Nº Processo PROAD: 202109000294564 (Evento nº 1)

1. Documento de Oficialização da Demanda (DOD)

Este documento tem por finalidade formalizar o início do processo de planejamento da contratação de TIC, vincular as necessidades da contratação aos objetivos estratégicos e às necessidades corporativas da instituição, bem como instituir a equipe de planejamento da contratação, em atendimento às diretrizes definidas pela Resolução nº 182/2013 do Conselho Nacional de Justiça (CNJ).

De acordo com o art. 12, § 5º desta Resolução, o Documento de Oficialização da Demanda (DOD) deverá conter, no mínimo:

> I – necessidade da solicitação, com a descrição sucinta da Solução de Tecnologia da Informação e Comunicação pretendida, bem como o alinhamento entre a demanda e o Planejamento Estratégico Institucional ou Planejamento Estratégico de Tecnologia da Informação e Comunicação do órgão;
> II – explicitação da motivação e o demonstrativo de resultados a serem alcançados com a solução; e
> III – indicação do Integrante Demandante para a composição da Equipe de Planejamento da Contratação.

2. Identificação da Solução de Tecnologia da Informação e Comunicação:

Nome do Projeto:	Contratação de solução gestão de segurança cibernética	**Data de envio:**	17/09/2021
Identificação do Projeto:	Itens nº 13 e 14 das Contratações da Diretoria de Tecnologia da Informação no Plano Anual de Contratações – 2021.		
Fonte de Recursos:	FUNDESP – Fundo Especial de Reaparelhamento e Modernização do Poder Judiciário		

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

3. Identificação da Área Demandante da Solução:

Em conformidade com o art. 2º, III, da Resolução 182/2013 – CNJ, a Área Demandante é "unidade do órgão que demanda uma Solução de Tecnologia da Informação e Comunicação".

O Departamento/Área apresentado abaixo atuará como Integrante Demandante no presente projeto:

Área Demandante:	Diretoria de Tecnologia da Informação / Núcleo de Segurança e Administração de Dados		
Responsável pela Demanda:	Anderson Yagi Costa	**Matrícula:**	5135710
E-mail do Responsável:	aycosta@tjgo.jus.br	**Telefone:**	3216-7700

Em conformidade com o art. art. 2º, XIII, a) da Resolução 182/2013 – CNJ, o Integrante Demandante é "servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação indicado pela respectiva autoridade competente, responsável pelos aspectos funcionais da solução a ser contratada, e pela condução dos trabalhos da equipe de planejamento".

O(s) seguinte(s) integrante(s) atuará(ão) como Integrante Demandante no presente projeto:

Integrante Demandante:	Bárbara Fernandes	**Matrícula:**	5132495
E-mail do Integrante Demandante:	bfernandes@tjgo.jus.br	**Telefone:**	3216-7700

3.1 Responsabilidades do Integrante Demandante:

O art. 3º, estabelece que são atribuições do Integrante Demandante definir, sempre que possível e necessário, os requisitos:

> I – de negócio, que independem de características tecnológicas, bem como os aspectos funcionais da Solução de Tecnologia da Informação e Comunicação, limitados àqueles indispensáveis ao atendimento das necessidades reais do órgão;
> II – de capacitação, que definem a necessidade de treinamento, número de participantes, carga horária, materiais didáticos, entre outros pertinentes;
> III – legais, que definem as normas com as quais a Solução de Tecnologia da Informação e Comunicação deverá estar em conformidade;
> IV – de manutenção, que independem de configuração tecnológica e que definem a necessidade de serviços complementares, tais como de manutenção preventiva, corretiva, adaptativa e evolutiva da solução;
> V – temporais, que definem os prazos de entrega dos bens e/ou do início e encerramento dos serviços a serem contratados;
> VI – de segurança da informação, juntamente com o Integrante Técnico; e
> VII – sociais, ambientais e culturais, que definem requisitos que a solução deverá atender para estar em conformidade com os costumes, os idiomas e o meio ambiente, entre outros pertinentes.

Também, de acordo com o mesmo artigo supracitado, é responsabilidade do Integrante Demandante a "coordenação dos trabalhos necessários para a efetiva concretização da demanda de Solução de Tecnologia da Informação e Comunicação".

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

4. Identificação da Área de Tecnologia da Informação e Comunicação

Em conformidade com o art. 2°, IV da Resolução 182/2013 – CNJ, a Área de Tecnologia da Informação e Comunicação é "unidade do órgão responsável por gerir a Tecnologia da Informação e Comunicação" e "indicará o Integrante Técnico para a composição da Equipe de Planejamento da Contratação após o recebimento do Documento de Oficialização da Demanda" (art. 12, § 6º).

Dessa forma, o(s) seguinte(s) integrante(s) atuará(ão) como Integrante Técnico no presente projeto:

Integrante Técnico:	Bárbara Fernandes	**Matrícula:**	5132495
E-mail do Integrante Técnico:	bfernandes@tjgo.jus.br	**Telefone:**	3216-7700

4.1 Responsabilidades do Integrante Técnico:

O art. 2º, XIII, b) considera Integrante Técnico o "servidor representante da Área de Tecnologia da Informação e Comunicação indicado pela respectiva autoridade competente, responsável pelos aspectos técnicos da solução a ser contratada".

O art. 4º, estabelece que são atribuições do Integrante Técnico, sempre que possível e necessário, os requisitos:

> I – de arquitetura tecnológica, composta de hardware, software, padrões de interoperabilidade e de acessibilidade, linguagens de programação e interfaces;
> II – do projeto de implantação da Solução de Tecnologia da Informação e Comunicação que definem, inclusive, a disponibilização da solução em ambiente de produção;
> III – de garantia e manutenção, que definem a forma como será conduzida a manutenção e a comunicação entre as partes envolvidas na contratação;
> IV – de capacitação, que definem o ambiente tecnológico dos treinamentos, os perfis dos instrutores e o conteúdo técnico;
> V – de experiência profissional da equipe que projetará, implantará e manterá a Solução de Tecnologia da Informação e Comunicação, que definem a natureza da experiência profissional exigida e as respectivas formas de comprovação;
> VI – de formação da equipe que projetará, implantará e manterá a Solução de Tecnologia da Informação e Comunicação, tais como cursos acadêmicos, técnicos e as respectivas formas de comprovação;
> VII – de metodologia de trabalho; e
> VIII – de segurança sob o ponto de vista técnico.

4.2 Autoridade Competente da Área de Tecnologia da Informação:

Nome:	Anderson Yagi Costa
Cargo:	Diretor de Tecnologia da Informação

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

5 – Identificação da Área Administrativa

Em conformidade com o art. 2°, V da Resolução 182/2013 – CNJ, a Área Administrativa é "unidade do órgão responsável pela execução dos atos administrativos e por apoiar e orientar as áreas Demandante e de Tecnologia da Informação e Comunicação no que se refere aos aspectos administrativos da contratação".

Dessa forma, o(s) seguinte(s) integrante(s) atuará(ão) como Integrante Administrativo no presente projeto:

Integrante Administrativo:		**Matrícula:**	
E-mail do Integrante Administrativo:		**Telefone:**	

5.1 Responsabilidades do Integrante Administrativo:

Compete ao Integrante da Área Administrativa (art. 12, § 7º – Resolução 182/2013-CNJ):

> I – autuar processo administrativo de contratação;
> II – verificar se a demanda está incluída no rol de contratações previstas e aprovadas no Plano de Contratações de STIC, e caso não esteja, o Documento de Oficialização da Demanda deverá ser submetido à autoridade competente do órgão para deliberação;
> III – indicar o Integrante Administrativo para a composição da Equipe de Planejamento da Contratação; e
> IV – instituir a Equipe de Planejamento da Contratação.

Além disso, o art. 2º, XIII, c) considera Integrante Administrativo o "servidor representante da Área Administrativa indicado pela respectiva autoridade competente, responsável por apoiar e orientar os integrantes das áreas Demandante e de Tecnologia da Informação e Comunicação nos aspectos administrativos da contratação".

O art. 5º e seu Parágrafo único, estabelecem que o Integrante Administrativo "deverá verificar se os aspectos administrativos da contratação constam nos documentos produzidos durante as fases do planejamento, os quais fundamentarão as decisões das demais áreas do órgão envolvidas no processo administrativo de contratação", bem como "informar aos integrantes das áreas Demandante e de Tecnologia da Informação e Comunicação quando não constarem nos documentos as devidas informações":

Em conformidade com a Resolução 182/2013 a Autoridade Competente da Área Administrativa indica o/a(s) Integrante(s) Administrativo(s), bem como aprova o prosseguimento do planejamento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Demandante.

5.2 Autoridade Competente da Área Administrativa:

Nome:	
Cargo:	

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

Nº Processo PROAD: 202109000294564 (Evento nº 1)

6. Motivação/Justificativa

Com o advento da implementação do "*home office"* (trabalho remoto) em grande escala no contexto da pandemia mundial de COVID-19, há um volume maior de acesso remoto, onde as pessoas acessam dados importantes diretamente de casa. Esse maior número de acessos facilita a invasão dos sistemas, e nesse sentido o avanço da tecnologia se faz necessário para que as organizações estejam preparadas profissionalmente frente as demandas que o setor de TI necessita para um pleno funcionamento. A importância da adoção de medidas contra ameaças relacionadas às informações exige soluções robustas, eficientes e eficazes na prevenção, análise e proteção do ambiente.

Verifica-se nos últimos anos uma onda de ataques do tipo cibernético. Independente do tamanho ou segmento da corporação, os ataques continuam se multiplicando e estar apenas atento aos *ransomwares* e *phishings* ou possuir sistemas primários de detecção já não é mais suficiente. A necessidade latente de instituir diretrizes, normas e procedimentos de segurança através do uso de ferramentas adequadas de detecção, proteção e resposta, além de possuir profissionais capacitados é cada dia mais importante e tem sido o assunto em voga, principalmente entre os órgãos públicos que carecem de maior investimento em segurança da informação, buscando minimizar os dandos de quando são vítimas de ações maliciosas por parte de *hackers* (agentes maliciosos) podendo ter como efeito a paralisação das estruturas de tecnologia de informação do Poder Judiciário.

Atualmente, a estrutura de Segurança da Informação do Tribunal de Justiça do Estado de Goiás (TJGO), através do Núcleo de Segurança e Administração de Dados, vem promovendo o estabelecimento de novas metodologias, por meio de processos e normas com intuito de modernizar e reestruturar as bases de segurança da informação dentro do Tribunal. Historicamente, a Segurança da Informação passou a ter uma unidade dedicada apenas recentemente, a qual ainda vem sendo pouco explorada num contexto de prerrogativa essencial para todo o ambiente de trabalho. Faz-se necessário, no entanto, que haja um maior planejamento e estruturação do ambiente que irá analisar, dirimir, mitigar os possíveis processos infecciosos dentro da instituição.

Uma das principais necessidades para a prevenção ou proteção de ações maliciosas de qualquer tipo dentro do TJGO é a visibilidade do que de fato acontece no ambiente, incluindo conexões, acessos, tráfego de rede, eventos e logs dos serviços e sistemas, entre outros. Para o *hacker*, o não conhecimento de suas atividades é seu ponto principal de sucesso, o que facilita sua ação e o deixa em situação oportuna para continuar atuando dentro da instituição. Nesse contexto, como o TJGO não possui uma ferramenta para realizar a gestão de segurança cibernética no ambiente, acaba seguindo vulnerável a diversos tipos de ameaças. Apesar de possuir sistemas e ferramentas de segurança de ativos de TIC, tais como Firewall, Antivírus, Reversos para Aplicações, esses não são suficientes para analisar de forma detalhada, centralizada e em sua totalidade os eventos e ações desempenhados pelos usuários de TIC do TJGO e, portanto, não localizando ações maliciosas.

Devido a isso, o presente projeto busca a aquisição de Solução de Gestão de Segurança Cibernética, para identificação, prevenção e proteção do ambiente quanto aos acessos indevidos, quanto às vulnerabilidades de equipamentos e sistemas, quanto à proatividade e antecipação de possíveis ações maliciosas, tais como roubo, furto, apropriação de informações sigilosas ou primordiais ao funcionamento do Tribunal, intrusão ao parque computacional com risco de criptografia indevida dos dados e backups dos sistemas, como tem ocorrido recentemente em outros

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

órgãos públicos e empresas privadas de grande porte.

Recentemente, têm-se verificado uma escalada de casos, tanto em órgãos públicos (com destaque ao caso do Superior Tribunal de Justiça, ocorrido em 2020), quanto em empresas privadas. Além disso, não raro ocorrem casos de vazamentos de dados de pessoas e empresas em grandes volumes, com exposição a dados pessoais críticos, que provocam vulnerabilidades tanto para os proprietários dos dados, quanto para as organizações que deveriam protegê-los.

> **Brasil sofre seu maior ataque hacker da história**
> Atualizado em 5 nov 2020, 19h20 - Publicado em 5 nov 2020, 19h03
> Superior Tribunal de Justiça, Ministério da Saúde e Distrito Federal foram alvos de cibercriminosos, que obtiveram acesso a informações sigilosas.
> Disponível em: <https://veja.abril.com.br/blog/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia/>. Acesso em 22 setembro 2021.
>
> **STJ restabelece sistemas de informática 15 dias depois de ataque hacker**
> 18.nov.2020 (quarta-feira) - 23h03
> A reabilitação do sistema foi concluída 15 dias depois do ataque hacker que culminou na suspensão dos julgamentos em todos os colegiados do tribunal. Prazos processuais tiveram de ser interrompidos.
> Disponível em: <https://www.poder360.com.br/justica/stj-restabelece-sistemas-de-informatica-15-dias-depois-de-ataque-hacker/>. Acesso em 22 setembro 2021.
>
> **Polícia Federal ainda está investigando ataque hacker ao STJ**
> 9 de junho de 2021, 13h17
> A Polícia Federal ainda está investigando o ataque hacker aos sistemas do Superior Tribunal de Justiça, conforme informado pela assessoria de imprensa do tribunal à ConJur nesta quarta-feira (9/6).
> (…)
> Além do STJ e do STF, o site do Tribunal de Justiça do Rio Grande do Sul (TJ-RS) foi alvo de dois ataques nos últimos meses. Da última vez, os sistemas ficaram fora do ar e os prazos processuais foram suspensos de 30 de abril a 17 de maio.
> No final do ano passado, o Tribunal já havia sofrido um ataque. Na ocasião, a corte informou em nota que nenhum dado foi comprometido e que apenas páginas de acesso aos processos foram afetadas.
> Em janeiro deste ano, o alvo de outro ataque foi o Tribunal Regional Federal da 3ª Região. O ataque teve como objetivo sobrecarregar os sistemas e torná-los indisponíveis.
> Disponível em: <https://www.conjur.com.br/2021-jun-09/policia-federal-ainda-investigando-ataque-hacker-stj>. Acesso em 22 setembro 2021.

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

Startup de cibersegurança diz que ataque à Renner gerou pânico nas empresas
21/08/21 - 18h20 - Atualizado em 22/08/21 - 14h43
Em janeiro de 2021, a startup brasileira de cibersegurança PSafe identificou o maior vazamento de dados da história do País, quando 223 milhões de brasileiros (incluindo já mortos) tiveram dados expostos e vendidos na internet. Diante de uma brecha desse tamanho, Marco DeMello, presidente da PSafe, não vê a alta de casos de sequestro de dados de empresas com surpresa. Segundo ele, as companhias ainda não se deram conta do tamanho do prejuízo a que podem estar expostas ao não proteger seus sistemas de forma diligente.
O caso da Renner criou pânico, diz Mello, que recebeu ligações de empresários com medo de virarem a próxima vítima. "Mas eu pergunto: por que o pânico só agora? A ficha tinha de ter caído há muito tempo."
Disponível em: <https://www.istoedinheiro.com.br/startup-de-ciberseguranca-diz-que-ataque-a-renner-gerou-panico-nas-empresas/>. Acesso em 22 setembro 2021.

PSafe encontra site que expõe 426 milhões de dados pessoais de brasileiros
21/09/2021 • 17:26
A empresa de segurança cibernética Psafe diz ter encontrado um site público com cerca de 426 milhões de dados pessoais de brasileiros e 109 milhões de informações de CNPJs e placas de veículos.
Disponível em: <https://blogs.oglobo.globo.com/capital/post/psafe-encontra-site-que-expoe-426-milhoes-de-dados-pessoais-de-brasileiros.html>. Acesso em 22 setembro 2021.

Anteriormente a preocupação relativa a ataques do tipo cibernético a um órgão ou empresa seria atacado, se o parque computacional estava seguro contra ações maliciosas, utilizando as ferramentas já existentes. Atualmente, esta perspectiva mudou para quando será o ataque e se será possível conter as ameaças e dar continuidade às atividades da organização. As notificações referentes a **ataques cibernéticos** contra empresas brasileiras **cresceram 220% no primeiro semestre** deste ano em comparação com o mesmo período de 2020. Os dados foram divulgados em julho pelo grupo Mz, empresa especializada em relações com investidores, com base em dados levantados pela Comissão de Valores Mobiliários (CVM), agência regulada pelo Ministério da Economia, causando perdas monetárias da ordem de trilhões de dólares.

Dentre as principais vantagens do investimento dentro do ambiente, entre outras, destaca-se:

- Análise de todo o tráfego, identificando as possíveis ameaças e riscos digitais;
- Organização e adequação de uma equipe de ETIR (Equipe de Tratamento e Respostas à incidentes);
- Monitoramento contínuo do ambiente;
- Integração e automatização com sistemas de segurança já existentes;
- Otimização de rotinas de segurança da informação;

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

Como referência de estudo para as aquisições do objeto em questão, utilizou-se as *Orientações para Elaboração/Ajuste de Especificações Técnicas de Ativos de TI – Versão 3*, do antigo Ministério do Planejamento, Orçamento e Gestão (MPOG), disponível através do seguinte link: https://www.governodigital.gov.br/documentos-e-arquivos/Orientacoes%20Especificas%20-%20Marco%20de%2017.pdf. Esse documento dispõe sobre boas práticas, orientações e vedações na elaboração de especificações técnicas de bens e serviços de Tecnologia da Informação (TI).

7. Resultados e Benefícios a serem alcançados com a solução de TI

São benefícios e objetivos da contratação, entre outros:

a) Adequação à Lei Geral de Proteção de Dados, às diretivas de gerenciamento e segurança do CNJ: Resolução n° 396/2021, Portaria n° 162/2021, Resolução 370/2021;
b) Criar estrutura de gestão de segurança cibernética no ambiente;
c) Obter visibilidade do fluxo de comunicações internas e externas oriundas do TJGO;
d) Identificar os possíveis incidentes de segurança existentes;
e) Prevenir ou, pelo menos, diminuir as ações maliciosas investidas;
f) Criar protocolos de segurança cibernética incidindo em prevenção, gerenciamento e análise de ilícitos;
g) Prover serviços de TIC com excelência, com ferramentas e recursos adequados;
h) Prover segurança aos sistemas e estruturas judiciais, aos usuários internos, aos cidadãos que acessam o Poder Judiciário;
i) Prover segurança aos dados e informações que são parte do serviço judicial prestado pelo TJGO;
j) Aumento no nível de controle e gerência;
k) Continuidade do negócio;
l) Satisfação dos usuários.

8. Alinhamento Estratégico

Em conformidade com o art. 2º, XVIII, XIX, XX da Resolução 182/2013 – CNJ, as contratações deverão ser precedidas de planejamento elaborado em harmonia com o Planejamento Estratégico Institucional (PEI), Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) e/ou Plano Diretor de Tecnologia da Informação (PDTIC) do órgão, alinhados com o Planejamento Estratégico do Poder Judiciário.

Dessa forma, a demanda inicialmente apresentada encontra-se alinhada com o Plano de Gestão do Poder Judiciário do Estado de Goiás para o biênio 2021-2023:

- Meta 03: Digitalizar 100% do acervo total de processos físicos em tramitação no Poder Judiciário de Goiás;
- Meta 04: Alcançar no mínimo 72% no Prêmio CNJ de Qualidade;
- Meta 07: Alcançar o nível de excelência com o índice de 0,90 no IGOVTIC-JUD.

Também está alinhada à Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026:

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

- Objetivo 01: aumentar a satisfação dos usuários do sistema judiciário;
- Objetivo 02: promover a transformação digital;
- Objetivo 05: aperfeiçoar a governança e a gestão;
- Objetivo 07: aprimorar a segurança da informação e a gestão de dados.

Diante do exposto, institui-se por meio do presente documento a Equipe de Planejamento da Contratação conforme exposto no art. 12° e 13º, da Resolução 182/2013, de 17 de Outubro de 2013, emitida pelo Conselho Nacional de Justiça, estando cientes todos os integrantes indicados acercas das suas respectivas responsabilidades sobre o projeto apresentado.

(assinado e datado digitalmente)

Assinado digitalmente por: BARBARA FERNANDES, AUXILIAR JUDICIÁRIO; e outros, em 02/10/2021 às 23:35.
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

ASSINATURA(S) ELETRÔNICA(S)

Tribunal de Justiça do Estado de Goiás
Para validar este documento informe o código 457343761392 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

Nº Processo PROAD: 202109000294564 (Evento nº 1)

BARBARA FERNANDES
AUXILIAR JUDICIÁRIO
NÚCLEO DE SEGURANÇA E ADMINISTRAÇÃO DE DADOS
Assinatura CONFIRMADA em 02/10/2021 às 23:35

ANDERSON YAGI COSTA
DIRETOR DE TECNOLOGIA DA INFORMAÇÃO
DTI - PRESIDÊNCIA
Assinatura CONFIRMADA em 01/10/2021 às 19:10