Estudo Técnico Preliminar 123/2023

1. Informações Básicas

Número do processo: 23205.031543/2023-72

2. Descrição da necessidade

As informações referente a este item encontram-se no tópico 2 do documento anexo.

3. Área requisitante

Área Requisitante	Responsável
Diretoria de Infraestrutura de Tecnologia da Informação	Jones Muneron

4. Necessidades de Negócio

As informações referente a este item encontram-se no tópico 4 do documento anexo.

5. Necessidades Tecnológicas

As informações referente a este item encontram-se no tópico 5 do documento anexo.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

As informações referente a este item encontram-se no tópico 6 do documento anexo.

7. Estimativa da demanda - quantidade de bens e serviços

As informações referente a este item encontram-se no tópico 7 do documento anexo.

8. Levantamento de soluções

As informações referente a este item encontram-se no tópico 8 do documento anexo.

9. Análise comparativa de soluções

As informações referente a este item encontram-se no tópico 9 do documento anexo.

10. Registro de soluções consideradas inviáveis

As informações referente a este item encontram-se no tópico 10 do documento anexo.

11. Análise comparativa de custos (TCO)

As informações referente a este item encontram-se no tópico 11 do documento anexo.

12. Descrição da solução de TIC a ser contratada

As informações referente a este item encontram-se no tópico 12 do documento anexo.

13. Estimativa de custo total da contratação

Valor (R$): 1.803.822,21

As informações referente a este item encontram-se no tópico 13 do documento anexo.

14. Justificativa técnica da escolha da solução

As informações referente a este item encontram-se no tópico 14 do documento anexo.

15. Justificativa econômica da escolha da solução

As informações referente a este item encontram-se no tópico 15 do documento anexo.

16. Benefícios a serem alcançados com a contratação

As informações referente a este item encontram-se no tópico 16 do documento anexo.

17. Providências a serem Adotadas

As informações referente a este item encontram-se no tópico 17 do documento anexo.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

As informações referente a este item encontram-se no tópico 18 do documento anexo.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

FLAVIO HUMBERTO TESTA
membro da equipe de planejamento

JONES JEFERSON MUNERON
membro da equipe de planejamento

MARCOS EUGENIO DIETRICH
membro da equipe de planejamento

ANDERSON MACHADO PEREIRA
membro da equipe de planejamento

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Estudo_tecnico_preliminar.pdf (274.99 KB)

Anexo I - Estudo_tecnico_preliminar.pdf

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo 23205.031543/2023-72

Solução de segurança da Informação

Chapecó, novembro de 2023.

Histórico de Revisões

Data	Versão	Descrição	Autor
06/11/2023	1.0	Finalização da primeira versão do documento	equipe de planejamento

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

INTRODUÇÃO

O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação.

O ETP tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização da Demanda – DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação.

1. INFORMAÇÕES BÁSICAS

Processo Administrativo nº 23205.031543/2023-72

1.1. 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 PORTARIA Nº 1503/PROAD/UFFS/2023, DE 16 OUTUBRO DE 2023, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, em consonância com o art. 11 da Instrução Normativa SGD-ME nº 01/2019.

1.2. O objeto do estudo é o fornecimento de solução tecnológica de segurança corporativa na modalidade SAAS, baseada em coleta e integração de dados, com ênfase na auditoria e monitoramento de segurança da informação da infraestrutura da UFFS a ser detalhada no presente documento que atenda de forma ampla às demandas institucionais de toda a UFFS, registradas no Plano Anual de Contratação (PAC), por meio do Sistema de Planejamento e Gerenciamento de Contratações (sistema PGC).

1.3. Os serviços contratados neste objeto terão como vigência 36 (trinta e seis) meses de contrato.

2. DESCRIÇÃO DA NECESSIDADE

Necessidade da contratação de solução de segurança da informação (cibersegurança) para os endpoints da UFFS (hosts).

2.1. Motivação/Justificativa

2.1.2 O TCU realizou, entre 3/8/2021 e 9/3/2022, o primeiro de sete ciclos previstos para o acompanhamento de controles críticos de segurança cibernética das organizações públicas federais. Este ciclo, que contemplou 377 organizações, avaliou a implementação de vinte medidas de segurança básicas relacionadas a cinco dos dezoito controles críticos de segurança cibernética estabelecidos no framework do Center for Internet Security (CIS): inventário e controle de ativos de hardware corporativos; inventário e controle de ativos de software; gestão contínua de vulnerabilidades; conscientização sobre segurança e treinamento de competências; e gestão de respostas a incidentes. Através do resultado desta auditoria foi possível estabelecermos pontos de melhoria.

2.1.3 À medida que o governo promove a transformação digital e oferece serviços online aos cidadãos, as organizações públicas ficam cada vez mais dependentes de soluções de tecnologia, como softwares, bancos de dados e sistemas informatizados. Isso implica em um aumento significativo nos riscos de ataques cibernéticos, devido a vulnerabilidades na segurança da informação e cibernética, afetando tanto o governo quanto os cidadãos de forma significativa. Buscar ferramentas, frameworks e processos de gestão modernos que auxiliem os órgãos públicos a manter integridade, disponibilidade e autenticidade de sua informação e infraestrutura se tornou um dever do gestor público de TIC nos últimos anos.

2.1.4 A instituição do PGD (Programa de Gestão e Desenvolvimento) consolidou a modalidade de trabalho remoto, dispersando o parque de máquinas da instituição para fora do perímetro da LAN institucional. Através do acesso remoto (VPN) os trabalhadores da UFFS conseguem acessar os recursos internos digitais de forma que possam desempenhar suas funções adequadamente. No entanto, com o crescimento deste tipo de acesso, se faz ainda mais urgente e necessário aumentar a segurança nas pontas (endpoints), através de inventário, gestão de vulnerabilidades (fragilidades), detecção e resposta em tempo real de ameaças e instalação de patches de segurança.

2.1.5 A modalidade de licitação definida neste processo cumpre o disposto nos Decretos no 5.450/2005 e 7.892/2013, permitindo assim a aquisição de forma

parcelada, nas quantidades e no momento adequado às necessidades da UFFS. A eventual aquisição da solução ora apresentada justifica-se pela impossibilidade de garantia de 100% de proteção aos ambientes de Tecnologia da Informação e Comunicação (TIC), sendo imprescindível nesse contexto a presença de solução de avaliação de riscos, ameaças e mitigação integrada.

3. ÁREA REQUISITANTE

Identificação da Área requisitante	Nome do responsável
Diretoria de Infraestrutura de Tecnologia da Informação	Jones Muneron

4. NECESSIDADES DE NEGÓCIO

4.1 Atendimento ao Programa de Privacidade e Segurança da Informação da Secretaria de Governo Digital instituído pela PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023.
4.2 Continuidade da conformidade das práticas institucionais à NBR ISO/IEC 17799 - Código de prática para a gestão da segurança da informação;
4.3 Atender a Política de Segurança da Informação e Comunicações da UFFS estabelecida através da PORTARIA Nº 216/GR/UFFS/2018.
4.4 Em conformidade com a ETIR (PORTARIA Nº 2535/GR/UFFS/2022). A gestão desta plataforma deverá ser exclusiva aos profissionais da área de Tecnologia da Informação e servidores públicos efetivos da UFFS.

5. NECESSIDADES TECNOLÓGICAS

5.1 Plataforma Central e ÚNICA: As soluções devem ser entregues como um serviço Software-as-a-Service (SaaS) em nuvem para todos os seus serviços e aplicativos exigidos neste documento.
5.1.2. A gestão de todos os módulos considerados neste termo deve ser feita através de uma console única, onde todas as funcionalidades deverão estar integradas, visando uma maior eficiência na operação da solução. Não serão aceitas solução que requeiram

custos extras de integração ou desenvolvimento adicional para integrar ferramentas de fabricantes diferentes.
5.1.3. Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365.1.e garantir 99% de disponibilidade.
5.1.4. A FABRICANTE deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço.
5.1.5.1. As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados e serviços fornecidos.
5.1.6. Será admitida apenas 1 desconexão por trimestre, por período não superior a 4 horas do serviço oferecido em janelas de manutenção programada e previamente avisado.
5.1.7. A plataforma que fornece os serviços deve ser certificada pela FedRAMP e certificada para os procedimentos de segurança SSAE 18 SOC 2.
5.1.8. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA25.1.
5.1.9. A solução deve permitir:
5.1.9.1. a criação de usuários distintos;
5.1.9.2. a separação de funções e permissões na console;
5.1.9.3. a integração através de SSO com, pelo menos, Okta e Azure Active Directory;
5.1.9.4. acessibilidade a partir de, pelo menos, um dos navegadores comerciais dentre GoogleChrome, Microsoft Edge e Firefox.
5.1.10. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS.
5.1.11. A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto.
5.1.12. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração.
5.1.13. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional.
5.1.14. A solução deve permitir o acesso de um usuário autorizado de qualquer local.
5.1.15.1. A solução deve suportar autenticação de dois fatores para usuários e login.
5.1.16. A solução deve suportar configurações de segurança de senha.
5.1.17. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por:
5.1.17.1. Idade e expiração da senha;
5.1.17.2. Conta do usuário bloqueada após uma série de logins com falha;
5.1.17.3. Comprimento mínimo da senha;
5.1.17.4. Complexidade da senha, caracteres alfanuméricos e numéricos a serem usados;
5.1.17.5. Forçar mudança de senha no login inicial;
5.1.17.6. Notificação de senha expirada antes de vários dias.
5.1.18. A solução deve suportar a capacidade de restringir o acesso apenas de rede interna da empresa.
5.1.19. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação.

5.2 PLATAFORMA GERAL - AGENTES

5.2.1. A solução proposta deve oferecer um ÚNICO agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede.
5.2.2. A solução deve ser instalada em servidores, estações de trabalho e máquinas virtuais,suportando sua implantação em rede local, em rede doméstica e na nuvem.
5.2.3. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais:
5.2.3.1. Windows 7/Windows Server 2003 SP2 e posterior (x86, x64)
5.2.3.2. Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64)
5.2.3.3. Ubuntu 14, 16,18,19,20 (x64)
5.2.3.4. Oracle Enterpise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6
5.2.3.5. Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03
5.2.3.6. SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11
5.2.4. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente.
5.2.5. A solução deve suportar plataformas de nuvem AWS, GCP e Azure.
5.2.6. A solução deve ser capaz de coletar informações sobre o inventário de ativos.
5.2.7. As funcionalidades de gestão de ativos e aplicação de patches devem ser fornecidas pelo mesmo agente de gerenciamento, não serão aceitas soluções com múltiplos agentes.
5.2.8. A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma.
5.2.9. O agente de gerenciamento deve suportar o uso de proxy.
5.2.10. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento.
5.2.11. Deve ser possível limitar o consumo de CPU e memória do agente.
5.2.12. Deve permitir a definição de um período global de inatividade dos agentes.
5.2.13. A solução deve prover nativamente um mecanismo de cache dos principais patches aplicados no ambiente visando a redução do consumo de banda.

5.3 Solução De Categorização e Inventário De Ativos: Verificar ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo.

5.4 Solução De Gerenciamento De Patch – Remediação De Ativos: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo.

5.5 Solução De Gerenciamento De Vulnerabilidades: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo.

5.6 Solução De Detecção E Resposta E Proteção Contra Malware: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo.

5.7 Solução De Verificação E Scan De Aplicações Web: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo.

5.8 Serviço De Implementação Categorização E Inventário De Ativos: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo. Deverá ser atendido por um único fornecedor do 5.8 ao 5.12 a fim de padronizar o projeto de implantação.

5.9 Serviço De Implementação De Gerenciamento De Patch – Remediação De Ativos: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo. Deverá ser atendido por um único fornecedor do 5.8 ao 5.12 a fim de padronizar o projeto de implantação.

5.10 Serviço De Implementação De Solução De Gerenciamento De Vulnerabilidades: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo. Deverá ser atendido por um único fornecedor do 5.8 ao 5.12 a fim de padronizar o projeto de implantação.

5.11 Serviço De Implementação De Solução De Detecção E Resposta E Proteção Contra Malware: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo. Deverá ser atendido por um único fornecedor do 5.8 ao 5.12 a fim de padronizar o projeto de implantação.

5.12 Serviço De Implementação De Solução De Verificação E Scan De Aplicações Web: ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO para detalhamento completo. Deverá ser atendido por um único fornecedor do 5.8 ao 5.12 a fim de padronizar o projeto de implantação.

6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

6.1 Prover a infraestrutura tecnológica suficiente para a manutenção das atividades fins institucionais ;
6.2 Manter os recursos necessários para a garantia da segurança das informações digitais sob custódia da instituição ;
6.3 Mitigar os riscos relacionados à perda de informações relativas às atividades institucionais ;
6.4 Otimizar o tempo de solução de incidentes relacionados a falhas de equipamentos ou falha de software, seja software de infraestrutura ou sistemas institucionais ;
6.5 Requisitos Ambientais: Atendimento à legislação ambiental brasileira para produção

e descarte de materiais.
6.6 Requisitos Legais: A contratação deverá estar em conformidade com a legislação que rege os processos de contratação no setor público (Lei 8.666/93, Lei 10.520/02, Lei 14.133/21, suas alterações e regulamentações);
6.7 Requisitos de Capacitação: A empresa CONTRATADA deverá executar um repasse de conhecimento para os técnicos de TIC da UFFS que farão o gerenciamento da solução.
6.8 Requisitos de Logística: A empresa vencedora deverá entregar todos os módulos da solução, quando aplicável, nos endereços listados no edital dentro do prazo de entrega estabelecido no mesmo;
6.9 Requisitos de Segurança: O acesso ao ambiente físico/lógico deverá ser realizado com supervisão de um técnico de TIC e de forma limitada ao escopo do projeto.
6.10 Requisitos de Suporte: A empresa vencedora deverá prestar garantia para todos os equipamentos adquiridos de acordo com as especificações do edital, obedecendo forma e prazo de atendimento/solução;

7. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

7.1 A presente contratação visa atribuir uma unidade de licença para cada host UFFS. Os hosts hoje são divididos em dois grandes grupos: Servidores de Aplicação e Equipamentos de usuários

7.2 Para o ambiente de infraestrutura de aplicações tem como unidade básica de organização uma máquina virtual (MV ou *VM - Virtual Machine*), onde executa um sistema operacional de servidor servindo de base para a execução de aplicações de diversas naturezas (aplicações de banco de dados, aplicações Web, *softwares* básicos de infraestrutura de rede, dentre outras aplicações).

7.3 A infraestrutura de aplicações institucionais é composta por 4 (quatro) ambientes virtualizados (desenvolvimento, testes, homologação e produção) utilizando o virtualizador VMware ESXi, coordenados pelo *software* VMware vCenter e distribuídos em 10 servidores físicos com 2 *sockets* de processamento cada.

7.4 Considera-se então para a estimativa da demanda o número de 400 (quatrocentas) máquinas virtuais (MVs) que necessitam da presente solução de segurança da informação, onde 60 (sessenta) MVs são responsáveis pela infraestrutura de rede, autenticação e repositório nos *campi* e 340 (trezentos e quarenta) são responsáveis pela infraestrutura de aplicações institucionais do ambiente de produção.

Ambiente do vCenter	Número de máquinas virtuais de produção
Datacenter	340
Campus Chapecó	10
Campus Erechim	10

Campus Cerro Largo	10
Campus Laranjeiras do Sul	10
Campus Realeza	10
Campus Passo Fundo	10

7.5 Já o ambiente de estações de trabalho do usuário deverá ter cobertura para o quantitativo adquirido nos últimos 5 anos, prazo médio que o equipamento fica ativo em ciclo de vida, totalizando 978 equipamentos ativos no parque, sendo divididos da seguinte forma:

Estações de Trabalho	Desktops	Notebooks
2019	514	15
2020	3	7
2021	50	109
2022	38	110
2023	100	42

7.6 Portanto o quantitativo estimado de licenças para cobrir o parque de máquinas da UFFS é de 1378. Lembrando que este número é uma estimativa, prevendo possível crescimento do parque ou equipamentos legados mais antigos que ainda podem ser utilizados e não entraram na conta é salutar prever, pelo menos, um quantitativo de 5% a 10% superior ao aqui calculado e considerando a vigência da ATA.

7.7 A demanda quanto aos serviços deverá atender abranger uma plataforma central (Dashboard), única, com as funcionalidades: Categorização de Ativos, Gerenciamento de Patches, incluindo aplicação através da plataforma, gerenciamento de vulnerabilidades, Detecção e resposta e proteção contra malware e scan de aplicações.

8. LEVANTAMENTO DE SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	Aquisição de solução de Segurança da Informação como um serviço Software-as-a-Service (SaaS) em nuvem, com todas as funcionalidades atendidas

	por uma única plataforma de gerenciamento e compra de licenças para 36 meses.
2	Terceirização de solução de Segurança da Informação como um serviço de SOC
3	Aquisição de solução de Segurança da Informação como um serviço Software-as-a-Service (SaaS) em nuvem, com todas as funcionalidades atendidas por mais de uma plataforma de gerenciamento e compra de licenças para 36 meses.

9. ANÁLISE COMPARATIVA DAS SOLUÇÕES

Requisitos		**Cenários**		
		Cenário 1	Cenário 2	Cenário 3
Negócio	Requisito 1	Atende	Atende	Atende
	Requisito 2	Atende	Atende	Atende
	Requisito 3	Atende	Não atende	Atende
	Requisito 4	Atende	Não Atende	Atende
Tecnológico	Requisito 1	Atende	Atende Parcialmente	Não Atende
	Requisito 2	Atende	Atende	Não Atende
	Requisito 3	Atende	Atende	Atende
	Requisito 4	Atende	Atende	Atende
	Requisito 5	Atende	Atende	Atende
	Requisito 6	Atende	Atende	Atende
	Requisito 7	Atende	Atende	Atende
	Requisito 8	Atende	Atende	Atende
	Requisito 9	Atende	Atende	Atende
	Requisito 10	Atende	Atende	Atende
	Requisito 11	Atende	Atende	Atende
	Requisito 12	Atende	Atende	Atende
Resultado da Análise		Viável	Não viável	Não Viável

10. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

10.1 Para a análise da inviabilidade da solução 2 considera-se que a segurança da informação é um tema bastante sensível, a manipulação de um sistema que irá manipular infraestrutura sensível e parametrização de cibersegurança deve ser tratada por servidores públicos efetivos, assim como preconiza a ETIR UFFS (PORTARIA Nº 2535/GR/UFFS/2022). É fato notório e conhecido que algumas das principais técnicas de invasão hoje se dá através da venda de credenciais e de terceiros com acesso aos sistemas. Garantir que esta solução seja de escopo apenas de servidores públicos autorizados estabelece um vínculo efetivo com aqueles que detêm o acesso aos controles de segurança da instituição.

10.2 Para a análise de inviabilidade da solução 3, verificamos que a maioria das soluções de mercado atendem parcialmente aos requisitos. Por exemplo, determinado fabricante tem um a solução de EDR/XDR, mas não tem o scan e gerenciamento de vulnerabilidades, ou então não possui o Patch Management de forma que não apenas verifique os patches pendentes, mas que também execute esta aplicação, ou o monitoramento ativo das principais URLs da UFFS. Ou seja, que possui todos as funcionalidades de mesmo fabricante, com fácil visualização através de dashboard centralizada e agente único, sem necessidade de integrações adicionais ou de se ter que se criar algo compondo com um emaranhado de fabricantes, o que envolveria custos adicionais.

10.3 A única solução que atendeu a todos estes critérios da Solução 1 foi a solução da Qualys, usada como referência na solicitação de orçamento junto a diferentes fornecedores.

11. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

O fornecimento de licenças do software pelo fabricante ocorre em 1 (uma) licença para cada 10 cargas de trabalho do servidor físico do qual será realizado *backup***.** Por carga de trabalho compreende-se servidor físico ou servidor virtual.

11.1 Solução Viável 1 - Aquisição de solução de Segurança da Informação como um serviço Software-as-a-Service (SaaS) em nuvem, com todas as funcionalidades atendidas por uma única plataforma de gerenciamento e compra de licenças para 36 meses.

11.1.1 Composição dos itens da solução

Id	Descrição da solução (ou cenário)
1	Serviço De Implementação Categorização E Inventário De Ativos
2	Serviço De Implementação De Gerenciamento De Patch – Remediaçao De Ativos
3	Solução De Gerenciamento De Vulnerabilidades
4	Solução De Detecção E Resposta E Proteção Contra Malware
5	Solução De Verificação E Scan De Aplicações Web

6	Serviço De Implementação Categorização E Inventário De Ativos
7	Serviço De Implementação De Gerenciamento De Patch – Remediaçao De Ativos
8	Serviço De Implementação De Solução De Gerenciamento De Vulnerabilidades (Fragilidades)
9	Serviço De Implementação De Solução De Detecção E Resposta E Proteção Contra Malware
10	Serviço De Implementação De Solução De Verificação E Scan De Aplicações Web

ID Cotação	Fonte	Descrição da Fonte
1	Pesquisa direta com fornecedor	Advanta Sistemas de Telecomunicações e Serviços de Informática LTDA
2	Pesquisa direta com fornecedor	CLEAR TECNOLOGIA DA INFORMAÇÃO LTDA
3	Pesquisa direta com fornecedor	Unnit Solucoes Tecnologicas LTDA

Solução Viável 1 – Aquisição de solução de Segurança da Informação como um serviço Software-as-a-Service (SaaS) em nuvem, com todas as funcionalidades atendidas por uma única plataforma de gerenciamento e compra de licenças para 36 meses.

ID Item	ID Cotação #1	ID Cotação #2	ID Cotação #3	MÉDIA
	Valor Unitário	Valor Unitário	Valor Unitário	Valor Unitário
1	R$144.827,77	R$ 152.500,00	R$ 155.433,00	150.920,25
2	121.377,54	127.000,00	130.234,00	126.203,84
3	111.071,39	117.700,00	121.300,00	116.690,46
4	141.392,38	149.750,00	153.110,00	148.084,12
5	60.056,03	69.700,00	73.400,00	67.718,67
6	4.357,24	5.450,00	6.300,00	5.359,08
7	4.357,24	6.930,00	6.300,00	5.852,41
8	4.357,24	5.450,00	6.300,00	5.359,08
9	4.357,24	5.450,00	6.300,00	5.359,08
10	6.790,04	8.590,00	9.340,00	8.240,01

11.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

11.1.1 Consideramos para o custo total de propriedade a quantidade de máquinas virtuais hospedadas nos servidores físicos do datacenter e dos servidores alocados nos *campi,* mais os equipamentos de usuários entre notebooks e desktops.

11.1.2 Considerando a abertura de ATA de registro de preços e a aquisição progressiva, tendo em vista que as licenças são rotativas, ou seja, elas podem ser remanejadas entre equipamentos, bem como estas licenças podem ser instaladas conforme a criticidade do ambiente. A aquisição total de uma só vez além de financeiramente não viável dado o orçamento disponível, acabaria criando um tempo de ociosidade destas licenças entre a compra e a efetiva instalação. Desta forma a aquisição modularizada ao longo do tempo, dividida em três etapas de 500 licenças, mostra-se a mais vantajosa para a Administração.

Solução Viável 1 – Contratação de licenciamento perpétuo do software				
Ano -->	**1**	**2**	**3**	**Menor Preço**
Item				
Solução Viável 1 – Aquisição de solução de Segurança da Informação como um serviço Software-as-a-Service (SaaS) em nuvem, com todas as funcionalidades atendidas por uma única plataforma de gerenciamento e compra de licenças para 36 meses.	R$ 601.274,07	R$ 601.274,07	R$ 601.274,07	**1.803.822,21**
Custo Total no Ano	R$ 601.274,07	R$ 601.274,07	R$ 601.274,07	**1.803.822,21**
Custo Total de Propriedade da Solução Viável 1				**1.803.822,21**

11.2. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	**Estimativa de TCO ao longo dos anos**			**Total**
	Ano 1	**Ano 2**	**Ano 3**	
Solução Viável 1	R$ 601.274,07	R$ 601.274,07	R$ 601.274,07	**R$ 1.803.822,21**

– Aquisição de solução de Segurança da Informação como um serviço Software-as-a-Service (SaaS) em nuvem, com todas as funcionalidades atendidas por uma única plataforma de gerenciamento e compra de licenças para 36 meses.				

12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

12.1 A solução escolhida foi a aquisição de 500 licenças da Qualys na modalidade de licenciamento por 36 meses. Através da formação de uma ATA de Registro de Preços a Administração poderá adquirir ainda outros dois pacotes de 500 licenças ao longo da vigência da ATA de 24 meses.

12.1.1 Optou por ATA de Registro de Preços, pois o recurso estará disponível no ano. Diluindo a contratação em três etapas, faz o custo total no ano para segurança da informação não ser tão pesado, permitindo que a área de Tecnologia da Informação contrate também em outras áreas de infraestrutura de TIC. Ainda, os contratos serão de 36 meses. Neste cenário, modularizar as contratações novamente fica mais interessante, pois diminui o risco de apagão, ou seja um momento no tempo onde a UFFS não terá nenhuma licença ativa. As licenças que estaremos adquirindo no último ano de vigência da ATA ainda terão validade de 36 meses. Ou seja, em um caso hipotético onde só adquirimos o que está na presente ATA, sem renovação. Teríamos o seguinte cenário:

2024 - 500 licenças ativas
2025 - 1000 licenças ativas
2026 - 1500 licenças ativas
2027 - 1000 licenças ativas
2028 - 500 licenças ativas

12.1.2 O que garante que o parque da UFFS esteja minimamente coberto e com uma solução abrangente de segurança da informação focada em endpoints. Ao iniciar um futuro processo

de renovação das licenças, ajuda também no controle e em uma renovação mais tranquila, buscando os momentos mais oportunos para a administração, evitando apagões em momentos de crise. Neste cenário, o processo de renovação de licenças poderia acontecer em 2027, 2028 ou 2029, sem que o parque ficasse completamente desassistido.

12.2 A escolha da solução é consequência dos seguintes requisitos de negócio e requisitos tecnológicos:

12.2.1 A solução possui console centralizada e a única que reuniu as funcionalidades de: patch management, com aplicação dos patches de segurança, via plataforma. Controle de inventário. Gerenciamento de Vulnerabilidades. Endpoint Detection & Response. Scan e monitoramento de URLs em um só pacote, tornando-se assim o melhor custo benefício.

12.2.2 Visando a competitividade e o menor preço, cada pacote de licenças de funcionalidade da solução poderá ser disputado por diferentes proponentes, no entanto o fabricante escolhido é a Qualys pelas razões já apresentadas. Para os itens relacionados a serviço, apenas uma empresa deverá ser escolhida, a fim de otimizar o projeto de implantação que deverá ser único. Desta forma, formou-se um grupo (**grupo 1**)para o item serviços que deverá ser arrematado no conjunto completo por um só proponente que deve ter todas as habilitações especificadas tanto neste documento, quanto no termo de referência e especificações técnicas da solução.

A decisão de agrupar os itens levou em consideração que a entrega parcial de alguns serviços do grupo, poderia resultar em dificuldades de implementação e não atenderia plenamente às demandas da instituição. Ao optar por obter todos os serviços necessários de um único fornecedor, garante-se a disponibilidade completa e simultânea dos elementos essenciais para a construção da solução.

13. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

O Valor estimado da contratação é de **R$ R$ 1.803.822,21 (Um milhão, oitocentos e três mil oitocentos e vinte e dois reais e vinte e um centavos).**

item	Grupo	Descrição	Unid	QTD	Menor valor	Menor valor Total
1		Solução De Categorização e Inventário De Ativos Pacote 500 ativos	serviço	3	R$ 144.827,77	R$ 434.483,31
2		Solução De Gerenciamento De Patch – Remediação De Ativos Pacote 500 ativos	serviço	3	R$ 121.377,54	R$ 364.132,62

3		Solução De Gerenciamento De Vulnerabilidades Pacote 500 ativos	serviço	3	R$ 111.071,39	R$ 333.214,17
4		Solução De Detecção E Resposta E Proteção Contra Malware Pacote 500 ativos	serviço	3	R$ 141.392,38	R$ 424.177,14
5		Solução De Verificação E Scan De Aplicações Web **Pacote 10 Url's**	serviço	3	R$ 60.056,03	R$ 180.168,09
6	**Grupo 1**	Serviço De Implementação Categorização E Inventário De Ativos Pacote de implementação para 500 ativos	serviço	3	R$ 4.357,24	R$ 13.071,72
7		Serviço De Implementação De Gerenciamento De Patch – Remediaçao De Ativos Pacote de implementação para 500 ativos	serviço	3	R$ 4.357,24	R$ 13.071,72
8		Serviço De Implementação De Solução De Gerenciamento De Fragilidades Pacote de implementação para 500 ativos	serviço	3	R$ 4.357,24	R$ 13.071,72
9		Serviço De Implementação De Solução De Detecção E Resposta E Proteção Contra Malware Pacote de implementação para 500 ativos	serviço	3	R$ 4.357,24	R$ 13.071,72
10		Serviço De Implementação De Solução De Verificação E Scan De Aplicações Web **Pacote de Implementação de 10 Url's**	serviço	3	R$ 5.120,00	R$ 15.360,00
					Valor Total	**R$ 1.803.822,21**

14. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

14.1 A solução escolhida caso adquirida possibilitará ter um pacote bastante abrangente para os hosts da instituição, hoje a ponta mais fraca na infraestrutura institucional, haja vista o bom nível de segurança perimetral já implantado:

14.1.1 Proteção contra *as principais ameaças* e atualizada através de novas listas de definições que são atualizadas diariamente. Desta forma, é possível mitigar conexões remotas através da VPN, já que as conexões de trabalho hoje podem vir em até 20% dos nossos servidores trabalhando de forma remota. A conexão a partir da UFFS é naturalmente mais segura e nos permite maior controle do que a conexão feita através de redes domésticas. Através desta solução, a equipe de TI e segurança da informação da UFFS, passa a ter uma melhor gerência sobre estes equipamentos vindos de rede externas.

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

15.1 Por ser uma solução que foi testada por um mês dentro da UFFS, através de Prova de Conceito. Mostrou-se segura e com uma curva de aprendizado relativamente rápida, o que faria a solução ser implementada desde o seu primeiro dia e com servidores já treinados no uso das ferramentas, diminuindo assim a curva de aprendizado e economizando tanto o custo de projeto, quanto de cursos para domínio da tecnologia. As soluções onde seriam necessários mais de um fabricante para ter as mesmas entregas, demandaria projetos mais complexos e uma terceira ferramenta para integrá-los e nem sempre o resultado final é de acordo com o esperado, aumentando assim os custos e sem garantias quanto à entrega.

16. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

16.1 Adequação ao Programa PPSI do SGD/MGI Nº 852. Adequação aos principais desafios de cibersegurança que tem se apresentado aos órgãos da Administração Pública nos últimos anos e maior gerência para que os servidores de tecnologia da informação possam possuir ferramentas mínimas visando manter a confidencialidade, disponibilidade e integridade da informação digital da instituição..

16.2 Aderência a padrões adotados pelo mercado para a proteção contra ameaças de segurança da informação, como por exemplo o processo de Patch Management e Gerenciamento de Vulnerabilidades.

16.3 Assegurar a garantia da segurança dos dados institucionais ao manter-se uma solução canivete focada em endpoints com atualizações em tempo real.

17. PROVIDÊNCIAS A SEREM ADOTADAS

17.1 Não há providências a serem adotadas, considerando que a solução já foi testada ao longo de um mês pela instituição de maneira exitosa.

18. DECLARAÇÃO DE VIABILIDADE

A equipe de planejamento declara pela viabilidade da contratação de solução para provimento de segurança da informação com as funcionalidades de Controle de Inventário, Patch Management, Gerenciamento de Vulnerabilidades, Endpoint Detection & Response e Monitoramento de URLs

18.1 JUSTIFICATIVA

A escolha pela contratação do licenciamento através de ATA de registro de preços e modularmente ao longo de 2 anos, é para se adequar ao orçamento disponível, bem como de forma mais compatível com a quantidade de servidores públicos disponíveis para trabalhar no projeto de implantação e posterior operação da plataforma. Bem como o fato das licenças não serem fixas, ou seja, pode-se realocar a licença entre equipamentos conforme necessidade, criando assim linhas de defesa, enquanto o parque tecnológico recebe a implantação de forma gradual e de forma mais realista com o orçamento disponível.

19. RESPONSÁVEIS

A Equipe de Planejamento da Contratação foi instituída pela PORTARIA Nº 1503/PROAD/UFFS/2023, DE 16 OUTUBRO DE 2023.

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
_____ FLAVIO HUMBERTO TESTA **Matrícula/SIAPE: 2388204**	_____ Jones Muneron **Matrícula/SIAPE: 1816277**
INTEGRANTE TÉCNICO	**INTEGRANTE ADMINISTRATIVO**
_____ Marcos Eugênio Dietrich **Matrícula/SIAPE: 2126948**	_____ Anderson Machado Pereira **Matrícula/SIAPE: 1766529**

20. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa IN SGD/ME nº 1, de 2019.

AUTORIDADE MÁXIMA DA ÁREA DE TIC (OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)
_____

Cassiano Carlos Zanuzzo

Secretário Especial de Tecnologia e Informação

2809631

F0054 - ENCARTE DO TERMO DE REFERÊNCIA Nº 16/2023 - SETI (10.53)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 28/11/2023 09:35)
CASSIANO CARLOS ZANUZZO
SECRETARIO
SETI (10.53)
Matrícula: ###096#1

(Assinado digitalmente em 28/11/2023 11:20)
EDIVANDRO LUIZ TECCHIO
PRO-REITOR
PROAD (10.46)
Matrícula: ###223#8

(Assinado digitalmente em 28/11/2023 09:07)
FLAVIO HUMBERTO TESTA
ANALISTA DE TEC DA INFORMACAO
DITI (10.53.05)
Matrícula: ###882#4

(Assinado digitalmente em 28/11/2023 11:04)
JONES JEFERSON MUNERON
DIRETOR
DITI (10.53.05)
Matrícula: ###162#7

(Assinado digitalmente em 28/11/2023 09:09)
MARCOS EUGENIO DIETRICH
TEC DE TECNOLOGIA DA INFORMACAO
DRT (10.53.05.02)
Matrícula: ###269#8