PODER JUDICIÁRIO DO ESTADO DO ESPÍRITO SANTO - PJES

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

FORMULÁRIO VI - NP 09 - PROJETO BÁSICO / TERMO DE REFERÊNCIA (AQUISIÇÃO DE BENS/PRESTAÇÃO DE SERVIÇOS DE INFORMÁTICA)

Termo de Referência de TIC Nº 46/2024 - SECRETARIA DE TECNOLOGIA DA INFORMACAO

Em 23 de agosto de 2024.

SUMÁRIO

1. EQUIPE RESPONSÁVEL PELA ELABORAÇÃO

1.1. Unidade Demandante:

Secretaria de Tecnologia da Informação

1.2. Equipe de Planejamento da Contratação:

Integrante Demandante:	Marcianne Ribeiro Antunes Lima	Matrícula:	211.113-41
E-mail do Integrante Demandante:	mrlima@tjes.jus.br	Telefone:	(27) 3357-4511
Integrante Técnico:	Havirdan Das Rodor Araújo	Matrícula:	209.745-31
E-mail do Integrante Técnico:	hdaraujo@tjes.jus.br	Telefone:	(27) 3357-4511
Integrante Administrativo	Vinícius Milere Moreira	Matrícula:	209.614-44
E-mail do Integrante Administrativo:	vmmoreira@tjes.jus.br	Telefone:	(27) 3357-4513

1.3. Contratante:

Poder Judiciário do Estado do Espírito Santo – PJES
CNPJ (MF): 27.476.100/0001-45
Inscrição Estadual: Isento
Inscrição Municipal: Isento
Nome Fantasia: Tribunal de Justiça do Estado do Espírito Santo
Rua Desembargador Homero Mafra, nº 60, Enseada do Suá - CEP 29050-906 - Vitória – ES

2. OBJETO DA CONTRATAÇÃO

Contratação de licença de subscrição de software de proteção contra ameaças avançadas (NGAV) com suporte técnico (atualização de versão e assistência técnica) pelo período de 36 meses, além de implantação, migração das políticas e configurações da solução atualmente utilizada e treinamento para administração da solução.

ITEM	DESCRIÇÃO	CATSER	Qtd

ITEM	DESCRIÇÃO	CATSER	Qtd
1	Subscrição de software de proteção para endpoint (desktops)	27502	6590
2	Subscrição de software de proteção para endpoint (servidores físicos e virtuais)	27502	160
3	Serviços de planejamento, configuração, migração e transferência de conhecimento de softwares, a fim de definir os padrões de utilização, as configurações básicas, e transferência de conhecimento para sua utilização.	26972	1
4	Treinamento para administração e configuração de software de proteção endpoint	3840	1

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. MOTIVAÇÃO:

Diante das ameaças cibernéticas cada vez mais sofisticadas, a proteção de endpoints tornou-se um aspecto crítico para grandes corporações. A solução atualmente em produção no PJES, definida como EPP (Endpoint Protection Platform), desempenha um papel fundamental na proteção dos dispositivos finais, como computadores e smartphones, contra uma ampla gama de ameaças, incluindo malware, vírus e exploits. As funcionalidades do EPP abrangem antivírus, firewalls, controle de dispositivos e técnicas de mitigação de ataques, com o objetivo de prevenir, detectar e bloquear tanto ameaças conhecidas quanto desconhecidas.

No entanto, à medida que as ameaças evoluem, as soluções de proteção de endpoint também devem se adaptar. As tecnologias que eram eficazes no passado podem não ser suficientes para enfrentar os desafios atuais e futuros. A solução atualmente em uso no PJES, embora tenha servido bem até agora, não inclui alguns dos métodos mais recentes de combate a ameaças que são essenciais para manter a segurança em um ambiente corporativo em constante mudança.

Para garantir que o ambiente tecnológico do PJES esteja protegido contra os milhares de vírus já existentes, bem como contra as novas ameaças que surgem mensalmente, é imprescindível que a organização adote uma solução de proteção de endpoint mais avançada. Isso inclui a incorporação de novas técnicas de segurança, como a detecção baseada em inteligência artificial e machine learning, proteção contra ameaças persistentes avançadas (APTs) e resposta automatizada a incidentes. Essas inovações não apenas fortalecem a defesa contra ameaças, mas também asseguram a continuidade dos serviços prestados pela Secretaria de Tecnologia da Informação (STI), maximizando a segurança do ambiente computacional do PJES.

Com a iminente expiração do contrato atual, em 08/02/2025, é necessária a realização de um novo procedimento licitatório para a contratação de uma solução de proteção de endpoint que inclua essas novas capacidades. A solução em uso, Symantec Endpoint Protection, adquirida em 2005, teve seu suporte e atualização prorrogados emergencialmente, mas está agora defasada frente aos requisitos de segurança modernos.

Além de garantir a atualização tecnológica, a realização de um certame de disputa aberta para a seleção das novas ferramentas de segurança pode propiciar economia significativa para o PJES. Em um processo competitivo, diferentes fornecedores poderão apresentar propostas, o que tende a reduzir os custos, pois as empresas competem para oferecer a melhor solução pelo menor preço. Essa competição saudável não só aumenta as chances de contratar uma ferramenta que atenda a todos os requisitos técnicos e de segurança, mas também assegura que o investimento público seja utilizado de maneira eficiente, alcançando o melhor custo-benefício possível.

Após nove anos de uso contínuo da solução atual, a Secretaria de Tecnologia da Informação decidiu realizar esse novo certame para garantir que o PJES esteja adequadamente preparado para enfrentar as ameaças cibernéticas atuais e futuras, protegendo a integridade de suas operações e dados sensíveis, enquanto também otimiza o uso dos recursos financeiros disponíveis.

3.2. ALINHAMENTO ESTRATÉGICO:

[ ] Elevar a produtividade do Poder Judiciário	[ ]	Gerenciar e adequar recursos tecnológicos de forma a maximizar sua utilização para uma melhor produtividade
[ ] Gerenciar as demandas repetitivas de grandes litigantes		
[ ] Implantar a governança de TI	[ ]	Implantar o Gerenciamento de Processos
	[ ]	Implantar o Gerenciamento de Projetos
	[ ]	Implantar o Gerenciamento de Serviços de TI
	[ ]	Contratar o serviço de suporte técnico – Service Desk
	[ ]	Implantar o Gerenciamento de Segurança da Informação
	[ ]	Reestruturar a STI – Recursos humanos e Estrutura organizacional
[ ] Implantar a gestão de custos	[ ]	Implantar um sistema informatizado de Gestão de Custos
[ ] Otimizar e incrementar as possibilidades de acesso à justiça	[ ]	Estruturar e unificar o sistema virtual de acesso à justiça
[x] Assegurar sistemas e infraestrutura de TI adequados	[x]	Atualizar o parque tecnológico
	[ ]	Implantar projeto Datacenter backup visando a Gestão de Continuidade de Negócio
	[ ]	Adquirir e Implantar um Sistema Integrado de Gestão Administrativa
	[ ]	Convergir e integrar os sistemas legados
	[ ]	Implantar o Processo Judicial Eletrônico
	[ ]	Implantar sistema de diárias e suprimento de fundos
	[ ]	Integração dos sistemas de folha de pagamento, almoxarifado, patrimônio e contábil
	[ ]	Melhoria do sistema de controle de contratos e inclusão do controle de convênios e termos congêneres

3.3. ESTUDOS PRELIMINARES:

O presente documento é derivado dos estudos realizados disponíveis em Estudo Técnico Preliminar (nº SEI 2242748).

3.4. DEMANDA PREVISTA:

Itens	Descrição
1	Subscrição de Software de Proteção para Endpoint (estações de trabalho, dispositivos móveis, servidores físicos e ambientes virtuais)
2	Subscrição de Software de Proteção para Endpoint (servidores físicos e ambientes virtuais)
3	Serviços de Planejamento, Configuração, Migração e Transferência de Conhecimento de Softwares, a fim de definir os padrões de utilização, as configurações básicas, e transferência de c
4	Treinamento para Administração e Configuração de Software de Proteção Endpoint

3.5. ANÁLISE DE PROJETOS SIMILARES REALIZADOS PELA ADMINISTRAÇÃO PÚBLICA E JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO:

Em um cenário onde um órgão público possui mais de 7.000 desktops, a contratação de uma solução de proteção de endpoints não apenas se justifica por si só, mas também é uma prática comum e essencial para a manutenção da segurança cibernética. Neste contexto, a implementação de soluções de proteção de endpoints é amplamente reconhecida como uma medida básica e necessária, fazendo parte do escopo regular de serviços de segurança que qualquer organização de grande porte deve providenciar.

Importância da Proteção de Endpoints:

A proteção de endpoints envolve a defesa de dispositivos que se conectam à rede, como desktops, laptops e servidores, contra uma variedade de ameaças, incluindo malware, ransomware, phishing e ataques direcionados. Em um órgão público com milhares de dispositivos conectados, a superfície de ataque é vasta, o que aumenta significativamente o risco de incidentes de segurança. A ausência de proteção adequada poderia resultar em brechas de segurança que poderiam comprometer dados sensíveis, interromper operações críticas e até mesmo violar legislações específicas sobre proteção de dados.

Práticas Comuns e Normativas Relevantes:

A contratação de soluções de proteção de endpoints é uma prática corriqueira em organizações de grande porte, particularmente em órgãos públicos que gerenciam grandes volumes de dados e necessitam de conformidade com diversas regulamentações. As boas práticas para a gestão de segurança cibernética em órgãos públicos incluem:

- **Gestão de Riscos e Conformidade**: Identificar e gerenciar riscos de segurança cibernética é crucial. Órgãos públicos devem seguir normas como a ISO/IEC 27001, que fornece requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação.
- **Plano de Resposta a Incidentes**: Ter um plano de resposta a incidentes é essencial. Esse plano deve incluir a capacidade de detectar, responder e mitigar ataques que possam comprometer a integridade dos endpoints.

Regulações e Legislação Pertinente

Várias regulamentações reforçam a necessidade de proteger endpoints em ambientes públicos:

- **Lei Geral de Proteção de Dados (LGPD)**: No Brasil, a LGPD impõe obrigações rigorosas sobre a proteção de dados pessoais, o que inclui a necessidade de proteger endpoints que armazenam ou processam esses dados.
- **Normas do Tribunal de Contas da União (TCU)**: O TCU exige que os órgãos públicos adotem práticas adequadas de segurança da informação, o que abrange a proteção de endpoints.
- **Marco Civil da Internet**: Embora focado principalmente na proteção de dados e privacidade online, o Marco Civil também reforça a necessidade de segurança cibernética em organizações públicas.

Abaixo, estão listadas contratações similares ao do objeto:

Identificação	Número do Item	Modalidade	CATSER	Quantidade Ofertada	Fornecedor	Órgão	UASG - Unidade Gestora	Data da Compra
00035/2023	00001	Pregão	27502	1.300	BRASOFTWARE INFORMATICA LTDA	TRIBUNAL DE CONTAS DO ESTADO DE RONDONIA	935002 - TRIBUNAL DE CONTAS DO ESTADO DE RONDONIA	21/11/2023
00977/2023	00001	Pregão	27502	1.100	CYBER WAN TECNOLOGIA LTDA	ESTADO DO RIO DE JANEIRO	986001 - PREFEITURA MUNICIPAL DO RIO DE JANEIRO	20/12/2023
00010/2023	00001	Pregão	27502	700	BRASOFTWARE INFORMATICA LTDA	TRIBUNAL DE CONTAS DO EST. DO ESPIRITO SANTO	925398 - TRIBUNAL DE CONTAS DO EST. DO ESPIRITO SANTO	27/10/2023
00011/2023	00003	Pregão	27502	10.000	SERVICE IT SECURITY LTDA.	FUNDACAO OSWALDO CRUZ	254420 - FUNDACAO OSWALDO CRUZ/RJ	25/04/2023
00010/2023	00001	Pregão	27502	700	QUALITEK TECNOLOGIA LTDA	TRIBUNAL DE CONTAS DO EST. DO R.G. DO NORTE	925468 - TRIBUNAL DE CONTAS DO EST.DO R.G. DO NORTE	16/08/2023
00012/2023	00001	Pregão	27502	4.520	SERVICE IT SECURITY LTDA.	COMISSAO NACIONAL DE ENERGIA NUCLEAR	113201 - SAE-CNEN-COMIS.NACIONAL DE ENERGIA NUCLEAR/RJ	06/12/2023
00012/2023	00002	Pregão	27502	175	SERVICE IT SECURITY LTDA.	COMISSAO NACIONAL DE ENERGIA NUCLEAR	113201 - SAE-CNEN-COMIS.NACIONAL DE ENERGIA NUCLEAR/RJ	06/12/2023
00011/2023	00001	Pregão	27502	14.600	SERVICE IT SECURITY LTDA.	FUNDACAO OSWALDO CRUZ	254420 - FUNDACAO OSWALDO CRUZ/RJ	25/04/2023
00007/2023	00001	Pregão	27502	150	ESTRATEGIA IT LTDA	CONSELHO FEDERAL DE PSICOLOGIA	389476 - CONSELHO FEDERAL DE PSICOLOGIA	11/05/2023
00007/2023	00002	Pregão	27502	32	ESTRATEGIA IT LTDA	CONSELHO FEDERAL DE PSICOLOGIA	389476 - CONSELHO FEDERAL DE PSICOLOGIA	11/05/2023
00011/2023	00002	Pregão	27502	830	SERVICE IT SECURITY LTDA.	FUNDACAO OSWALDO CRUZ	254420 - FUNDACAO OSWALDO CRUZ/RJ	25/04/2023

3.6. AVALIAÇÃO DO AMBIENTE PARA VIABILIZAR A CONTRATAÇÃO:

A troca de uma solução de EPP por outra, ainda que de fornecedores diferentes, envolve principalmente a substituição de agentes e a reconfiguração das políticas de segurança. Dado que os princípios básicos de proteção de endpoints permanecem os mesmos (detecção de malware, firewall, controle de dispositivos, etc.), a transição entre soluções não exigirá uma mudança radical na arquitetura ou na operação diária.

4. REQUISITOS DA CONTRATAÇÃO

4.1. REQUISITOS TÉCNICOS ESPECÍFICOS ITEM 1 e 2 (SUBSCRIÇÃO DE SOFTWARE DE PROTEÇÃO PARA ENDPOINT)

4.1.1. A solução deve ser compatível com Microsoft Windows 10 e versões posteriores (e suas edições), para estações de trabalho;

4.1.2. A solução deve ser compatível com Docker e Amazon EKS para proteger os containers;

4.1.3. A solução deve ser compatível com as seguintes distribuições/versões de sistema operacional Linux:

- Red Hat Enterprise 8.x e superiores, 64bits;

- SUSE Linux Enterprise Server 12.x e superiores, 64bits;
- Ubuntu 18.04 e superiores, 64bits;
- CentOS 7.x e superiores, 64bits;
- Oracle Linux 7.x e superiores, 64bits.

4.1.4. A solução deve ser compatível com Microsoft Windows Server 2016 e versões posteriores (e suas edições);

4.1.5. A solução deve ser compatível com MacOS;

4.1.6. A solução deve ser compatível com dispositivos Android, versão 13 e superiores.

4.1.7. Deve possuir mecanismo de atualização em rede local para otimização do uso de banda de internet;

4.1.8. Deve suportar e possuir agente para máquinas virtuais instaladas em ambiente VMware;

4.1.9. Deve permitir a comunicação entre os endpoints e a plataforma de gerenciamento através de filtro web;

4.1.10. Deve permitir a coleta de indicadores para IoC (Indicator of Compromise);

4.1.11. Proteção contra desinstalação não autorizada dos agentes de endpoint que compõem a solução;

4.1.12. Proteção contra a desativação não autorizada dos serviços que compõem a solução;

4.1.13. Ser eficaz na prevenção de vulnerabilidades e malwares mesmo quando estiver sem conectividade com servidores de gerenciamento e/ou recursos baseados em nuvem;

4.1.14. O agente de endpoint deve continuar funcionando e aplicando políticas de controle mesmo se houver interrupção da comunicação com o gerenciamento centralizado;

4.1.15. Impedir executável malicioso, sem requerer nenhum conhecimento prévio do artefato;

4.1.16. Deve prevenir contra ameaças conhecidas baseado em assinatura;

4.1.17. Possibilidade de colocar arquivos, diretórios e processos em listas de exclusões para não serem verificados pela proteção em tempo real;

4.1.18. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados;

4.1.19. Iniciar varreduras automáticas e manuais baseados em IOCs detectados;

4.1.20. Detectar atividade maliciosa de criptografia por ransomware e interromper o processo de criptografia, restaurando os arquivos ao seu estado original, impedindo a perda de dados corporativos.

4.1.21. A solução deve fornecer a capacidade de configurar listas brancas globais para permitir que determinados arquivos executáveis sejam executados dentro de determinadas condições da instituição;

4.1.22. A solução deve ter a capacidade de criar, a partir de incidentes, uma regra de exceção para permitir que um processo seja executado em um determinado endpoint;

4.1.23. Deve permitir bloquear nos endpoints o uso de dispositivos portáteis USB como pen drives, discos, drives de CD/DVD/BluRay a fim de prevenir contra a transferência de arquivos maliciosos por meio destes dispositivos;

4.1.24. Deve possuir firewall de host permitindo o controle da comunicação do endpoint através de regras de permissão e bloqueio do tráfego ;

4.1.25. A solução deve armazenar as informações de alertas, incidentes e suas respectivas atividades e ações e demais dados relacionados aos eventos de segurança detectados por um período mínimo de 30 (trinta) dias;

4.1.26. A solução deve suportar a proteção de processos e aplicativos em execução no sistema operacional;

4.1.27. A solução deve suportar a adição de aplicações proprietárias e personalizadas na lista de aplicações protegidas;

4.1.28. A solução deve ser capaz de fornecer prevenção em tempo real contra exploração de vulnerabilidades de aplicações, bloqueando em tempo real a exploração, não limitadas a falhas de lógica de software, corrupção de memória e sequestro de DLL;

4.1.29. A solução deve ser capaz de proteger contra explorações de quaisquer vulnerabilidades não descobertas (desconhecidas) dos aplicativos através do bloqueio de métodos (técnicas e subtécnicas) utilizados para exploração;

4.1.30. Ao impedir ou bloquear uma técnica de exploração, a solução deve congelar o processo, coletar informações forenses, de no mínimo, nome do processo, origem e caminho do arquivo, data/hora, dump de memória, versão do SO, usuário, versão vulnerável do aplicativo;

4.1.31. Ao impedir ou bloquear uma técnica de exploração, a solução deve finalizar apenas o processo específico alvo do ataque;

4.1.32. A solução deve utilizar módulos de métodos de exploração para prevenir ou bloquear tentativas de exploração. Os módulos de métodos de exploração devem proteger aplicações conhecidas,bem como aplicações desconhecidas e desenvolvidas internamente pela instituição;

4.1.33. A solução deve ser capaz de criar regras de exclusão para excluir endpoints específicos e processos específicos do log de eventos de ameaças de segurança da console de gerenciamento da solução;

4.1.34. Suportar detecção e bloqueio de, no mínimo, os seguintes métodos, devendo ser capaz de:

4.1.34.1. Impedir execução de dados na memória;

4.1.34.2. Impedir acessos não autorizados a DLLs do sistema;

4.1.34.3. Prevenir utilização de DLLs protegidas com fim de ganhar controle de processos e carregar arquivos CPL (painel de controle) maliciosos;

4.1.34.4. Interromper a ocorrência de heap sprays após detecção de exceções suspeitas ou indicativos de tentativas de exploração no host monitorado;

4.1.34.5. Prevenir processamento incorreto de fontes de texto em documentos e arquivos, técnica comum de exploração em processadores de texto;

4.1.34.6. Prevenir o acionamento de vulnerabilidades que resultem na corrupção da área heap na memoria. Exemplo: “free() double”;

4.1.34.7. Prevenir o uso de novas técnicas que possam evadir o DEP (prevenção de execução de dados em memória) e ASLR (randomização do layout de endereçamento em memória);

4.1.34.8. Obrigar a realocação de módulos do sistema operacional, protegendo-os de tentativas de exploração;

4.1.34.9. Ser capaz de detectar e prevenir instâncias de heap spray usando algoritmo de detecção de aumento de consumo de memória, indicando execução de exploração de vulnerabilidade;

4.1.34.10. Prevenir mapeamento de código no endereço zero (início da memória) do espaço de memória do sistema operacional, dessa forma impedindo uso de explorações de referência nula para execução de código arbitrário, exposição de informações de debug, etc;

4.1.34.11. Proteger o acesso a metadados de bibliotecas críticas do sistema operacional quando estas são descompactadas em memória;

4.1.34.12. Agir preventivamente contra heap spray ao checar periodicamente a zona heap da memória virtual;

4.1.34.13. Prevenir a exploração de vulnerabilidade através da pré-alocação aleatória do layout de memória de processos no sistema operacional;

4.1.34.14. Prevenir uso de programação orientada a retorno (return oriented programming) protegendo APIs (interface de programação de aplicação) usadas em cadeias de ROP e técnicas de exploração usando compilações “Just-in-time” (JIT);

4.1.34.15. Mitigar o abuso e captura das estruturas de gerenciamento de exceções (SEH) em memória, impedindo a execução de código malicioso arbitrário no sistema operacional;

4.1.34.16. Reservar e proteger determinadas áreas da memória comumente utilizadas para armazenamento de cargas (payload) e instruções maliciosas usando técnicas como heap spray, por exemplo;

4.1.34.17. Prevenir vulnerabilidades lógicas na estrutura de atalhos (links) de sistemas operacionais Windows, onde o carregamento impróprio de atalhos permite execução arbitrária de código em memória;

4.1.34.18. Prevenir contra vulnerabilidades utilizadas em ataques de escalação de privilégios no sistema operacional explorando a instrução sys.exit para retornar ao nível de execução de usuário, após execução de código em nível de sistema (privilege level 0);

4.1.34.19. Aprimorar ou implementar a randomização do layout de endereços em memória (ASLR), garantindo maior aleatoriedade e robustez. Deve também ser capaz de tornar obrigatório o uso da função ASLR;

4.1.35. A solução deve fornecer a capacidade de fazer controle e restringir os parâmetros sobre como executáveis podem executar incluindo proteção contra criação de processos filhos;

4.1.36. Deve ser capaz de restringir a execução de arquivos específicos somente em diretórios conhecidos e protegidos;

4.1.37. Deve prevenir execução de arquivos não assinados;

4.1.38. Deve prevenir a execução de arquivos em mídia externa;

4.1.39. Deve ser capaz de controlar executáveis não assinados por meio do uso de WhiteLists;

4.1.40. Deve ser capaz de definir e classificar Hashs conhecidos;

4.1.41. A solução deve coletar dados forenses capturados pelo agente de endpoint, contemplando, pelo menos, os seguintes:

- Dump de memória;
- Arquivos Acessados;
- Módulos carregados;
- URIs acessadas;
- Local de execução do arquivo;
- Tempo de execução;
- Nome do arquivo;
- Hash do arquivo;
- Nome do usuário relacionado;
- Endereço IP;
- Versão de sistema operacional;
- Histórico de arquivos maliciosos.

GERENCIAMENTO

4.1.42. A console de gerenciamento deverá ser baseada em nuvem e acessada através de navegadores web, devendo conter de forma centralizada os recursos para a monitoração e controle da proteção dos dispositivos;

4.1.43. Deverá apresentar Dashboard com o resumo do estado de proteção dos dispositivos protegidos, bem como indicar os alertas de eventos de criticidades alta, média e baixa;

4.1.44. Deve permitir, dentro da estrutura de gerenciamento, a organização dos dispositivos protegidos em grupos;

4.1.45. Deve permitir a aplicação de regras diferenciadas baseadas em dispositivos ou grupos de dispositivos;

4.1.46. Deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

4.1.47. Permitir a visualização de alertas, logs e relatórios relacionados aos IoCs detectados nos endpoints;

4.1.48. Correlacionar dados de múltiplos endpoints, fornecendo uma visão mais ampla sobre uma possível intrusão ou ataque coordenado;

4.1.49. A console de gerenciamento deverá ser compatível, no mínimo, com os navegadores Firefox e Chrome;

4.1.50. A comunicação entre a console de gerenciamento e os clientes gerenciados deve ser feita através do uso de protocolos seguros e protegidos por criptografia;

4.1.51. Deve ser possível realizar acesso direto aos endpoints protegidos a partir da console central de gerenciamento da solução, a fim de permitir a execução de ações para investigação e reposta aos incidentes de segurança como: visualizar e encerrar processos, apagar, mover e renomear arquivos, prover interface de linha de comando capaz de executar comandos do sistema operacional e executar scripts nos endpoints;

4.1.52. Deve ser possível salvar um relatório contendo todas as atividades realizadas durante a sessão de acesso aos endpoints gerenciados;

4.1.53. Deve ser possível realizar, a partir da console de gerenciamento, a execução simultânea de scripts nos diversos endpoints de forma centralizada;

4.1.54. A solução deve permitir, a partir da console central de gerenciamento, isolar um endpoint impedindo a comunicação do mesmo com a rede para evitar que um possível ataque se propague pela rede;

4.1.55. Deve possuir mecanismo de comunicação pré-definido, em tempo determinado e configurável pelo administrador, entre os agentes nos endpoints e a console de gerenciamento, provendo a consulta de novas configurações, políticas ou conteúdo;

4.1.56. Permitir a criação de, no mínimo, três perfis de acesso distintos para os usuários administradores da solução;

4.1.57. Deve registrar nos logs as alterações realizadas pelos administradores da solução, provendo auditoria de mudanças;

4.1.58. A solução deve ser capaz de exportar seus logs no formato syslog para outras soluções de gerenciamento de logs;

4.1.59. A atualização do motor de detecção de ameaças deve ser realizada de forma transparente para o usuário;

4.1.60. A console de gerenciamento deve exibir lista com todos os alertas de incidentes detectados na console central de gerenciamento. Deve mostrar, para cada alerta da lista, no mínimo, a data e hora que o incidente ocorreu, o nome ou endereço IP envolvido, a ação tomada pelo agente com relação ao incidente e a categoria do incidente informando se o mesmo se trata de exploit ou malware, por exemplo;

4.1.61. Deve permitir notificar eventos ao administrador por e-mail;

4.1.62. Deve permitir a criação de políticas para prevenção e mitigação de:

- Vulnerabilidades conhecidas e desconhecidas (Exploits);
- Códigos Maliciosos (Malware);
- Restrições de execução.

4.1.63. Deve centralizar e gerenciar na console de administração qualquer evento de segurança detectado, seja na camada de rede ou nos endpoints protegidos;

4.1.64. Deve ser exibida também, na console central de gerenciamento, a lista de CVE – Common Vulnerabilities and Exposures – conhecidos e permitir visualizar quais endpoints estão sendo afetados por uma determinada CVE;

4.1.65. Deve identificar e gerar log de qualquer interferência no serviço de proteção nas estações e servidores protegidos, como por exemplo:

- Tentativa de encerramento do processo de proteção;
- Tentativa de encerramento do serviço de proteção;
- Logs de sistema relacionados a tentativa de interferência com o serviço, processo ou arquivos do sistema de proteção;

4.1.66. Deve ser possível visualizar, em uma linha do tempo, a cadeia de processos e eventos, desde a execução do primeiro processo responsável pela execução dos demais, que geraram um alerta de incidente. Para cada processo executado deve ser possível visualizar, no mínimo, o caminho onde o processo estava localizado, o nome do usuário que iniciou o processo e o tempo em que o processo ficou em execução informando a data e hora do início e do fim da execução do mesmo;

4.1.67. Além dos processos executados deverão ser exibidas informações sobre conexões de entrada e saída, conexões fracassadas e download e upload de dados;

4.1.68. A solução deve permitir o ajuste de políticas de coleta de informações forenses, dentro da console de gerenciamento centralizado, com definições do tipo de informações sobre o incidente que serão coletadas quando uma ameaça ou ataque for identificado;

4.1.69. Deve possuir ferramenta de busca para a investigação de incidentes permitindo a realização de buscas com base em, no mínimo, processos executados, em arquivos criados, alterados e deletados, em atributos de rede como endereço IP, nome do host, porta e protocolo, em registros criados, modificados e deletados, em eventos de log do Windows e do Linux. Deve permitir também realizar a busca através da combinação destes atributos;

4.1.70. Deve ser possível a realização de busca com base no caminho completo onde o arquivo pode estar localizado e também com base no hash do arquivo gerado pela solução;

4.1.71. A solução deve permitir realizar a configuração de alertas com base em incidentes e em indicadores de comprometimento, como nome do arquivo, domínio e endereço IP de destino. A solução deve permitir importar listas de indicadores de comprometimento de serviços externos de inteligência contra ameaça, além de permitir a criação destes indicadores;

4.1.72. A solução deve permitir realizar a configuração de alertas baseados no comportamento do endpoint. Os tipos de comportamentos que devem ser detectados são, no mínimo, execução de processos, manipulação de privilégios em arquivo, ofuscação do tipo do arquivo, atividade de reconhecimento na rede, escalonamento de privilégio e movimentos laterais na rede;

4.1.73. A solução deve permitir realizar a atualização de versão dos agentes instalados nos endpoints a partir da console central de gerenciamento;

4.1.74. Capacidade de geração de relatórios, estatísticas e gráficos contendo no mínimo os seguintes tipos pré-definidos:

- As 10 máquinas com maior ocorrência de códigos maliciosos;
- Os 10 usuários com maior ocorrência de códigos maliciosos;
- Localização dos códigos maliciosos;
- Sumário das ações realizadas;
- Número de infecções detectadas diária, semanal e mensalmente;
- Deve abranger os códigos maliciosos detectados.

4.1.75. A solução deverá ter os seguintes dashboards nativos para monitorar a postura de segurança e o status da instituição:

- Relatório de restrição de acesso a arquivos e processos;
- Técnicas de Malwares utilizadas;
- Técnicas de exploração utilizadas;
- Informações Forenses coletadas.

4.1.76. A solução deverá ter os seguintes dashboards de controle para monitorar a situação dos endpoints da instituição:

- Detalhes da saúde dos agentes de endpoints;
- Dashboard de controle do histórico de regras dos endpoints;
- Dashboard de controle da Política de Segurança instalada nos endpoints;
- Dashboard de controle do histórico de status do serviço nos endpoints;

4.2. **REQUISITOS TÉCNICOS ESPECÍFICOS ITEM 3 (SERVIÇOS DE PLANEJAMENTO, CONFIGURAÇÃO, MIGRAÇÃO E TRANSFERÊNCIA DE CONHECIM SOFTWARES, A FIM DE DEFINIR OS PADRÕES DE UTILIZAÇÃO, AS CONFIGURAÇÕES BÁSICAS, E TRANSFERÊNCIA DE CONHECIMENTO PARA SUA UTILIZAÇÃO)**

4.2.1. Os prazos para execução são descritos no item 4.4 deste Termo de Referência;

4.2.2. Os serviços deverão ser executados pela CONTRATADA, por técnicos comprovadamente credenciados pelo fabricante;

4.2.3. A CONTRATADA deverá informar nome, e-mail e telefone dos componentes da equipe técnica responsável pela solução, ou seja, do gerente do projeto, técnico e do responsável comercial;

4.2.4. A implantação inicial consiste em aplicar as regras de acordo com a Politica de Segurança da Informação do Tribunal de Justiça do Estado do Espírito Santo assim como a migração das regras existentes na solução atualmente em uso (Symantec Endpoint Protection), podendo ainda serem definidas e criadas novas regras de acordo com as necessidades informadas pela equipe técnica de TI do PJES, sempre levando em consideração as melhores práticas estabelecidas no mercado;

4.2.4.1. É de responsabilidade da CONTRATADA a implantação da solução contemplando todos os itens apresentados neste Termo de Referência ou selecionados de acordo com as necessidades apresentadas pela equipe técnica da CONTRATANTE, incluindo todas as configurações necessárias à implantação e integração da solução ao ambiente de segurança da CONTRATANTE, sempre com acompanhamento e apoio da equipe técnica.

a) A instalação dos agentes da solução contratada nos endpoints deverá ser feito em conjunto com a equipe da CONTRATANTE.

b) A instalação, atualização ou migração dos softwares em estações de trabalho deverá ocorrer sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

4.2.4.2. Todas as configurações a serem feitas e aplicadas pela CONTRATADA no ambiente de infraestrutura do PJES deverão ser previamente apresentadas para a equipe técnica da CONTRATANTE no momento da implantação/configuração da solução.

a) Tais configurações só poderão ser aplicadas com o aval da equipe técnica;

b) No caso de inadequação técnica, a equipe ténica do TJES encaminhará à CONTRATADA os critérios inadequados encontrados nos serviços no prazo máximo de 03 (três) dias úteis;

4.2.5. Em relação ao agente:

4.2.5.1. Realizar a desinstalação da solução de endpoint existente (Symantec Endpoint Protection versões 12 ou 14) em todo o parque do Poder Judiciário do Estado do Espírito Santo;

4.2.5.2. Realizar a desinstalação da ferramenta existente sem solicitar ações do usuário da estação/servidor, preferencialmente sem necessitar de reboot do equipamento e de forma silenciosa para o usuário;

4.2.5.3. Comunicar imediatamente à CONTRATANTE sobre problemas na execução da desinstalação do agente;

4.2.5.4. Informar a CONTRATANTE, nos casos específicos onde seja necessário reboot, para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar;

4.2.5.5. O equipamento onde for instalada a nova solução deverá estar LIMPA e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações em que mais de uma solução além da vigente por este certame estejam instaladas no equipamento ao mesmo tempo;

4.2.5.6. Caso ocorra algum problema na desinstalação do atual agente e instalação do novo agente, deverá ser comunicado imediatamente à CONTRATANTE e apresentado uma alternativa para a avaliação;

4.2.6. Durante todo o processo de implantação a CONTRATADA deve prestar suporte em eventuais dificuldades que venham a surgir, sem custo adicional para a CONTRATANTE;

4.2.7. Todas as configurações de implantação serão revisadas pelos analistas do TJES, antes de serem inseridas na nova solução;

4.2.8. Todas as etapas das configurações da nova solução deverão ser supervisionadas pela equipe de TI do TJES;

4.2.9. O planejamento da implantação/migração deverá ser acordado na reunião de alinhamento do projeto e apresentado antes do início das atividades à equipe responsável da CONTRATANTE, incluindo mas não se limitando, a análise do ambiente de infraestrutura atual e o planejamento da implantação da nova solução;

4.2.9.1. A CONTRATADA deverá se reunir com a equipe técnica da CONTRATANTE e elaborar um plano de migração, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço de migração;

4.2.9.2. A migração da solução deverá seguir e respeitar todas as normas, políticas e procedimentos internos da CONTRATANTE, incluindo os processos de registro de mudanças, liberações e incidentes.

4.2.10. Ao final da implantação e configuração da solução, deverá ser realizado o repasse de informações hands-on, apresentando as configurações implementadas na solução;

4.2.11. Todas as despesas referentes aos serviços de implantação serão de responsabilidade da CONTRATAD A.

4.3. **REQUISITOS TÉCNICOS ESPECÍFICOS ITEM 4 (TREINAMENTO PARA ADMINISTRAÇÃO E CONFIGURAÇÃO DE SOFTWARE DE PROTEÇÃO ENDPOINT)**

4.3.1. O treinamento será direcionado aos técnicos da CONTRATANTE, deverá ser focado na solução adotada, de forma que haja transferência do conhecimento dos recursos, configurações existentes e sua utilização;

4.3.2. Deverá ser entregue para a CONTRATANTE a proposta com o conteúdo do treinamento;

4.3.3. A CONTRATANTE reserva-se o direito de não aceitar o módulo ministrado, podendo, a seu critério, solicitar a troca de instrutor ou até mesmo repetição do mesmo, caso não seja satisfatório;

4.3.4. Deverá ser ministrado por instrutor capacitado na ferramenta, devendo ser comprovado por meio de certificados ou declaração formal de disponibilidade, exigível após a emissão da ordem de serviço para o referido item durante a execução do contrato;

4.3.5. Deverá ser fornecido pela contratada certificado de capacitação para os participantes do treinamento.

OBJETIVO

4.3.6. Capacitação da contratante para a operacionalização da ferramenta tecnológica;

4.3.7. Formação de facilitadores que possam vir a replicar futuramente o conhecimento no âmbito do órgão contratante.

MÉTRICA

4.3.8. Deverá ter carga horária mínima 40 (quarenta) horas;

4.3.9. O treinamento deverá ser realizado em dias úteis e não poderá exceder o horário comercial;

4.3.10. O treinamento deverá ser ministrado para equipe mínima de 10(dez) participantes.

FORMA DE REALIZAÇÃO

4.3.11. O treinamento será em português, ministrado na modalidade remota, em plataforma virtual disponibilizada pela contratada;

4.3.12. Materiais didáticos e acessórios são de responsabilidade da contratada todo material audiovisual, didático e eletrônico para a realização dos treinamentos, e quaisquer outras despesas diretas ou indiretas;

4.3.13. O material didático será fornecido em português, pela contratada, abordando todos os tópicos do curso.

CONTEÚDO PROGRAMÁTICO

4.3.14. Deverá ser disponibilizado nos prazos estabelecidos no item 4.4 deste Termo de Referência;

4.3.15. O treinamento deverá englobar a realização de laboratórios práticos, fornecidos pela CONTRATADA, para configuração e execução de exercícios práticos na mesma versão dos produtos ofertados;

4.3.16. O evento abordará no mínimo: o uso da ferramenta, instalação, configuração, operação da ferramenta, gerenciamento, resolução de problemas, e poderá ser gravado para fins de documentação, caso seja de interesse da CONTRATANTE.

4.4. **REQUISITOS TEMPORAIS**

4.4.1. Os prazos para execução do objeto da contratação estão estabelecidos na tabela abaixo, em dias úteis, e terão como termo inicial a data da assinatura do contrato.

Evento	Marco	Serviço	Prazo	Responsável
Assinatura do contrato	I	Assinar o contrato	Em 5 (cinco) dias úteis após a convocação para esse fim	CONTRATADA
Indicação do preposto do contrato		Indicação do preposto para centralização da comunicação durante a execução do objeto	I + 5 (cinto) dias úteis	CONTRATADA
Reunião e nomeação do preposto e gerente técnico		Reunião de apresentação das equipes, leitura do contrato e demais atividades pertinentes. (Alinhamento)	I + 5 (cinco) dias úteis	CONTRATANTE e CONTRATADA
Entrega do Planejamento	II	Planejamento para migração e distribuição dos clientes nos endpoints	I + 10 (dez) dias úteis	CONTRATADA
Análise e aprovação do Projeto Executivo	III	Análise do planejamento pelo fiscal do contrato e equipe de TI da CONTRATADA, com possível solicitação de correções e aceite.	II + 3 (três) dias úteis	CONTRATANTE
Ordem de Serviço para execução do item 3 do objeto		Migração de políticas e configurações existentes na solução em uso para a solução a ser fornecida	III + 10 (dez) dias úteis	CONTRATADA
Testes e validação	IV	Procedimentos de teste de todas as funcionalidades e relatórios requeridos pela CONTRATANTE para a solução, realização do repasse e aceite da migração.	III + 10 (dez) dias úteis	CONTRATANTE e CONTRATADA
Licenciamento		Fornecimento das subscrições para todos os softwares disponibilizados.	IV + 5 (cinco) dias úteis	CONTRATADA
Ordem de serviço para distribuição do item 1 e/ou 2 do objeto	V	Distribuição e instalação dos clientes para proteção de endpoint para desktops	IV + 20 (vinte) dias úteis	CONTRATANTE e CONTRATADA
Ordem de Serviço para execução do item 3 do objeto		Fornecimento do conteúdo programático, data, documentação do instrutor etc.	V + 5 (cinco) dias úteis	CONTRATADA

Tabela : Tarefas e prazos.

5. **OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE**

5.1. **CONTRATADA**

5.1.1. **Todas já descritas no item 4;**

5.1.2. A CONTRATADA deverá realizar a distribuição de no mínimo 5500 (cinco mil e quinhetos) clientes nas estações de trabalho da CONTRATANTE;

5.1.3. A CONTRATADA será responsável pela remoção da solução em uso no PJES (Symantec Endpoint protection) dos desktops e instalação do novo cliente;

5.1.4. A metodologia, softwares, scripts e quaisquer outras ferramentas necessárias deverão ser descritas no planejamento a ser entregue;

5.1.5. O montante mínimo para aceite e ativação das subscrições será aferido através da plataforma de gerenciamento, devendo a comunicação entre cliente e plataforma não superar 7 (sete) dias de inatividade;

5.1.6. Caso a CONTRATADA não alcance a quantidade mínima exigida de distribuição, será exigida a instalação local com acompanhamento dos técnicos da CONTRATANTE;

5.1.7. Os desktops estão distribuídos nas localidades informadas abaixo podendo estas localidades divergirem em até 5 km de raio:

Item	Localidade	Endereço
1	AFONSO CLAUDIO	Rua José Garcia, nº 32 – Centro - CEP.: 29600-000 Distância em relação ao Município de Vitória: 145 km
2	AGUA DOCE DO NORTE	Rua Padre Franco, s/nº - Centro - CEP.: 29820-000 Distância em relação ao Município de Vitória: 308 km
3	AGUIA BRANCA	Rua Dr. Wanlery Koszarowski, s/nº - Praça dos Três Poderes - CEP.: 29795-000 Distância em relação ao Município de Vitória: 235 km
4	ALEGRE	Rua Romualdo Nogueira da Gama, s/nº - Centro - CEP.: 29500-970 Telefone: Distância em relação ao Município de Vitória: 200 km
5	ALFREDO CHAVES	Av. Getúlio vargas, nº 969, Centro - CEP.: 29240-000 Distância em relação ao Município de Vitória: 86 km
6	ALTO RIO NOVO	Rua Paulo Martins, nº 1211, - Bairro: Santa Bárbara - CEP.: 29760-000 Distância em relação ao Município de Vitória: 244 km
7	ANCHIETA	Rodovia do Sol, nº 2539, Ed. Tramonto Room, Ponta dos Castelhanos - CEP.: 29230-000 Distância em relação ao Município de Vitória: 78 km
8	APIACÁ	Rua Jader Pinto, nº 88 – Bairro Boa Vista - CEP.: 29450-000 Distância em relação ao Município de Vitória: 209 km
9	ARACRUZ	Rua Osório da Rocha Silva, nº 22, Bairro: Paraíso - CEP.: 29190-256 Distância em relação ao Município de Vitória: 82 km
10	ATÍLIO VIVACQUA	Rua Carolina Fraga, nº 67 / 69 – Centro Distância em relação ao Município de Vitória: 156 km
11	BAIXO GUANDU	Av. Carlos Medeiros, nº 977 – Centro - CEP.: 29730-000 Distância em relação ao Município de Vitória: 182 km
12	BARRA DE SÃO FRANCISCO	Rua Des. Danton Bastos, nº 95 – Centro - CEP.: 29800-000 Distância em relação ao Município de Vitória: 276 km
13	BOA ESPERANÇA	Av. Virgílio Simonetti, nº 1206, Bairro: Ilmo Covre - CEP.: 29845-000 Distância em relação ao Município de Vitória: 300 km
14	BOM JESUS DO NORTE	Rua Carlos Firmo, nº 119 – Centro - CEP.: 29460-000 Distância em relação ao Município de Vitória: 223 km
15	CACHOEIRO DE ITAPEMIRIM	Av. Monte Castelo, s/nº - Bairro: Independência - CEP.: 29306-500 Distância em relação ao Município de Vitória: 138 km
16	CARIACICA	Rua São João Batista, nº 1000, Alto Laje - CEP.: 29151-230 Distância em relação ao Município de Vitória: 17 km
17	CASTELO	Av. Nossa Senhora da Penha, nº120, Centro - CEP.: 29360-000 Distância em relação ao Município de Vitória: 148 km
18	COLATINA	Praça do Sol Poente, nº 100, Bairro: Esplanada - CEP.: 29702-710Distância em relação ao Município de Vitória: 135 km
19	CONCEIÇÃO DA BARRA	Rua Graciano Neves, nº 292 – Centro - CEP.: 29660-000Distância em relação ao Município de Vitória: 251 km
20	CONCEIÇÃO DO CASTELO	Rua José Grillo, nº 166 – Centro - CEP.: 29370-000Distância em relação ao Município de Vitória: 126 km
21	DOMINGOS MARTINS	Av. Presidente Vargas, nº 589 – Centro - CEP.: 29260-000Distância em relação ao Município de Vitória: 49 km
22	DORES DO RIO PRETO	Av. Firmino Dias, nº 428 – Centro - CEP.: 29580-000Distância em relação ao Município de Vitória: 250 km
23	ECOPORANGA	Av. Jurvalim Gerônimo de Souza, nº 987 – Centro - CEP.: 29850-000Distância em relação ao Município de Vitória: 334 km
24	FUNDÃO	Rua São José, nº 145 – Centro - CEP.: 29188-000Distância em relação ao Município de Vitória: 53 km
25	GUAÇUI	Rua Agenor Luiz Tomé, s/nº - Bairro Quincas Machado - CEP.: 29560-000Distância em relação ao Município de Vitória: 223 km
26	GUARAPARI	Alameda Francisco Vieira Simões, s/nº - Muquiçaba - CEP.: 29214-110Distância em relação ao Município de Vitória: 51 km
27	IBATIBA	Rua Orly Barros, nº195, Bairro: Novo Horizonte - CEP.: 29395-000Distância em relação ao Município de Vitória: 164 km
28	IBIRAÇU	Rua Mário Antônio Modenesi, nº 15, Bairro: São Cristovão - CEP.: 29670-000Distância em relação ao Município de Vitória: 69 km
29	IBITIRAMA	Rua Anísio Ferreira da Silva, nº 98 – Centro - CEP.: 29540-000Distância em relação ao Município de Vitória: 220 km
30	ICONHA	Rua Muniz Freire, nº 653 – Centro - CEP.: 29280-000Distância em relação ao Município de Vitória: 94 km
31	ITAGUAÇU	Rua Vicente Peixoto de Mello, nº 32 – Centro - CEP.: 29690-000 Distância em relação ao Município de Vitória: 128 km

32	ITAPEMIRIM	Rua Melchíades Félix de Souza, nº 200 – Serramar - CEP.: 29330-000Distância em relação ao Município de Vitória: 120 km
33	ITARANA	Rua Santos Venturini, s/nº, Centro - CEP.: 29620-000Distância em relação ao Município de Vitória: 117 km
34	IÚNA	Rua Galaos Rius, nº 301 – Centro - CEP.: 29390-000Distância em relação ao Município de Vitória: 187 km
35	JAGUARÉ	Av. Nove de Agosto, nº 1410 – Centro - CEP.: 29950-000Distância em relação ao Município de Vitória: 201 km
36	JERÔNIMO MONTEIRO	Av. Dr. José Farah, nº 383 - Centro - CEP.: 29550-000Distância em relação ao Município de Vitória: 180 km
37	JOÃO NEIVA	Av.: Presidente Vargas, nº 279 – Centro - Cep.: 29680-000Distância em relação ao Município de Vitória: 75 km
38	LARANJA DA TERRA	Av. Luiz Obermüller Filho, nº 85 – Centro - CEP.: 29615-000Distância em relação ao Município de Vitória: 183 km
39	LINHARES	Rua Alair Garcia Duarte, s/nº - Bairro: Três Barras - CEP.: 29906-660Distância em relação ao Município de Vitória: 134 km
40	MANTENÓPOLIS	Praça Dom Luiz, nº 12 – Centro - CEP.: 29770-000Distância em relação ao Município de Vitória: 278 km
41	MARATAÍZES	Av. Rubens Rangel, nº 663 – Cidade Nova - CEP.: 29345-000Distância em relação ao Município de Vitória: 116 km
42	MARECHAL FLORIANO	Av. Arthur Haese, nº 656 – Centro - CEP.: 29266-000Distância em relação ao Município de Vitória: 53 km
43	MARILÂNDIA	Rua Luís Catelan, nº 206 – Centro- CEP.: 29725-000Distância em relação ao Município de Vitória: 147 km
44	MIMOSO DO SUL	Praça Coronel Paiva Gonçalves, nº 184 – Centro - CEP.: 29400-000Distância em relação ao Município de Vitória: 179 km
45	MONTANHA	Av. Antônio Paulino, nº 445 – Centro - CEP.: 29890-000Distância em relação ao Município de Vitória: 329 km
46	MUCURICI	Rua Presidente Castelo Branco, s/nº - Centro - CEP.: 29880-000Distância em relação ao Município de Vitória: 347 km
47	MUNIZ FREIRE	Rua Pedro Deps, nº 54 – Centro - CEP.: 29380-000Distância em relação ao Município de Vitória: 176 km
48	MUQUI	Rua Coronel Marcondes, nº 100 – Centro - CEP.: 29480-000Distância em relação ao Município de Vitória: 172 km
49	NOVA VENÉCIA	Praça São Marcos, s/nº - Centro - CEP.: 29830-000Distância em relação ao Município de Vitória: 273 km
50	PANCAS	Rua Jovino Nonato da Cunha, nº 295 – Centro - CEP.: 29750-000Distância em relação ao Município de Vitória: 210 km
51	PEDRO CANÁRIO	Rua Deodato Vital do Anjos, s/nº - Bairro: Novo Horizonte - CEP.: 29970-000Distância em relação ao Município de Vitória: 266 km
52	PINHEIROS	Rua Agenor Luiz Heringer, nº 880, - Centro - CEP.: 29980-000Distância em relação ao Município de Vitória: 285 km
53	PIUMA	Praça Oenes Taylor, s/nº - Centro - CEP.: 29285-000Distância em relação ao Município de Vitória: 89 km
54	PRESIDENTE KENNEDY	Rua Olegário Fricks, nº 20 – Centro - CEP.: 29350-000Distância em relação ao Município de Vitória: 158 km
55	RIO BANANAL	Rua Roão Cipriano, nº 810 – Centro - CEP.: 29920-000Distância em relação ao Município de Vitória: 176 km
56	RIO NOVO DO SUL	Rua Muniz Freire, nº 16 – Centro - CEP.: 29290-000Distância em relação ao Município de Vitória: 113 km
57	SANTA LEOPOLDINA	Av. Presidente Vargas, nº 1559 – Centro - CEP.: 29640-000Distância em relação ao Município de Vitória: 51 km
58	SANTA MARIA DE JETIBA	Rua Hermano Miertschink, nº 160 – Centro - CEP.: 29645-000Distância em relação ao Município de Vitória: 85 km
59	SANTA TERESA	Av. Maria Angélica Vervloet dos Santos, nº 392, Vale do Canaã.Distância em relação ao Município de Vitória: 79 km
60	SÃO DOMINGOS DO NORTE	Rod. ES 080, Km 44, s/nº, Bairro: Emílio Calegari - CEP.: 29745-000 Distância em relação ao Município de Vitória: 207 km
61	SÃO GABRIEL DA PALHA	Rua 14 de maio, nº 131 – Centro - CEP.: 29780-000Distância em relação ao Município de Vitória: 228 km
62	SÃO JOSÉ DO CALÇADO	Av.: Heber Fonseca, s/nº - Bairro: João Marcelino de Freitas - CEP.: 29470-000Distância em relação ao Município de Vitória: 236 km
63	SÃO MATEUS	Av. João Nardoto, nº 140 – Bairro: Jaqueline - CEP.: 29936-160Distância em relação ao Município de Vitória: 217 km
64	SERRA	Av. Carapebus, nº 226, São Geraldo / CarapinaCEP.: 29163-392Distância em relação ao Município de Vitória: 25 km
65	VARGEM ALTA	Av. Tuffy David, s/nº - Centro - 29295-000Distância em relação ao Município de Vitória: 127 km
66	VENDA NOVA DO IMIGRANTE	Av. Evandi Américo Comarela – nº 971 – Bairro Marmin - CEP.: 29375-000Distância em relação ao Município de Vitória: 109 km
67	VIANA	Rua Major Domingos Vicente, nº 70, Centro - CEP.: 29130-911 Distância em relação ao Município de Vitória: 26 km
68	VILA VELHA	Rua Dr. Annor Silva, nº 191, Boa Vista II, Vila Velha - CEP.: 29107-355 - r. 9Distância em relação ao Município de Vitória: 8 km
69	VITÓRIA	Rua Muniz Freire, s/nº - Centro - Cep.: 29015-140 Distância em relação ao Município de Vitória: 0 km
70	TRIBUNAL DE JUSTIÇA	Rua Des. Homero Mafra, 60 - Enseada do Suá, Vitória - ES, CEP: 29050-906 Distância em relação ao Município de Vitória: 0 km

5.1.8. Cumprir todas as obrigações resultantes da observância da Lei 14.133/21;

5.1.9. Fornecer o(s) objeto(s) conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital e seus anexos, na Proposta e no Contrato;

5.1.10. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos vinculados ao fornecimento, dentro dos prazos e condições estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas contratualmente, caso os prazos e condições não sejam cumpridos;

5.1.11. Responsabilizar-se pela observância de Leis, Decretos, Regulamentos, Portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do contrato;

5.1.12. Atender prontamente às solicitações do contratante no fornecimento do objeto nas quantidades e especificações previstas no Termo de Referência, de acordo com a necessidade do contratante, a partir da solicitação do Gestor do Contrato;

5.1.13. Seguir as instruções e observações efetuadas pelo Gestor do Contrato, bem como reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, partes do objeto em que se verificarem vícios, defeitos ou incorreções;

5.1.14. Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução contratual;

5.1.15. Assumir responsabilidade irrestrita sobre a totalidade do fornecimento de insumos e serviços associados ao objeto;

5.1.16. Indicar, formalmente, preposto apto a representá-la junto à CONTRATANTE que deverá responder pela fiel execução do Contrato;

5.1.17. Cuidar para que o preposto indicado mantenha permanente contato com o Gestor do Contrato e adote as providências requeridas pelo contratante quando da execução do objeto;

5.1.18. Prestar todos os esclarecimentos que forem solicitados pelo contratante, devendo, ainda, atender e resolver prontamente às reclamações;

5.1.19. Comunicar, imediatamente e por escrito, qualquer anormalidade ou problema detectados, prestando à CONTRATANTE os esclarecimentos necessários;

5.1.20. Manter, durante a execução contratual, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para o fornecimento do objeto;

5.1.21. Assumir inteira responsabilidade técnica e operacional pelo fornecimento do objeto e os serviços diretamente vinculados, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na execução;

5.1.22. Responder integralmente por quaisquer perdas ou danos causados à CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus profissionais em razão da execução contratual, independentemente de outras cominações contratuais ou legais a que estiver sujeito;

5.1.23. Arcar com todas as despesas decorrentes de transporte, diárias, tributos, seguros, alimentação, assistência médica e de pronto socorro, ou qualquer outra despesa de seus empregados;

5.1.24. Arcar com o pagamento de todas as despesas decorrentes do fornecimento do objeto, incluindo as despesas definidas em leis sociais, trabalhistas, comerciais, tributárias e previdenciárias, impostos e todos os custos, insumos e demais obrigações legais, inclusive todas as despesas que onerem, direta ou indiretamente, o objeto ora contratado, não cabendo, pois, quaisquer reivindicações da CONTRATADA, a título de revisão de preço ou reembolso;

5.1.25. Promover, por sua conta e risco, o transporte de seus empregados, materiais e utensílios necessários à execução contratual, até as instalações da CONTRATANTE;

5.1.26. Respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no Estado do Espírito Santo, bem como atentar para as regras de cortesia onde sejam executados os serviços;

5.1.27. Substituir qualquer de seus profissionais cuja qualificação, atuação, permanência ou comportamento durante a execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público por outro de qualificação igual ou superior, sempre que exigido pela CONTRATANTE;

5.1.28. Garantir a execução dos serviços vinculados à execução contratual, mantendo equipe adequadamente dimensionada para tanto, sem ônus adicionais para o órgão contratante;

5.1.29. Zelar pela boa e completa execução dos serviços vinculados à execução contratual, mantendo recursos técnicos e humanos necessários para evitar a interrupção indesejada dos mesmos;

5.1.30. Facilitar, por todos os meios a seu alcance, a ampla ação fiscalizadora do órgão contratante, atendendo prontamente às observações e exigências que lhe forem dirigidas;

5.1.31. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, especialmente em relação a: dados, informações, regras de negócios, documentos, e outros;

5.1.32. Honrar os honorários e encargos sociais devidos pela sua condição de única empregadora do pessoal designado para execução dos serviços vinculados ao fornecimento, incluindo indenizações decorrentes de acidentes de trabalhos, demissões, vales-transporte, entre outros, obrigando-se, ainda, ao fiel cumprimento das legislações trabalhistas e previdenciárias, sendo-lhe defeso invocar a existência deste contrato para eximir-se destas obrigações ou transferi-las para a CONTRATANTE;

5.1.33. Responder, perante a CONTRATANTE e terceiros, pela conduta dos seus empregados designados para execução do objeto do contrato, com o propósito de evitar condutas que possam comprometer a segurança ou a credibilidade da CONTRATANTE;

5.1.34. Adotar regras de vestimenta para seus profissionais adequadas com o ambiente do órgão, com trajes em bom estado de conservação e portando crachá de identificação funcional com foto e nome visível, arcando com o ônus de sua confecção;

5.1.35. Utilizar as melhores práticas de mercado no gerenciamento de recursos humanos e supervisão técnica e administrativa para garantir a qualidade da execução do objeto e o atendimento das especificações contidas no Contrato, Edital e seus Anexos;

5.1.36. Cumprir e fazer cumprir por seus profissionais as normas e procedimentos estabelecidos na Política de Segurança da Informação da CONTRATANTE;

5.1.37. Manter os contatos com a CONTRATANTE sempre por escrito, ressalvados os entendimentos verbais determinados pela urgência na execução do Contrato que, posteriormente, devem sempre ser confirmados por escrito, dentro de até 72 (setenta e duas) horas, a contar da data de contato;

5.1.38. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários de até 25% (vinte e cinco por cento) do valor inicial do contrato;

5.1.39. Comunicar à CONTRATANTE, com antecedência de 48 (quarenta e oito) horas os motivos que eventualmente impossibilitem a prestação dos serviços no prazo estipulado, nos casos em que houver impedimento justificado para funcionamento normal de suas atividades, sob a pena de sofrer as sanções da Lei 14.133/21.

5.1.40. São expressamente vedadas à CONTRATADA:

a) A contratação de servidor pertencente ao quadro de pessoal do contratante durante o período de vigência contratual.

b) A subcontratação total do objeto do Contrato. E sendo parcial, somente para implantação da solução (item 3) ou capacitação (item 4), desde que o prestador de serviço seja autorizado pelo fabricante, em qualquer caso, com a anuência do contratante e com total responsabilidade da CONTRATADA, observadas as mesmas condições de habilitação e qualificação da licitação.

5.2. **São Obrigações do CONTRATANTE:**

5.2.1. Cumprir todas as obrigações resultantes da observância da Lei 14.133/21;

5.2.2. Validar e aprovar os produtos e serviços entregues.

5.2.3. Receber o objeto de acordo com as disposições deste Termo de Referência.

5.2.4. Definir o Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, o Fiscal Administrativo, responsáveis por fiscalizar a execução contratual, conforme disposto no Art. 16 da Resolução 182/2013 do Conselho Nacional de Justiça – CNJ.

5.2.5. Efetuar o pagamento nas condições e preços pactuados, dentro do prazo fixado no contrato;

5.2.6. Nenhum pagamento será efetuado enquanto houver pendência de liquidação ou qualquer obrigação financeira em virtude de penalidade ou inadimplência.

5.2.7. Comunicar à CONTRATADA, o mais prontamente possível, qualquer anormalidade observada no fornecimento do objeto requisitado que possa comprometer a tempestividade, a qualidade e a eficácia do uso a que se destina.

5.2.8. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA.

5.2.9. Fornecer, a qualquer tempo e com a máxima presteza, mediante solicitação escrita da CONTRATADA, informações adicionais, dirimir dúvidas e orientá-la em todos os casos julgados necessários.

5.2.10. Manter os contatos com a CONTRATADA por escrito, ressalvados os entendimentos verbais determinados pela urgência que, posteriormente, devem ser confirmados por escrito no prazo de até 72 (setenta e duas) horas.

5.2.11. A CONTRATANTE não aceitará, sob nenhum pretexto, transferência de responsabilidade da CONTRATADA para terceiros, sejam fabricantes, representantes ou quaisquer outros.

5.2.12. Permitir acesso dos empregados da CONTRATADA às dependências do TJES para entrega do objeto.

5.2.13. Fornecer a infraestrutura necessária para a realização das atividades que devam ser executadas em suas instalações conforme as especificações estabelecidas no Termo de Referência.

5.2.14. Providenciar o acesso controlado aos recursos de TIC do TJES para os profissionais da CONTRATADA durante a fase de execução do objeto, caso necessário.

5.2.15. Supervisionar e gerenciar os procedimentos a serem realizados pelos fiscais de contrato.

5.2.16. Exigir o afastamento de qualquer funcionário ou preposto da CONTRATADA que venha a causar embaraço ou que adote procedimentos incompatíveis com o exercício das funções que lhe forem atribuídas.

5.2.17. Responsabilizar-se pela observância às Leis, Decretos, Regulamentos, Portarias e demais normas legais, direta e indiretamente aplicáveis ao contrato.

5.2.18. Aplicar à CONTRATADA as penalidades regulamentares e contratuais em caso de algum descumprimento.

6. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

6.1. DA FORMA DE SELEÇÃO:

6.1.1. Tratando-se de lote único, a adjudicação do objeto deverá ser realizada para o mesmo fornecedor com vias a garantir a interoperabilidade entre os itens constantes do lote.

6.1.2. Considerando que os serviços são caracterizados como comuns no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos, recomenda-se a utilização do sistema de pregão na sua modalidade eletrônica do tipo menor preço.

6.1.3. Os seguintes documentos servirão como condição para aceite da proposta:

6.1.3.1. Especificação clara, completa e minuciosa do produto cotado, informando a marca, o modelo e o fabricante, bem como a indicação precisa da comprovação de cada característica constante nas especificações técnicas deste Termo de Referência, pontuando em forma de planilha cada exigência do edital com sua respectiva comprovação, que deve conter uma ou mais das seguintes:

6.1.3.2. Indicação da página/item do manual/datasheet;

6.1.3.3. URL;

6.1.3.4. Seção/subseção ou número de item de página WEB;

6.1.3.5. Print de tela da solução;

6.1.3.6. Imagem ou vídeo que demonstre a funcionalidade;

6.1.3.7. Outra comprovação, desde que seja oficial do fabricante do produto ofertado.

6.1.4. Entende-se por documento (s) a documentação técnica oficial do fabricante do produto ofertado, seja em meio eletrônico ou materializada em papel;

6.1.5. Não serão aceitas declarações ou cartas de conformidade ou adequação ao solicitado e especificado no termo de referência em substituição ou complementação da documentação técnica oficial e original.

6.1.6. Caso a licitante não seja o próprio fabricante, deverá apresentar documento emitido pelo fabricante dos produtos, que comprove que a licitante é um parceiro oficial habilitado a comercializar seus produtos.

6.2. **DOS CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA:**

6.2.1. Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos compatíveis com o objeto desta licitação, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado que comprovem que a licitante já prestou serviços semelhantes ao objeto licitado.

6.2.2. Os atestados apresentados devem demonstrar o fornecimento de no mínimo 1000 (mil) unidades do item 1 (Subscrição de software de proteção para endpoint);

6.2.3. A quantidade mínima de fornecimento do item 6.2.2 poderá ser resultante de múltiplos atestados;

6.2.4. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

6.2.4.1. Os atestados deverão referir-se aos serviços fornecidos no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

6.2.4.2. Considerar-se-ão fornecimentos de serviços semelhantes aqueles de natureza e complexidade similar ao objeto e compatível em características, quantidades e prazos de execução relacionada com o objeto desta licitação, conforme Acórdão nº 914/2019-Plenário TCU;

6.2.4.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, no mínimo, 12 (doze) meses do início de sua execução, exceto se firmado para ser executado em prazo inferior;

6.2.5. Quando solicitado pelo pregoeiro, a empresa deverá disponibilizar todas as informações necessárias à comprovação da legitimidade do atestado entregue, apresentando, dentre outros documentos, cópia dos contratos, notas fiscais e dos documentos do responsável técnico pela execução do contrato, com registro no conselho de classe, conforme o caso.

6.3. **DA PROPOSTA COMERCIAL:**

6.3.1. A proposta comercial deverá conter, ao menos, as informações constantes no modelo do ADENDO I, cujo julgamento será pelo menor valor global.

7. MODELO DE EXECUÇÃO E GESTÃO DO CONTRATO

7.1. **Papéis:**

I - Equipe de Gestão da Contratação: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares;

II - Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, sendo responsável por gerir a execução consoante às atribuições regulamentares;

III - Fiscal Técnico do contrato: 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;

IV - Preposto: funcionário representante da CONTRATADA, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. Em caso de substituição do Preposto, a CONTRATADA deverá comunicar formalmente à equipe de fiscalização, via e-mail, o nome do preposto substituto.

7.2. **Dinâmica da Execução:**

7.2.1. O prazo de entrega dos itens que compõem o objeto são descritos no item 4.4 do Termo de Referência:

7.2.1.1. Excepcionalmente, os prazo de recebimento poderão ser prorrogados por até 30 (trinta) dias corridos, desde que solicitado pelo fornecedor e com apresentação de justificativa, nos termos da Lei nº 14.133/21.

7.2.1.2. Toda prorrogação de prazo deverá ser justificada por escrito e previamente autorizada pela autoridade competente que assinar o Contrato ou a Ordem de Fornecimento.

7.2.1.3. Caberá à Equipe de Fiscalização e ao setor demandante auxiliarem a autoridade competente na análise do pedido de prorrogação.

7.2.2. Por ocasião do recebimento do objeto serão aferidas a qualidade e a quantidade de acordo com o disposto neste Termo de Referência e na proposta vencedora.

7.2.3. O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do material fornecido ou dos serviços prestados, cabendo-lhe sanar quaisquer irregularidades quando detectadas.

7.3. **Cronograma de execução dos serviços:**

7.3.1. De acordo com o item 4.4.1 deste Termo de Referência.

7.3.2. **Cronograma da realização do item 4 (Treinamento para administração e configuração de software de proteção endpoint):**

7.3.2.1. Caso haja, preferencialmente os treinamentos serão realizados antes da fase especificada deste Termo, de acordo com o cronograma pactuado na Reunião de Alinhamento. Alternativamente, poderá ser definido prazo distinto deste item, como por exemplo, seguir o calendário oficial de treinamentos do fabricante do software da solução, desde que acordado expressamente entre CONTRATANTE e CONTRATADA.

7.4. **Instrumentos formais de solicitação de fornecimento:**

7.4.1. Documento de solicitação de fornecimento: Contrato ou Ordem de fornecimento devidamente assinado por ambos os contratantes.

7.4.2. Documento de recebimento provisório: Termo de Recebimento Provisório assinado pela Equipe de Fiscalização da contratação.

7.4.3. Documento de recebimento definitivo: Termo de Recebimento Definitivo assinado pela Equipe de Gestão da contratação.

7.5. **Solicitações de chamado técnico:**

a) Chamado Técnico por meio de Mensagem eletrônica (e-mail) como ferramenta preferencial de solicitação, acompanhamento e de aferição do serviço prestado pela CONTRATADA;

b) Chamado Técnico de forma eletrônica por meio de Central on-line;

c) Chamado Técnico por meio telefônico para a Central de Atendimento.

7.6. **Prazos de garantia, suporte e Níveis Mínimos de Serviço Exigidos:**

7.6.1. Durante o prazo de garantia técnica, a CONTRATADA deverá garantir o funcionamento da solução como um todo, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção, incluindo:

7.6.1.1. Atualizações corretivas e evolutivas, de drivers, firmwares, softwares e manuais, durante a vigência da garantia e suporte da solução;

7.6.1.2. Ajustes e configurações conforme manuais e normas técnicas do fabricante;

7.6.1.3. Demais procedimentos destinados a recolocar a solução em perfeito estado de funcionamento;

7.6.1.4. Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos;

7.6.1.5. Fornecimento de informações e esclarecimentos de dúvidas sobre instalação, administração, configuração, otimização, troubleshooting ou utilização dos produtos adquiridos.

7.6.1.6. A CONTRATADA deverá apresentar, até a data do recebimento definitivo da implantação, instrumento que comprove, junto ao fabricante, o início do serviço de suporte técnico da solução.

7.6.1.7. A garantia deverá incluir todas as atualizações de todos os softwares que compõem a solução durante o período contratado.

7.6.1.8. Devem ser disponibilizados serviços de suporte durante 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia, executando-os sempre que acionados pela CONTRATANTE, mediante a abertura de chamado técnico, prestados por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional;

7.6.1.9. Os serviços de atendimento da Central de Assistência técnica deverão ser providos das seguintes formas:

7.6.1.10. Um canal de suporte técnico através de um número telefônico de serviço, em língua portuguesa, para abertura de chamados técnicos de hardware e software. Este serviço deverá obrigatoriamente estar disponível 8x5 (oito horas por dia, 5 dias por semana, durante o horário comercial) sem custos para a CONTRATANTE;

7.6.1.11. Um canal de suporte técnico através de Portal web e/ou correio eletrônico (e-mail), deverá ser disponibilizado de forma ininterrupta 24x7 (vinte e quatro horas por dia, sete dias por semana);

7.6.1.12. Deverá ser disponibilizada, para a equipe técnica da CONTRATANTE, uma conta de acesso (somente leitura) para acompanhamento de chamados de suporte e manutenção abertos;

7.6.1.13. Deverá ser disponibilizada, para a equipe técnica da CONTRATANTE, uma conta de acesso para consulta de documentação técnica do fabricante e atualizações de software;

7.6.1.14. Os chamados técnicos deverão possuir identificador de ocorrência próprio, data e hora de abertura devidamente repassada a CONTRATANTE, a fim de registro e acompanhamento das ocorrências;

7.6.1.15. A CONTRATADA deverá informar o número do chamado e disponibilizar um meio de acompanhamento das ocorrências e de seus estados;

7.6.1.16. Ao final de cada atendimento, a CONTRATADA deverá emitir relatório técnico contendo as seguintes informações:

a) Número do chamado;

b) Categoria de prioridade;

c) Descrição do problema e da solução;

d) Procedimentos realizados (passo a passo);

e) Data e hora da abertura e do fechamento do chamado;

f) Data e hora do início e do término da execução dos serviços;

g) Identificação do técnico da empresa.

7.6.2. O tempo de solução para os chamados técnicos abertos será contado a partir do registro dos mesmos em qualquer um dos meios disponíveis da Central de Atendimento da CONTRATADA;

7.6.2.1. O encerramento do chamado será dado por técnico da CONTRATANTE na conclusão dos serviços;

a) Em caso de atraso na conclusão do atendimento, em qualquer nível de prioridade, será admitida a proposição, pela CONTRATADA, de justificativa técnica, a qual deverá conter os motivos do atraso, acompanhados da devida comprovação;

b) A justificativa eventualmente apresentada será analisada pela Administração a qual emitirá parecer, para fins de sua aceitação ou não;

c) Em sendo aceita, ocorrerá tão somente a interrupção dos prazos contratuais, sem prejuízo da conclusão do chamado. Em não sendo aceita, impor-se-á as sanções previstas neste documento, bem como no Termo de Referência e eventual Contrato Administrativo.

d) A justificativa deverá ser apresentada em até 03 (três) dias úteis da conclusão do chamado. Uma vez apresentada fora deste prazo, caberá à Administração conhecer ou não o documento;

7.6.3. A CONTRATADA/FABRICANTE deverá disponibilizar site na internet incluindo pelo menos a relação de licenças de uso disponíveis, base de conhecimento, fórum de discussão, documentação técnica dos produtos ofertados, comunidades técnicas, abertura e acompanhamento do histórico de chamados, sem limite de quantidade, download de produtos, atualizações e correções;

7.7. **EXECUÇÃO DOS SERVIÇOS:**

7.7.1. Previsto nos itens 4 e 7 deste Termo de Referência.

7.8. **DAS MULTAS E SANÇÕES ADMINISTRATIVAS:**

7.8.1. Com fulcro nos artigos 86, 87 e 88 da Lei nº 14.133/2021 (nova lei de licitações) e art. 28 do Decreto-Lei Estadual nº 1.527-R, a Administração poderá, garantida a defesa prévia, aplicar aos licitantes e/ou adjudicatários as seguintes penalidades, sem prejuízo das responsabilidades civil e criminal:

7.8.2. Advertência: Aplicada na hipótese de execução irregular que não resulte prejuízo direto para a contratante; pela repetição de falhas no atendimento de um mesmo serviço; e pela repetição de não atendimento a um mesmo nível de qualidade contratado.

Níveis das Multas	
Nível	**Correspondência**
1	Advertência
2	Multa de 1% sobre o valor do contrato (somatório dos valores dos itens)

3	Multa de 2% sobre o valor do contrato (somatório dos valores dos itens)
4	Multa de 3% sobre o valor do contrato (somatório dos valores dos itens)
5	Multa de 5% sobre o valor do treinamento

Referência para as Multas			
Item	**Descrição**	**Referência**	**Nível**
1	Não mantiver a proposta; não assinar o contrato; ou recusar o recebimento da Nota de Empenho.	-	2
2	Apresentar declaração e/ou documentação falsa; e/ou cometer fraude fiscal.	-	4
3	Não prestar a garantia contratual dentro do prazo estabelecido.	-	2
4	Na hipótese de rescisão contratual por inexecução total ou parcial do Contrato.	-	4
5	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços solicitados, e que não sejam justificados e aceitos pelo Contratante.	Por ocorrência	4
6	Não observar as políticas de segurança e normas de acesso do CONTRATANTE.	Por ocorrência	1
7	Manter empregado, que mantém relacionamento direto com o Contratante, tais como Preposto, Responsável Técnico e outros, sem qualificação para executar os serviços contratados.	Por ocorrência	3
8	Não zelar pelas instalações/ equipamentos do Contratante.	Por ocorrência	2
9	Não apresentar documentação exigida da empresa.	Por ocorrência	2
10	Violar quaisquer cláusulas do Acordo de Confidencialidade de Informação.	Por ocorrência	3
11	Deixar de comunicar qualquer fato relacionado ao serviço que leve à interrupção dos ambientes de TI do CONTRATANTE.	Por ocorrência	3
12	Transferir a outrem, no todo ou em parte, o serviço que não tenha sido objeto de subcontratação.	Por ocorrência	4
13	Atraso na realização dos itens 1, 2, 3 e 4 do objeto.	3% (três por cento) aplicados sobre o valor do item (12 meses), ao dia, até o vigésimo dia, limitada a 6% (seis por cento); 6% (seis por cento) aplicados sobre o valor do item (12 meses), ao dia, limitada a 18% (dezoito por cento), se o atraso ultrapassar 20 (vinte) dias, até o limite de 30 (trinta) dias; e 25% (vinte e cinco por cento) aplicados sobre o valor do item (12 meses), para atraso superior a 30 (trinta) dias.	
14	Descumprimento das SLA's estabelecidas por 2 (duas) vezes subsequentes.	Por ocorrência	1
15	Não emitir os certificados de participação aos participantes da capacitação.	Por ocorrência	5
17	Deixar de cumprir quaisquer das obrigações estabelecidas no instrumento contratual e anexos, desde que a multa não esteja prevista neste item.	Por ocorrência	2

7.8.3. Caso múltiplos itens sejam descumpridos simultaneamente, as multas podem ser acumuladas até o limite de 10% do valor total do contrato.

7.8.4. Para falhas severas e não corrigidas dentro do prazo máximo de 30 dias, a rescisão do contrato poderá ser solicitada sem prejuízo das multas já aplicadas.

7.9. **TERMO DE COMPROMISSO:**

7.9.1. Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados, colaboradores ou prestadores de serviços, que façam parte, a qualquer título, da equipe executante do Objeto deste Termo de Referência, a assinatura do ADENDO II - Termo de Confidencialidade , onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, cientes das obrigações assumidas e solidário no fiel cumprimento das mesmas.

7.10. **FORMA DE PAGAMENTO:**

7.10.1. **ITEM 1 (SUBSCRIÇÃO DE SOFTWARE DE PROTEÇÃO PARA ENDPOINT)**

7.10.1.1. Os pagamentos serão realizados em parcelas anuais;

7.10.1.2. Os valores serão reajustados de acordo com o item 7.22 deste Termo de Referência;

7.10.1.3. A primeira parcela referente às 6590 (seis mil quinhentas e noventa) licenças será paga após a distribuição e ativação do mínimo de 5500 (cinco mil e quinhetos) clientes;

7.10.2. **ITEM 3 (SERVIÇOS DE PLANEJAMENTO, CONFIGURAÇÃO, MIGRAÇÃO E TRANSFERÊNCIA DE CONHECIMENTO DE SOFTWARES, A FIM DE I OS PADRÕES DE UTILIZAÇÃO, AS CONFIGURAÇÕES BÁSICAS, E TRANSFERÊNCIA DE CONHECIMENTO PARA SUA UTILIZAÇÃO)**

7.10.2.1. Parcela única após aceite dos serviços pela CONTRATANTE;

7.10.3. **ITEM 4 (TREINAMENTO PARA ADMINISTRAÇÃO E CONFIGURAÇÃO DE SOFTWARE DE PROTEÇÃO ENDPOINT)**

7.10.3.1. Parcela única após aceite dos serviços pela CONTRATANTE;

7.11. **ACORDO DE NÍVEIS DE SERVIÇOS:**

SEVERIDADE	DESCRIÇÃO	PRAZO PARA ATENDIMENTO INICIAL	PRAZO PARA SOLUÇÃO DEFINITIVA

SEVERIDADE	DESCRIÇÃO	PRAZO PARA ATENDIMENTO INICIAL	PRAZO PARA SOLUÇÃO DEFINITIVA
ALTA	**Infecção por Malware ou Ransomware**: Detecção e disseminação de malware, ransomware, ou outras ameaças críticas que comprometem múltiplos sistemas ou a rede corporativa. Situações em que dados importantes estão em risco de serem criptografados, exfiltrados ou destruídos, exigindo ação imediata para conter a ameaça. **Comprometimento de Múltiplos Sistemas ou Servidores**: Incidentes em que um número significativo de dispositivos, servidores ou sistemas críticos está infectado ou indisponível, interrompendo operações essenciais da empresa. Ataques que afetam a continuidade dos negócios, como a paralisação de serviços críticos ou a impossibilidade de acessar sistemas e dados vitais. **Falha Crítica na Proteção do Antivírus:** Problemas em que o antivírus falha em detectar ou bloquear ameaças conhecidas, deixando a rede e os dados corporativos expostos a riscos graves. Falhas em módulos essenciais, como a proteção em tempo real, firewall, ou sistema de detecção de ameaças, que comprometem a segurança geral. **Ameaça Ativa de Segurança**: Incidentes onde há uma ameaça de segurança em andamento, como uma tentativa de invasão, exfiltração de dados, ou atividade maliciosa dentro da rede corporativa, exigindo resposta imediata. Casos de ataques direcionados, como spear-phishing ou ameaças internas, que colocam em risco dados sensíveis ou a integridade dos sistemas. **Interrupção de Serviços Críticos**: O antivírus está causando ou contribuindo para a interrupção de serviços ou operações essenciais, como sistemas de produção, banco de dados, ou serviços de rede, afetando a continuidade dos negócios. Conflitos graves entre o antivírus e outros softwares ou sistemas críticos, resultando em falhas ou paralisação de processos importantes. **Vulnerabilidades Não Resolvidas**: Situações em que o antivírus não consegue aplicar atualizações ou patches de segurança críticos, expondo a rede a vulnerabilidades conhecidas. Incapacidade de proteger a empresa contra novas ameaças devido a falhas na atualização das definições de vírus ou outros componentes de segurança. **Perda de Dados ou Risco de Violação**: Incidentes em que há perda de dados sensíveis, ou risco iminente de violação de dados, devido a falhas no antivírus ou ataques bem-sucedidos. Comprometimento de informações confidenciais ou estratégicas, exigindo medidas emergenciais para contenção e recuperação.	02 (duas) horas úteis	24 (vinte e quatro) horas corridas
MÉDIA	**Problemas de Desempenho Notáveis**: Relatos de degradação significativa no desempenho de sistemas ou aplicativos devido ao funcionamento do antivírus, afetando a produtividade de uma equipe ou departamento, casos onde a execução de verificações ou atualizações do antivírus está causando lentidão perceptível em múltiplos dispositivos. **Infecções Suspeitas ou Não Confirmadas**: Detecção de ameaças em arquivos ou sistemas que, embora não representem uma ameaça imediata, necessitam de investigação para evitar possível propagação. Casos onde o antivírus detectou uma ameaça, mas não foi capaz de removê-la completamente, requerendo ação manual ou ferramentas adicionais. **Configurações de Políticas ou Regras de Segurança**: Necessidade de ajuste em políticas ou configurações que estão causando problemas operacionais, como bloqueios indevidos de arquivos ou aplicativos necessários para o trabalho diário. Incidentes onde a configuração de políticas está impactando a capacidade de acessar recursos de rede ou serviços essenciais para um grupo de usuários. **Falhas em Atualizações ou Escaneamentos**: Problemas com atualizações de definições de vírus que não foram aplicadas corretamente, deixando os sistemas potencialmente vulneráveis. Falhas em escaneamentos programados ou manuais que não estão sendo concluídos, impactando a segurança de áreas específicas da organização. **Conflitos com Outros Softwares**: Conflitos com outros softwares de segurança ou sistemas operacionais que estão causando interrupções em processos ou serviços importantes. Incompatibilidades entre o antivírus e outros aplicativos corporativos que afetam a usabilidade ou a segurança, mas sem causar uma paralisação completa. **Propagação Limitada de Malware**: Casos onde um malware ou adware foi detectado e removido, mas há preocupação sobre uma possível propagação que precisa ser investigada em um ambiente específico. Incidentes onde um malware afetou um número limitado de dispositivos, mas foi contido antes de se espalhar. **Perda de Funcionalidades**: Falhas em módulos específicos do antivírus, como proteção em tempo real ou firewall, que afetam a segurança, mas não comprometem todo o sistema. Incapacidade de acessar ou utilizar determinadas funcionalidades do antivírus que são importantes para um grupo de usuários.	04 (quatro) horas úteis	48 (quarenta e oito) horas corridas

SEVERIDADE	DESCRIÇÃO	PRAZO PARA ATENDIMENTO INICIAL	PRAZO PARA SOLUÇÃO DEFINITIVA
BAIXA	**Dificuldades de Usabilidade**: Problemas menores relacionados à interface do antivírus, como dificuldades para encontrar determinadas configurações ou acessar relatórios. Pequenas inconsistências na interface do usuário, como mensagens de erro que não afetam a funcionalidade. **Questões de Configuração Não Críticas**: Solicitações para ajustar configurações específicas do antivírus, como modificar a frequência dos escaneamentos ou alterar as notificações de alertas, sem impacto significativo na segurança. Ajustes em políticas de exclusão para permitir que arquivos ou aplicativos específicos sejam ignorados durante escaneamentos. **Falsos Positivos Isolados**: Casos onde o antivírus identifica erroneamente um arquivo ou programa seguro como uma ameaça, sem impacto direto nas operações. Solicitações para revisar ou ajustar a lista de falsos positivos. **Alertas Informativos**: Notificações de alertas que não requerem ação imediata, como a detecção de arquivos potencialmente indesejados que não são considerados maliciosos. Atualizações de status informativas, como a confirmação de que um escaneamento foi concluído com sucesso, mas sem a necessidade de ação adicional. **Pequenos Problemas de Desempenho**: Relatos de impacto menor no desempenho de um ou mais dispositivos devido ao funcionamento do antivírus, como uma leve lentidão durante o escaneamento. Questões onde o antivírus está consumindo mais recursos do que o normal, mas sem comprometer a usabilidade. **Solicitações de Informações ou Relatórios**: Pedidos para gerar ou acessar relatórios de segurança ou logs de eventos, sem urgência. Dúvidas sobre o significado de determinados alertas ou mensagens do antivírus. **Compatibilidade Menor**: Pequenas incompatibilidades ou problemas de integração com outros softwares ou sistemas, que não impactam significativamente as operações diárias. Sugestões de melhoria para melhor compatibilidade ou integração com outros sistemas corporativos.	06 (seis) horas úteis	72 (setenta e duas) horas corridas

7.12. **MECANISMOS FORMAIS DE COMUNICAÇÃO:**

7.12.1. Sempre que se exigir, a comunicação entre o Gestor do Contrato e o Preposto da CONTRATADA deverá ser formal, considerando-se como documentos formais, além de documentos do tipo Ofício, as comunicações por correio eletrônico e/ou por software de gestão de contratos.

7.12.2. O Gestor do Contrato, os Fiscais e o Preposto responderão sobre todas as questões do contrato a ser firmado, procurando solucionar todos os problemas que defrontarem, dentro dos limites legais e dentro da razoabilidade.

7.12.3. Na eventualidade de problemas fortuitos, poderão ser convocadas reuniões por qualquer uma das partes, desde que comunicadas com antecedência.

7.13. **APROVAÇÃO E ATESTAÇÃO DAS ORDENS DE SERVIÇO:**

7.13.1. Os itens serão aceitos quando todos os objetivos propostos forem plenamente atingidos, e os produtos e serviços realizados e entregues com a qualidade demandada e devidamente aceita e aprovada pelo GESTOR/ FISCAL.

7.14. **VIGÊNCIA CONTRATUAL:**

7.14.1. A vigência contratual será de 36 (trinta e seis) meses;

7.14.2. O contrato poderá ser renovado até o limite estipulado pela lei 14.133/21 para o objeto da contratação, em havendo interesse das partes e respeitadas as exigências da legislação vigente;

7.14.3. Os pagamentos em caso de renovação devem seguir o especificado no item 7.10 deste Termo de Referência.

7.15. **GARANTIA CONTRATUAL:**

7.15.1. Não será exigida garantia contratual.

7.16. **TRANSFERÊNCIA DE CONHECIMENTO:**

7.16.1. A CONTRATADA realizará o repasse de conhecimento em capacitação à equipe técnica do CONTRATANTE, através de treinamento técnico realizado no item 4;

7.16.2. A CONTRATADA será responsável por especificar o ambiente necessário e prover o material a ser utilizado durante o treinamento;

7.16.3. A CONTRATADA fornecerá documentação completa do procedimento de instalação e migração da solução ao final dos trabalhos relacionados ao item 3 (as built);

7.16.4. Todo treinamento técnico e sua documentação deverão ser previamente aprovados pela CONTRATANTE e passarão a fazer parte do seu acervo documental;

7.16.5. Se o treinamento técnico fornecido não for satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizar novo treinamento sem ônus adicional à CONTRATANTE.

7.17. **DO REAJUSTAMENTO DE PREÇOS:**

7.17.1. Os preços inicialmente contratados são fixos e irrea justáveis no prazo de um ano contado da data do orçamento;

7.17.2. Após o interregno de um ano contado da data do orçamento, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, na forma do art. 24 da Instrução Normativa nº 01/2019;

7.17.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

7.18. **DO REGIME DE CONTRATAÇÃO:**

7.18.1. A presente contratação será processada sob o regime de empreitada por preço global, na forma do art. 6º, VIII, da Lei nº 14.133/21.

8. CRONOGRAMA FÍSICO-FINANCEIRO

8.1. O item 1 do objeto será pago em parcelas anuais correspondentes ao período de 12 meses de subscrição;

8.2. O item 3 do objeto será pago em parcela única após sua execução e aceite;

8.3. O item 4 do objeto será pago em parcela única após sua execução e aceite;

8.4. Estimativas:

ITEM	PREVISÃO PARA PAGAMENTO	EXIGÊNCIAS
1	48 (quarenta e oito) dias úteis	Assinatura do contrato, aceite do item 3 do objeto e distribuição mínima
2	Após ordem de fornecimento	Assinatura do contrato, aceite do item 3 do objeto
3	28 (vinte e oito) dias úteis	Assinatura do contrato, aceite do planejamento, aceite da migração
3	De acordo com o especificado nos itens 4.4.1 e 7.3.2	Assinatura do contrato, aceite do planejamento, aceite da migração

9. CLASSIFICAÇÃO ORÇAMENTÁRIA

Fonte de Recursos	Elemento(s) de Despesa
[X] FUNEPJ – Fundo Especial do Poder Judiciário	3.3.90.40.08 3.3.90.40.35 3.3.90.40.48

10. RESPONSÁVEIS PELA ELABORAÇÃO DO DOCUMENTO

Marcianne Ribeiro Antunes Lima

Integrante Demandante

Havirdan Das Rodor Araújo

Integrante Técnico

Vinícius Milere Moreira

Integrante Administrativo

11. APROVAÇÃO

Marcianne Ribeiro Antunes Lima

Secretária de Tecnologia da Informação

12. VALIDAÇÃO

Marcianne Ribeiro Antunes Lima

Secretária de Tecnologia da Informação

ADENDO I - PROPOSTA COMERCIAL

Ao
Poder Judiciário
TRIBUNAL DE JUSTIÇA DO ESTADO DO ESPÍRITO SANTO

Apresentamos a nossa proposta comercial para a prestação de serviços, conforme especificado abaixo.

Objeto: Contratação de licença de subscrição de software de proteção contra ameaças avançadas (NGAV) com suporte técnico (atualização de versão e assistência técnica) pelo período de 36 meses, além de implantação, migração das políticas e configurações da solução atualmente utilizada e treinamento para administração da solução.

ITEM	DESCRIÇÃO	QUANTIDADE A SER FORNECIDA	VALOR UNITÁRIO	VALOR TOTAL
1	Subscrição de software de proteção para endpoint (desktops) (12 meses)	6590		
2	Subscrição de software de proteção para endpoint (servidores físicos e virtuais) (12 meses)	160		
3	Serviços de planejamento, configuração, migração e transferência de conhecimento de softwares, a fim de definir os padrões de utilização, as configurações básicas, e transferência de conhecimento para sua utilização.	1		
4	Treinamento para administração e configuração de software de proteção endpoint	1		

VALOR GLOBAL*	

*Valor Global = Soma do item 1 cotado para 12 meses de subscrição + Soma do item 2 cotado para 12 meses de subscrição + item 3 + item 4.

Validade da proposta: mínimo de **90** ***(noventa)*** dias corridos, a contar da data de apresentação.

Declaramos que nos valores estão incluídas todas as obrigações legais e as despesas decorrentes e necessárias à efetiva execução dos serviços contratados, não sendo admitido nenhum acréscimo na proposta, tais como despesas com pessoal, seja de mão de obra própria ou locada, salários, alimentação, transportes, fretes, tributos em geral, incidências fiscais, comerciais, taxas e contribuições de qualquer natureza ou espécie, emolumentos em geral, seguros, encargos sociais, trabalhistas, previdenciários, comerciais e quaisquer outros encargos decorrentes do exercício profissional de seus funcionários ou terceirizados, que venham a incidir direta ou indiretamente sobre a execução do objeto contratado, não cabendo à proponente qualquer reclamação posterior.

Dados da Empresa:

Razão Social:

Endereço:

CNPJ:

Dados do Representante:

Nome do representante:

Cargo:

Telefones:

E-mail:

Local e data.

_____

Assinatura do Representante

ADENDO II - TERMO DE CONFIDENCIALIDADE

Ao Poder Judiciário

TRIBUNAL DE JUSTIÇA DO ESTADO DO ESPÍRITO SANTO

Rua Desembargador Homero Mafra, 60 Enseada do Suá, Vitória - ES - CEP 29050-906

Pelo presente termo, eu, conforme abaixo discriminado:

Nome Completo:	
CPF:	RG:
Nome da Empresa:	
Cargo ou função:	Nº da matrícula funcional (se aplicável):
Observações:	
Categoria:	

Comprometo-me a:

1) Manter, por tempo indeterminado, ou até autorização em contrário do PJES, a devida confidencialidade, requerida ou não, de quaisquer dados e/ ou informações pertencentes ao PJES ou por ele tratados ou custodiados e aos quais terei acesso ou conhecimento, seja verbalmente, por escrito ou visualmente (inclusive mantendo sigilo interno, quando aplicável, necessário ou solicitado), não os comercializando, reproduzindo, cedendo ou divulgando para pessoas não autorizadas a acessá-los ou conhecê-los, no todo ou em parte, direta ou indiretamente, sejam quais forem os meios ou formas utilizados – exceto quando necessário, justificável e autorizado pelo PJES.
2) Zelar pela integridade, disponibilidade, autenticidade e legalidade de quaisquer dados e/ ou informações pertencentes ao PJES ou por ele tratados ou custodiados e aos quais terei acesso ou conhecimento, não os utilizando para benefício próprio ou para fins que possam trazer prejuízos de qualquer natureza ao PJES, aos proprietários dos dados/ informações, a terceiros, ao Governo do Estado do Espírito Santo e/ ou União.
3) Não compartilhar nomes de usuários (logins), senhas, crachás, cartões magnéticos, tokens ou quaisquer outros dados, meios de autenticação ou credenciais individuais que a mim sejam fornecidos para meu uso exclusivo de serviços, recursos e/ou ativos gerenciados pelo PJES, cuja utilização será de minha total responsabilidade e deverá observar os aspectos de segurança da informação descritos no item 2 (dois).
4) Não permitir que pessoas não autorizadas manuseiem ou acessem quaisquer serviços e/ ou ativos de informação do PJES, ou tratados ou custodiados pelo mesmo (software, sistemas, equipamentos, acesso a redes físicas e sem fio) que estejam sob minha co-responsabilidade, seja em suas dependências ou fora delas.
5) Não autorizar que pessoas ingressem em ambientes restritos do PJES no qual, eu e/ ou elas, não tenhamos permissão de acesso, exceto mediante autorização do PJES e sob acompanhamento de um responsável do local.
6) Devolver, após o término de minha relação com o PJES, todas as mídias eletrônicas e/ ou impressas que possuam quaisquer dados e/ ou informações pertencentes ao PJES ou por ele tratados ou custodiados. Nos casos em que não houver essa possibilidade, comprometo-me a efetuar seu descarte seguro (ação sujeita à verificação do PJES).
7) Cumprir, a qualquer tempo, os controles da PSI (Política de Segurança da Informação) do PJES que sejam aplicáveis e relacionados ao escopo de minha relação com esta instituição, desde que a PSI e suas alterações sejam a mim fornecidas ou informadas por um gestor da área com a qual estou lidando, caso a PSI não possa ser encontrada no site oficial do PJES.
8) Informar imediatamente ao gestor do contrato, ou servidor indicado, com o qual estou interagindo, quaisquer incidentes de segurança da informação ocorridos ou prováveis de ocorrer, ou seja, quaisquer eventos que coloquem em risco a confidencialidade, integridade, disponibilidade, autenticidade e/ ou legalidade de dados e/ ou informações pertencentes ao PJES ou tratados ou custodiados pelo mesmo.

Adicionalmente, declaro estar ciente de que as atividades por mim executadas nas dependências do PJES, e/o u em locais onde eu utilize ativos de sua propriedade, poderão ser monitoradas, fiscalizadas e auditadas pelo PJES, a qualquer tempo, mesmo sem minha anuência ou aviso prévio, excetuando-se as restrições legais vigentes e aplicáveis.

OBSERVAÇÕES: Estão em vigor a Resolução nº 06/2018, que estabeleceu a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Espírito Santo; o Ato Normativo nº 41/2018, que instituiu a Norma de Controle de Acesso aos Sistemas de Informação do Poder Judiciário do Estado do Espírito Santo; e o Ato Normativo nº 42/2018, que instituiu a Norma de Controle de Acesso aos Sistemas de Informação do Poder Judiciário do Estado do Espírito Santo, que estabelecem as regras para a política de segurança do Contratante.

Para dirimir quaisquer controvérsias acerca do presente termo, fica eleito o Foro da cidade de Vitória/ES, com exclusão de qualquer outro, por mais privilegiado que seja.

Vitória/ES, XX de..... de 20XX.

<Nome>

<Empresa>

Representante Legal da Empresa

Para Uso do PJES			
Recebido por:	Área:	Data:	Assinatura:
Nº do contrato:		Nº do processo:	

Nos termos do FORMULÁRIO VI da Norma de Procedimento 09, assinam:

o Integrante Demandante, o Integrante Técnico, o Integrante Administrativo responsáveis pela elaboração do documento;

o Secretário(a)/Assessor titular da área demandante responsável pela aprovação do documento;

e o Secretário de Tecnologia de Informação responsável pela validação do documento .

Documento assinado eletronicamente por **HAVIRDAN DAS RODOR ARAUJO**, **COORDENADOR DE SUPORTE E MANUTENCAO**, em 26/09/2024, às 14:52, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **VINICIUS MILERE MOREIRA**, **TECNICO JUDICIARIO AE TECNICO EM INFORMATICA**, em 26/09/2024, às 15:33, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCIANNE RIBEIRO ANTUNES LIMA**, **SECRETARIO DE TECNOLOGIA DA INFORMACAO**, em 26/09/2024, às 18:04, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sistemas.tjes.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2242776** e o código CRC **1286314E**.

7006039-55.2024.8.08.0000 2242776v224