ESTUDO TÉCNICO PRELIMINAR - TJ/AM/SETIC/DVITIC

1. Introdução

Estudo Técnico Preliminar - ETP - para a primeira etapa do planejamento de uma contratação para assegurar a viabilidade e embasar o Termo de Referência, conforme previsto na Resolução N.º 025/2019 TJAM, bem como fornecer informações necessárias para o processo de contratação.

2. Descrição da Necessidade da Contratação

2.1. MOTIVAÇÃO

2.1.1. O Tribunal de Justiça do Estado do Amazonas (TJAM) utiliza o método de proteção em camadas de segurança. Este método consiste em criar várias camadas de proteção distintas e complementares, sendo que cada camada atua de forma especializada em algum componente de segurança. Uma das principais camadas de proteção em um ambiente de TI é o equipamento de firewall, ativo que possui a capacidade de inspecionar, controlar e bloquear o tráfego proveniente da Internet com destino aos sistemas e serviços do TJAM, sendo também possível aplicar políticas e restrições de acessos inter-redes e controlar os acessos dos usuários internos com destino à Internet;

2.1.2. A solução atual possui contrato de suporte técnico especializado e garantia, bem como módulos de subscrições de IPS (*Intrusion Prevention System*), Filtro de conteúdo Web, Análise de Malware, VPN (*Virtual Private Network*) e software de gerenciamento de plataforma de segurança, que expira em Novembro/2023. Destaca-se que uma solução de segurança cibernética somente se sustenta se estiver plenamente atualizada, uma vez que as funcionalidades das ferramentas de segurança fazem uso de recursos de inteligência de reputação, providos através das subscrições e fornecidos pelo fabricante da plataforma de segurança da solução. Dessa forma, muitas atividades e ações podem ser automatizadas, reduzindo o esforço da equipe técnica e também diminuindo possíveis falhas de operação que podem impactar na disponibilidade e estabilidade do ambiente;

2.1.3. Devido a complexidade das soluções de segurança, faz-se necessário manter um suporte técnico especializado, 24x7, com o objetivo de poder acionar um suporte técnico, obter recomendações de melhores práticas e assessoramento para o funcionamento da plataforma de solução de segurança. Além disso, a garantia é fundamental para manter contratos de substituição de peças e equipamentos durante a vigência do contrato;

2.1.4. Considerando que o TJAM já utilizada há mais de 05 anos a plataforma de solução de segurança da fabricante Palo Alto Networks, que vem mantendo a estabilidade, pleno funcionamento e a confiabilidade em um ambiente complexo como a infraestrutura do TJAM, busca-se também expandir as soluções de segurança integradas na plataforma para as unidades descentralizadas do TJAM, bem como suportar o aumento das capacidades operacionais necessários para acompanhar as cargas de trabalho demandados pelos equipamentos do núcleo da rede;

2.1.5. Com os recursos adquiridos, será possível modificar a arquitetura atual e realizar a expansão da tecnologia de firewall do TJAM para as unidades descentralizadas, equipando-as com *apliances* Palo Alto de menor capacidade, mas com recursos suficientes para permitir gerenciamento centralizado através do Panorama e ainda interconexão de múltiplos links com a tecnologia SD-WAN;

2.1.6. As motivações também estão alinhadas com as recomendações de diferentes órgãos e instruções normativas à respeito da adoção de controles gerais de segurança da informação, dentre os quais destacam-se:

2.1.6.1. O decreto 10.222, de 5 de fevereiro de 2020, que dispõe sobre a Estratégia Nacional de Segurança Cibernética, cita com um dos seus objetivos o aumento da resiliência brasileira às ameaças cibernética elevando principalmente o nível de proteção do Governo.

> “Aperfeiçoar e manter atualizados os sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética, adotando que abordem iniciativas integradoras”

2.1.6.2. A Lei 13.709, de 14 de agosto de 2018, intitulada como a Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 46 cita que:

> “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”

2.1.6.3. A Resolução 370 de 28/01/2021, Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), onde orientada em seu preâmbulo pelos objetivos dos seguintes componentes:

> “Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados”.

2.1.6.4. Na Resolução 396 de 07/06/2021 do CNJ, que institui a Instituir a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF), destaca-se o artigo:

> "Art. 9º São ações da ENSEC-PJ:
>
> I - fortalecer as ações de governança cibernética;
>
> II - elevar o nível de segurança das infraestruturas críticas;
>
> III - estabelecer rede de cooperação do Judiciário para a segurança cibernética;
>
> IV - estabelecer modelo centralizado de governança cibernética nacional."

2.1.7. A renovação das subscrições e a expansão da solução de firewall para as unidades descentralizadas é a alternativa mais apropriada para o TJAM, permitindo que o Tribunal mantenha toda as barreiras de proteção já implementadas e proporcione um incremento nessas barreiras com a expansão desses recursos de proteção contra os ataques cibernéticos que crescem assustadoramente e que atingem diversos outros órgãos e tribunais, como por exemplo, os ataques ocorridos no Supremo Tribunal Federal (2021), Superior Tribunal de Justiça (2021), Tribunal de Justiça do Estado do Rio Grande do Sul (2021), Tribunal de Justiça do Estado do Amazonas (2021), TRT 4 Região (2021), TRF 3 Região (2022), TRT-ES (2022), Tribunal de Contas do Ceará (2022), Justiça Federal de Pernambuco (2022), entre outros;

2.1.8. Além das razões apresentadas, existem as necessidades em manter a eficácia, integração e a qualidade da plataforma de segurança em um ambiente de TI complexo como o do TJAM, bem como reduzir possíveis impactos gerados pela indisponibilidade dos serviços e sistemas de TIC e também evitar a reimplementação das barreiras de seguranças já em operação do TJAM.

2.2. OBJETIVOS

2.2.1. Esta contratação tem o objetivo de aumentar a estabilidade e a confiabilidade da solução de Firewall existente no TJAM, que atua na proteção da borda de Internet, na proteção dos ativos de rede do datacenter, bem como permitir a expansão da tecnologia de firewall do TJAM para as unidades descentralizadas, permitindo gerenciamento centralizado através do Panorama e ainda interconexão de múltiplos links com a tecnologia SD-WAN;

2.2.2. Busca-se também preservar os investimentos realizados no ambiente do TJAM, pois durante o período de vigência dos equipamentos o corpo técnico da SETIC adquiriu amplo conhecimento e experiencia na solução de segurança atual, permitindo o desenvolvimento de projetos específicos para levar segurança aos usuários internos e remotos do TJAM.

2.3. BENEFÍCIOS

2.3.1. Manter a estabilidade, confiabilidade e proteção da segurança do tráfego de perímetro e da borda de acesso à Internet, através da renovação da solução de segurança atual que se encontra em pleno funcionamento;

2.3.2. Expandir os recursos de segurança da tecnologia de firewall do TJAM para as unidades descentralizadas, equipando-as com *apliances* Palo Alto de menor capacidade, mas com recursos suficientes para permitir gerenciamento centralizado através do Panorama e ainda interconexão de múltiplos links com a tecnologia SD-WAN;

2.3.2. Introduzir o conceito de Zero Trust na arquitetura nas unidades descentralizadas do TJAM, permitindo que todo o Judiciário Amazonense esteja atualizado com as melhores práticas e referências quanto à segurança da informação;

2.3.3. Dispor de equipamentos e soluções com tecnologias e recursos atualizados para o enfrentamento dos riscos de segurança no ambiente de TI;

2.3.4. Prover a garantia da solução de segurança em firewall com eficaz substituição de peças dos equipamentos, para que seja mantida a alta disponibilidade das operações;

2.3.5. Garantir o nível de suporte técnico necessário para atender um ambiente corporativo complexo e robusto como o do TJAM;

2.3.6. Aperfeiçoar a detecção e a diminuição do tempo respostas às ameaças cibernéticas contra o ambiente do TJAM;

2.3.7. Obter suporte adequado do fabricante quanto às necessidade de aperfeiçoamento, adoção das melhores práticas na solução de segurança e resoluções de problemas.

2.3. ALINHAMENTO ESTRATÉGICO

2.3.1. Entende-se que a presente aquisição compartilha dos objetivos pretendidos no Plano Diretor de Tecnologia da Informação e Comunicação- PDTIC, referente ao biênio 2023-2024, do TJAM;

2.3.1.1. Perspectiva: Processos Internos

2.3.1.2. Objetivo Estratégico: Aperfeiçoamento administrativa e da governança judiciária

2.3.1.3. Iniciativa Estratégica: Renovação das Licenças do Palo Alto

2.3.1.4. Descrição: Contratação de empresa especializada para licenciamento das *appliances* Palo Alto

2.4. Portanto, faz-se necessário contratar solução de TI consistente na renovação do licenciamento de software da solução de firewall de borda, expansão da solução de firewall para as unidades descentralizadas do Tribunal de Justiça do Estado do Amazonas.

2.5. As normas legais que servirão como subsídio para a aquisição/contratação pretendida são:

2.5.1. Lei nº. 8.666/93, de 21 de junho de 1993;

2.5.2. Lei n°10.520, de 17 de julho de 2002;

2.5.3. Resolução nº 25/2019 - TJAM.

3. Estimativa das Quantidades

LOTE 1: Renovação de licenciamento de software da solução de Firewall de Datacenter			
ITEM	**ESPECIFICAÇÕES**	**QUANTIDADE MÍNIMA POR CONTRATAÇÃO**	**QUANTIDADE TOTAL**
1	Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
2	Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
3	Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
4	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5220, com suporte Premium oficial Palo Alto	2	2

	Networks 24x7 em Alta Disponibilidade, pelo período de 60 meses.		

LOTE 2: Expansão de solução de firewall para o ambiente de datacenter e unidades descentralizadas			
ITEM	**ESPECIFICAÇÕES**	**QUANTIDADE MÍNIMA POR CONTRATAÇÃO**	**QUANTIDADE TOTAL**
1	Firewall Palo Alto PA-410	10	70
2	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN), pelo período de 60 meses.	10	70
3	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	10	70
4	Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks, pelo período de 60 meses.	1	1
5	Garantia da Solução de Panorama, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	1	1
6	Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
7	Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
8	Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks PA-410 e PA-5410.	12	72
9	Treinamento oficial do fabricante remoto, em língua portuguesa, com disponibilização de voucher para certificação de administração da solução Palo Alto.	2	4
10	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
11	Firewall Palo Alto PA-5410	2	2
12	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN) para PA-5410, pelo período de 60 meses.	2	2
13	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	2	2
14	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5410, pelo período de 60 meses.	2	2

4. Estimativa de Preços

4.1 Tomando por base alguns preços que levantamos informalmente, a expectativa é de que a Ata de Registro de Preços tenha o valor total de **R$ 18.572.562,90**, conforme detalhado na tabela abaixo:

LOTE	**ITEM**	**QUANTIDADE**	**ESPECIFICAÇÕES**	**VALOR ESTIMADO**	
				UNITÁRIO	**TOTAL**
1	1	2	Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	R$ 583.853,33	R$ 1.167.706,66
	2	2	Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	R$ 875.581,67	R$ 1.751.163,34

	3	2	Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	R$ 583.853,33	R$ 1.167.706,66
	4	2	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5220, com suporte Premium oficial Palo Alto Networks 24x7 em Alta Disponibilidade, pelo período de 60 meses.	R$ 732.398,33	R$ 1.464.796,66
2	1	70	Firewall Palo Alto PA-410	R$ 13.381,00	R$ 936.670,00
	2	70	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN), pelo período de 60 meses.	R$ 8.829,00	R$ 618.030,00
	3	70	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	R$ 19.462,00	R$ 1.362.340,00
	4	1	Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks, pelo período de 60 meses.	R$ 259.151,00	R$ 259.151,00
	5	1	Garantia da Solução de Panorama, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	R$ 301.514,00	R$ 301.514,00
	6	2	Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	R$ 583.853,33	R$ 1.167.706,66
	7	2	Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	R$ 259.151,00	R$ 518.302,00
	8	72	Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks PA-410 e PA-5410.	R$ 3.172,97	R$ 228.454,00
	9	4	Treinamento oficial do fabricante remoto, em língua portuguesa, com disponibilização de voucher para certificação de administração da solução Palo Alto.	R$ 19.402,00	R$ 77.608,00
	10	2	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	R$ 489.839,00	R$ 979.678,00
	11	2	Firewall Palo Alto PA-5410	R$ 1.000.000,00	R$ 2.000.000,00
	12	2	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN) para PA-5410, pelo período de 60 meses.	R$ 1.430.301,83	R$ 2.860.603,66
	13	2	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	R$ 512.678,83	R$ 1.025.357,66
	14	2	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5410, pelo período de 60 meses.	R$ 342.887,30	R$ 685.774,60
				TOTAL	**R$ 18.572.562,90**

5. Análise de Risco

O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, da execução do objeto e da gestão contratual.

O Mapa de Gerenciamento de Riscos contém a identificação e a análise dos principais riscos, consistindo na compreensão da natureza e determinação do nível de risco, que corresponde à combinação do impacto e de suas probabilidades que possam comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC.

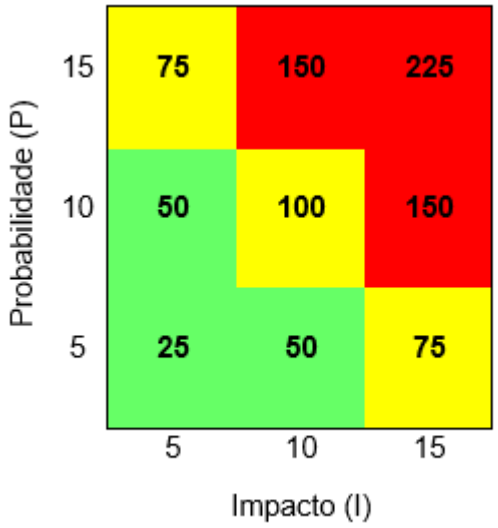
Para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos e impacto caso o risco ocorra, possíveis ações preventivas e de contingência (respostas aos riscos), a identificação de responsáveis pelas ações, bem como o registro e o acompanhamento das ações de tratamento dos riscos.

Como exemplo, parâmetros escalares são utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão as ações relacionadas aos riscos durante as fases de contratação (planejamento, seleção de fornecedor e gestão do contrato).

Escala de Classificação

Classificação	Valor
Baixo	5
Médio	10
Alto	15

A tabela a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.



Exemplo de diretrizes de tratamento de riscos: O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz probabilidade x impacto. Caso o risco enquadre-se na região verde, seu nível de risco é entendido como baixo, logo admite-se a aceitação ou adoção das medidas preventivas. Se estiver na região amarela, entende-se como médio; e se estiver na região vermelha, entende-se como nível de risco alto.

- **Risco do processo de contratação**

Risco 1	Risco:	Não aprovação de Estudo Técnico ou do Termo Referência.		
	Probabilidade:	Média	Id	Dano Potencial
	Impacto:	Alto	1	Atraso no processo de contratação e consequentemente atraso na execução da

				aquisição.	
	Id	Ação Preventiva			Responsável
	1	Instruir o Estudo Técnico Preliminar e o Projeto Básico de forma clara e baseando-se na Instrução Normativa nº 04/2010, na resolução 25/2019 do TJAM, assim como no Guia de Boas Práticas em Contratação de Soluções de tecnologias da Informação do TCU.			Equipe de Planejamento
	Id	Ação Contingência			Responsável
	1	Exposição de motivos e embasamentos legais em que a contratação dos serviços de TI deva seguir.			Equipe Técnica
Risco 2	Risco:	Não Aquisição da Solução de Segurança			
	Probabilidade:	Média	Id	Dano Potencial	
	Impacto:	Médio	1	Exposição dos ativos de rede (servidores, softwares, sistemas e aplicações) além dos dados e informações sensíveis ao negócio do TJAM deixando-os vulneráveis ao não funcionamento correto, contínuo, traduzindo na indisponibilidade de acesso aos serviços oferecidos pelo órgão para os clientes internos e para a Sociedade consumidora dos Sistemas Computacionais hospedados nos computadores servidores.	
	Id	Ação Preventiva			Responsável
	1	Validar o processo de análise e estudo, iniciando com brevidade o processo de aquisição por meio de adesão a registro de preço em ata vigente.			Equipe de Planejamento
	Id	Ação Contingência			Responsável
	1	Exposição de motivos e embasamentos legais em que a contratação dos serviços de TI deva seguir de forma emergencial.			Equipe Técnica
Risco 3	Risco:	Atraso da contratação por necessidade de ajuste do Termo de Referência para adequação à nova lei de licitação.			
	Probabilidade:	Média	Id	Dano Potencial	
	Impacto:	Alto	1	Demora na disponibilização da solução para o TJAM; não cumprimento dos prazos acordados.	
	Id	Ação Preventiva			Responsável
	1	Acompanhamento e apoio; prever prazos amplos para realização de análises			Equipe Técnica
	Id	Ação Contingência			Responsável
	1	Apoio de servidores envolvidos na conclusão do processo.			Equipe Técnica

- **Risco da solução de tecnologia da informação**

Risco 1	Risco:	Falta de compatibilidade entre os itens e subitens que compõem a solução.			
	Probabilidade:	Baixa	Id	Dano Potencial	
	Impacto:	Alto	1	Atraso no processo de implantação da solução e aceite.	
	Id	Ação Preventiva			Responsável

	1	Instruir e revisar o Projeto Básico de forma clara e validar o cumprimento aos itens técnicos de compatibilidade.	Equipe Técnica
	Id	Ação Contingência	Responsável
	1	Realizar estudos teóricos e comprovação de compatibilidade entre os itens e subitens que compõem a solução, se necessário fazer consulta formal a cada fabricante.	Equipe Técnica

6. Do Parcelamento

6.1 Não será admitido parcelamento da solução, pois os itens, descritos nas **Estimativas das Quantidades**, são fortemente relacionados entre si, o que exige um nível de coesão no fornecimento que seria dificultado pela presença de mais de uma CONTRATADA.

7. Providências para Adequação do Ambiente do Órgão

7.1. Não haverá necessidade de adequação de ambiente.

8. Da Viabilidade de Contratação

8.1 Considerando todo o exposto acima, esta Secretaria de Tecnologia da Informação e Comunicação declara que a renovação do suporte e das licenças do cluster de equipamentos de Next-Generation Firewall, assim como expansão da solução de firewall para as unidades descentralizadas do Tribunal de Justiça do Estado do Amazonas (TJAM), são necessários e viáveis, dada a necessidade de se preservar a estabilidade, o pleno funcionamento e a confiabilidade em um ambiente complexo como a infraestrutura de TIC do TJAM.

Manaus, data registrada no sistema.

Diogo Mendonça de Sousa

Diretor da Divisão de Infraestrutura de TIC

SETIC/DVITIC

Breno Figueiredo Corado

Secretário de Tecnologia da Informação e Comunicação

SETIC

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 05/05/2023, às 13:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **RODRIGO DOS SANTOS MARINHO**, **Diretor(a)**, em 05/05/2023, às 13:10, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 05/05/2023, às 13:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0990217** e o código CRC **5204694A**.