PODER JUDICIÁRIO
JUSTIÇA FEDERAL DA 2ª REGIÃO

ESTUDO TÉCNICO PRELIMINAR

Solicitação Eletrônica de Contratação nº JFES-SEC-2023/00058

Renovação da solução de proteção de *endpoint* (antivírus)

ESTUDO TÉCNICO PRELIMINAR

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Destina-se a identificar e analisar a necessidade projetada pela unidade administrativa no planejamento estratégico e no plano de contratações, buscando evidenciar o problema a ser resolvido e as soluções possíveis, com o fim de avaliar as informações necessárias para subsidiar o respectivo processo de contratação.

1 DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

Identificação das necessidades de negócio	
1.	Prover recursos para preservar a segurança das informações.
2.	Manter a disponibilidade e segurança do ambiente de tecnologia da informação.
Identificação das necessidades tecnológicas	
1.	Acesso às atualizações e correções do software da solução de proteção de *endpoint.*
2.	Acesso às atualizações das assinaturas e mecanismos de proteção utilizados.
3.	Acesso à base de conhecimento do fabricante
4.	Renovação do licenciamento para o quantitativo atual de 1.100 dispositivos
5.	Manutenção das funcionalidades do licenciamento atual para a proteção dos *endpoints*.
6.	Funcionalidades inteiramente integradas e gerenciadas através de uma única console de gerenciamento.
7.	Gerenciamento da solução deverá possibilitar a distribuição de carga e administração em níveis hierárquicos, em grupos lógicos independentes da estrutura de domínio de rede.
8.	Comunicação cliente/servidor através dos protocolos de rede TCP/IP.
9.	Proteção e remoção integrada, através de um única solução, contra vírus, *trojans*, *worms* de rede, *spywares*, *adwares* e *rootkits*, bem como incorporar funcionalidades de *firewall* pessoal e *IPS (Intrusion Prevention System).*
10.	Proteção de ameaças da Web através de serviço de reputação de *site*.
11.	Efetuar backup da base de dados da solução.
12.	*File Reputation* (reputação de arquivos), integrada e gerenciada através da console, cancelando o *download* ou execução do arquivo, de forma automática caso o mesmo tenha conteúdo malicioso, baseado na resposta à consulta da base da empresa desenvolvedora da solução.
13.	Configuração de bloqueio de acesso aos *sites* maliciosos pela console de gerenciamento.
14.	Criar *blacklists* e *whitelists* de URLs para estações pela console de gerenciamento.

15.	Instalação em clientes e servidores *Windows* através de *login script* com instalação remota a partir da console ou através da rede
16.	Customização dos pacotes de instalação em clientes e servidores.
17.	Os pacotes de instalação deverão ser otimizados para em cada uma das plataformas existentes no ambiente de TIC do órgão.
18.	Instalações em clientes remotos e móveis (*notebooks*) sem depender de outro *software* ou agente previamente instalado.
19.	Capacidade de detecção de violações na integridade da instalação ou dos arquivos do antivírus instalado nos clientes e servidores.
20.	Ferramenta para analisar toda a rede e identificar os computadores que porventura não estejam com o antivírus instalado ou atualizado, de acordo com as políticas determinadas na console de administração.
21.	Identificar computadores que tenham antivírus de outros da empresa desenvolvedora da SOLUÇÃO, ou que tenham o antivírus instalado, porém desativado.
22.	Administração centralizada de todos os clientes e servidores *Windows* em console única de gerenciamento baseado na tecnologia MMC (*Microsoft Management Console)* ou através de interface WEB.
23.	A console única de gerenciamento deve exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, versão do antivírus, versão dos mecanismos de verificação (*engine*), data da vacina, data da última verificação e endereço IP.
24.	Console única de gerenciamento deverá permitir travamento das configurações em clientes e servidores para que somente o administrador possa alterar a configuração, desinstalar ou parar a solução.
25.	Console única de gerenciamento deve permitir a proteção de acesso aos servidores de administração do sistema e grupos lógicos de computadores, através de senhas configuradas pelo administrador.
26.	Console única de gerenciamento deve exibir logs e alertas de todos os clientes e servidores, em tempo real, sem a necessidade de exportar ou transferir arquivos manualmente ou através de batches entre clientes, servidores e central de gerenciamento.
27.	Aplicar mudanças na configuração do antivírus em clientes e servidores *Windows*, com possibilidade de mudança para todos os computadores, para um determinado grupo de computadores ou para um único computador.
28.	Configurações da solução em clientes e servidores, após modificadas na central de administração, deverão ser distribuídas para os computadores, automaticamente, sem a necessidade de uso de agentes externos, *login scripts*, tarefas manuais ou outros módulos adicionais.
29.	Novas configurações deverão ser efetivamente instaladas e ativadas no computador destino sem a necessidade de reinicialização ou *logoff / logon* do usuário.
30.	Capacidade de envio de alertas, no caso de mudanças de configuração, ativação ou desativação do antivírus, atualização de vacinas e incidência de vírus.
31.	Console de gerenciamento deverá ter a capacidade de abrir uma única janela de alerta de vírus com todas as ocorrências, com o intuito de se evitar a exibição de uma nova janela para cada alerta gerado.
32.	Instalação sem necessidade de reiniciar a estação de trabalho.

33.	Gerar imagens (modelos padronizados para instalação) de estações de trabalho com a SOLUÇÃO.
34.	Possibilitar o agrupamento de máquinas em grupos, com configurações específicas para cada grupo criado.
35.	Realizar a auto-reparação de danos causados por *Trojan Horses*, de forma automática, sem necessidade de agentes ou pacotes adicionais.
36.	Capacidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado.
37.	Permitir a utilização de fontes de agentes de atualização secundários em localidades remotas com objetivo de minimizar o consumo do *link* durante a atualização de vacinas; Estes agentes devem ser configurados através da própria console de gerenciamento sem a necessidade de intervenção local ou instalação de outro *software*.
38.	Permitir a varredura dos dispositivos removíveis e periféricos (*usb, floppy disk, cdrom*) mesmo com a política de bloqueio total ativa.
39.	Console única de gerenciamento deverá permitir a criação de usuários com diferentes níveis de administração.
40.	Console única de gerenciamento deverá permitir integração com o *Active Directory* para identificar maquinas presentes no AD e que não tenham a ferramenta de antivírus instalada, possibilitando ainda a instalação automática da ferramenta para garantir a integridade da rede.
41.	Proteção contra desinstalação e desativação não autorizada da solução.
42.	Permitir a instalação em ambientes em *Cluster Microsoft*.
43.	Implementação de *Dashboard* com medição do nível de atualização do ambiente e o nível de cumprimento de política de segurança previamente definida.
44.	Capacidade de atualizar remotamente e em tempo real a vacina e *engine* da solução, em um único pacote para todas as plataformas suportadas.
45.	Atualizações deverão ser feitas a partir de comunicações agendada ou manual, entre o servidor de administração e o centro de pesquisas da empresa desenvolvedora da solução.
46.	Prover mecanismos de distribuição de vacinas para toda a rede a partir de servidor de administração, de forma agendada e real-time, e com pacotes incrementais, de forma a prevenir a alta utilização de banda de rede.
47.	Ter mecanismos de configuração para o agendamento do envio de vacinas, com tolerância a falhas.
48.	Tarefa de atualização das vacinas deverá possuir mecanismos de randomização, diminuindo assim o tráfego de rede gerado pela solução no processo de atualização.
49.	Processo de atualização deverá prover mecanismos de configuração para que os clientes façam a busca por novas vacinas, nos servidores de antivírus, em intervalos periódicos e em escala de minutos.
50.	Capacidade de executar a volta imediata para a vacina anterior, através da console de gerenciamento, de forma silenciosa e sem intervenção do usuário, para o caso da vacina atual apresentar problemas.

51.	Ser capaz de instalar as correções de acordo com a severidade.
52.	Compatível com plataformas existentes no ambiente de TIC do órgão.
53.	Rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados, incluindo sessões DOS abertas pelo Windows, bem como servidores Linux.
54.	Rastreamento manual com interface Windows, customizável, com opção de limpeza.
55.	Capacidade de detecção de vírus desconhecidos utilizando análise heurística, análise comportamental ou aprendizado de máquina (*machine learning*).
56.	Detecção de programas maliciosos como *spyware*, programas de propaganda, ferramentas como *password crackers*, dentre outros.
57.	Detecção e reparo de arquivos contaminados, mesmo compactados por ZIP, CAB, e ARJ.
58.	Permitir configurar ações a serem tomadas na ocorrência de vírus, incluindo, dentre outras, reparar, deletar, mover para a área de Isolamento (quarentena) e ignorar
59.	Possibilidade de criar uma cópia *backup* do arquivo suspeito antes de limpá-lo. Rastreamento remoto, de modo manual ou agendado.
60.	Possuir mecanismos de área de isolamento de arquivos para vírus desconhecidos ou sem possibilidade de reparação (área de quarentena).
61.	Deverá existir a possibilidade de envio de amostras para o centro de pesquisas da empresa desenvolvedora da solução, que deverá prover a respectiva vacina.
62.	Área de isolamento deverá possibilitar a devolução dos arquivos livres de vírus que tenham sido colocados em quarentena para seus pontos de origem.
63.	Capacidade para, em caso de epidemia, bloquear acesso a pastas compartilhadas, a portas TCP e UDP, e escrita em diretórios e arquivos específicos, restaurando as configurações originais ao término da epidemia de forma automática através de políticas recebidas da empresa desenvolvedora da solução ou de forma manual pela console de gerenciamento.
64.	Possibilidade de colocar arquivos e diretórios em listas de exclusões para não serem verificados pelo antivírus. Possibilidade de bloquear aplicações com base no nome, diretório ou extensão do arquivo ou também com base no hash da aplicação.
65.	Possibilidade de proteger o computador permitindo que somente determinadas aplicações (com base no hash) possam ser executadas.
66.	Notificação automática ao administrador em caso de epidemia de vírus.
67.	*Firewall* com capacidade de verificação dos pacotes que estão entrando e/ou saindo da estação de trabalho, com detecção e bloqueio de ataques de *malwares* que exploram vulnerabilidades em *software*.
68.	Capacidade de detecção de ameaças que utilizam algoritmos de compactação em tempo real não padronizados com objetivo de não serem identificados.
64	Permitir o reinício automático dos serviços do antivírus caso esse tenha sido parado devido a algum código malicioso, sem a necessidade da intervenção do administrador.

65	Permitir autoproteção ao cliente de antivírus em nível de registro, arquivos de programa e processos.
66	Capacidade de identificar a origem (servidores ou estações) de ataques de *malwares* na rede local.

Requisitos necessários e suficientes à escolha da solução de TIC	
1.	Os serviços serão prestados no ed. Sede da contratante, localizado à Av. Marechal Mascarenhas de Moraes, 1877, Monte Belo, Vitória – ES, CEP: 29.053-245
2.	As especificações devem ser consideradas como requisitos mínimos, sendo aceitas especificações idênticas ou superiores
3.	Os serviços de suporte deverão ser prestados em regime 8x5, sem limite de incidentes, durante o prazo de vigência do contrato de suporte.
4.	Os serviços de proteção e de atualização das assinaturas e mecanismos de segurança deverão funcionar em regime 24x7x365.
5.	Deverá ser fornecido certificado do fabricante que comprove o quantitativo e validade do contrato de suporte técnico.
6.	Validade do serviço de 21/12/2023 até 31/03/2025, data em que vencem as licenças do TRF2, visando a manutenção do alinhamento regional das soluções de TI
7.	O serviço de suporte deverá ser associado ao usuário atual da JUSTICA FEDERAL DE PRIMEIRO GRAU NO ESPIRITO SANTO no site do fabricante, ID: 295935
8.	A interface de operação do agente instalado nos *endpoints* dos usuários deve estar no idioma português brasileiro.

Do alinhamento da contratação e o planejamento estratégico da JF	
1.	A solução está alinhada aos planos estratégico, diretor e de contratações de Tecnologia da Informação e Comunicação, conforme apresentado nos quadros a seguir.

ALINHAMENTO À ESTRATÉGIA NACIONAL DE TI – ENTIC-JUD 2021/2026	
Id	**Objetivo Estratégico**
6	Aprimorar a Segurança da Informação e a Gestão de Dados

ALINHAMENTO AO PLANO DIRETOR – PDTI 2021/2023	
Id	**Necessidade/Iniciativa**
4	Segurança da informação no âmbito da TI

2.	O objeto da contratação também está previsto no Plano de Contratações Anual – PAC da Seção Judiciária do Espírito Santo

ESTUDO TÉCNICO PRELIMINAR

2 ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Atualmente o órgão possui em operação a solução da Kaspersky para proteção dos *endpoints*, com licenciamento para 1.100 (mil e cem) dispositivos e validade até 21/12/2023.

Essa demanda corresponde à renovação do quantitativo e condições do licenciamento atual, com validade do serviço até 31/03/2025, que é a data de vencimento das licenças do TRF2, com o objetivo de manter o alinhamento regional das soluções de TI.

Assim, o quantitativo de bens e serviços foi dimensionado de forma a manter as funcionalidades atuais de operação da solução, estando adequado às necessidades do órgão.

3 ANÁLISE DE SOLUÇÕES

3.1 IDENTIFICAÇÃO DAS SOLUÇÕES – LEVANTAMENTO DE MERCADO

Id	Descrição da solução (ou cenário)
1	Renovação da solução de segurança de proteção de *endpoint* "*Kaspersky Endpoint Security for Bussiness – Select Brazilian Edition"*.
2	Aquisição de nova solução de segurança de proteção de *endpoint*.

3.2 ANÁLISE COMPARATIVA DE SOLUÇÕES

Na comparação das soluções estão sendo considerados, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação, observando que somente será apresentado o custo total de propriedade das soluções consideradas viáveis para a demanda.

O quadro abaixo apresenta a utilização e a aderência da solução a determinadas políticas, modelos e padrões de governo existentes, sendo que o detalhamento das alternativas é aplicável especialmente para o caso de soluções de aquisição de licenças de *software*.

Requisito	Solução / Alternativa	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1 Solução 2	X X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 Solução 2			X X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 Solução 2			X X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 Solução 2			X X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2			X X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1 Solução 2			X X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão	Solução 1 Solução 2			X X

Requisito	Solução / Alternativa	Sim	Não	Não se Aplica
de Processos e Documentos do Judiciário – MoReq-Jus?				

3.3 PESQUISA DE PREÇOS DE MERCADO – ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Id	Descrição da solução (ou cenário)
1	Renovação da solução de segurança de proteção de *endpoint* "*Kaspersky Endpoint Security for Business - Select Brazilian Edition"*, com validade de 21/12/2023 a 31/03/2025. Solução Viável 1: 135.300,00

3.4 JUSTIFICATIVAS PARA O PARCELAMENTO, OU NÃO, DA CONTRATAÇÃO

Trata-se de serviço de renovação do licenciamento da solução de segurança de proteção de *endpoint*, com período de validade definido e pagamento integral quando do recebimento do contrato de suporte, não sendo possível o parcelamento da contratação dada as condições de fornecimento do serviço pelo fabricante.

4 REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

4.1 SOLUÇÃO 2: AQUISIÇÃO DE NOVA SOLUÇÃO DE SEGURANÇA DE PROTEÇÃO DE *ENDPOINT*.

A escolha da solução 2 implicaria na substituição da solução existente por nova de outro fabricante. Nesse caso, a implantação de uma nova solução implicaria em desalinhamento da solução de TI da 2ª Região, haja vista que a solução existente no órgão é a mesma utilizada pelo TRF2 e pela SJRJ, indo de encontro ao planejamento regional da TI.

Adicionalmente, além do serviço de suporte pretendido por essa demanda, seriam necessários serviços de instalação da nova solução em todo o parque de estações de trabalho e servidores de rede e treinamento oficial para a equipe técnica do órgão, ocasionando dessa forma um aumento de escopo e prazo na execução contratual, o que provavelmente elevaria os custos da contratação.

Considerando o aumento da complexidade, custos esperados e tempo de execução dessa solução, além da perda de alinhamento regional das soluções de TI, entendemos que solução 2 é inviável.

5 ANÁLISE COMPARATIVA DE CUSTOS (TCO)

A análise comparativa de custos será realizada apenas nas soluções que sejam técnica e funcionalmente viáveis para serem implantadas no órgão.

5.1 CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Para análise dos custos estão sendo consideradas as funcionalidades atuais do órgão, sendo

componentes da formação do custo total de propriedade (*Total Cost Ownership – TCO*) todos os elementos funcionais da solução pretendida.

Solução Viável 1

Descrição:

Renovação da solução de segurança de proteção de *endpoint* "*Kaspersky Endpoint Security for Bussiness – Select Brazilian Edition*".

Custo Total de Propriedade – Memória de Cálculo

Os preços dos bens e serviços pretendidos foram obtidos do por breve pesquisa de mercado.

Foram solicitadas propostas para cinco empresas, especificando 1.100 licenças com validade de 21/12/2023 a 31/03/2025, mas apenas duas empresas enviaram proposta, sendo que ambas consideraram licenças com validades de 1 ou 3 anos, e não o período determinado.

Os valores unitários das propostas estão apresentados a tabela abaixo, bem com o cálculo da média.

Validade da Licença	Cotação Empresa 1 (Vlr Unit R$)	Cotação Empresa 2 (Vlr Unit R$)	Média Cotações (Vlr Unit R$)
1 ano	65,52	98,00	81,76
3 anos	131,02	199,00	165,01

Considerando a possibilidade do fabricante da solução não fornecer licenciamento fracionado, tal como pretendido pelo órgão, e para uma estimativa conservadora dos valores esperados para a contratação, o valor unitário da licenças para o período de 2 anos foi calculado como a média dos valores médios obtidos para 1 e 3 anos, obtendo-se o seguinte resultado:

$Valor_{2anos}$ = (165,01 + 81,76) / 2 = 123,39 ≈ 123,00

Dessa forma, oa CTO esperado para essa solução está apresentado na tabela abaixo.

Elemento de despesa	Quant.	Valor Unit. (R$)	Valor Total (R$)
Renovação da solução de segurança de proteção de *endpoint* "*Kaspersky Endpoint Security for Business - Select Brazilian Edition"*, com validade de 21/12/2023 a 31/03/2025	1.100	123,00	135.300,00
Total			**135.300,00**

É importante ressaltar que a realização da pesquisa de preços detalhada, conforme as normas vigentes do órgão, é elaborada por área específica e apresentada em documento próprio anexado ao processo de contratação.

5.2 MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

O quadro abaixo apresenta a consolidação do cálculo do TCO das alternativas viáveis, observando que o desembolso financeiro ocorre uma única vez durante a prestação dos serviços,.

Descrição da solução	Estimativa de TCO ao longo dos anos (R$)			Total
	Ano 1	Ano 2	Ano 3	
Solução Viável 1	135.300,00	0,00	0,00	135.300,00

6 DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

6.1 DESCRIÇÃO

Conforme apresentado na análise comparativa das soluções, a alternativa viável consiste na Solução Viável 1, isto é, renovação da solução de segurança de proteção de *endpoint Kaspersky Endpoint Security*, pelo período de 21/12/2023 a 31/03/2025, respectivamente a data de vencimento do licenciamento do órgão e a data de vencimento do licenciamento do TRF2 e da SJRJ.

Esse serviço compreende atividades de suporte e atualizações da solução existente, de forma a manter as condições operacionais da rede de dados corporativa.

6.2 MODELOS DE AQUISIÇÃO

A contratação da solução pretendida se dá por meio de aquisição de contrato de suporte, por período de tempo definido, não sendo prevista sua contratação como serviço continuado.

7 ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Na tabela abaixo estão sendo apresentados os bens e serviços necessários à solução escolhida, com os custos estimados.

Bens e Serviços	Quant.	Valor Unit. (R$)	Valor Total (R$)
Renovação da solução de segurança de proteção de *endpoint* "*Kaspersky Endpoint Security for Business - Select Brazilian Edition"*, com validade de 21/12/2023 a 31/03/2025	1.100	123,00	135.300,00
Total			**135.300,00**

8 DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

8.1 DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS

DISPONÍVEIS

8.1.1 Benefícios a serem alcançados

- Alta disponibilidade dos serviços e sistemas de TI.
- Maior celeridade na solução de eventuais problemas de segurança nos equipamentos.
- Ambiente operacional atualizado e menos suscetível a falhas de funcionamento e de segurança.

8.1.2 Necessidades de adequação do ambiente interno para execução contratual

Não há necessidade de adequação, haja vista que toda infraestrutura necessária já está disponível e em operação.

8.1.3 Recursos materiais

Não há necessidade de adequação, haja vista que toda infraestrutura necessária já está disponível e em operação.

8.1.4 Recursos humanos

Não há necessidade de recursos humanos adicionais do órgão, além da equipe técnica já disponível.

8.2 POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

Justifica-se a alternativa escolhida em termos de economicidade dos recursos da Administração, haja vista a adequação dos quantitativos pretendidos às necessidades imediatas do órgão, além do atendimento às demandas de negócio formuladas e aos benefícios pretendidos para o ambiente de rede corporativo do órgão, pelo qual recomendamos e declaramos viável a aquisição proposta.

O presente estudo está de acordo com as necessidades técnicas, operacionais e ao alinhamento estratégico do órgão, tendo como principal objetivo a continuidade e disponibilidade da infraestrutura de TI.

9 ASSINATURA DOS INTEGRANTES E APROVAÇÃO DA AUTORIDADE MÁXIMA DE TIC

A Equipe de Planejamento foi instituída pelo despacho JFES-DES-2023/10495.

Seguem as assinaturas dos integrantes técnico e demandante, bem como a aprovação da autoridade máxima da área de TIC, em atenção ao modelo previsto no Guia de Contratações de TIC do Poder Judiciário do Conselho Nacional de Justiça – CNJ.

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
Rodrigo Queiroga Barros Supervisor da Seção de Rede de Computadores Matrícula: 10726	**Rodrigo Queiroga Barros** Supervisor da Seção de Rede de Computadores Matrícula: 10726

PODER JUDICIÁRIO
JUSTIÇA FEDERAL DA 2ª REGIÃO

ESTUDO TÉCNICO PRELIMINAR

AUTORIDADE MÁXIMA DA ÁREA DE TIC **(OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)**
Fabrício Vasconcelos Costa Diretor do Núcleo de Tecnologia da Informação Matrícula: 10365