ESTUDO TÉCNICO PRELIMINAR (*SIMPLIFICADO*)

ÁREA REQUISITANTE
Unidade Requisitante: Departamento de Tecnologia da Informação.
Responsável(is) pela demanda: Departamento de Tecnologia da Informação.

IDENTIFICAÇÃO DA SOLICITAÇÃO

Objeto: Contratação de empresa para o fornecimento de renovação de licenciamento de software de soluções de segurança da informação do Fabricante Fortinet em caráter emergencial para ser fornecida ao Conselho Regional de Engenharia e Agronomia de Santa Catarina – Crea-SC.

INTRODUÇÃO

Aplicar-se-á no presente Estudo Técnico Preliminar - ETP o disposto no artigo 15 do Regulamento de Licitações e Contratos Administrativos do Crea-SC, que dispõe sobre os Estudos Técnicos Preliminares - ETP - para a aquisição de bens e a contratação de serviços e obras, no âmbito do Conselho Regional de Engenharia e Agronomia de Santa Catarina – Crea-SC.

O Crea-SC, por meio do Processo Licitatório n° 5-230052387-6, Pregão Eletrônico nº 023/2023, contratou a empresa **HEXAIT**, cuja razão social atual é **HEXAIT SERVIÇOS E TECNOLOGIA DA INFORMAÇÃO LTDA - EM RECUPERAÇÃO JUDICIAL**, para o fornecimento de soluções de segurança da informação, para atender às necessidades do Crea-SC.

O referido processo resultou no contrato de n° 003/2024, o qual levou a ativação de licenças de software que possuem data de vencimento em 9, 16 e 17 de maio de 2025 e não pode mais ser prorrogado por não poder ser recebido aditivo pelo fato de se tratar de licenças de softwares com prazo máximo de 12 meses de utilização.

O presente ETP visa a embasar e verificar a viabilidade da Contratação de empresa para o fornecimento de renovação de licenciamento de software de soluções de segurança da informação do Fabricante Fortinet em caráter emergencial para o Crea-SC, à luz da Nova Lei de Licitações e Contratos (Lei nº 14.133/2021).

Esta contratação vigerá até que seja concluído o **novo processo de contratação** das soluções, o qual englobará a contratação destes licenciamentos ora citados para o período de 36 (trinta e seis) meses além de outros serviços, e que substituirá o serviço descrito no presente ETP. Já havia um processo de contratação em andamento sendo que o mesmo incorreu em problemas no edital após a sua publicação, tendo assim que ser republicado, gerando uma situação na qual o Conselho irá incorrer em riscos de acabar ficando sem os serviços de licenciamento ora descritos neste instrumento, sendo que tal ausência impactará diretamente na prestação dos serviços do Crea-SC aos profissionais e empresas registradas, causando indisponibilidade dos serviços críticos, como Creanet, SICWEB, Anotação de Responsabilidade Técnica – ART, E-mail, dentro outros, podendo ainda ocasionar em aumentar significativamente o risco de ataques cibernéticos e eventuais invasões e sequestro de dados, pela ausência de ferramentas dessas ferramentas de segurança da informação atualmente em operação.

Cabe ressaltar que o processo chegou a ser publicado através de processo licitatório por meio do **protocolo nº 5-250017769-8 e Pregão Eletrônico nº 90005/2025, mas com a incorrência de problemas encontrados no edital, o mesmo deverá ser republicado, após sanado as correções e visando mitigar eventuais pedidos de impugnações com conta desses problemas**.

Dessa forma, informamos ainda que está em fase de tramitação interna **o novo processo licitatório (republicação)** por meio do **protocolo nº 5-250060040-2**.

Documento assinado eletronicamente, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.
07/05/2025 as 22:46:41 por Lucas dos Santos Gerente Informatica, Matricula: 604.

1. Especificações, Estimativas, Quantidades e Valores de bens/serviços a serem contratados

1.1. No que tange o quantitativo estimado, deve ser respeitado as mesmas quantidades já contratadas anteriormente, efetuando apenas a renovação de tais licenças, conforme abaixo segue:

ITEM	DESCRIÇÃO	QTDE
1	FortiCare Premium Support (1 - 500 USERS) / **SKU: FC1-10-0ACVM-248-02-DD / Serial Number: FAC-VMTM24002715**	1
2	FortiClient VPN/ZTNA Agent Subscription for 25 endpoints. Includes EMS hosted by FortiCloud with FortiCare Premium. / **SKU FC1-10-EMS05-428-01-DD / Serial Number: FCTEMS8824003906**	2
3	Subscription license for 5 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard Outbreak Detection Service. / **SKU FC1-10-AZVMS-465-01- DD / Serial Number: FAZVMSTM24002479**	4
4	Subscription license for FortiWeb-VM (2 CPU) with Advanced bundle included **(SKU FC2-10-WBVMS-582-02-DD) / Serial Number: FWBVMSTM24000433**	1
5	FortiEDR Discover, Protect & Respond and Standard MDR Cloud Subscription and FortiCare Premium for 500 endpoints **(SKU FC2-10-FEDR1-349-01-DD) / Serial Number: FEDR00TM24000277**	1
6	FortiMail Cloud - Gateway Premium w. Cloud Email API support for Microsoft 365 or Google (101-1000 mailboxes) **(SKU FC2-10-FECLD-423-02-DD) contendo o FortiGuard Content Analysis Service for FortiMail Cloud (per mailbox) (SKU FC-10-FMLC0-160-02-DD) / Serial Number: FEVMCLM000237154**	350

1.2. Os preços são os propostos pela empresa SIGMA SERVIÇOS DE TECNOLOGIA LTDA**, bem como pelas demais empresas que participaram da pesquisa de preços,** encontram-se juntados neste processo sob os **Identificadores SicWeb nº 4327008**, **nº 4327009, nº 4327010 e nº 4327011**.

1.3. Além disso, pode ser encontrado nos **Identificadores SicWeb nº 4327012 e nº 4327013** demais documentos e as planilhas com os valores da pesquisa de preço de mercado efetuado junto a esses fornecedores e junto a outros órgãos.

2. Prazo de Vigência da Contratação

2.1. Data prevista para o início da vigência da contratação: 10/05/2025.

2.2. O contrato decorrente da presente contratação terá **vigência máxima de 120 (cento e vinte) dias**, nos termos do inciso VIII do artigo 75 da Lei nº 14.133/2021.

Documento assinado eletronicamente, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.
07/05/2025 as 22:46:41 por Lucas dos Santos Gerente Informatica, Matricula: 604.

2.3. As licenças devem ser fornecidas com data de início de validade, no máximo, a partir do dia 12 de maio de 2025;
6.1.2. As licenças devem ter validade de 90 (noventa dias), devendo a Contratada fornecer um COTERM com igual período de validade.

2.2. Diante do disposto no **item 2.1**, o contrato decorrente deste ETP poderá ser rescindido unilateralmente pelo Crea-SC, mediante aviso prévio à contratada de no mínimo 30 (trinta) dias, na hipótese de ser efetivada a contratação que tramita via **protocolo nº 5-250060040-2**.

3. Outra Possível Solução

3.1. Há outra alternativa de compra/serviços?

(X) Não, conforme justificativas do **tópico 4**.

( ) Sim

3.2. Se SIM, DESCREVER o CENÁRIO 02:

3.3. Se SIM, JUSTIFICAR porque optou pelo CENÁRIO 01:

4. Justificativas e descrição da necessidade da contratação e da escolha do tipo de solução

4.1. O Conselho Regional de Engenharia de Santa Catarina – Crea-SC, por conta da sua condição de entidade pública, que presta serviço para a sociedade, armazena e trabalha com dados de múltiplos entes, sejam eles profissionais do sistema, empresas, e da população em geral. Dentre esses dados, o Crea-SC emite Anotações de Responsabilidade Técnicas para cada obra executada pelos Profissionais e Empresas cadastrados e registrados no sistema.

4.2. A segurança de rede e aplicações corporativas é uma preocupação cada vez mais latente e importante para empresas de todos os tamanhos e setores. Uma das soluções mais populares para proteger as redes é o uso de appliances de firewall. Esses dispositivos oferecem uma camada de segurança entre a rede da empresa e a Internet, permitindo que o tráfego de entrada e saída seja monitorado e controlado.

4.3. A Segurança Cibernética, visa à proteção das redes e ativos de informação, preparando e operando as linhas de defesa contra eventuais invasores, externos e/ou internos, que tentem executar tarefas não permitidas, contra ou através da infraestrutura de Tecnologia da Informação e Comunicações (TIC) instalada.

4.4. Vale ressaltar que é primordial manter e evoluir o atual estágio de maturidade dos serviços que, para assegurar um ambiente apto e produtivo de TIC, evoluiu através das diversas medidas que foram tomadas, a partir de experiências anteriores, com o objetivo de eliminar ou reduzir problemas causados por eventuais falhas no ambiente computacional, como por exemplo: os serviços mais críticos passaram a ser apoiados por softwares também da marca Fortinet e que aumentaram o nível de segurança das aplicações e sistemas, bem como de toda a rede corporativa do órgão onde foram implantados novos procedimentos e processos de segurança mais rigorosos.

4.4.1. Atualmente o Crea-SC possui dois apliances físicos da Fortinet que contam vários perfis de segurança como webfilter, antivirus, video filter, controle de aplicação, IPS, File Filter, e etc, contudo esta solução por si só não abrange todos os recursos necessários para aumentar a segurança de rede e garantir um nível de segurança adequado aos desafios enfrentados diariamente pelas equipes de segurança da informação e cibersegurança. Aliado a isso, como já citado anteriormente o órgão já possui algumas dessas ferramentas, porém há uma necessidade cíclica de renovação destas licenças para melhor aproveitamento de todos os recursos disponibilizados pela fabricante, levando o órgão a renovar a licença atual de suporte por mais 36 (trinta e seis) meses, evitando incorrer no risco de ficarmos sem as atualizações de segurança, bem como parada nos serviços caso essa renovação não ocorra.

4.4.2. Nesse contexto, é importante ressaltar que a solução de firewall questão desempenha um papel crucial na viabilização do acesso remoto ao ambiente de TI do Crea-SC, permitindo o teletrabalho por meio da implementação de uma conexão VPN (Rede Virtual Privada). Além disso, ele desempenha a função de garantir a segurança da rede de dados do Crea-SC, mantendo o firewall atualizado e operacional 24 horas por dia, 7 dias por semana.

4.5. Considerando o disposto na Política de Segurança da Informação e Comunicação (POSIC) publicado e implementado no âmbito do Conselho Regional de Engenharia e Agronomia - CREA-SC e considerando ainda sua atualização, que institui diretrizes, responsabilidades e competências que visam assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações, bem como a conformidade, padronização e normatização das atividades de gestão de segurança da informação e comunicações da Instituição. Dentre as quais irão destacar-se a implementação de diretrizes e ações que atendam as normas e legislação existentes sobre segurança, definição de normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinadas à proteção da informação e à disciplina de sua utilização, no âmbito do Conselho Regional de Engenharia e Agronomia de Santa Catarina. E ainda no que tange a Gestão de Risco, ações que visem a implementação e atualização do processo com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações. Tal processo deverá possibilitar ainda a seleção e priorização dos ativos a serem protegidos, bem como a definição e implantação de controles para a identificação e tratamento de problemas de segurança. Estas medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança.

4.6. Convém acrescentar que nos últimos anos a tecnologia tornou-se uma ferramenta fundamental para a execução dos serviços nas empresas públicas e privadas. No governo, a maior parte dos processos de trabalho já opera em sistemas de informação. Para tanto, há necessidade de uma equipe especializada em infraestrutura de rede e segurança de rede que possa operar sobre uma arquitetura de alta disponibilidade mantendo o controle de acesso à rede, garantindo a plena operação das atividades administrativas em todas as unidades do órgão, de maneira segura.

4.7. Dessa forma, a equipe de planejamento pretende melhorar o alcance e desempenho de seus objetivos institucionais, realizando o aprimoramento, a construção e/ou adequação de sua infraestrutura e suporte de tecnologia da informação e comunicação. E para atender a essas crescentes demandas, bem como para manter a alta disponibilidade dos serviços de TI, o Crea-SC precisa contar com uma estrutura de prestação de serviços de TI adequada às exigências das áreas demandantes, fazendo-se necessário, neste caso, a contratação de empresas especializadas na operacionalização das tarefas afetas à condução dos processos de TI, tais como produção e manutenção da infraestrutura de informação e suas soluções tecnológicas.

4.8. Outra motivação que deve ser imprescindivelmente levada em consideração é que uma eventual mudança de plataformas impactaria drasticamente nos projetos de infraestrutura, bem como o custo do período de adaptação e treinamento a serem realizados com a equipe, além do custo de migração de plataformas, não poderem ser mensurados diretamente.

4.8.1. Ao estruturar a rede de informática do Conselho, a estratégia adotada foi padronizar, sempre que possível, produtos de hardware e software. Isso possibilita economia de escala na aquisição de novos produtos e, indiretamente, reduz os custos de treinamento para os servidores. Essa abordagem é adotada especialmente quando esses produtos são competitivos no mercado e atendem aos requisitos técnicos estabelecidos pela Departamento de Tecnologia da Informação. O objetivo é fornecer à sociedade e aos servidores um serviço contínuo, estável e de alta qualidade.

4.8.2. Considerando ainda a evolução dos riscos diário de segurança da informação, da crescente variedade das formas de violação de segurança que um datacenter pode sofrer diariamente, a equipe técnica optou por buscar no mercado soluções de segurança baseadas em inteligência artificial, participando de apresentações de algumas soluções (e fabricantes diversos) no passado, podemos relatar também que a solução que se mostrou mais adequada ao ambiente atual do órgão foi a solução da Fortinet que apresenta total compatibilidade com a solução de Firewall adquirido pelo Conselho em 2018 e atualmente em operação.

Documento assinado eletronicamente, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.
07/05/2025 as 22:46:41 por Lucas dos Santos Gerente Informatica, Matricula: 604.

4.9. Podemos observar ainda conforme o sumário de perfil de vulnerabilidade para o ano de 2023, que boa parte das ameaças se dão por execução de código malicioso de maneira remota, e conforme tudo já justificado e apresentado acima, todo as aquisições almejadas atuam de maneira a mitigar esse tipo de ataque, dentro outros conforme ilustrado na imagem abaixo:

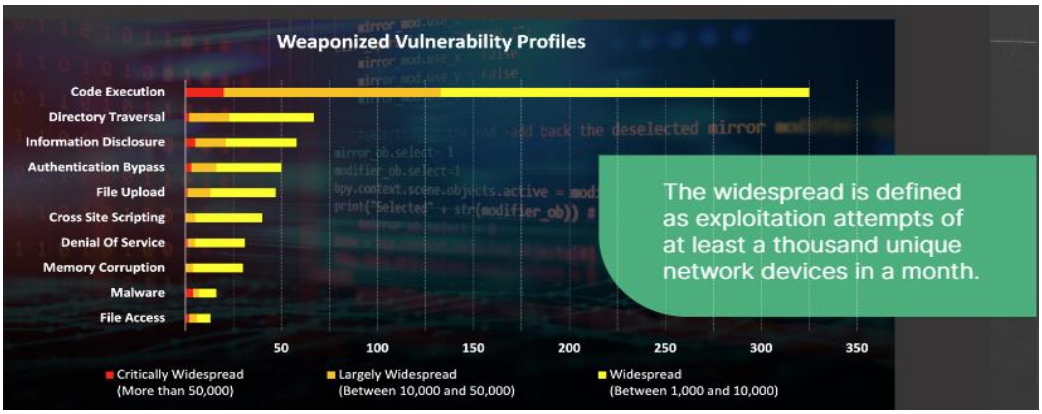

Figura 1- Contador de vulnerabilidades ativas e detectadas em um mês

Acessado em 23/11/2024.

4.10. Considerando ainda eventuais riscos de credenciais privilegiadas desprotegidas tendo em vista que a maioria dos vetores de ataques cibernéticos envolvem a exploração desse tipo de credencial. Tal risco se traduz no relatório Verizon Data breach Investigation 2023, 40% dos vazamentos de dados pesquisados envolveram credenciais privilegiadas. Sendo que o custo desse tipo de ataque é bem maior para as organizações.

4.10.1. Segundo a IBM no documento Cost of Data Breach Report 2023, enquanto o custo médio de um vazamento de dados costuma ser de USD 4,45 milhões, quando o vazamento de dados envolve credenciais privilegiadas, esse valor pode chegar a USD 4,62 milhões.

4.10.2. E, ao que tudo indica, com o crescente avanço da tecnologia, as ameaças cibernéticas devem se intensificar ainda mais nos próximos anos. Isso porque novas ferramentas tecnológicas adotadas amplamente pelas organizações aumentam a superfície de ataque, dando espaço para a atuação de agentes maliciosos.

4.11. Diante do exposto e das justificativas e necessidades apresentadas, motivou-se não apenas por manter no parque tanto os softwares supracitados atualizados, para garantir a preservação dos investimentos anteriores, mas também acrescentar uma solução de cofre de senhas e gestão de acesso privilegiado, visto tratar-se de solução no mesmo padrão dos já instalados, o que potencializa a utilização dos atuais por todo o tempo de vida de cada dispositivo.

4.12. Conforme já relatado anteriormente, esses licenciamentos vigentes estão programados para expirar em maio de 2025, resultando na interrupção de serviços essenciais, além de outros como suporte técnico, atualizações e correções. Sem os mecanismos de suporte e atualização, o Crea-SC enfrentará dificuldades significativas para resolver problemas no ambiente, corrigir vulnerabilidades de segurança e assim por diante. Isso comprometeria a estabilidade da infraestrutura de rede corporativa e, consequentemente, a segurança das informações. Dessa forma fica justificado também a necessidade da contratação com maior brevidade possível, visando não incorrer em paradas e/ou períodos que o órgão fique descoberto de tais licenciamentos.

4.13. Portanto, a solução da fabricante Fortinet foi escolhida para garantir a preservação dos investimentos anteriores, pois trata-se de solução no mesmo padrão dos já instalados o que facilita a adaptabilidade pelos colaboradores do Departamento de Tecnologia da Informação - DTI, aliado a potencialização que é viabilizada pela renovação das licenças,

sem a necessidade de incorrer em mudanças na arquitetura de segurança atualmente em operação e que mitigue o alto custo com capacitações/treinamentos em novas ferramentas de segurança e o lento processo da curva de aprendizagem pela equipe interna em cima de uma nova gama de plataformas, caso essa mudança ocorresse.

4.14. Além do fator econômico, é importante destacar que a solução já implantada facilita a interoperabilidade entre os componentes, o gerenciamento centralizado, a economia de escala e o aproveitamento do conhecimento da equipe técnica que irá atuar neste momento, e da futura equipe técnica que será necessária para dar continuidade nos trabalhos de inspeção e monitoramento futuro de todo ambiente tecnológico.

4.15. **REQUISITOS TECNOLÓGICOS**

4.15.1. A presente contratação não se encontra no Catálogo de Soluções de TIC com Condições Padronizadas, da Secretaria de Governo Digital do Ministério da Economia, uma vez que se trata de uma entrega customizada, pontual e específica para as características de software e de configurações do CREA-SC, descartando-se qualquer paralelo com soluções de outros entes públicos;

4.15.2. A necessidade apresentada acima, reside não só na atualização (renovação) urgente que tais softwares necessitam dentro da organização por conta de seu fim de suporte e licenciamento, conforme será exarado mais abaixo tais riscos, mas também na manutenção desses softwares de segurança da informação para garantir maior integridade e segurança de todo ambiente, conforme resultado obtido a partir da última contratação.

4.15.3. Um dos requisitos que podemos apresentar é o serviço de Virtual Private Network (VPN) que funciona como um complemento de segurança ao firewall que age como uma barreira, filtrando e analisando tanto o tráfego proveniente do ambiente externo ao Crea-SC quanto o tráfego interno na rede do órgão. Mas aliado a esse acesso VPN, observou-se a necessidade de implementar novas técnicas de segurança como Múltiplo Fator de Autenticação (MFA/2FA) para garantir que mesmo com roubo de credenciais iniba certos tipos de ataques e como ferramentas do tipo Zero Trust garantindo que qualquer equipamento que utilize esses serviços de acesso VPN e esteja com alguma atualização de softwares utilizados pendente, fique de fora da rede evitando trazer riscos e ataques não conhecidos para a rede, a exemplo de ataques de exploração a falhas do tipo zero day.

4.15.4. Outra grande necessidade é o WAF, ou Web Application Firewall, é uma tecnologia que protege aplicativos web contra ameaças cibernéticas, como injeção de SQL e cross-site scripting. Ele faz isso interceptando o tráfego HTTP/HTTPS antes que ele alcance o servidor de aplicativos e filtrando o conteúdo para garantir que ele seja seguro.

4.15.5. O WAF é particularmente importante para empresas que possuem aplicativos web críticos ou sensíveis. Além disso uma solução que possa ser integrada com uma licença de Antispam. Ele pode detectar e bloquear mensagens de spam antes que elas cheguem pela caixa de entrada, reduzindo a carga de trabalho dos servidores de email e melhorando a eficiência da comunicação.

4.15.6. Além disso, o Antispam pode identificar e bloquear emails maliciosos que contenham phishing, malware ou outras ameaças cibernéticas. Todas essas soluções podem ser incluidas através da aquisição de licenças especificas dentro do appliance de firewall, ou com a substituição do hardware em uma solução de segurança de rede mais completa e eficaz. Essas tecnologias adicionais oferecem camadas extras de proteção contra ameaças cibernéticas que podem colocar em risco a segurança dos dados do CREA-SC.

4.15.7. Não obstante a evolução dos riscos diário de segurança da informação, aliado a crescente variedade das formas de violação de segurança que um datacenter pode sofrer diariamente, a equipe técnica optou por buscar no mercado soluções de segurança baseadas em inteligência artificial EDR/XDR, participando de apresentações de algumas soluções (e fabricantes diversos) no passado, podemos relatar também que a solução que se mostrou mais adequada ao ambiente atual do órgão foi a FortiEDR que apresenta total compatibilidade com o Firewall adquirido pelo Conselho em 2018. Tal solução já se encontra implantada e com licenciamento ativo e que deverá ter sua renovação realizada juntamente com as demais soluções de segurança já em operação, com seus vencimentos previstos para final do mês abril de 2025.

Documento assinado eletronicamente, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.
07/05/2025 as 22:46:41 por Lucas dos Santos Gerente Informatica, Matricula: 604.

4.15.8. Esta renovação também deve ser realizada de maneira impreterível dentro do prazo solicitado e com urgência, possibilitando que não haja nenhuma parada do ambiente e ou limitações de funcionalidades às ferramentas de segurança em operação na organização, o que poderá representar um grande risco ao ambiente corporativo.

4.15.9. Considerando também que na atualidade o CREA-SC não possui um especialista de segurança da informação e muito menos um profissional que trabalhe única e exclusivamente com este tipo de tema, fica também aberto a necessidade de contratação iminente de um profissional a atuar nesta área, dentro da instituição. O apoio da equipe de especialistas auxiliará na implantação das ferramentas e realização dos procedimentos de investigação e efetiva caça as ameaças que ainda possam estar abertas.

3.2.10. Ainda, a indicação da marca segue as orientações de soluções de tecnologia Gartner, a melhor abordagem para proteger ambiente de tecnologia, principalmente considerando funcionários remotos, é através de uma arquitetura chamada CSMA (Cyber Security Mesh Architecture). Existindo uma integração entre as mais diferentes ferramentas, permitindo a correlação dos eventos, bloqueio mais rápido das ameaças e um menor tempo de identificação da ameaça (MTTD) e menor tempo para resolução (MTTR).

4.15.11. Cabe acrescentar ainda que a solução Fortinet possui atendimento também a segurança de ambientes legados, ou seja, sistemas que utilizam sistemas operacionais fora da vida útil do fabricante (end-of-life), pois o nosso parque de máquinas possui ainda, computadores com Windows 7 e servidores com Windows Server 2008 e 2012 em funcionamento no órgão.

4.15.12. Ainda em observância aos procedimentos de Prevenção e proteção contra vírus disposto na POSIC que tem por objetivo estabelecer os critérios, regras e comportamentos (permitidos, obrigatórios ou proibidos) para proteção contra vírus de computador na rede do Crea-SC, principalmente no que tange em manter os softwares e sistemas atualizados e estáveis divulgadas pelos fabricantes. Diante do exposto, a DTI requer maior atenção para estas brechas e vulnerabilidades de segurança, visto que, dentre as ameaças presentes no mercado, temos o malware ransoware, que tem por característica através do uso de criptografia, tornar inacessíveis os dados armazenados nos equipamentos e(ou) servidores da Instituição, exigindo o pagamento de resgate para restabelecer os acessos aos dados.

4.15.13. No que tange a requisito de segurança e prevenção ao malware ransoware, podemos observar casos de ataques cibernéticos, relacionado a este tipo de ataque, principalmente em órgãos da administração pública, conforme matérias à saber:

> *"Matéria: Ransomware e a LGPD: o que as empresas devem se preocupar? Nos últimos meses o Brasil sofreu uma onda de ataques cibernéticos, principalmente em órgãos da administração pública, tais como os sites do Governo do Distrito Federal e do Superior Tribunal de Justiça. No dia 3 de novembro, por exemplo, os servidores do STJ foram alvos de um ataque de hackers, ministros e servidores ficaram sem acessos à e-mails e arquivos.*
> *[...]*
>
> ***Fonte:*** *https://cartilha.cert.br/ransomware. Acessado em 30 de julho de 2022.*
>
> *"Matéria: A crescente ameaça do ransomware à Administração Pública Através da exemplificação de casos concretos em que os criminosos colocaram a Administração e seus dados como reféns, se verá como tal fraude tende a ser mais frequente e a necessidade premente de se voltar os olhos para a segurança da informação.*
> *[...]*
> *De acordo com o especialista da DELL, Erik Scoralick6, o Brasil é o país da América Latina que mais concentra casos de ransomware, reunindo cerca de 92% dos casos relatados.*
> *[...]*
> *III - A Administração Pública como vítima:*
> *O caso mais emblemático que envolve o ransomware e ataque à Administração Pública, porquanto teve maior estrépito foi sem dúvida o sucedido em Pratânia (SP) no ano de 2015, quando hackers (em verdade crackers) invadiram e bloquearam totalmente o sistema de dados daquela Prefeitura no interior paulista."*

Fonte: *Por Priscila Ungaretti de Godoy Walder e Vinícius Lobato Couto. https://www.migalhas.com.br/depeso/315847/a-crescente-ameaca-do-ransomware-a-administracao-publica. Publicado em 26-nov-2019. Acessado em 30 de julho de 2024.*

"Matéria: Secretaria do Tesouro Nacional é a mais nova vítima de ransomware A rede interna da Secretaria do Tesouro Nacional foi alvo de um ataque de ransomware na noite de sexta-feira (13). O Ministério da Economia — que revelou o ataque em uma nota publicada no sábado (14) — disse que "medidas de contenção" foram aplicadas e que a ação não gerou danos aos sistemas da entidade.
[...]

Esta não é a primeira vez que um sistema do governo brasileiro ou de uma empresa pública nacional é alvo de um ataque ransomware. Em novembro do ano passado, o Superior Tribunal de Justiça (STJ) teve seus sistemas infectados com o RansomExx. Em abril de 2021, foi a vez de os sistemas do Tribunal de Justiça do Rio Grande do Sul (TJRS) ficarem fora do ar após um ataque do grupo REvil, que teria cobrado US$ 5 milhões para descriptografar os arquivos e não vazar dados. Além disso, houve uma ameaça de ataque DDoS. Em outros episódios, a prefeitura de Saquarema (RJ), a Eletronuclear (da Eletrobras) e a Cemig foram alguns dos órgãos afetados"

Fonte: Por Giovanni Santa Rosa. https://tecnoblog.net/480231/secretaria-do-tesouro-nacional-e-a-mais-nova-vitima-de-ransomware/. Publicado em 16-ago-2021. Acessado em 30 de julho de 2024.

4.15.14. Podemos observar ainda, que não apenas órgãos públicos, mas empresas privadas também são alvos desses ataques:

"Matéria: Surto de Ransomware impacta mais de mil empresas em 2024: Em 2024, o cenário global de cibersegurança enfrenta uma alta nos ataques cibernéticos. Especialmente, os ataques de grupos de ransomware se tornaram uma preocupação central, sequestrando dados de empresas e exigindo resgates milionários para devolvê-los."

Fonte: https://www.cartacapital.com.br/do-micro-ao-macro/surto-de-ransomware-impacta-mais-de-mil-empresas-em-2024 Publicado em 13-nov-2024. Acessado em 02 de janeiro de 2025.

"Matéria: Segundo trimestre de 2024 registra quase 1.300 ataques de ransomware, aponta levantamento: Um levantamento da ISH Tecnologia alerta para o crescente perigo representado pelos ataques de ransomware – sequestro de dados. No segundo trimestre de 2024, foram 1.294 ataques confirmados pelo mundo – o que representa um aumento de 32% em relação aos três primeiros meses do ano, e de 10% no comparativo com o mesmo período em 2023.
[...]
Os números também revelam que os incidentes cresceram em praticamente todos os comparativos. Além da relação entre trimestres, os ataques também aumentaram quando comparamos os primeiros semestres de 2023 e 2024 (alta de 10,6%) e o mês de junho (24,6%).

Fonte: https://securityleaders.com.br/segundo-trimestre-de-2024-registra-quase-1-300-ataques-de-ransomware-aponta-levantamento/ Publicado em 25-jul-2024. Acessado em 02 de janeiro de 2025."

"Matéria: Ransomware em 2024: impacto recorde e lucros estrondosos: Em 2024, o ransomware alcançou cifras de resgates inéditas, com ataques que colocaram em risco dados sensíveis de milhões de pessoas. O ransomware se consolidou como uma das principais ameaças digitais, deixando um impacto significativo em empresas e usuários.
[...]
Como detalharemos a seguir, 2024 foi um ano recorde para o ransomware: desde seu alcance até os lucros obtidos pelos atacantes com seus golpes. Para entender como essa ameaça desempenhou um papel crucial na cibersegurança de empresas e organizações, vamos destacar os ataques mais paradigmáticos do ano e o impacto que tiveram na América Latina.
Não há dúvida de que o ransomware continua sendo uma das maiores ameaças para a cibersegurança em nível global. Um relatório da Rapid 7 afirma que foram registrados mais de 2.500 ataques de ransomware apenas na primeira metade de 2024, o que equivale a quase 15 ataques reivindicados publicamente por dia.
Nesse contexto, um estudo publicado pela Statista, com base na opinião de líderes de cibersegurança de todo o mundo, revela que quase 60% das organizações globalmente foram vítimas de um ataque de ransomware apenas entre janeiro e fevereiro de 2024.
E, de acordo com o ESET Security Report deste ano, na América Latina, 14% das organizações afirmaram estar dispostas a pagar um resgate. O que é ainda mais preocupante é que a perda de dados aumentou de forma significativa: de 17,2% registrado

em 2023, passou para 30,2% em 2024. Em consonância com isso, o Relatório Global da Veeam revela que 27% das organizações que pagaram o resgate não conseguiram recuperar seus dados, mesmo após efetuar o pagamento."

Fonte: https://securityleaders.com.br/segundo-trimestre-de-2024-registra-quase-1-300-ataques-de-ransomware-aponta-levantamento/ Publicado em 25-jul-2024. Acessado em 02 de janeiro de 2025.

4.15.15. Como requisitos para combater algumas dessas ameaças deve-se tomar algumas:

4.15.15.1. Promover campanhas de treinamento e conscientização para colaboradores;

4.15.15.2. Implementar medidas de segurança cibernética, como autenticação multifatorial (MFA), segmentação de rede, backups de dados e restrição de privilégios de acesso aos dados;

4.15.15.3. Utilizar ferramentas de monitoramento contínuo, para detectar atividades suspeitas ou anômalas na rede em tempo real;

4.15.15.4. Desenvolver e testar regularmente planos de resposta a incidentes para garantir uma resposta rápida e eficaz em caso de um ataque;

4.15.15.5. Participar de redes de compartilhamento de informações e colaborar com outras organizações e autoridades para estar atualizado sobre as ameaças e melhores práticas de segurança.

4.15.15.6. Medidas essas que convertidas em soluções tecnológicas se traduzem em parte do que se faz como objeto desta contratação.

4.15.16. Importante ressaltar que todos os sistemas e softwares são passíveis de estarem vulneráveis, cabendo à Instituição adotar as medidas de segurança necessárias e defensivas para minimizar ao máximo os riscos e impactos relacionados à incapacidade destes sistemas de resistirem aos efeitos de um ambiente hostil. Logo manter os sistemas e softwares desatualizados, aumentam os riscos com as falhas do tipo zero-day (zero dias), que ocorrem quando brechas graves de segurança são encontradas e(ou) quando ataques de hackers que exploram essas brechas são identificados. A partir do momento em que a falha é detectada, o fabricante do software tem efetivamente "zero dias" para produzir uma atualização que corrija o problema, impedindo a exploração por criminosos antes disso. Tais atualizações normalmente ocorrem através de pacotes de segurança contendo atualizações e correções que são disponibilizados para instalação.

4.16. Com o objetivo de garantir a qualidade da aquisição, é importante analisar a comparação dos vários fornecedores do segmento para que possamos nos certificar de que suas soluções podem de fato atender às necessidades e requisitos apresentados.

4.16.1. Assim, partindo de fonte de comparação de soluções temos o Gartner, uma entidade de pesquisa que se consolidou como referência e é muito conhecida por seu "quadrante mágico" de comparação de soluções, muito utilizado no planejamento de contratações públicas por sua confiabilidade. O quadrante mágico para soluções de Firewall mais recente até o momento é de dezembro/2022 e pode ser visto a seguir:

Figura 2 - Quadrante Mágico Gartner para soluções de Firewall

4.16.2. Pelo que é apresentado no gráfico da figura 2, tomando como base para comparação a solução atual utilizada no CREA-SC, vemos que a Fortinet se destaca como um dos líderes do mercado em seu segmento.

4.16.3. Podemos notar pelo quadrante mágico do Gartner que no segmento de firewalls temos destaque para quatro fabricantes:

- Check Point Software Technologies;
- Cisco;
- Fortinet;
- Palo Alto Networks.

4.16.4. Para esta avaliação, também tivemos acesso a outro recurso do Gartner, que aprofunda a comparação entre os principais fornecedores listados, considerando vários critérios de segurança e definindo um score relacionado a esses critérios para cada fabricante. A comparação foi baseada em características como:

4.16.4.1. Plataforma: incluindo suporte para grandes implantações, suporte a cluster, suporte de mitigação de negação de serviço distribuída (DDoS), flexibilidade de implantação e estabilidade de plataforma;

4.16.4.2 Gestão: Incluindo a funcionalidade da ferramenta de gestão central e gestão de regras;

4.16.4.3. Logging: incluindo recursos analíticos e logs de segurança;
4.16.4.4. Integração de rede: Incluindo suporte de rede, suporte de roteamento, rede de longa distância definida por software (SD-WAN), qualidade de serviço (QoS), VPN e Transport Layer Security (TLS);

4.16.4.5. Prevenção de ameaças: Inclui sistema de prevenção de intrusão (IPS), Threath Intelligence e recursos de sandbox;

4.16.4.6. Controle de aplicativos: incluindo assinatura de aplicações, filtragem web e integração com o Office 365.

4.16.4.7. Com isso, temos o seguinte quadro comparativo:

4.16.4.8. Podemos derivar o quadro de comparação para um resumo geral da seguinte forma:

	Cisco	Fortinet	Palo Alto	Check Point
High	12	14	10	13
Medium	12	11	15	10
Low	3	2	2	4

Figura 4 - Classificação das funcionalidades das principais soluções de Firewall

4.16.4.9. Com base na Tabela acima, vemos que a Fortinet apresenta o maior número de características avaliadas como "HIGH" e o menor número de características avaliadas como "LOW". Além disso, com base em consultas realizadas junto ao Gartner, podemos listar alguns pontos fortes no âmbito técnico da solução Fortinet:

4.16.4.9.1. Amplo suporte para plataformas de implantação, incluindo dispositivos físicos, dispositivos virtuais e soluções baseadas em nuvem;

4.16.4.9.2. Boa classificação de acordo com critérios de outras entidades;

4.16.4.9.3. Boas capacidades de gerenciamento central;

4.16.4.9.4. Flexibilidade nos critérios de regras;

4.16.5. Podemos avaliar que os “appliances” físicos são o modelo que, funcionam através de um hardware dedicado à função de concentrador/analisador de logs e gerador de relatórios. Já os “appliances” virtuais, como o próprio nome sugere, contemplam a solução virtualizada a ser instalada no ambiente físico, utilizando os recursos computacionais de armazenamento e processamento. De acordo com o datasheet mencionado, temos as seguintes especificações e dimensionamento para a solução virtualizada

4.16.5.1. É possível constatar pelo datasheet que deve ser levada em consideração a geração de logs diária para o dimensionamento do modelo a ser licenciado, além obviamente dos recursos que deverão ser alocados para a instalação da solução. O licenciamento do FortiAnalizer-VM, utilizada neste estudo técnico apresenta o seguinte:

FortiAnalyzer VM

Fortinet offers the FortiAnalyzer-VM licensing in a stackable perpetual license model with a-la-carte technical support and subscription services.

This software-based version of the FortiAnalyzer hardware appliance is designed to run on many virtualization platforms, which allows you to expand your virtual solution as your environment expands.

FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacity						
GB/ day of Logs *	+1	+5	+25	+100	+500	+2,000
Devices/VDOMs Maximum	10 000	10 000	10 000	10 000	10 000	10 000
FortiGuard IOC Service	✓					
Security Automation Service	✓					
Hypervisor Support	Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version. Visit https://docs.fortinet.com/product/fortianalyzer/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization"					
vCPU Support (Minimum / Maximum)	4 / Unlimited					
Network Interface Support (Min / Max) **	1 / 12					
Memory Support (Minimum / Maximum)	16 GB / Unlimited for 64-bit					

* Unlimited GB/ day when deployed in collector mode.
** VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

Figura 5-Licenciamento do FortiAnalyzer-VM

4.16.5.2.De acordo com o que é apresentado sobre o licenciamento, há uma distribuição dos tipos de licença de acordo com o volume de logs gerados diariamente e capacidade de armazenamento, distribuídos em várias faixas.

4.16.6. Ainda nesta sentada, podemos também ilustrar soluções de Web Application Firewall:

Figura 6-Quadrante Gartner para soluções WAF

4.16.6.1. as quais os players que se destacam no quadrante de Nicho de Mercado são:

4.16.6.1.1. F5 Networks
4.16.6.1.2. Fortinet
4.16.6.1.3. Barracuda
4.16.6.1.4. ThreatX

4.16.6.2. Conforme é almejado uma solução com log centralizado e soluções que possam ter a possibilidade de interoperabilidade sem grandes dificuldades, será optado pela solução do fabricante Fortinet, visto seu posicionamento de mercado, bem como demais soluções do mesmo fabricante já estarem sendo adquiridas, de acordo as justificativas previamente apresentadas. Segue abaixo uma imagem que ilustra o quadrante Gartner que realizou esse estudo em 2022 demonstrando a vantajosidade em seguir com tal solução de mercado:

4.16.7. Foi ainda avaliado ainda soluções de mercado que atuam com proteção de E-mail on premises e em nuvem, e chegou-se nos principais fornecedores, conforme também aponta pesquisa da Gartner. Abaixo podemos observar os principais e novamente o fabricante Fortinet se destaca e ganha relevância devido a possibilidade de trabalhar integrado as demais soluções também de mesma marca.

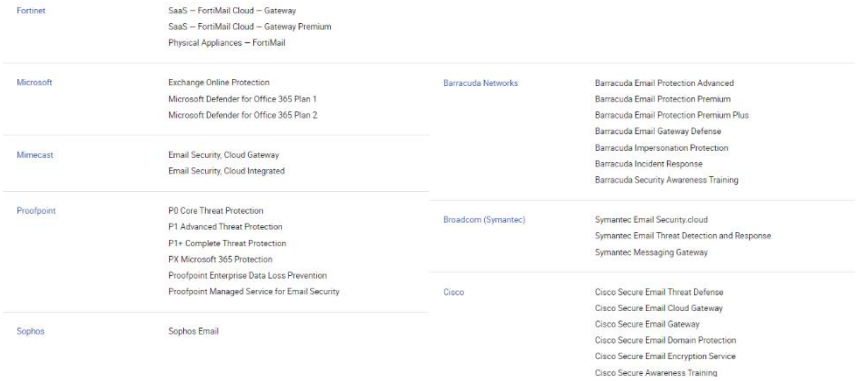

Figura 7-Fabricantes que mais se destacam em soluções de Proteção de E-mail

4.16.7.1. Dentre as funcionalidades dos mais diversos fabricantes de soluções de proteção de e-mail podemos citar:
4.16.7.1.1. URL rewriting
4.16.7.1.2. Multi-antivirus (AV) scanning
4.16.7.1.3. Sandbox integration
4.16.7.1.4. Spam quarantine with end-user digests
4.16.7.1.5. Graymail handling
4.16.7.1.6. BEC protection
4.16.7.1.7. Postdelivery clawback
4.16.7.1.8. Data leakage prevention for compliance, either blocking or reporting PII being sent
4.16.7.1.9. Email encryption, transport layer security (TLS), or push or pull encryption
4.16.7.1.10. Large message sending, through a secure portal, often linked to the encryption

4.16.7.2. É possível notar que as alternativas de mercado fornecendo licenças de outros fabricantes foi considerada, mas dado o atual cenário e levando em conta que todo estudo efetuado anteriormente nestas soluções, demonstrou que as soluções do Fabricante Fortinet continuam a atender muito bem as expectativas e necessidades do Crea-SC. Além disso, não é possível de ser considerada também por conta de que para se renovar as licenças atuais, deve ser mantido as soluções em operação no parque, sem que haja novas implantações de softwares e incorra em um elevado tempo de implantação, como ocorreu com as atuais licenças já em operação. Tal opção, agravaria ainda mais situação crítica na qual o órgão já se encontra e não seria vantajosa para a Administração Pública,

4.16.7.2.1. Sendo assim, que a solução atualmente em uso no CREA-SC além de demonstrar que desponta como uma das mais efetivas no segmento, poderá ser mantida sem causar impactos e interrupções do serviço, conforme demonstrado neste levantamento e nos demais capítulos deste ETP. Sendo assim, a única alternativa que se mostra viável, quando se pensa na continuidade da solução de segurança, bem como quando não interrupção dos serviços, são as aqui apresentadas.

4.17. Dessa forma, conforme já citado anteriormente, o Crea-SC, por meio do Processo Licitatório n° 5-230052387-6, Pregão Eletrônico nº 023/2023, contratou a empresa **HEXAIT**, cuja razão social atual é **HEXAIT SERVIÇOS E TECNOLOGIA DA INFORMAÇÃO LTDA - EM RECUPERAÇÃO JUDICIAL**, para o fornecimento de soluções de segurança da informação, para atender às necessidades do Crea-SC no estado de Santa Catarina.

4.18. O referido processo resultou no contrato de n° 003/2024, o qual levou a ativação de licenças de software que possuem data de vencimento em 9, 16 e 17 de maio de 2025 e não pode mais ser prorrogado por não poder ser recebido aditivo pelo fato de se tratar de licenças de softwares com prazo máximo de 12 meses de utilização e a renovação dessas licenças vinha ocorrendo através do protocolo nº 5-250017769-8 e Pregão Eletrônico nº 90005/2025, o qual terá que ser republicado devido a problemas identificados no Edital e anexos, após a sua publicação, tendo assim que ser republicado, e que acabou por ocasionar uma situação à qual Conselho irá incorrer em riscos de ficar sem os serviços de licenciamento ora descritos neste instrumento.

4.19. Tal ausência impactará diretamente na entrega e na qualidade dos serviços do Crea-SC aos profissionais e empresas registradas, bem como a sociedade causando indisponibilidade dos serviços críticos, como Creanet, SICWEB, Anotação de Responsabilidade Técnica - ART, E-mail, podendo ainda ocasionar em aumentar significativamente o risco de ataques cibernéticos e eventuais invasões e sequestro de dados.

4.20. Atualmente, está sendo priorizado e andamento de fase interna de contratação (revisão do Estudo Técnico Preliminar e do Termo de Referência e Edital), por meio de trabalho conjunto entre o Departamento de Administração, o Departamento de Tecnologia da Informação e Superintendência, **a republicação**, que tramita via protocolo nº **5-250060040-2**.

4.21. Desse modo, para que o Crea-SC não sofra com o interrompimento dos serviços de software, não incorrendo em interrupções dos serviços digitais da organização, demonstra-se assim necessário contratar o objeto descrito neste ETP.

4.22. A presente contratação se dará por meio de Contratação Direta, especificamente Dispensa de Licitação por Contratação Emergencial, nos termos do inciso VIII do artigo 75 da Lei nº 14.133/2021 e do artigo 69 do Regulamento de Licitações e Contratos Administrativos do Crea-SC.

4.23. Assim, considerando a inviabilidade de prorrogação do contrato de n° 003/2024 pelas questões já mencionadas anteriormente e ainda pela impossibilidade de renovação das referidas licenças através do contrato supracitado, além da necessidade de manutenção das ferramentas de segurança da informação em operação, a Contratação Emergencial se justifica por ser a alternativa legal adequada de contratação que viabilize ao Crea-SC a manutenção de suas atividades sem prejuízo de atendimento aos seus usuários.

4.24. A opção pela contratação da empresa SIGMA SERVIÇOS DE TECNOLOGIA LTDA se justifica pelo fato dela ser a proponente que forneceu o **menor preço global identificado através de pesquisa de mercado efetuada contatando 7 empresas**, obtendo o retorno de 4 (quatro) proponentes, além de contratos similares com outros órgãos da Administração Pública em diversas esferas, inclusive internacional, sendo identificado serviços de natureza similar ao do objeto deste ETP.

4.24.1. Também foi envolvida a atual fornecedora das soluções, dando ainda mais transparência ao processo de contratação ora apresentado. Pelo fato da **característica dos serviços a serem contratados de maneira emergencial serem de única e exclusivamente o fornecimento e ativação de licenças de software**, através da renovação das licenças já em operação no órgão, **não se justifica que seja necessário a contratação da mesma empresa que já forneceu tais serviços**, tendo como amparo ainda um preço que gerou maior vantajosidade para a administração pública conforme demonstrado na ampla pesquisa de preços realizada junto ao mercado.

4.25. Tal situação também é sustentada pelo fato da ativação das licenças renovadas poder ocorrer de maneira remota (on-line) e automática, não exigindo mobilização de equipe técnica da Contratada à Sede da Contratante, tão pouco uma parada dos serviços disponibilizados pelas licenças de software.

4.26. Por fim, a presente contratação se enquadra como prestação de serviços contínuos, nos termos do art. 6º, inciso XV, da Lei nº 14.133/2021, por ela servir à manutenção de atividade administrativa, decorrentes de necessidades permanentes ou prolongadas, que no caso é prestação de serviços digitais a sociedade sem que afete os usuários dos serviços disponibilizados pelo Crea-SC.

5. Objetivos Estratégicos relacionados com a Contratação/Aquisição

5.1 Assegurar a governança pública organizacional e a viabilidade de continuidade da governança de segurança das informações;

5.2. Garantir que o CREA-SC preste serviços de qualidade à sociedade, bem como atenda as próprias necessidades institucionais, com base nos pilares de confiabilidade, integridade e disponibilidade;

5.3. Prover infraestrutura e serviços de TIC padronizados, integrados e atualizados, com o emprego das melhores práticas utilizadas atualmente;

5.4. Atender às necessidades de negócio, garantindo infraestrutura de TI adequada para a execução dos programas e ações do órgão;

5.5. Aumento da eficiência da comunicação corporativa: melhorando inclusive os mesmos parâmetros atuais;

5.6. Mitigar possíveis riscos, danos ou indisponibilidade a prestação de serviços de TI, decorrentes de problemas técnicos identificados nos equipamentos;

5.7. Dotar o órgão de serviços especializados com o objetivo de assegurar o pleno funcionamento dos seus ativos de comunicação;

5.8. Aumento do nível de controle em relação à segurança e confidencialidade das informações e dados armazenados pelos sistemas corporativos do Crea-SC;

5.9. Garantia da prestação ininterrupta de serviços que fazem uso de Redes de Comunicação de Dados, tais como o acesso à Internet e aos sistemas da Administração Pública Federal, a fim de conferir agilidade e presteza aos processos institucionais que se utilizam de tais serviços;

5.10. Maior visibilidade do tráfego de rede e aplicações, possibilitando a detecção e proteção em tempo real contra ameaças;

5.11. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

5.12. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários etc.;

5.13. Criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados através do fechamento de portas não utilizadas, controlando a banda de internet a fim de evitar abusos em sua utilização;

5.14. Ampliar a capacidade de retenção das cópias de segurança de dados corporativos guardados no Data Center do órgão;

5.15. Diminuir o risco de perda de informações por meio do uso de tecnologias que não permitam a alteração dos dados no caso de ataques cibernéticos;

5.16. Permitir, no menor tempo possível, o retorno dos serviços de TI locais das Inspetorias, com os dados em sua versão mais recente possível;

5.17. Garantir a manutenção de dados sensíveis exclusivamente em infraestrutura proprietária do órgão ou protegida pela

legislação brasileira;

5.18. Garantir a disponibilidade e a integridade das cópias de segurança vigentes (backup legado) até sua expiração;

5.19. Aumento da segurança operacional devido à disponibilidade de suporte e manutenção para os equipamentos;

5.20. Garantia de integridade dos dados;

5.21. Aumento da Segurança da informação;

6. Descrição dos Requisitos da Contratação

6.1. A Contratada deverá demonstrar sua regularidade fiscal mediante a apresentação de:

6.1.1. Inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ)
6.1.2. Certidão de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União;
6.1.3. Certidão de Débitos Estaduais;
6.1.4. Certidão de Débitos Municipais;
6.1.5. Certificado de Regularidade do FGTS – CRF;
6.1.6. Certidão Negativa de Débitos Trabalhistas – CNDT;
6.1.7. Cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.
6.1.8. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União;
6.1.9. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça;
6.1.10. Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU;

6.1.2. *Para a consulta de licitantes pessoas jurídicas poderá haver a substituição das consultas dos subitens "6.1.10", "6.1.11" e "6.1.12" acima pela Consulta Consolidada de Pessoa Jurídica do TCU.*

6.2. A Contratada deve ser capaz de atender a todos os critérios técnicos informados nas informações relevantes no dimensionamento da proposta.

6.3. Apresentação de proposta comercial.

6.4. Deverá ser atendido a todos os requisitos detalhados no **Anexo A** do Termo de Referência, onde consta a especificação técnica das ferramentas.

6.5. **DO SERVIÇO DE LICENCIAMENTO DE SOFTWARES**

6.5.1. A solução a ser contratada envolve o licenciamento de software em caráter de renovação emergencial, proporcionando a CONTRATANTE o direito de uso das licenças de software no período de vigência do contrato necessárias para a implementação da solução.

6.5.2. Os direitos de utilização do software pela contratante serão plenos em relação ao uso pela mesma no seu contexto, devendo esta receber atualizações e treinamentos à medida que o software da contratada recebe upgrades. O modelo de licenciamento será do tipo SaaS (Software as a Service – Software como serviço).

6.5.3. Deve ser respeitado o PARTNUMBER/SKU e SERIAL NUMBER dos produtos, na apresentação das propostas de preço no momento do certame, quando couber.

6.5.4. Todos as soluções de software objetos dessa contratação, deverão ser do mesmo fabricante;

6.5.5. As soluções de software objetos dessa contratação, somente serão considerada devidamente entregue após a sua completa instalação e a realização de testes, devendo o sistema estar em perfeitas condições de funcionamento;

6.5.6. Para os objetos dessa contratação, deverá ser apresentada declaração de revenda autorizada para as soluções ofertadas, conforme disposto mais abaixo neste instrumento;

6.5.6.1. A empresa deverá constar ainda na lista de parceiros do fabricante Fortinet, podendo ser consultada no link abaixo: https://partnerportal.fortinet.com/directory/search?l=brazil

7. Levantamento de Mercado

7.1. Conforme pesquisa de mercado efetuada junto a fornecedores de soluções do Fabricante Fortinet, foi identificado uma proposta mais vantajosa para o Crea-SC, à qual irá resultar na contratação de maneira emergencial, provendo a renovação das licenças por mais 90 (noventa) dias, sem causar indisponibilidade dos serviços.

7.2. Abaixo segue um levantamento feito junto a outros contratos da administração pública:

FONTE DE PESQUISA /ÓRGÃO / CONTRATOS SIMILARES / BANCO DE PREÇOS	ITEM PESQUISADO	VALOR GLOBAL DO ITEM P/ 3 MESES (90 DIAS)	OBSERVAÇÕES
TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS - PREGÃO ELETRÔNIICO Nº 90039//2024 / PROCESSO ADMINISTRATIVO Nº 0007093-07.2023.6.02.8000	FortiAnalyzer	R$ 18.335,75	
SECRETARIA DE ESTADO DA FAZENDA - SEFAZ-PB - Edital nº 20000-212/2024	SOLUÇÃO WAF – Web Application Firewall	R$ 48.750,00	
SECRETARIA ESPECIAL DE GESTÃO DAS CONTRATAÇÕES, LICITAÇÕES E LOGÍSTICA - Edital nº PE0132/2025	FortiAnalyzer	R$ 18.072,56	
SECRETARIA DE ESTADO DA SAUDE/GO - Edital nº 112111/2025	FortiAnalyzer	R$ 21.467,71	
UASG 070011 - TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS - Pregão Eletrônico Edital nº 90039/2024	FortiAnalyzer	R$ 18.335,75	
	Subscription license for 5 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard	R$ 9.681,84	****Pesquisa de preços internacional conforme recomendação do ACÓRDÃO do TCU nº 1432/2024 - PLENÁRIO -**

****Referência internacional citado no relatório do referido Acórdão é o programa Enterprise Software Initiative (ESI) do Departamento de Defesa dos Estados Unidos (DoD ESI)**	Outbreak Detection Service. / SKU FC1-10-AZVMS-465-01-36		**Aplicado fator de proporção de 1,06 em cima de preços praticados em dólar através de um Acordo entre o fabricante e o Departamento de Defesa dos Estados Unidos da América**
	Subscription license for FortiWeb-VM (2 CPU) with Advanced bundle included (SKU FC2-10-WBVMS-582-02-36)	R$ 16.120,07	
	FortiEDR Discover, Protect & Respond and Standard MDR Cloud Subscription and FortiCare Premium for 500 endpoints (SKU FC2-10-FEDR1-349-01-36)	R$ 69.585,53	
	FortiMail Cloud - Gateway Premium w. Cloud Email API support for Microsoft 365 or Google (101-1000 mailboxes) (SKU FC2-10-FECLD-423-02-36) contendo o FortiGuard Content Analysis Service for FortiMail Cloud (per mailbox) (SKU FC-10-FMLC0-160-02-36)	R$ 16.776,81	

7.2. Diante do que foi exposto**,** a forma viável de contratação do objeto deste ETP é por Contratação Emergencial, contudo, para verificar a adequação dos preços ofertados pela empresa SIGMA SERVIÇOS DE TECNOLOGIA LTDA ao que é praticado no mercado e outros fornecedores de soluções similares, foi realizada ainda pesquisa de preços conforme demonstrado no quadro mais abaixo, de acordo com os parâmetros prescritos no artigo 33 do Regulamento de Licitações e Contratos Administrativos do Crea-SC, tendo sido consultadas outras empresas fornecedoras de serviços similares.

FONTE DE PESQUISA / FORNECEDOR	VALOR GLOBAL DO ITEM P/ 3 MESES (90 DIAS)	OBSERVAÇÕES
FONTE 1 – MENOR VALOR	**R$ 64.900,00**	
FONTE 2 – SEGUNDO MENOR VALOR	R$ 66.307,11	
FONTE 3– TERCEIRO MENOR VALOR	R$ 129.474,00	
FONTE 2 – QUARTO MENOR VALOR	R$ 162.402,78	
FONTE 5		NÃO RESPONDIDO
FONTE 6		NÃO RESPONDIDO
FONTE 7		NÃO RESPONDIDO

7.3. Merece destaque o fato de que, conforme já exposto anteriormente, a manutenção desses softwares são imprescindíveis para que seja garantido a segurança da informação dos dados trafegados dentro do Crea-SC, bem como das suas aplicações

auxiliando na mitigação e assim possibilitar a redução de que ataques cibernéticos logrem êxito em eventuais tentativas de invasão e disseminação de códigos maliciosos, como vem ocorrendo cada vez mais constantemente com outros órgãos e empresas privadas.

7.4. Verifica-se assim. que os valores apresentados pela empresa **SIGMA SERVIÇOS DE TECNOLOGIA LTDA** estão abaixo dos valores apresentados nas propostas pelos demais fornecedores, além de estar abaixo daqueles praticados por outras empresas para outros órgãos, tornando-a a proposta mais vantajosa para a Administração Pública.

8. Descrição da Solução Como um Todo

8.1. Todo o detalhamento e especificações técnicas, bem como o ciclo de vida do objeto estão exarados no **Anexo A** do Termo de Referência.

9. Resultados Pretendidos

9.1. Conforme **tópico 1** deste ETP.

10. Justificativas para o Parcelamento ou Não da Solução

10.1. No decorrer deste Estudo Técnico Preliminar não foram parcelados, ou seja, divididos os itens a serem contratados, por tratar-se de contratação de forma global, com fins a não prejudicar a realização/prestação dos serviços de forma simultânea e não-contínua.

10.2. A prestação parcelada dos itens seria prejudicada com a contratação de empresas distintas, uma vez que todos os bens e serviços pretendidos estão intrinsecamente relacionados. Tal organização permite ganhos quanto à instalação, configuração e operacionalização de toda a solução. A adjudicação dos itens para empresas diferentes pode resultar na aquisição de soluções incompatíveis, o que acarretaria prejuízo à administração pública.

10.3. Em atendimento ao princípio da eficiência e no sentido de preservar a elevada necessidade de manter a qualidade e nível da execução e acompanhamento dos serviços, foi adotado como critério de seleção o Menor Preço Global.

10.4. As propostas devem apresentar o valor global e os valores unitários, respeitando os limites máximos indicados nas planilhas que compõem o processo.

10.5. No tocante aos aspectos legais que envolvem a matéria, faz-se prudente destacar que não se configura, tendo em vista nosso entendimento, ilegalidade na realização do aludido pregão com previsão de adjudicação por grupo, e não por itens, tendo em vista que os serviços englobados se encontram integrados por itens de uma mesma natureza e que guardam estreita relação.

10.6. Impende ainda destacar que, comparativamente à adjudicação por item, a adjudicação global, no presente caso, não restringe a competitividade do certame, pois não inviabiliza a participação de empresas especializadas em um único gênero, em favor de grandes distribuidores atacadistas ou prestadores de serviços, dada a natureza dos materiais e serviços definidos no termo de referência.

10.7. Além do mais, a opção por adjudicar globalmente grupo único agrupa elementos com características semelhantes garante maior celeridade e eficiência às várias etapas procedimentais relativas à licitação, à contratação e ao acompanhamento da aquisição e da execução dos serviços, bem como do controle dos atos processuais, com reflexos positivos na economia processual e financeira, além de proporcionar maior atratividade para as empresas participantes da licitação.

11. Contratações Correlatas e/ou Interdependentes

11.1. Esta contratação irá ter sua vigência até que seja concluído o **novo processo de contratação** das soluções, o qual englobará a contratação destes licenciamentos ora citados para o período de 36 (trinta e seis) meses além de outros serviços, e que substituirá o serviço descrito no presente ETP.

11.2. Convém salientar que já havia um processo de contratação em andamento através do **protocolo nº 5-250017769-8 e Pregão Eletrônico nº 90005/2025, mas com a identificação de problemas no edital e anexos após sua publicação, ele foi revogado e deverá ser republicado.**

11.3. Sua tramitação interna já ocorre por meio do **protocolo nº 5-250060040-2**.

12. Providências para Adequação do Ambiente do Órgão

12.1. Não haverá necessidade de adequação do ambiente do Crea-SC.

13. Possíveis Impactos Ambientais – Critérios e Práticas de Sustentabilidade

13.1. A contratação observará as orientações e normas voltadas para a sustentabilidade ambiental, em especial o disposto na Instrução Normativa nº 1, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências, *in verbis*:

> *"Art. 6º Os editais para a contratação de serviços deverão prever que as empresas contratadas adotarão as seguintes práticas de sustentabilidade na execução dos serviços, quando couber:*
> *I – use produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA;*
> *II – adote medidas para evitar o desperdício de água tratada, conforme instituído no Decreto nº 48.138, de 8 de outubro de 2003;*
> *III – Observe a Resolução CONAMA nº 20, de 7 de dezembro de 1994, quanto aos equipamentos de limpeza que gerem ruído no seu funcionamento;*
> *IV – forneça aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços;*
> *V - realize um programa interno de treinamento de seus empregados, nos três primeiros meses de execução contratual, para redução de consumo de energia elétrica, de consumo de água e redução de produção de resíduos sólidos, observadas as normas ambientais vigentes;*
> *VI - realize a separação dos resíduos recicláveis descartados pelos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, na fonte geradora, e a sua destinação às associações e cooperativas dos catadores de materiais recicláveis, que será procedida pela coleta seletiva do papel para reciclagem, quando couber, nos termos da IN/MARE nº 6, de 3 de novembro de 1995 e do Decreto nº 5.940, de 25 de outubro de 2006;*
> *VII – respeite as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos; e*
> *VIII – preveja a destinação ambiental adequada das pilhas e baterias usadas ou inservíveis, segundo disposto na Resolução CONAMA nº 257, de 30 de junho de 1999.*
>
> *Parágrafo único. O disposto neste artigo não impede que os órgãos ou entidades contratantes estabeleçam, nos editais e contratos, a exigência de observância de outras práticas de sustentabilidade ambiental, desde que justificadamente."*

13.2. Assim, a contratada deverá seguir, no que couber, as diretrizes de sustentabilidade da Instrução Normativa n° 1, de 2010. A contratada também pode adotar outros critérios que garantam a sustentabilidade.

14. Estimativa do Valor da Contratação
14.1. Valor Total: R$ 64.900,00 (Sessenta e quatro mil e novecentos Reais).
15. Posicionamento Conclusivo sobre a Viabilidade e Razoabilidade da Contratação
15.1. Com base nas informações levantadas ao longo deste Estudo Técnico Preliminar, conclui-se que a contratação é razoável e possui viabilidade de sucesso, nos termos do inciso XIII, do artigo 7º, da INSTRUÇÃO NORMATIVA SEGES Nº 58, DE 8 DE AGOSTO DE 2022.
(assinado eletronicamente) **LUCAS DOS SANTOS** **Gerente do Departamento de Tecnologia Da Informação**

Documento assinado eletronicamente, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.
07/05/2025 as 22:46:41 por Lucas dos Santos Gerente Informatica, Matricula: 604.