TJMG

Demanda 17371

Título:

Contratação de serviços gerenciados de segurança, de natureza continuada, com fornecimento de

Gestor da Carteira de Demandas DIRFOR:

DIRFOR

A demanda será conduzida como projeto tradicional?:

Sim

Descrição:

Contratação de serviços gerenciados de segurança (*managed security services* - MSS), de natureza continuada, com fornecimento de ferramentas e de equipe técnica especializada, incorporando, no mínimo: governança de segurança de TIC; centro de operações de monitoramento e detecção de eventos de segurança [SOC e SIEM] e equipe de tratamento e resposta a incidentes de segurança [ETIR]; gestão e avaliação de risco, ameaças e vulnerabilidades de segurança de TIC; avaliação, testes, mentoria e melhoria contínua da segurança de sistemas e aplicações.

Motivação:

A segurança cibernética e da informação é tema que sempre foi de fundamental importância para as organizações e, com o vertiginoso crescimento da digitalização dos serviços e das atividades fim e administrativas do Tribunal, com o uso intensivo e direto de tecnologia da informação, se torna um aspecto cada vez mais crítico para o Tribunal, para a prestação jurisdicional e, em especial, para a Diretoria Executiva de Informática (DIRFOR).
Segurança da informação ganhou notoriedade e padronização a nível global quando o British Standards Institution (BSI) Group, organismo de padrões nacionais do Reino Unido, publicou a primeira norma BS 7799 em 1995, adotada como norma internacional ISO/IEC 17799 em 2000 e se tornando a série de normas internacionais ISO 27000 em 2005, com muitos acréscimos e atualizações desde então. Boa parte das normas está traduzida no Brasil pela ABNT. Destacam-se as normas ABNT/ISO 27001 e 27002, largamente difundidas, que detalham respectivamente os requisitos para sistemas de gestão da segurança da informação (SGSI) e código de prática para controles de segurança da informação, baseadas em conceitos fundamentais de confidencialidade, integridade, disponibilidade, autenticidade, não repúdio.
A segurança da informação vem evoluindo e crescendo continuamente nas décadas que se seguiram, e atualmente no mundo digital, tem sido utilizado o termo cibersegurança ou segurança cibernética, englobando o gerenciamento de riscos de segurança da informação, salvaguardando pessoas, organizações e sociedades contra vulnerabilidades, ameaças e ataques, quando a informação está em forma digital em computadores, armazenamento e redes.
Integram também o universo de temas abordados: gestão e avaliação de riscos (em especial os de segurança e de tecnologia da informação), continuidade de negócios e resiliência organizacional, tratamento e resposta a incidentes de segurança, forense digital, privacidade e proteção de dados

pessoais, segurança em nuvem.

Além de ISO e ABNT, outras organizações de referência internacional, governamentais e independentes da comunidade, tem consolidado, difundido e atualizado constantemente modelos (frameworks) e controles de cibersegurança, dentre os quais podemos citar alguns mais proeminentes: National Institute of Standards and Technology (NIST) dos Estados Unidos, Center for Internet Security (CIS), MITRE (originário do Massachussets Institute of Technology), Cloud Security Alliance (CSA), a fundação de código aberto Open Web Application Security Project (OWASP), dentre outros.

Observa-se, portanto, que o universo de cibersegurança é muito amplo e muito complexo. Exige conhecimentos altamente especializados, atualização constante, atuação dinâmica e eficaz, em suma, grandes e variados esforços, organização, orquestração e governança em termos de processos, pessoas e ferramentas.

Desde o início dos anos 2000 a DIRFOR tem envidado investimentos em planejamento, formação de pessoal, aquisição de produtos e serviços, normativos, ações específicas, campanhas de sensibilização etc. relativos a segurança da informação no âmbito de tecnologia.

Contudo, fatores recentes ampliaram e aceleraram muito os desafios e necessidades, de forma urgente e sem precedentes:

- O uso ainda mais intensivo, complexo e distribuído de tecnologia da informação, serviços e recursos digitais nas atividades fim e administrativas, dentro e fora das dependências do Tribunal, com os adventos da pandemia de COVID-19 e do teletrabalho e a crescente adoção de serviços em nuvem.
- As demandas decorrentes da entrada em vigor da Lei Federal nº 13.709 de 14/08/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).
- As exigências decorrentes da Resolução CNJ nº 396 de 07/06/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
- Casos recentes cada vez mais frequentes de ameaças avançadas e direcionadas, incidentes em instituições próximas de ataques de ransomware (sequestro digital), vazamento de dados, hacktivismo (ativismo político hacker).

Mesmo com os esforços da DIRFOR, a capacidade limitada de pessoal -- não só em quantidade e especialização mas em experiência adequada --, bem como a carência de ferramentas internas -- muitas delas software livre com recursos e suporte restritos --, além do acelerado avanço das necessidades estratégicas e operacionais, ameaças e obrigações de conformidade legal e normativa, tornam inviável a DIRFOR atender e operacionalizar adequadamente os níveis de segurança cibernética e proteção de dados sem recorrer ao mercado especializado.

Demonstrativo dos benefícios e resultados a serem alcançados:

Benefícios e resultados a serem alcançados:

- Prover meios adequados e especializados, em termos de pessoas, processos e tecnologias, para a gestão, implementação e manutenção eficaz dos controles e salvaguardas de segurança cibernética e proteção de dados pessoais e prover o apoio à gestão e governança da segurança da informação na DIRFOR;
- Operacionalizar um centro de segurança cibernética que componha as funções de segurança de identificar, proteger, detectar/diagnosticar, responder e recuperar, atuando desde o monitoramento e detecção de eventos de segurança, gestão de riscos, vulnerabilidades e ameaças, até o tratamento e resposta a incidentes e o apoio às diversas áreas da DIRFOR na prevenção, remediação e melhorias relacionadas;

•Elevar o nível de segurança cibernética no TJMG, sua maturidade e melhoria contínua, visando estabelecer o nível adequado de controle sobre a confidencialidade, integridade e disponibilidade dos ativos de TIC e das informações digitais do TJMG;
•Garantir conformidade e alinhamento com os requisitos de negócio, regulamentos pertinentes, a tolerância a riscos e os recursos da organização, com visibilidade e transparência;
•Contribuir na difusão e disseminação da cultura e sensibilização dos conceitos, procedimentos, práticas e controles de segurança cibernética na DIRFOR e, por consequência, no TJMG.

Detalhamento das características, abrangência, legislação, normativos, restrições de prazo

Detalhamento das características:
•Planejamento e gestão dos serviços, incluindo alocação de gerente de projeto e de contas, preposto e mobilização inicial;
•Governança de segurança de TIC, incluindo diagnósticos e análises, definição de métricas, políticas, processos e procedimentos, elaboração de painéis (dashboards) e relatórios periódicos;
•Monitoramento e detecção de eventos e tratamento e resposta de incidentes de segurança, incluindo estabelecimento de um centro de operações de segurança (SOC) 24x7 e de uma equipe de tratamento e resposta a incidentes de segurança (ETIR) e ferramenta de gerenciamento de eventos e informações de segurança (SIEM);
•Gestão e avaliação de riscos, vulnerabilidades e ameaças de segurança de TIC, incluindo ferramenta de varredura e avaliação de vulnerabilidades, testes periódicos de penetração;
•Operacionalização de um framework de cibersegurança, incluindo um plano de ação continuada de controles e salvaguardas de segurança cibernética, medidas de remediação e mitigação;
•Avaliação, testes, mentoria e melhoria contínua da segurança de sistemas e aplicações, incluindo ferramenta de testes de segurança de aplicações (AST).
Abrange diretamente pelo menos 9 dos 18 Controles Críticos de Segurança do CIS v8 -- 04. Configuração segura de ativos, 07. Gestão contínua de vulnerabilidades, 08. Gestão de registros de auditoria, 10. Defesas contra malware, 13. Monitoramento e defesa da Rede, 14. Conscientização sobre segurança e treinamento de competências, 16. Segurança de aplicações, 17. Gestão de respostas a incidentes, 18. Testes de invasão -- e contribui para os demais.

Esta demanda se alinha perfeitamente ao Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados, em processos internos da ENTIC-JUD, Resolução CNJ nº 370/2021, art. 2º, inciso I, alínea c; e atende à maioria das medidas para elevar o nível de segurança das infraestruturas críticas na ENSEC-PJ, Resolução CNJ nº 396/2021, em especial quase todos os incisos do artigo 11:
•I - Estabelecer ações que possibilitem **capacidade de responder de forma satisfatória a incidentes de segurança**;
•II - Instituir e manter **Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)**;
•III - Elaborar e aplicar **processo de resposta e tratamento a incidentes de segurança cibernética**;
•IV - Utilizar **tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes** de ativos de informação e de ações de usuários;
•V - Utilizar **tecnologia que permita a inteligência em ameaças cibernéticas** em redes de informação;
•VII - elaborar **requisitos específicos de segurança cibernética** relativos aos ativos sob sua

- VII - elaborar **requisitos específicos de segurança cibernética** relativos aos ativos sob sua jurisdição;
- X - Realizar, ao menos semestralmente, **avaliação e testes de segurança cibernética** de forma a **aferir a eficácia dos controles estabelecidos**;
- XI - Realizar prática em **gestão de incidentes e efetivar o aprimoramento contínuo do processo**.

Principais leis e normas pertinentes:

- Lei Federal nº 13.709 de 14/08/2018, Lei Geral de Proteção de Dados Pessoais (LGPD);
- Resolução CNJ nº 396 de 07/06/2021, institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Portaria CNJ nº 162 de 10/06/2021, Anexos I a V, Protocolos e Manuais de Referência complementares da ENSEC-PJ;
- Resolução CNJ nº 370 de 28/01/2021, estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Portaria da Presidência TJMG nº 4718/PR/2020 de 10/02/2020, institui a Política de Segurança da Informação (PSI) no âmbito da Tecnologia da TIC do TJMG e dispõe sobre o Modelo de Gestão de Segurança da Informação (MGSI);
- Resolução TJMG nº 969/2021 de 12/07/2021, dispõe sobre os Comitês de Assessoramento e as unidades organizacionais diretamente subordinadas à Presidência;
- Normas internacionais ISO/ABNT série 27000 de tecnologia da informação - técnicas de segurança da informação;
- Normas internacionais ISO/ABNT série 22300 de segurança e resiliência - gestão de continuidade de negócios;
- Normas internacionais ISO/ABNT série 31000 de gestão de riscos.

Detalhamento Técnico Inicial:

Estimativa de Esforço:

Estimativa de Recursos Humanos Envolvidos:

Estimativa de Custo (Aquisição):

3 - Acima de R$ 176.000,00