1- DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Contratação de empresa especializada em Serviços Gerenciados de Segurança da Informação (GSTI) para implantação e execução de serviços de Segurança da informação, cibernética e da proteção de dados incluindo as ferramentas e alocação de mão de obra dedicada nas dependências do PJERJ, de acordo com as condições e especificações técnicas estabelecidas neste Termo de Referência, pelo prazo de 24 meses.

VISÃO GERAL DO SERVIÇOS			
Item	**Descrição**	**Medição**	**Atuação**
1	**Governança e Gestão de Segurança Informação:** Tem como premissa geral a garantia da confidencialidade, a integridade, a disponibilidade e a autenticidade de todos os serviços e informações do PJERJ e objetivo principal apoiar a implantação da Governança de Segurança da Informação no CONTRATANTE, realizando serviços de levantamento e planejamento de ações em conjunto com o CONTRATANTE para implantação das políticas e normas vigentes, bem como, a revisão periódica destas ações e normas, promovendo uma conformidade legal e procedimental baseado em boas práticas, inclusive fatores sociais e culturais importantes para processo de governança.	Mensal	Rotineira
2	**Gestão de Risco de Segurança da Informação:** Executar serviços para estabelecer uma gestão de riscos de segurança da informação que permitam identificar, analisar e avaliar riscos, criar uma matriz de riscos e possibilitar o tratamento adequado, através da evitação, da aceitação, da mitigação, da eliminação ou da transferência.	Mensal	Rotineira
3	**Privacidade e Proteção de Dados:** executar serviços para estabelecer um gerenciamento de dados de forma a proteger dados e informações em todos os processos, (coleta, processamento, disseminação, armazenamento de dados) abrangendo inclusive	Mensal	Rotineira

	questões de privacidade, proteção de dados pessoais, direitos de titulares e possíveis efeitos e danos decorrentes de incidentes.			
4	**Gestão de Segurança de Ativos:** Executar serviços para implantar o gerenciamento de todos os ativos previstos nos normativos do CONTRATANTE, em especial o ATO NORMATIVO TJ N.º 10/2019, planejando e coordenando ações juntamente com a área de operações para uma proteção efetiva desses ativos, contemplando segurança de infraestrutura, de software e de dados.	Mensal	Rotineira	
5	**Gestão de Incidentes de Segurança, Vulnerabilidades, Ameaças:** Executar serviços para o gerenciamento incidentes, com ferramentas automatizadas, levantar e monitorar vulnerabilidades e ameaças. Propor e coordenar a criação de protocolos de prevenção de incidentes e gestão de crises, além de propor ações preventivas e corretivas, de forma proativa, bem como testes periódicos de segurança. Coordenar ações defensivas e ofensivas de segurança, incluindo ataques cibernéticos	Mensal	Rotineira	
6	**Gestão de Usuários**: executar serviços para implementar uma proteção adequada para informação do PJERJ baseada nas pessoas, contemplando gerenciamento de identidades, acessos e privilégios, abrangendo usuários comuns internos e externos, administradores e desenvolvedores.	Mensal	Rotineira	
7	**Gestão de Problemas:** Executar serviços de segurança que permitam a identificação da causa raiz de incidentes, apresentando e coordenando plano para correções definitivas ou soluções de contorno.	Mensal	Rotineira	
8	**Gestão de Continuidade de Serviços:** Executar serviços para planejar e coordenar ações e procedimentos padronizados para recuperação de	Mensal	Rotineira	

	desastres e continuidade dos serviços essenciais no menor tempo possível, mesmo em condições adversas.		
9	**Gestão do Conhecimento:** Executar serviços que permitam a criação em conjunto com o CONTRATANTE de uma base de conhecimento permanente e sempre atualizada de boas práticas e lições aprendidas, com o auxílio de ferramenta automatizada.	Mensal	Rotineira
10	**Gestão de Comunicação e Educação:** Executar serviços que permitam a criação de um plano de comunicação permanente e institucionalizado, em especial em caso de incidentes graves com procedimentos padronizados e estabeleçam uma política educacional e de conscientização de segurança da informação.	Mensal	Rotineira
11	**Gestão de Projetos e Inovações de Segurança da Informação:** Executar serviços que possam prospectar soluções ou inovações que possam contribuir para a melhoria da qualidade da segurança da informação do CONTRATANTE, apoiando tecnicamente projetos e aquisições.	Mensal	Rotineira
12	**Auditoria e Investigação:** Executar serviços que façam a verificação periódica de conformidade dos normativos e procedimentos implantados, propondo e coordenando ações corretivas. Propor a criação de normas e protocolos de investigação, correlacionando histórico de eventos, em especial os relacionados a ilícitos, que permitam de forma integrada a continuidade dos serviços e a preservação de possíveis evidências da investigação.	Mensal	Rotineira
13	**Melhorias:** Executar serviços para planejar e coordenar ações visem permanentemente a melhoria da qualidade da segurança da informação do CONTRATANTE.	Mensal	Rotineira

2- REQUISITOS DE NEGÓCIOS - UNIDADE DEMANDANTE	
2.1 – Necessidade do Negócio	
Necessidade 1: Prover soluções de segurança em diversos níveis para o PJERJ.	
Funcionalidade	**Ator Envolvido**
Existem várias funcionalidades que devem ser providas para se garantir uma segurança efetiva, seja para as informações de usuário como para as informações corporativas, que no caso do PJERJ, envolvem conjuntos de dados e em muitas vezes de caráter sigiloso.	Ativos e sistemas de informática que, direta ou indiretamente, fazem uso do Data Center do PJERJ.
Necessidade 2: Estrutura e equipe específica de segurança da informação	
Funcionalidade	**Ator Envolvido**
Profissionais capazes de fazer a gestão em tempo integral com ferramentas de detecção, prevenção e correção de possíveis vulnerabilidades e ameaças internas e externas, como preconiza Res. CNJ n.º 396/2021.	Profissionais capacitados, ativos de informática, sistemas e ferramentas.
Necessidade 3: Permitir que a solução seja escalável.	
Funcionalidade	**Ator Envolvido**
Escalabilidade é a capacidade que uma solução tem de ser aumentada em seus recursos, conforme a necessidade, e desta forma ser capaz de fazer o aumento da demanda com relativo baixo investimento.	Ativos e sistemas de informática que, direta ou indiretamente, fazem uso do Data Center do PJERJ.
Necessidade 4: Ampla defesa do perímetro.	
Funcionalidade	**Ator Envolvido**
Com o tempo, a medida que novas tecnologias foram empregadas na prestação jurisdicional, foi necessária a abertura de novas frentes de comunicação, não apenas a internet com o mundo exterior, como por exemplo a comunicação com órgãos parceiros, como bancos, além de redes virtuais privadas com outros órgãos do judiciário, como por exemplo o CNJ e também a comunicação com as comarcas e regionais. Todos estes perímetros, podem ser alvos de ataque e como consequência, serem porta de entrada para ataques na rede interna do PJERJ.	Perímetros de entrada na rede do PJERJ: Internet, links de parceiros, VPN com demais órgãos públicos, comarcas e regionais.
2.2– Demais Requisitos	

Tipo 1: Capacitação	A empresa contratada deverá comprovar possuir em seu quadro de funcionários, pelo menos, os seguintes títulos/certificações: • Certificação ITIL 4 Foundation. • Pós-graduação em Gerência de Projetos ou certificação PMI PMP. • Certificação CISSP (ISC2) ou CISM (ISACA) • Certificação Security+. • Certificação CEH. • Certificação OSCP – Offensive Security. • Certificação OSCE - Offensive Security. • Certificação Hacking Forensics Investigator. • Certificação Information Security Foundation ISO IEC 27001. • CompTIA Security+ (Comptia). • LPIC-1. • ECIH – EC-Council Certified Incident Handler.
Tipo 2: Requisitos Legais	A contratação a que se refere esta análise de viabilidade observará as seguintes leis e normas: Lei n° 14.133, de 01 de abril de 2021, que institui as normas para licitações e contratos na Administração Pública. Lei n° 10.520 de 17 de julho de 2002, que institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns. Resolução N° 182, de 17 de outubro de 2013, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos Órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).
Tipo 3: Requisitos de Manutenção	Deverá ser fornecido suporte técnico especializado, que englobará os serviços realizados onde haja necessidade de prestação de assistência intelectual, pela transmissão de conhecimentos e informações específicas, que auxiliem na operação da solução tecnológica, incluídos aí quaisquer alterações na implementação do projeto original.
Tipo 4: Requisitos Temporais	A solução deverá possuir garantia técnica de 90 (noventa) dias, após o término do contrato, sobre os serviços concluídos ou pendentes.

Tipo 5: Requisitos de Segurança	A contratada deverá executar todas as atividades da prestação de serviço objeto da contratação com base nas boas práticas de segurança da informação, em especial as indicadas nos normativos do PJERJ, norma NBR ISO/IEC 27002 e Gerenciamento de Segurança da Informação da Biblioteca ITIL4.
Tipo 6: Requisitos sociais, ambientais e culturais	A contratada deverá obedecer aos critérios de gestão ambiental estabelecidos na legislação, normas e regulamentos específicos do serviço, visando à melhoria dos processos de trabalho quanto aos aspectos ambientais, sociais e econômicos.

3- LEVANTAMENTO DAS SOLUÇÕES EXISTENTES

Solução	Entidade	Valor
1– Serviços contínuos de SOC (Security Operation Center ou Centro de Operações de Segurança), no intuito de garantir a segurança das informações.	TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO	R$ 5.569.100,13
Fornecedor: NEC SOLUCOES DE SEGURANCA CIBERNETICA BRASIL S.A.		
Solução	**Entidade**	**Valor**
2 – Serviços Gerenciados de Segurança da Informação	CONSELHO DA JUSTIÇA FEDERAL - CJF	R$ 2.440.054,88
Fornecedor: ISH TECNOLOGIA S.A.		
Solução	**Entidade**	**Valor**
3 – Serviço de administração, operação e manutenção, atendimento a requisições e serviços gerenciados a segurança da informação.	CONSELHO DA JUSTIÇA FEDERAL - CJF	R$ 3.205.030,43
Fornecedor: ISH TECNOLOGIA S.A.		

4- ANÁLISE DAS SOLUÇÕES E ALTERNATIVAS EXISTENTES

Requisito	Identificação da Solução existente	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração pública federal?		X		
A solução está disponível no Portal do Software Público Brasileiro				X
A solução é um software livre ou software público				X
A solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?				X
A solução é aderente às regulamentações da ICP-Brasil?				X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do – Moreq-Jus Brasil?				X

5- JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

5-1- Solução Escolhida

Descrição:

O Brasil ocupa a 70ª colocação no índice de segurança cibernética da União Internacional de Telecomunicações (ITU, na sigla em inglês), órgão da Organização das Nações Unidas (ONU) que coordena esforços nesta área. Essa situação de fragilidade faz com que o país seja hoje o segundo no mundo que mais tem sofrido perdas econômicas advindas de ataques cibernéticos. Segundo os dados mais recentes da ITU, numa medição de 12 meses entre 2017 e 2018, os prejuízos advindos dos ataques cibernéticos no Brasil ultrapassaram US$ 20 bilhões (mais de R$ 80 bilhões). Portanto, qualquer infraestrutura de Tecnologia da Informação e Comunicação no Brasil está sujeita a ataques e, com isto, a segurança cibernética é de suma importância para a proteção de dados e serviços oferecidos aos cidadãos.

O Poder Judiciário Brasileiro tem estabelecido estratégias nacionais em períodos sexenais, nos quais cada vez mais a tecnologia está presente. Transformação Digital e Plataforma Digital do Poder Judiciário são termos incorporados ao cotidiano dos Tribunais, criando uma dependência cada vez maior da tecnologia para a eficácia da prestação jurisdicional.

A mais recente estratégia nacional foi estabelecida pelo Conselho Nacional de Justiça (CNJ) através da Resolução CNJ n.º 325/2020, tendo ainda uma estratégia suplementar e específica para a área de Tecnologia da Informação e Comunicação (Res. CNJ n.º 370/2021), no qual um dos macroprocessos é a segurança da informação.

Essa diretriz de segurança da informação é justificável, pois a informação passou a circular não só em meio físico, mas também em meio eletrônico, o que requer cuidados maiores.

Paralelamente aos benefícios incorporados pelas tecnologias, aumenta a preocupação com a proteção desses dados e informações, que podem ser alvo de cobiça e consequentemente ataques cibernéticos.

A Segurança da Informação é a proteção de dados de propriedade das organizações contra ameaças diversas. Trata-se de um esforço pautado por ações que objetivam mitigar riscos e garantir a continuidade das operações.

Para que essa proteção seja efetivada é necessário um conjunto de recursos organizacionais especializado em 3 (três) níveis: Estratégico, Tático e Operacional garantido que ações integradas sejam planejadas e executadas reduzir os riscos e proteger as informações.

O Poder Judiciário do Estado do Rio de Janeiro (PJERJ) possui uma estrutura dedicada a segurança da informação, portanto ações de gerenciamento de riscos, ameaças e vulnerabilidades não são realizadas de forma continuada por falta de pessoal qualificado e dedicado, bem como ferramentas adequadas para enfrentar possíveis ataques cibernéticos.

Buscou-se através desta análise realizar um estudo para concluir qual das alternativas elencadas deveria ser a escolhida, levando-se em conta requisitos de qualidade da solução, atendimento ao propósito, além da economicidade. Como as soluções analisadas servem como um parâmetro, mas não atendem em todos as necessidades do PJERJ, é necessária a contratação de um serviço técnico especializado para atender as demandas e ações que garantam de forma gerenciada e contínua a proteção das informações do PJERJ.

A pretensa contratação irá contribuir para concretizado do objetivo estratégico "Promoção da proteção de dados organizacionais" contemplados no Mapa Estratégico do PJERJ 2021-2026.

O PJERJ ao realizar a presente contratação também atenderá aos requisitos elencados na Res. CNJ n.º 370/2021, na Res. TJ/OE n.º 09/2017, Res. TJ/OE n.º 05/2019, Ato Normativo TJ nº 08/2019, Ato Normativo TJ n.º 10/2019 e Ato Normativo TJ n.º 27/2020.

Bens e Serviços	Valor Total Estimado
1. Serviço de Governança e de Gestão de Segurança da Informação;	Aguardando o resultado da pesquisa de mercado.
2. Serviço de Privacidade e Proteção de Dados;	
3. Serviço de Gestão de Segurança de Ativos;	
4. Serviço de Gestão de Incidentes de Segurança, Vulnerabilidades, Ameaças;	
5. Serviço de Gestão de Usuários;	
6. Serviço de Gestão de Problemas;	
7. Serviço de Gestão de Continuidade de Serviços;	
8. Serviço de Gestão do Conhecimento;	
9. Serviço de Gestão de Comunicação e Educação;	
10. Serviço de Gestão de Projetos e Inovações de Segurança da Informação;	
11. Serviço de Gestão de Risco de Segurança da Informação;	
12. Serviço de Auditoria e Investigação;	
13. Serviço de Melhorias.	

Justificativa:

Face ao alto grau de informatização do Poder Judiciário Nacional em geral e o grau de dependência da TIC para garantir uma prestação jurisdicional mais eficiente, a área de TIC do PJERJ tem sofrido um aumento constante em escala exponencial da demanda por seus serviços, agregada a uma complexidade cada vez maior deles.

Associados a esse aumento de demanda existe uma necessidade de proteção desses serviços contra ameaças e vulnerabilidades que podem ser exploradas em ataques cibernéticos.

O PJERJ, apesar de ter estabelecido uma Política de Segurança da Informação através da Res. TJ/OE n.º 05/2019, ainda não possui estrutura específica de segurança da informação, nem profissionais capazes de fazer essa gestão em tempo integral com ferramentas de detecção, prevenção e correção de possíveis vulnerabilidades e ameaças internas e externas, como preconiza Res. CNJ n.º 370/2021. Todo o processo de segurança da informação é executado apenas no nível operacional, vinculado ao Departamento de Infraestrutura de TIC, da Diretoria-Geral de Tecnologia da Informação e Comunicação de Dados.

Sem a implementação de uma gestão de segurança com profissionais qualificados e dedicados, a proteção dos serviços de TIC pode ficar comprometida, causando graves impactos e danos para toda a atividade do PJERJ, se as medidas protetivas adequadas não forem adotadas.

Assim sendo, é imprescindível a contratação de uma empresa especializada para o gerenciamento de segurança da informação no PJERJ.

6-BENEFÍCIOS ESPERADOS

Benefícios Operacionais
1 - Melhoria do gerenciamento de capacidade dos serviços de segurança.
2 - Aumento da capacidade da prestação de serviços de segurança proativos.
3 - Melhoria no tempo de solução das requisições de incidentes.
4 - Redução no número de incidentes.
5 - Melhoria no gerenciamento do conhecimento.
6 - Redução da dependência sobre as pessoas chaves.
7 - Ganho de eficiência no atendimento de incidentes de maior impacto.
8 - Redução dos riscos de segurança.
9 - Melhoria da qualidade no tratamento de risco de segurança.
10 - Melhoria na capacidade de recuperação de incidentes e desastres de segurança.
11 - Redução da indisponibilidade dos serviços vitais para o negócio.
12 - Redução no número de mudanças com falhas ou não autorizadas.
Benefícios aos clientes e usuários dos serviços do PJERJ
1 - Clareza na definição de regras e responsabilidades.
2 - Conscientização de segurança da informação.
3 - Melhoria da proteção das informações utilizadas nos serviços.
4 - Melhoria da confiança na utilização dos sistemas informatizados.
5 - Melhoria generalizada na reputação da Segurança da Informação.

7-AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO PARA EXECUÇÃO CONTRATUAL

Tipo de Necessidade	Descrição
Infraestrutura prevista no subitem 6.5.7 do TR.	Disponibilizar instalações físicas, telefones fixos para comunicação interna entre as serventias do PJERJ, computadores, sistemas para uso interno e impressoras para os profissionais da CONTRATADA lotados nas dependências do PJERJ com a finalidade única de exercer atividades relacionadas à execução do contrato.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Técnico	Integrante Demandante	Integrante Administrativo
_____ Rafael Petronilha de Lima Matrícula 31457	_____ Ivan Lindenberg Júnior Matrícula 19346	_____ Beatriz Elisa Amorim dos Santos Matrícula 32071

Rio de Janeiro, 13 de outubro 2021.