modo que ações de criação, alteração, escalonamento, documentação e fechamento de incidentes possam ser realizadas automaticamente pela solução.	
2.4.4-49	Prover acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redesenvolvimento.	
2.4.4-50	Possuir funcionalidades de atualização, gerenciamento e configuração centralizadas de todos os agentes ou conectores distribuídos da solução.	
2.4.4-51	Permitir a categorização manual de eventos inéditos não categorizados por padrão e sua aplicação em eventos futuros de mesma natureza.	
2.4.4-52	Permitir pesquisas no histórico de eventos, fornecendo capacidade de visualizar os detalhes dos eventos (drill down), inclusive no formato bruto, quando aplicável, para análise forense e investigação de incidentes.	
2.4.4-53	A partir de um evento ou conjunto de eventos, apresentar seus relacionamentos de forma gráfica e possibilitar fazer drill down para efetiva investigação e identificação de causa raiz.	
2.4.4-54	Gerenciamento, análise, orquestração e automação de políticas, posturas, casos de uso, playbooks e integrações, com capacidade de resposta autônoma e aplicação próxima a tempo real, com componente de Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation and Response - SOAR), totalmente e nativamente integrado à solução, com o objetivo de automatizar os processos e fluxos de trabalho, a execução de atividades repetitivas ou de difícil execução e a orquestração das diversas ferramentas de segurança, com necessidade mínima de atuação humana.	

2.4.4-55	Deve possuir integração nativa com os diversos ativos e recursos de infraestrutura e segurança de TIC e capacidade de integrar, consolidar, agregar e correlacionar também todas as informações oriundas de outras fontes de telemetria disponíveis.	
2.4.4-56	Deve prover plataforma para gerenciamento e documentação de eventos/incidentes/casos de uso de ponta a ponta, automação de resposta a incidentes, investigação, automação de playbooks e repositório único de evidências.	
2.4.4-57	Não deve ter restrições com limitações de licença sobre o número de casos, número de playbooks criados ou número de ações realizadas pelos usuários do sistema.	
2.4.4-58	O recurso de gerenciamento de incidentes deve permitir a definição de um processo abrangente desde o registro e triagem inicial de um incidente até a sua resolução e prevenção, gerenciando eficazmente incidentes.	
2.4.4-59	A CONTRATADA deverá promover a automação de processos e fluxos de trabalho em solução interativa, prática e de fácil implementação, sem a necessidade de customização ou alteração do código-fonte.	
2.4.4-60	Os Dashboards (painéis), gráficos e relatórios, devem: • Fornecer dashboards e relatórios pré-configurados e permitir a criação de dashboards e relatórios personalizados de forma flexível, ágil e intuitiva, incluindo gráficos como tipo pizza, linha, colunas, barras e tabelas dinâmicas, contemplando as diversas necessidades de visão gerencial; • Possuir dashboards de monitoramento em tempo real e de dados históricos; • Permitir a emissão de relatórios de forma tempestiva ou agendada, permitindo configurar o envio automático e agendado para grupos de usuários ou usuários específicos; • Permitir a sobreposição e o cruzamento de informações, e agrupamentos por critérios comuns; • Permitir ao usuário organizar os gráficos e informações, em seus painéis e dashboards, ajustando o layout e conteúdo do painel de acordo com suas necessidades.	
2.4.4-61	Permitir que a partir de qualquer gráfico de gestão, contido em painéis e dashboards, o usuário possa, de forma gráfica e interativa: • Clicar e listar os registros relacionados com os dados contidos no gráfico (drill down);	

	• Realizar alterações dinâmicas de atributos, como a alteração de eixos, título, legenda, escala, rótulos de dados, tamanho; • Permitir o gerenciamento de permissões por usuários e grupos para acesso aos dashboards e relatórios e para compartilhamento; • Permitir a geração de relatórios, impressão e exportação para arquivos em formatos como .csv e .pdf.	
2.4.4-62	Permitir integração com a Solução Informatizada para Gestão de Vulnerabilidades, adquirida pelo TRIBUNAL.	
2.4.4-63	Quanto ao mecanismo de detecção e resposta na rede (NDR): • Ser capaz de analisar o tráfego TCP/UDP na rede da CONTRATANTE para detectar comportamentos e possíveis ameaças, gerando eventos de alerta de acordo com o tipo de tráfego; • Ser capaz de produzir e coletar informações de telemetria em tempo real de tráfego de rede, tomando como base no mínimo as conexões de rede principais do data center do TRIBUNAL; • Suportar a análise de no mínimo 08 (oito) Gbps de tráfego total, incluindo tráfego criptografado, devendo ser fornecidos equipamentos capazes de realizar espelhamento de tráfego (seja incluso em Appliance ou por meio de derivação de rede - Network Tap) com no mínimo duas interfaces fibra óptica de 10 (dez) Gbps cada, com especificações de SFP a serem oportunamente fornecidas pelo TRIBUNAL; • Ser capaz de funcionar em modo de monitoramento, sem bloquear comunicações maliciosas de entrada ou saída; • Ser capaz de inspecionar cada pacote individualmente e detectar e extrair adequadamente o protocolo e serviço, contornando de forma confiável eventuais medidas de evasão.	
2.4.4-64	Ter a capacidade de identificar ameaças no tráfego de rede e realizar o monitoramento proativo de forma automatizada o tráfego passante na rede da CONTRATANTE, contemplando os seguintes critérios: • Utilização da largura de banda; • Tentativas de invasão e varreduras de IPs e portas; • Autenticações recusadas ou com falhas; • Análise de arquivos benignos e maliciosos e suas respectivas categorias; • Ataques de negação de serviço;	

	• Conexões de comando e controle presentes, internamente ou para a Internet; • Dispositivos que representam o maior risco; • Tempos de resposta, tráfego de entrada e saída (inbytes/outbytes); • Aplicações que consomem mais recursos de rede; • Análise de DNS (tempos de resposta, comunicação, time-out, erros e desempenho); • Identificação de aplicações da Camada 7; • Principais eventos críticos de segurança; • Monitoramento de certificado SSL; • Identificação da versão do Windows; • Ataques de adivinhação de credenciais (força bruta, password spraying).	
2.4.4-65	Suportar o protocolo HTTP/2.	
2.4.4-66	Ser capaz de detectar tráfego de rede potencialmente malicioso, como ransomware, movimentação lateral, consultas e conexões de comando e controle (C&C), mineração de criptomoedas (crypojacking), Mimikatz e outros, incluindo as que se aproveitam do tráfego RPC e SMB.	
2.4.4-67	Ser capaz de exportar de forma inteligente arquivos duplicados e limitar o comprimento das exportações, reduzindo a carga nas estruturas de análise de arquivos.	
2.4.4-68	Ser capaz de ativar monitoramento personalizado e prover extensibilidade de detecção por meio de padrões abertos.	
2.4.4-69	Ser capaz de identificar táticas e técnicas adversárias segundo o modelo MITRE ATT&CK.	
2.4.5-1	A CONTRATADA deve realizar Proteção contra Riscos Digitais (Threat Intelligence) com o monitoramento da marca e da reputação institucional na Internet, na Deep Web e na Dark Web, incluindo redes sociais, serviços de comunicação, repositórios de informação e lojas de aplicativos, identificando fraudes e golpes, conteúdo malicioso, vazamentos de dados e ameaças externas globais e com foco em Brasil, Governo e Judiciário, e providenciar Takedown em nome do TRIBUNAL mediante procuração e autorização.	

2.4.5-2	As fontes de monitoramento devem incluir, no mínimo: • Sites e serviços na internet (aberta ou superficial), na deep web (internet profunda) e na dark web (internet obscura); • Registros de domínios nacionais e internacionais, incluindo TLDs e gTLDs; • Perfis e comunidades em redes sociais e plataformas de mídias sociais, contemplando no mínimo Facebook, Instagram, Twitter, YouTube e LinkedIn, e desejável também Flickr; • Grupos, canais e comunidades em serviços de comunicação por mensagens e fóruns, contemplando no mínimo Telegram e Discord, e desejável também WhatsApp; • Repositórios e serviços de conteúdo e informação de grande abrangência, como Github e Gitlab; • Lojas de aplicativos (catálogo ou repositório de distribuição de software instalável para determinada plataforma de sistema operacional), contemplando no mínimo Google Play (Android), Apple App Store (iOS/iPadOS) e Microsoft Store (Windows), e desejável também Samsung Galaxy Store (Android) e F-Droid (Android).	
2.4.5-3	O monitoramento deve abranger conteúdo e informações em texto, mídias de imagem, áudio e vídeo, incluindo o reconhecimento e análise de texto em arquivos e bases de dados, e desejável também em imagens (Optical Character Recognition - OCR).	
2.4.5-4	O serviço deve identificar, no mínimo: • Fraudes, phishing e outros tipos de golpes, conteúdo malicioso e ameaças relacionadas; • Réplicas, conteúdos ilegítimos, abusos e violações aos serviços utilizando nome, marca e/ou logomarca institucionais do TRIBUNAL; • Typosquatting (variações de nome, permutações de caracteres e outras variantes visando erros comuns de digitação) e variações ilegítimas ou maliciosas de domínio, certificado SSL/TLS, marca institucional e outros nomes objeto do monitoramento; • Vazamento de dados, credenciais e informações de segurança e institucionais sensíveis e confidenciais;	

	• Violação de direitos de uso do TRIBUNAL ou a tentativa de burlar os meios de proteção desses direitos.	
2.4.5-5	Em caso de suspeita ou identificação de ocorrências monitoradas, a CONTRATADA deve realizar no mínimo as seguintes atividades: • Registrar e gerenciar o incidente em todo o seu ciclo de vida; • Notificar e emitir alertas, bem como confirmar eventuais suspeitas junto ao TRIBUNAL; • Comunicar a obrigação de Takedown (desativação administrativa e retirada do ar) do objeto do incidente aos administradores do seu anfitrião (host); • Acompanhar o andamento e efetivação do Takedown; • Analisar e investigar a rastreabilidade da ocorrência, visando identificar informações relevantes como autoria, linha do tempo, técnicas, meios e caminho de obtenção, exfiltração, propagação e veiculação; • Elaborar e apresentar relatórios de andamento e análise; • Monitorar a possibilidade de reincidência da ocorrência por, no mínimo, 30 (trinta) dias corridos a partir da efetivação do Takedown; • Tomar providências cabíveis em seu âmbito de atuação visando garantir a eficácia do Takedown, incluindo reiterar e obter esclarecimentos junto aos administradores do anfitrião; • Subsidiar informações ao TRIBUNAL para a criação e melhoria de controles de segurança aplicáveis para evitar ocorrências similares futuras.	
Item 2.6	GESTÃO DE VULNERABILIDADES E TESTES DE SEGURANÇA	
2.6.2.1-1	Fornecimento e sustentação de solução informatizada de Simulação de violações e ataques (Breach and Attack Simulation - BAS), composta por agentes (softwares) ou atores (simuladores virtuais), conforme exigências descritas neste documento.	
2.6.2.1-2	Os itens que compõem a Solução de BAS e seu sistema de gerenciamento devem ser produzidos pelo mesmo fabricante.	
2.6.2.1-3	Não serão aceitas ferramentas gratuitas, desenvolvidas pela, ou para, própria LICITANTE e/ou baseadas em softwares projetados para uso genérico, devendo estas serem providas por fabricantes amplamente consolidados no mercado.	

2.6.2.1-4	A solução deve contemplar a versão de software e/ou firmware mais estável e recomendado pelo fabricante.	
2.6.2.1-5	O fabricante deve possuir rede de inteligência (threat inteligence) própria da solução para atualização constante de ameaças (threat feed) de forma automática.	
2.6.2.1-6	Deve ser capaz de realizar baterias de testes de simulação de ataques baseados em bibliotecas atualizadas de ameaças e exploits, com execução imediata ou agendamentos, abrangendo infiltração de rede e aplicações web, ambos com o fluxo de ator malicioso externo para ativo-alvo interno, e endpoint, com comprometimento e exfiltração em ativo-alvo interno, estação de trabalho ou servidor, cobrindo no mínimo o sistema operacional Microsoft Windows.	
2.6.2.1-7	As simulações devem garantir ambiente controlado e sem impacto nocivo real, ou seja, não deverá trazer qualquer risco real de infectar a rede do TRIBUNAL em suas atividades.	
2.6.2.1-8	Os resultados devem validar e indicar controles de prevenção e proteção ineficazes e/ou suplantados, vulnerabilidades exploradas, caminhos de ataque e TTPs (táticas, técnicas e procedimentos) envolvidos de acordo com o framework MITRE ATT&CK.	
2.6.2.1-9	Permitir o gerenciamento centralizado da ferramenta, por meio de interface gráfica (GUI), nos formatos web segura (https) ou em formato de aplicativo cliente compatível com Windows 10 e superior, podendo ser em nuvem (cloud), appliance virtual ou por meio da própria solução.	
2.6.2.1-10	A solução deve possuir agentes (softwares) que possam ser instalados em máquinas, ou em ambientes virtuais (servidores), confeccionadas para simulação de ataques, ou apresentar atores (simuladores) virtuais, podendo ser arquivos em formato Open Virtualization Appliance (OVA), com a capacidade de criar um local próprio capaz de permitir a reprodução de ataques, além disso: • Os agentes devem ser compatíveis com sistemas operacionais Linux e Windows (Server e Professional); • Possibilitar a instalação de agentes ou máquinas OVA/ISO em ambientes de nuvem (cloud); • Permitir que os agentes possam ser removidos (desinstalados) de uma máquina ou ambiente e instalados em outro local reaproveitando uma mesma licença.	

2.6.2.1-11	Ser capaz de criar contas de usuários de forma local ou a autenticação e autorização de usuários por meio dos protocolos TACACS ou LDAP ou AD (Active Directory) ou mecanismos de autenticação e autorização utilizando credenciais corporativas no modelo de federação, usando o protocolo SAML.	
2.6.2.1-12	Ser capaz de simular ataques e validar as capacidades de prevenção e detecção para invasões em rede, gateways de web e e-mail, web application firewall (WAF), endpoints (EPP/EDR, antivírus) e Microsoft Active Directory, simular ataques em toda a cadeia de destruição cibernética (Cyber Kill Chain), incluindo infiltração, movimento lateral e exfiltração de dados, phishing, ransomwares, violações de segurança e ataques persistentes avançados (APTs).	
2.6.2.1-13	O portfólio de ameaças e ataques da solução deve ser baseado em frameworks de segurança cibernética, tais como MITRE ATT&CK, OWASP, CVSS ou NIST, e abranger todo o ciclo de ataque.	
2.6.2.1-14	Possuir portfólio de ameaças e ataques, templates ou cenários, que deverá ser atualizado continuamente contemplando ameaças atuais e emergentes, de forma manual e automática, com a opção de agendar a atualização em determinado período.	
2.6.2.1-15	Possibilitar a configuração de cenários de ataque, permitindo a seleção de quais ataques executar no teste.	
2.6.2.1-16	Permitir a criação de novas simulações de ataques e a customização destas a partir dos existentes em sua base de ameaças, de forma a permitir adaptações no comportamento e na ação dos ataques.	
2.6.2.1-17	Permitir o agendamento de simulações com a opção de execução contínua e automatizada.	
2.6.2.1-18	Possuir a instrumentação de indicadores de comprometimento (IOCs) provenientes de provedores de Threat Intelligence e/ou laboratório de inteligência de ameaça do fabricante da solução.	
2.6.2.1-19	Disponibilizar APIs (interfaces de programação de aplicações) que permitam sua integração com demais soluções de segurança do TRIBUNAL.	
2.6.2.1-20	Possuir integração com solução de monitoramento, detecção e resposta.	
2.6.2.1-21	Possuir dashboard com visualização dos resultados das simulações que retratem o nível de risco para cada fase da “Cyber Kill Chain”, baseado no MITRE ATT&CK com a possibilidade de customizar as visões apresentadas.	

2.6.2.1-22	Apresentar dados históricos de diferentes ataques simulados, bem como a visão de rastreamento.	
2.6.2.1-23	Possuir visualização por no mínimo: • Tipo de ataque simulado; • O que o artefato executou; • Data em que a simulação do ataque aconteceu; • Taxa de penetração.	
2.6.2.1-24	Permitir a realização de backup ou a opção de recuperação da solução, em caso de desastre, para no mínimo as configurações da solução de BAS.	
2.6.2.1-25	Podendo ser funcionalidade não disponível para o cliente, realizado sob demanda junto ao fabricante.	
2.6.2.1-26	Possuir registros que identifiquem o histórico completo de acessos (logins) e ações, por cada usuário ou grupo de usuários, incluindo as contas administrativas e com privilégios, podendo ser apresentado por meio de relatórios ou através de APIs ou scripts.	
2.6.2.1-27	Ter a opção de gerar relatórios após cada avaliação comparando com o resultado de testes anteriores, mostrando as vulnerabilidades mais críticas.	
2.6.2.1-28	Permitir exportar relatórios para formatos PDF e CSV.	
2.6.2.1-29	Apresentar relatório detalhando a ação do ataque simulado.	
2.6.2.1-30	Possuir capacidade de entregar relatório ou disponibilizar por meio de interface gráfica informações da sequência de execução do artefato malicioso, baseado na matriz do MITRE ATT&CK, bem como detalhar as alterações na máquina local e conexões externas executadas durante a simulação.	
2.6.2.1-31	Permitir exportar os logs da solução BAS, via API ou conectores, para a solução de SIEM.	
2.6.2.1-32	Não serão aceitas ferramentas gratuitas, desenvolvidas pela, ou para, própria LICITANTE e/ou baseadas em softwares projetados para uso genérico, devendo estas serem providas por fabricantes amplamente consolidados no mercado.	
2.6.2.1-33	Possibilitar a execução ilimitada de todos os vetores de simulação disponíveis pela plataforma durante a vigência do mesmo.	

2.6.2.1-34	Possuir base ampla de recomendação de remediação possibilitando visualizar ações de correção, redução do impacto da vulnerabilidade/ataque e prevenção alinhados com as recomendações específicas dos fabricantes de elementos de segurança.	
2.6.2.1-35	A solução deve possuir atualização diária da base de malwares.	
2.6.2.1-36	Possuir simulações de campanhas de ameaças, com link para o relatório da identificação e descrição da ameaça em campo, descrevendo seus impactos e identificando as regiões do mundo afetadas pela campanha.	
2.6.2.1-37	Ser capaz de criar incidentes de forma manual e automática por meio de integrações com o SIEM.	
2.6.2.1-38	Possuir as seguintes opções para o formato do registro da hora dos eventos gerados com a integração do EDR: ISO 8601, UTC segundos, UTC milisegundos e UTC nanosegundos.	
2.6.2.1-39	Permitir customização de simulação de campanhas de ameaças, utilizando no mínimo os seguintes IOCs: hash de arquivos, nome do host, URLs e endereços IPv4.	
2.6.2.1-40	Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado, adotando como referência de mercado estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC, ISG Group.	
Item 2.7	GESTÃO DE IDENTIDADE	
2.7.1-1	Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado, adotando como referência de mercado estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC, ISG Group.	
2.7.1-2	A solução não deverá possuir EOL (End-of-life) e EOS (End-of-support) anunciados para um prazo superior a 36 meses.	
2.7.1-3	A solução poderá ser ofertada em ambiente de nuvem, em appliance virtual (virtualizado sob a plataforma VMware) ou appliance físico composto de hardware e software devidamente licenciado pela CONTRATADA.	
2.7.1-4	A solução deve possuir ferramenta de monitoração própria para que seja possível especificar limiares (thresholds) referente ao uso	

	de memória, CPU, disco e banco de dados, e demais interações por meio do protocolo proprietário ou aberto (SNMP).	
2.7.1-5	Independente do modelo adotado, será necessário proporcionar uma retenção dos logs de até 180 dias, com gravações na ordem de 8 horas/dia, 5 dias por semana, no mínimo.	
2.7.1-6	A solução deve apoiar, no mínimo, os requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como: • Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento; • Proteger o acesso a dados pessoais sensíveis; • Responsabilizar pessoal e responder a incidentes; • Aplicar boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados.	
2.7.1-7	Apoiando os requisitos da LGPD, a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas-alvo diversos do ambiente.	
2.7.1-8	A solução deverá monitorar sessões, gravar, detectar, correlacionar e mitigar todos os comportamentos anormais de, pelo menos, 80 (oitenta) usuários administrativos simultâneos, acessando todos os sistemas-alvo do ambiente tecnológico, dentre eles Servidores Linux/Unix e Windows, banco de dados, appliances e demais ativos de rede e sistemas computacionais diversos.	
2.7.1-9	A solução deve atender no mínimo os sistemas-alvo os baseados nas seguintes tecnologias: • Sistemas Operacionais Linux/Unix e Microsoft Windows; • Microsoft Hyper-V e VMWare; • Contas de usuários de sistemas e de serviço; • Credenciais do Microsoft COM+, IIS;	

	• Apache TomCat, RedHat Jboss, Wildfly, Nginx; • Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP; • Contas de usuários e administradores de bancos de dados Microsoft SQL Server, PostgreSQL, MySQL; • Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) - switches, roteadores, balanceadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage); • Contas de usuários e administradores de consoles de gerenciamento de servidores; • Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo; • Credenciais de nuvem em VMWare ESXi, Azure, AWS, GCP, Microsoft 365.	
2.7.1-10	A solução deverá realizar a gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, monitoramento e gravação de sessões privilegiadas.	
2.7.1-11	A solução deverá conceder acesso aos sistemas utilizando “Remote Desktop” e “SSH”, disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no S.O. do servidor de destino, possibilitando habilitar gravação da sessão, caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino.	
2.7.1-12	A solução deve permitir integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando no mínimo as seguintes funcionalidades: • Integração e gestão de acessos privilegiados em contas de serviços em nuvem;	

	• Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e Gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem.	
2.7.1-13	A solução deve possuir as sessões administrativas acessadas e monitoradas em tempo real, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada e possibilitando pesquisar ações específicas na sessão gravada.	
2.7.1-14	A solução deve proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios.	
2.7.1-15	A solução deve ser capaz de descobrir e alterar credenciais Microsoft Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, exibindo em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento.	
2.7.1-16	A solução deve gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado.	
2.7.1-17	A solução deve possuir funcionalidades de “AD Bridge” para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD.	
2.7.1-18	A solução deve provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente.	

2.7.1-19	A solução deve permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características: • Permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável; • Permitir a aprovação perante um agendamento de ações administrativas.	
2.7.1-20	Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução.	
2.7.1-21	Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas.	
2.7.1-22	A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP.	
2.7.1-23	A solução deve oferecer em sua console de gerenciamento diferentes visões e opções de acordo com as permissões dos usuários.	
2.7.1-24	A solução deve suportar métodos para registrar e relatar qualquer ação realizada, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail e integração com SIEM.	
2.7.1-25	Permitir o envio automático de logs para servidores syslog, de forma aderente ao disposto em RFC 5424 - The Syslog Protocol (IETF).	
2.7.1-26	A solução deve registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkouts, mudanças de delegação, relatórios e outras atividades, incluindo: • Registros de acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas; • Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários; • Alterações nas funções de delegação; • Adições, deleções e alterações de senhas gerenciadas pela solução;	

	• Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas; • Relatórios filtrados por período, tipo de operação, sistema, gerente e outros critérios.	
2.7.1-27	A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como: • Lista de sistemas gerenciados; • Senhas armazenadas/Contas gerenciadas; • Eventos de alteração de senha; • Permissões de acesso web; • Auditoria de contas, sistemas e usuários.	
2.7.1-28	A solução deve realizar análise comportamental e mitigação de risco no ambiente crítico para Identidades Privilegiadas.	
2.7.1-29	A solução deverá realizar a identificação e o correlacionamento de ações, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros) do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução.	
2.7.1-30	A solução deve identificar e combinar ações que caracterizam abusos, montando perfis de comportamento anormal e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas, tais como, nova autenticação, suspensão e encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo: • Acesso privilegiado à solução durante horários irregulares. Detectado quando um usuário recuperar uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental; • Acesso privilegiado à solução durante dias irregulares. Detectado quando um usuário recuperar uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental; • Acesso excessivo a contas privilegiadas. Detectado quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental; • Acesso privilegiado à solução através de IP irregular ou desconhecido. Detectado quando um usuário acessa contas	

	privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental; • Acesso privilegiado não gerenciado. Detectado quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução; • Máquina acessada a partir de endereços IP incomuns; • Máquina acessada durante horários irregulares. Detectado quando uma máquina é acessada em um horário irregular, de acordo com seu padrão de utilização; • Acessos excessivos a uma máquina; • Acesso anômalo a várias máquinas. Detectado quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto; • Máquina incomum originando acesso; • Usuário incomum logando de uma máquina de origem conhecida; • Suspeita de roubo de credenciais. Detectado quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução; • Alteração de senha suspeita. Detectado quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução; • Atividades suspeitas detectadas durante uma sessão privilegiada. Detectado quando é identificada uma sessão privilegiada com atividades (comandos e anomalias na solução) definidas como suspeitas. Para atendimento do item acima, poderão ser utilizados recursos integrados às soluções do Item 2.4 MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTAS A INCIDENTES DE SEGURANÇA.	
2.7.1-31	A solução deverá permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador.	
2.7.1-32	Ser capaz de, durante o processo de definição da política de composição de senha:	

	• Gerar senhas aleatórias com extensão de 127 (cento e vinte e sete) caracteres ou mais; • Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos; • Especificar qual o tipo de caractere na composição das senhas a serem geradas; • Implementar controle de acesso baseado em papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada; • Deve permitir a formação de grupos de usuários e dispositivos, bem como a atribuição de privilégios de acesso a esses grupos, onde esses privilégios de acesso possam ser atribuídos por critérios como tipo de dispositivo, sistemas operacionais, banco de dados e aplicativos de virtualização; • Garantir que a senha gerada seja diferente do nome da conta correspondente. Exemplo: se a credencial ou conta tem o nome "Administrador" a senha gerada jamais pode ser composta da mesma forma; • Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha.	
2.7.1-33	Realizar automaticamente a descoberta, detecção, importação e armazenamento no repositório seguro de chaves SSH em sistemas Linux, implementando: • Suporte a chaves criptográficas nos tamanhos 1024, 2048, 4096; • Auditoria e controle dos acessos às chaves por sistema de aprovações; • Reconciliação de chaves, renovando-as e armazenando-as novamente; • Conexão transparente a ativos da rede utilizando as chaves armazenadas; • Gerenciamento em grupos, permitindo que múltiplas máquinas herdem a mesma chave SSH.	
2.7.1- 34	Possibilitar colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador.	
2.7.1-35	Permitir o encerramento automatizado da sessão em caso de detecção de atividade suspeita de alta criticidade.	

2.7.1-36	Fornecer meio de integração para que soluções de terceiros também possam encerrar sessões suspeitas (ex: SIEM executa terminação de sessão).	
2.7.1-37	Criar relatórios que podem ser exportados em pelo menos um dos formatos editáveis: HTML, CSV, XLSX ou XLS.	
2.7.1-38	A solução deverá disponibilizar: • Mecanismo de retirada e devolução de contas e senhas compartilhadas; • Definição de tempo de validade, permitindo o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas; • Troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido; • Troca de senhas por demanda, permitindo a troca de senhas nos sistemas gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (grupo de todos os sistemas operacionais UNIX, por exemplo).	
2.7.1-39	Suportar, através da interface Web para acesso e recuperação das senhas, de forma nativa, a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução.	
2.7.1-40	A solução deve fornecer dados ad-hoc agendados, relatórios em tempo real dos usuários, contas, configuração da solução e informações sobre os processos da solução.	
2.7.1-41	Permitir que os comandos executados em sistemas Linux monitorados sejam gravados em modo texto.	
2.7.1-42	Permitir, através de interface gráfica, que administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.	
2.7.1-43	Suportar em sua interface web e de administração métodos autenticação de duplo fator, compatíveis com os métodos a seguir: • Algoritmo de One-time Password, com pelo menos um dos aplicativos: Google Authenticator, Oauth, Authy, YubioAth, RSA SecureID, SAASPASS e 1Password;	

	• Smart cards; • Tokens em geral; • Certificados Digitais.	
2.7.1-44	Possuir interface única, na mesma solução, para o gerenciamento de senhas e sessões.	
2.7.1-45	A solução deverá prover mecanismos de atualização de segurança sob demanda e com rastreabilidade dos pacotes instalados por meio de interface gráfica intuitiva (desejável).	
2.7.1-46	A solução não deve depender da instalação de agentes para realizar a troca de senhas e gravação de sessão.	
2.7.1-47	A solução deve ter uma console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas.	
2.7.2-1	A solução deverá possuir mecanismo de segurança que mantenha a entrega de credenciais em caso de queda da rede ou parada total do cofre digital, evitando assim a parada de aplicações críticas.	
2.7.2-2	Utilizar banco de dados em alta disponibilidade, para armazenamento de credenciais, com as melhores práticas de segurança e mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução.	
2.7.2-3	Todos os elementos que compõem a solução, devem ser instalados em regime de alta disponibilidade.	
2.7.2-4	Caso a solução seja na mobilidade on-premisse, a solução deve replicar as configurações em 02 (duas) localidades, de modo que, no evento de falha total de seus elementos instalados em uma localidade, a solução continue disponível via uso dos elementos da outra localidade, com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação.	
2.7.2-5	Todos os sistemas e recursos necessários para operação do módulo de cofre de senhas, deverão ser passíveis de plena utilização a partir de uma única localidade (site), em caso de contingência.	
2.7.2-6	Em caso de utilização de ambiente on-premisse, tanto os appliances virtuais quanto sistemas operacionais da solução devem ser “hardenizados” e protegidos com firewall interno.	

2.7.2-7	Deve permitir o backup e restore de seu banco de dados, bem como das configurações de software estabelecidas.	
2.7.2-8	Deve permitir a execução de tarefas de backup e criptografia sem a necessidade de agentes de terceiros ou parada do ambiente ou comprometimento de qualquer funcionalidade, provendo assim o maior nível possível de segurança e integridade dos dados a serem copiados.	
2.7.2-9	Deve permitir a execução de Backups automatizados, permitindo a programação/agendamento de horários e configuração de locais para seu armazenamento local e remoto.	
2.7.2-10	Deve ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (cofre), por meio de backup ou método análogo, para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas e dados gerenciados pela solução.	
2.7.2-11	Ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos.	
2.7.2-12	Ainda que as gravações estejam armazenadas em locais diferentes, a solução deve permitir que essas evidências sejam consultadas a partir de qualquer console web instalada, de maneira centralizada.	
2.7.2-13	A solução deve ser disponibilizada com um SDK (Software Development Kit) que pode ser configurado para permitir que aplicações possam: • Atualizar informações de contas automaticamente no banco de dados de senhas; • Alterar senhas em texto-claro incorporados em aplicações de uma forma segura no banco de dados de senhas; • Solicitar as credenciais sob demanda via REST ou SOAP ao invés de utilizar credenciais estáticas; • Deverá integrar-se nativamente ao cofre digital da solução, utilizando sua mesma interface web.	
2.7.2-14	Deve possuir REST APIs detalhadamente documentadas no website do fabricante, estas APIs devem fornecer minimamente as funcionalidades de gestão das identidades, grupos e perfis, gestão de métodos de MFA, gestão de aplicações web, gestão de senhas,	

	gestão do portal dos usuários finais e autenticação de usuários finais utilizando os métodos de MFA oferecidos.	
2.7.2-15	A solução deverá fornecer credenciais tanto por meio de acesso interativo via interface da solução na rede quanto por integração programática via APIs (Webservice).	
2.7.2-16	O uso de agente deve permitir instalação em múltiplos servidores web dos sistemas gerenciados pela solução, sem necessidade de aquisição de licenças, visando fornecer a melhor adaptação à arquitetura do CONTRATANTE.	
2.7.2-17	Deverá manter um cache atualizado das credenciais utilizadas localmente no servidor da aplicação, a fim de prevenir falhas na comunicação com o cofre digital e trazer velocidade às consultas.	
2.7.2-18	Deverá suportar a utilização de executável para scripts e aplicações nativas em plataforma Windows.	
2.7.2-19	Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em comandos Linux, comandos, janelas e aplicações Windows, Expressões regulares para comandos em geral e Eventos configurados manualmente, permitindo a atribuição de nível de risco customizado.	
2.7.2-20	Caso a solução fornecida faça uso das funcionalidades disponibilizadas pelas CALs (Client Access License) do serviço Microsoft Remote Desktop Services (RDS) para acessos através da mesma, a CONTRATANTE irá disponibilizar tal Infraestrutura, para que não seja afetada a experiência dos usuários.	
2.7.2-21	Permitir a opção de implementar o gerenciamento de troca de senhas em redes segregadas e remotas a fim de acomodar links de alta latência, redes isoladas (DMZ) e outras restrições semelhantes.	
2.7.2-22	A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, WMI, SSH e HTTP/HTTPS.	
2.7.2-23	Integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas.	
2.7.2-24	Permitir o agrupamento lógico de credenciais, obedecendo uma hierarquia, a fim de simplificar a configuração e aplicação de políticas apropriadas para diferentes tipos de sistemas alvo, além	

	de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas.	
2.7.2-25	Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e realizar verificações agendadas e automáticas, a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino correspondam às mesmas senhas armazenadas no banco de dados da solução. Caso a senha da conta gerenciada pela solução seja diferente daquela armazenada no banco de dados, a solução deve ser capaz de gerar relatórios e alertas notificando este evento.	
2.7.2-26	A solução deve conter meios de acessar os vídeos de gravações, incluindo: • Filtrar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado; • A função de gravação de sessões, devendo realizar o isolamento de sessões de acesso, atuando como um proxy/servidor de salto entre a máquina do usuário e o ativo a ser acessado.	
2.7.2-27	Permitir que os usuários solicitem acesso aos gestores através de interface web intuitiva.	
2.7.2-28	Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma.	
2.7.2-29	Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dasboards, filtros e gráficos configuráveis, sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos.	
2.7.2-30	Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores.	
2.7.2-31	Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo: • E-mail com conteúdo do alerta; • Envio de alerta para solução SIEM.	

2.7.2-32	Possuir dashboards pré-configurados com informações e gráficos com as seguintes características: • Comportamento dos usuários na utilização das aplicações; • Visão sobre a segurança das aplicações; • Mapa com a geolocalização das autenticações; • Visão sobre o comportamento dos endpoints (Mobile e Computadores); • Visão sobre o comportamento das Identidades.	
2.7.2-33	A solução deve permitir a configuração de dashboards personalizados.	
2.7.3-1	A solução deve prover proteção e gerenciamento de secrets que atenda as demandas de segurança de credenciais e suas subcategorias, onde entende-se como secrets uma estrutura de dados que possa conter senhas, chaves privadas, tokens e chaves de APIs e ser entregue de maneira segura e criptografada para aplicações, contêineres e serviços.	
2.7.3-2	Deve criptografar todas as chaves privadas SSL utilizadas por quaisquer serviços da solução, ou utilizadas na criptografia da base de dados evitando que sejam armazenadas em texto claro no sistema de arquivos. A criptografia deve ocorrer antes da escrita em armazenamento persistente, evitando que informações sejam comprometidas em caso de acesso aos dados. Deve permitir que a chave master de criptografia seja armazenada e provida por soluções de HSM.	
2.7.3-3	A solução deverá atuar como gerador e intermediário (broker) de secrets para diversos clientes, como aplicações, contêineres e clientes de criptografia e possibilitar o armazenamento de múltiplas versões de um mesmo secret. O fornecimento de secrets deve oferecer meios de controle de solicitante com múltiplos fatores, incluindo minimamente Tempo de vida (TTL) e restrições de IP/range.	
2.7.3-4	Os secrets devem ser modificáveis, com base em critérios de tempo de uso (Lease time) ou expiração, sendo que após expiração, a rotação ocorre de acordo com políticas definidas no sistema. Todo secret deve conter por padrão, pelo menos duas listas de acesso com papéis/grupos que podem ler o secret e que podem alterar o secret.	
2.7.3-5	Todos os registros de eventos de segurança como autenticação de clientes, solicitação de secrets, revogação de secrets, acesso de	

	usuários, aplicações ou clientes a secrets, mudanças de permissão, deverão ser armazenados de maneira que impossibilite a sua alteração e se mantenha a correta integridade das evidências.	
2.7.3-6	As operações com secrets devem gerar trilha de auditoria contendo, no mínimo a identificação do cliente (usuário ou usuário sistêmico), a identificação do secret, horário (Timestamp completo), ação (leitura ou alteração) e se a ação foi permitida ou não.	
2.7.3-7	Deve utilizar definição de papéis (RBAC) para autorização de identidades de usuários e de aplicações onde possam ser definidos e relacionados entre si quando possível para usuários, grupos de usuários, usuários sistêmicos (máquinas, serviços e processos) e grupos de usuários sistêmicos.	
2.7.3-8	Todas as operações envolvendo usuários e grupos sistêmicos e não-sistêmicos, políticas e secrets, incluindo a criação, leitura e alteração, devem ser feitas via linguagem aberta de serialização YAML.	
2.7.3-9	A obtenção de secrets deve ser permitida por diversos meios, incluindo, pelo menos, linha de comando (CLI) e RestAPI. Os secrets deverão ser disponibilizados unicamente para as aplicações ou serviços que os consomem, sendo que em hipótese alguma, devem ser disponibilizados no nível do sistema operacional ou “namespaces” acessíveis por outras aplicações.	
2.7.3-10	A solução deverá guardar e rotacionar os secrets no repositório central de credenciais da solução, sem necessidade de criação de novo ambiente de administração de credenciais, mantendo os mesmos requisitos de segurança já definidos para aquela solução.	
2.7.3-11	Deve oferecer recursos de redundância, alta disponibilidade e suporte a balanceamento de carga se utilizando da infra-estrutura disponibilizada pela CONTRATANTE. A alta disponibilidade deve conter funcionalidade de replicação automática entre as bases da solução, oferecendo pelo menos 2 réplicas. O conjunto de réplicas deve oferecer funcionalidade de Failover automático, onde uma das réplicas assumirá a operação em caso de problemas. Deve haver funcionalidade de backup seguro do conteúdo armazenado e configurações do produto, possibilitando a prática de Disaster Recovery.	
2.7.3-12	Para que não haja sobrecarga nem exposição do repositório central da solução e suas redundâncias, a solução deve oferecer componentes que absorvam a carga de requisições. Esses	

	componentes devem agregar capacidade de requisições por segundo de maneira quantitativa ao total da solução.	