Controle de versão - 28/11/2024

PODER JUDICIÁRIO DO ESTADO DE MINAS GERAIS - TRIBUNAL DE JUSTIÇA

LEIA E SIGA COM ATENÇÃO AS ORIENTAÇÕES ABAIXO.

ORIENTAÇÕES PARA PREENCHIMENTO:

Esse documento deverá ser preenchido para Programas, Projetos ou Ações que envolvam demandas de Tecnologia da Informação e encaminhado para o NUGEPRO - Núcleo de Gestão de Projetos.

· As demandas exclusivamente relacionadas às requisições de equipamentos de Tecnologia da Informação devem ser encaminhadas para a DIRFOR - Diretoria Executiva de Informática.

· O formulário deverá ser preenchido em todos os seus campos e assinado pelo magistrado responsável pela área.

· Em caso de dúvidas com relação ao preenchimento deste formulário, favor entrar em contato com o NUGEPRO - Núcleo de Gestão de Projetos: (31) 3306-3047.

· Abra somente um DOD por processo SEI.

1. Identificação da área demandante:

1.1. Se área de Primeira Instância (Se não for de Primeira Instância, selecione "NÃO" em "Comarca" e "Nome da área"):

1.1.1. Comarca:
0024 - Belo Horizonte

1.1.2. Nome da área:
NÃO

1.2. Se área de Segunda Instância ou Secretaria do TJMG (Se não for de Segunda Instância, selecione "NÃO" em "Superintendência" e "Unidade Gestora"):

1.2.1. Superintendência:
NÃO

1.2.2. Unidade Gestora:
GEOPE-Gerência de Suporte à Operação de Equipamentos

2. Servidor responsável pela demanda:

2.1. Nome:
Tatiana Cristiana Mendes Hanum

2.2. Matrícula (ex.: t0000000):
t0063784

2.3. Cargo:
Gerente

2.4. E-mail:
tatianamendes@tjmg.jus.br

3. Identificação da demanda:

3.1. Detalhar o título da demanda (Exemplo: Compra de Sistema para Gestão de Projetos):
Contratação de solução de proteção endpoint

3.2. Descrição da demanda:
Descrever a demanda como um todo. Recomenda-se indicar se a demanda decorre de determinação da Lei, do CNJ ou de atos normativos, bem como indicar eventuais prazos para o cumprimento dessa.
A solução atualmente utilizada pelo TJMG, Symantec Endpoint Protection, possui uma tecnologia de proteção já defasada em relação as ferramentas disponíveis no mercado. Utilizada desde 2018, essa solução não atende às necessidades tecnológicas e operacionais atuais do Tribunal.
É necessário então uma solução moderna e integrada de Gerenciamento de Endpoint para atender às necessidades do TJMG relacionadas ao gerenciamento, controle e segurança de dispositivos conectados à sua infraestrutura de TI.

3.3. Essa demanda está vinculada à alguma Resolução do CNJ?
Não

Se "Sim", qual?
-

3.4. Existe alguma expectativa de prazo para implantação (Alta Administração/Normativo/Resolução CNJ)?
Sim, prazo para contratação até julho/2025.

4. Descrição da demanda:

4.1. Justificativa(s) da necessidade
(Pergunta a ser respondida: Por que essa demanda é necessária?):

O avanço tecnológico e a crescente digitalização dos processos institucionais exigem que o TJMG assegure uma infraestrutura de TI robusta e segura. No entanto, o ambiente atual enfrenta desafios significativos na gestão e proteção dos dispositivos de endpoint, que incluem computadores, notebooks e outros dispositivos conectados à rede. Esses dispositivos representam pontos críticos de acesso, sendo alvos potenciais de ataques cibernéticos, além de impactarem diretamente na eficiência e produtividade dos serviços prestados.
Atualmente, o Tribunal carece de uma solução abrangente e integrada para gerenciamento de endpoints, o que resulta em lacunas no controle e monitoramento desses ativos. Os processos de provisionamento, atualização de sistemas operacionais, instalação de softwares, aplicação de patches e correções, além da gestão de políticas de segurança, são realizados de forma descentralizada e manual, gerando inconsistências, maior consumo de recursos e vulnerabilidades à segurança.
A ausência de uma solução específica também dificulta o cumprimento de regulamentações e melhores práticas de governança, como o controle de conformidade de licenças de software, o rastreamento eficiente de ativos e a implementação de medidas de proteção contra ameaças cibernéticas. Com a expansão do trabalho remoto e híbrido, torna-se ainda mais desafiador gerenciar e proteger endpoints fora das dependências do Tribunal, expondo a rede institucional a riscos elevados.

4.2. Resultados a serem alcançados
(Pergunta a ser respondida: Quais os resultados que se pretende obter com essa demanda?):
- Aumentar a segurança de endpoint: Garantir maior segurança dos endpoint, reduzindo riscos de ataque cibernéticos.
- Aumentar a segurança contra ameaças: Implementar políticas de proteção robustas, como criptografia, controle de acessos e resposta a incidentes, mitigando vulnerabilidades e prevenindo ataques.
- Melhorar o controle de conformidade: Assegurar o rastreamento dos ativos, controle de licenças de software e atendimento às regulamentações aplicáveis.

4.3. Qual é o público alvo da demanda?

Magistrados (Juízes e/ou Desembargadores).
Sim

Servidores (servidores diretamente contratados pelo TJMG).
Sim

Colaboradores (terceirizados ou cedidos).
Sim

Jurisdicionados (cidadãos que buscam a justiça).
Não

Operadores do Direito (Advogados, Ministério Público etc.).
Não

Todos acima.
Não

4.4. A demanda está prevista em algum plano estratégico? Qual?

Planejamento Estratégico Institucional (PEI).
Sim

Projef 5.0.
Não

Plano Diretor de TIC (PDTIC).
Sim

Plano de Transformação Digital (PTD).
Não

Outro(s).
Não

Se "Outro(s)", especificar:
-

4.5. A execução da demanda necessita de apoio administrativo/gerencial de outras áreas do TJMG? Se sim, quais?

A execução depende apenas da minha Diretoria.
Não

DIRFOR: aquisição, manutenção ou desenvolvimento de sistema informatizado ou outra solução de TIC.
Sim

DIRCOM: comunicação.
Não

EJEF/DIRDEP: desenvolvimento de competências e capacitação.
Não

SEGOVE: edição de ato normativo, análises estatísticas e consultoria em melhoria de processos de trabalho.
Não

SEPLAN e DIRCOR: edição de provimento e orientações aos magistrados de 1ª instância.
Não

SEPAD: orientações aos magistrados de 2ª instância.
Não

Outras.
Não

Se "Outras", descrever quais as áreas:
-

5. Declaração de ciência:
Declaro conhecer os limites de responsabilidades estabelecidos para a execução da demanda e ter ciência que a não realização de qualquer atividade aqui estabelecida pode prejudicar o cumprimento dos prazos acordados.

Documento assinado eletronicamente por **Tatiana Cristina Mendes Hanum**, **Gerente**, em 05/12/2024, às 11:46, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Márcio Henrique Camargos D''Ávila**, **Assessor(a) Técnico(a)**, em 10/12/2024, às 17:49, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Denilson dos Santos Rodrigues**, **Gerente**, em 16/12/2024, às 11:02, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjmg.jus.br/autenticidade informando o código verificador **21190029** e o código CRC **C9A78F04**.