TERMO DE REFERÊNCIA
SITSI - SUPERVISÃO DE INFRA, TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO

1. DO OBJETO

1.1 Contratação de soluções de segurança da informação, serviços especializados e equipamentos de rede para o Tribunal de Contas do Estado do Rio Grande do Sul (TCE-RS), compreendendo subscrições de licenças, aquisição de equipamentos e serviços especializados, divididos em dois lotes, conforme segue:

LOTE 1		
	Descrição	**Descrição Detalhada e Requisitos**
Item 1	Renovação de solução EDR por 36 meses.	ENCARTE I
Item 2	Contratação de solução XDR por 36 meses.	ENCARTE II
Item 3	Compra de equipamento Switch CORE	ENCARTE III
LOTE 2		
	Descrição	**Descrição Detalhada e Requisitos**
Item 1	Serviços gerenciados de detecção e resposta de incidentes através de SOC com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, incluindo feriados pelo período de 36 (trinta e seis) meses.	ENCARTE IV

1.2 Conforme tabela acima, a presente contratação visa:
1.2.1 Renovar a solução (EDR Endpoint Detection and Response) já existente no TCE-RS;
1.2.2 Adquirir uma solução XDR (Extended Detection and Response);
1.2.3 Efetuar a compra de um equipamento de Switch CORE;
1.2.4 Contratar serviços de SOC (Security Operations Center).

1.3 Vigência

1.3.1 Para o Lote 1 (Soluções EDR, XDR e Switch CORE):

a) O prazo para implantação das soluções será de até 120 (cento e vinte) dias, contados do início da vigência contratual.

b) O prazo de subscrição/garantia das soluções será de 36 (trinta e seis) meses, com início após o recebimento definitivo da implantação, prorrogável na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021, até o limite de 10 (dez) anos.

1.3.2 Para o Lote 2 (Serviços SOC), a vigência será de 36 (trinta e seis) meses, com início após o recebimento definitivo da implantação das soluções referentes aos ENCARTES I e II (EDR e

XDR) do Lote 1, ou no prazo máximo de 120 (cento e vinte) dias contados do início da vigência contratual, o que ocorrer primeiro, prorrogável na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021, até o limite de 10 (dez) anos.

1.3.2 A classificação dos serviços como continuados justifica-se pela natureza permanente e crítica da segurança da informação. Estes serviços exigem monitoramento ininterrupto e atualização constante para enfrentar ameaças cibernéticas em constante evolução. Sua eficácia depende de uma operação contínua para prevenir, detectar e responder rapidamente a incidentes de segurança. Portanto, sua natureza continuada é imperativa para garantir um ambiente de TI seguro, resiliente e capaz de proteger efetivamente os ativos informacionais do TCE-RS.

1.3 Alguns dos itens descritos na tabela acima possuem final da cobertura em período superior a doze meses. Isso é justificado porque as propostas são mais vantajosas ao TCE se comparadas com aquelas estimadas para o período de 12 (doze) meses. Com a garantia de um contrato mais longo, é nítida a economia de escala ao permitir que a futura contratada dilua os custos iniciais de instalação da solução e ofereça preços menores devido ao poder de negociação maior que o representante comercial tem com o fabricante ao lidar com prazos maiores de licenciamento. Isso reforça a importância da contratação direta por prazo superior, gerando economia financeira para este tribunal.

1.4 O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2 FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 A Supervisão de Infraestrutura de Tecnologia e Segurança da Informação (SITSI) do TCE-RS enfrenta um desafio crítico com a aproximação do vencimento de licenças de proteção endpoint/antivírus atual, também conhecido como solução EDR (Endpoint Detection e Response), essenciais para a manutenção de suas operações de TI e segurança da informação, adquiridas a partir do contrato 263/2019.

Além disso, o Switch CORE de rede, equipamento central de rede que desempenha um papel essencial no roteamento e conexão de diversos dispositivos de rede como firewall, switches e balanceadores de links, encontra-se sem garantia, sendo necessária a sua substituição. O nosso Switch CORE atual foi adquirido em 2011 através do contrato que se originou do Edital número 32/2011 (Processo-SEI n. 8189-0200/11-0), ou seja, trata-se de um equipamento com 13 (treze) anos de uso, cujo valor investido foi diluído ao longo desses anos, chegando a hora de ser substituído por uma versão mais moderna.

Em setembro de 2022 o TCE-RS foi alvo de um ataque hacker. Diante da gravidade da situação e com o objetivo de evitar novos ataques, em 2023, foi realizada a contratação das soluções de múltiplo fator de autenticação (MFA), proteção DNS em cloud e controle de acesso à rede NAC. No entanto, observar e classificar os alertas de todos estes produtos, criar incidentes de acordo com a gravidade e garantir uma resposta rápida e efetiva aos ataques sem um time e ferramentas necessárias torna-se um risco inerente à segurança. Embora os produtos atuais ofereçam um ótimo nível de proteção automatizada, ataques mais sofisticados podem passar despercebidos.

Portanto, além da renovação do EDR e substituição do Switch CORE citadas acima, são necessárias as contratações de um XDR (Extended detection and response) capaz de correlacionar dados em diversas camadas de segurança já existentes no TCE-RS, bem como o serviços especializados de Centro de Operações de Segurança (SOC) para evitar/minimizar interrupções no funcionamento dos sistemas e serviços do TCE-RS. Tais aquisições são vitais para garantir a segurança, a eficiência operacional e a continuidade dos serviços oferecidos pelo TCE-RS à sociedade.

3 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

Tendo em vista as opções identificadas para atendimento às necessidades objeto do presente estudo, bem como os custos envolvidos em cada um dos respectivos modelos, conclui-se que a única opção para atendimento às necessidades deste Tribunal é a renovação do EDR atual, a contratação de um XDR (*Extended detection and response*) e a substituição do equipamento *Switch CORE* conforme as seguintes tabelas:

Tabela 1 - Renovação do EDR e aquisição do XDR

Item	Descrição Cisco	Descrição Completa	Part Number	Contrato	Subscrição/ Serviço SKU	QTD	Data de Início da Cobertura	Data Final da Cobertura
1	Cisco Secure Endpoint XaaS Subscription	Subscrição do Gerenciador Cloud da solução de proteção para endpoints - 03 anos	**AMP4E-SEC-SUB**	202944586	Subscrição da solução Cisco Secure Endpoint Cloud por 3 anos para acesso ao dashboard em cloud.	1	05/02/2025	04/02/2028
2	Cisco Secure Endpoint Cloud subscription	Subscrição da Licença Cloud da solução de proteção para endpoints - 03 anos	**AMP4E-CL-LIC**	202944586	Subscrição da solução Cisco Secure Endpoint Essentials por 3 anos. Software EDR e antimalware para proteção de computadores e servidores.	1000	05/02/2025	04/02/2028
3	Cisco AMP for Endpoints Basic SW Service	Garantia de Software da Licença Cloud da solução de endpoint - 03 anos	**SVS-AMPE-SUP-B**	202944586	Suporte da solução Cisco Secure Endpoint Essentials fornecido pelo fabricante pelo período de 3 anos.	1	05/02/2025	04/02/2028
4	Cisco XDR	Subscrição do Gerenciador Cloud da solução de proteção Cisco XDR - 03 anos	**XDR-SEC-SUB**	NA	Subscrição da solução Cisco XDR Cloud por 3 Anos para acesso ao dashboard em cloud.	1	NA	NA
5	Cisco XDR Essential Tier subscription	Subscrição da Licença do Cisco XDR Essentials - 03 anos	**XDR-ESS**	NA	Subscrição da solução Cisco XDR Essentials por 3 anos. Software XDR com módulo NDR para detecção de comportamento anormal no ambiente de TI, geração, classificação e correlação de alertas de	1000	NA	NA

					segurança.			
6	Enhanced Support Service for XDR	Garantia de Software da Licença Cisco XDR Essentials - 03 anos	**SVS-XDR-SUP-E**	NA	Suporte da solução Cisco XDR Essentials fornecido pelo fabricante pelo período de 3 anos.	1	NA	NA

Tabela 2 - Compra de Switch Core						
Item	**Descrição Cisco**	**Descrição Completa**	**Part Number**	**Contrato**	**Subscrição/ Serviço SKU**	**Quantidade**
7	BUNDLE COMPOSTO DE: 1X C9410R-96U-BNDL-A, 4X C9400-PWR-3200AC, 1X C9400X-SUP-2/2, 1X C9400-LC-48P, 1X C9400-LC-48XS, 1X C9400-LC-12QC, 1X C9400X-SUP-2-B, 1X CON-L1SWT-C94A	Switch Core	C9410R-96U-BNDL-A	NA	NA	1
8	CX LEVEL 1 8X7NCDCatalyst 9400 Series 10 slotSup 2xC940	Garantia de Hardware - Cisco C9410 Series - Switch Core	CON-L1NCD-C9410R9A	NA	NA	1
9	Cisco Catalyst 9400 DNA Advantage 3 Year License	Subscrição da Licença do Cisco Catalyst 9400 DNA Advantage - 3Y	C9400-DNA-A-3Y	NA	NA	1
10	10GBASE-SR SFP Module, Enterprise-Class	Conversor de fibra Multimodo (MÓDULO 48XS - 48 PORTAS)	SFP-10G-SR-S=	NA	SFP-10G-SR-S=	8
11	40GBASE-CSR QSFP+ module, Extended Reach, Duplex Fiber	Conversor de fibra Multimodo (MÓDULO 12QC= - 12 PORTAS)	QSFP-40G-CSR-S	NA	QSFP-40G-CSR-S	4
12	40GBASE Active Optical Cable, 3m	Cabo com transceivers 40Gb AOC (Adaptive Optical Cable) QSFP com no mínimo 3m	QSFP-H40G-AOC3M=	NA	NA	2

Tabela 3 – Contratação de Serviço Especializado de SOC (Centro de Operações de Segurança)	
Item	**Descrição do Serviço:**
13	Serviços gerenciados de detecção e resposta de incidentes através de SOC com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, incluindo feriados pelo período de 36 (trinta e seis) meses.

A escolha da referida solução justifica-se sob os aspectos de eficiência, eficácia e viabilidade econômica.

Por fim, tendo em vista as características do mercado em que o objeto encontra-se inserido, verifica-se que há ampla disponibilidade de fornecedores, de forma que não encontramos óbice à contratação por meio de Pregão Eletrônico.

4 REQUISITOS TÉCNICOS

4.1 Lote 1: Renovação de EDR, Contratação de XDR, Aquisição de equipamento Switch CORE:

4.1.1 Renovação de solução de proteção de endpoint EDR já existente, conforme PartNumbers e serviços contidos no ENCARTE I;

4.1.2 Contratação de solução de proteção XDR, conforme PartNumbers e serviços contidos no ENCARTE II;

4.1.3 Aquisição de novo equipamento Switch CORE, para substituição do equipamento existente, conforme PartNumbers e serviços contidos no ENCARTE III;

4.2 Lote 2: Contratação de Serviço Especializado de Centro de Operações de Segurança (SOC):

4.2.1 Contratação de serviços gerenciados de detecção e resposta de incidentes através de SOC com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, incluindo feriados, pelo período de 36 (trinta e seis) meses, conforme descrição contida no ENCARTE IV.

4.3 Considerações Gerais (serve para o Lote 1 e Lote 2):

a. A CONTRATADA deverá realizar todo o planejamento para implementar a solução, dispondo de todos os recursos necessários (pessoas, materiais e ferramentas), sem ônus adicional à CONTRATANTE.

b. As ferramentas de softwares que compõem os itens do ENCARTE I e ENCARTE II deverão ser licenciadas junto aos seus devidos FABRICANTES e com suporte ativo em regime 24 (vinte e quatro) horas x 7 (sete) dias da semana durante a vigência do contrato.

c. A CONTRATADA é responsável, durante a vigência contratual, por dar manutenção e atualizar as versões dos softwares, mantendo sempre a versão mais estável disponível pelo FABRICANTE, bem como acionar o suporte do fabricante, caso se faça necessário.

5 Requisitos da Contratação

5.1 Obrigações da Contratada:

a. Executar os serviços contratados, de acordo com as especificações solicitadas, bem como aquelas contidas no ETP e TR (Estudo Técnico Preliminar e Termo de Referência).

b. Planejar, conduzir e executar os serviços com integral observância das disposições deste Contrato, obedecendo rigorosamente o prazo estabelecido entre a CONTRATADA e o TRIBUNAL.

c. Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação.

d. Apresentar durante a execução do contrato, se solicitado, documentos que comprovem estar cumprindo a legislação em vigor quanto às obrigações assumidas, em especial encargo social, trabalhistas, previdenciários, tributários, fiscais e comerciais.

e. Reparar ou corrigir, às suas expensas, no todo ou em parte, os serviços em que verificarem vícios, defeitos ou incorreções resultantes da execução.

f. Responsabilizar-se por todos e quaisquer ônus e encargos decorrentes da legislação fiscal (Federal, Estadual e Municipal) e da legislação social, previdenciária, trabalhista e comercial, decorrentes da execução do presente contrato.

g. A inadimplência da Contratada, com referência aos encargos trabalhistas, fiscais e comerciais, não transfere à Contratante a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato.

h. Providenciar a imediata correção das deficiências apontadas pelo responsável pela fiscalização do Contrato.

i. Comunicar por escrito ao gestor, eventual atraso ou paralisação da prestação dos serviços, apresentando justificativas que serão objeto de apreciação pelo Contratante.

j. Comunicar por escrito ao gestor, quando verificar condições inadequadas para a prestação do serviço.

k. Garantir sigilo e inviolabilidade das conversações realizadas através do serviço que constitui o objeto deste contrato.

5.2 Acompanhamento contratual

a. A CONTRATANTE e a CONTRATADA realizarão a Reunião de Abertura do Projeto, visando dispor sobre os detalhes da implantação da solução em até 15 (quinze) dias após a assinatura do termo de contrato. A CONTRATADA enviará por correio eletrônico a ATA da Reunião Abertura do Projeto para aprovação da CONTRATANTE.

b. A CONTRATANTE e a CONTRATADA realizarão reuniões de acompanhamento, visando dispor sobre os detalhes da prestação dos serviços.

5.3 Qualificação Técnica

5.3.1 Qualificação Técnica para o LOTE 01:

a. A proponente deverá, comprovadamente, ser um canal autorizado a comercializar produtos da marca ofertada. Caso a empresa licitante seja o próprio fabricante, excluem-se as exigências com relação a esta declaração.

Justificativa: Trata-se de uma medida para qualificar a proponente e minimizar riscos. O investimento financeiro é grande e optamos pelo que nos pareça mais seguro para o Tribunal. É uma questão de prudência.

b. A proponente deverá possuir, no mínimo, a certificação "Cisco Premier";

Justificativa: as revendas autorizadas e capacitadas a comercializar os produtos compreendidos por este termo de referência devem possuir, no mínimo, a certificação Cisco Premier. Este item apenas complementa e reforça o item anterior.

c. A proponente deverá possuir, no mínimo, as certificações: Advanced Enterprise Networks Architecture Specialization e Advanced Security Architecture Specialization, emitidas pela Cisco Systems;

Justificativa: certificações necessárias para garantir que a empresa seja especializada nas arquiteturas de redes e segurança, as quais garantem a capacidade e expertise da empresa para soluções de conectividade wifi e rede cabeada, roteamento de pacotes, balanceamento de WAN, SDWAN, firewall, NAC, IPS, antimalware e integrações com o novo ambiente.

d. Apresentar equipe qualificada nos produtos objetos da contratação, que detenham, individualmente ou em conjunto, certificados ou certificações vigentes abaixo:

A proponente deverá comprovar que possui pelo menos um profissional da sua equipe, com vínculo CLT ou PJ, ou que figure como sócio no contrato social, que possua a certificação de CCNP Security (Cisco Certified Network Professional Security), com comprovação expedida pela própria Cisco Systems. A verificação será feita através do site http://www.ciscocertificates.com/verify.cfm.

A proponente deverá comprovar que possui pelo menos um profissional da sua equipe, com vínculo CLT ou PJ, ou que figure como sócio no contrato social, que possua a certificação de CCNP Enterprise (Cisco Certified Network Professional Enterprise), com comprovação expedida pela própria Cisco Systems. A verificação será feita através do site http://www.ciscocertificates.com/verify.cfm.

A proponente deverá comprovar que possui pelo menos um profissional da sua equipe, com vínculo CLT ou PJ, ou que figure como sócio no contrato social, que possua a certificação PCE (Peplink Certified Engineer), com comprovação expedida pela própria Peplink. A verificação será feita através do site http://peplink.com/certifications ou de carta do fabricante.

e. As certificações listadas acima, que fazem referência aos profissionais responsáveis pelo planejamento e implantação, são necessárias para garantir que a empresa tenha em seu quadro de colaboradores especialistas para atender demandas relativas à segurança, infraestrutura de redes necessário para a instalação de novo switch Core a ser adqurido e processos, as quais englobam a implementação e integração do ambiente de rede as soluções Cisco DUO, Cisco Umbrella e Cisco ISE, sendo capaz de consolidá-las ao atual sistema de detecção e resposta de ameaças a ser adquirio, o Cisco XDR.

f. Atestado (s) fornecido (s) por Pessoa Jurídica de Direito Público ou Privado, comprovando a prestação de serviços em ambientes corporativos que englobem ao menos duas soluções

de redes ou segurança do fabricante Cisco implementadas e mantidas atualmente com serviços gerenciados.

Justificativa: Tendo em vista a alta complexidade da solução e da especificidade dos profissionais técnicos alocados para a prestação dos serviços, a exigência de atestado de capacidade técnica tem por objetivo comprovar a experiência anterior na realização de serviços similares, proporcionais à dimensão e complexidade do objeto a ser executado.

g. Não é admitida a subcontratação do objeto contratual por se entender que existem empresas no mercado que conseguem atender em sua integralidade o objeto da contratação de forma plena e sem necessidade de buscar com terceiros serviços ou bens acessórios para conseguir cumprir na integralidade as obrigações contratuais.

5.3.2 Qualificação Técnica para o LOTE 02:

a. A proponente deverá possuir, no mínimo, as certificações: Advanced Enterprise Networks Architecture Specialization e Advanced Security Architecture Specialization, emitidas pela Cisco Systems;

Justificativa: certificações necessárias para garantir que a empresa contratada para a prestação de serviço SOC seja especializada nas arquiteturas de redes e segurança, as quais garantem a capacidade e expertise para a pronta resposta à incidentes.

b. Apresentar equipe qualificada para a prestação do serviço SOC, de forma que a empresa tenha em seu quadro de colaboradores, individualmente ou em conjunto, certificados ou certificações vigentes abaixo:

A proponente deverá comprovar que possui pelo menos um profissional da sua equipe, com vínculo CLT ou PJ, ou que figure como sócio no contrato social, que possua a certificação de ITIL 4 (ITIL® 4 Foundation), com comprovação expedida pela própria empresa certificadora.

A proponente deverá comprovar que possui pelo um profissional da sua equipe, com vínculo CLT ou PJ, ou que figure como sócio no contrato social, que possua a certificação de CCNP Security (Cisco Certified Network Professional Security), com comprovação expedida pela própria Cisco Systems. A verificação será feita através do site http://www.ciscocertificates.com/verify.cfm.

A proponente deverá comprovar que possui pelo menos um profissional da sua equipe, com vínculo CLT ou PJ, ou que figure como sócio no contrato social, que possua a certificação de CCNP Enterprise (Cisco Certified Network Professional Enterprise), com comprovação expedida pela própria Cisco Systems. A verificação será feita através do site http://www.ciscocertificates.com/verify.cfm.

A proponente deverá comprovar que possui pelo menos um profissional da sua equipe, com vínculo CLT ou PJ, ou que figure como sócio no contrato social, que possua a certificação PCE (Peplink Certified Engineer), com comprovação expedida

pela própria Peplink. A verificação será feita através do site http://peplink.com/certifications ou de carta do fabricante.

c. As certificações listadas acima são necessárias para atender demandas relativas à segurança e integração do ambiente atual do TCE-RS, sendo capaz de consolidar as diversas ferramentas da CONTRATANTE no sistema de detecção e resposta à incidentes SOC a ser contratado.

d. A proponente deverá apresentar Atestado(s) de Capacidade Técnica fornecido(s) por Pessoa Jurídica de Direito Público ou Privado, que comprove(m) a experiência na prestação de Serviços Gerenciados que englobe ao menos duas soluções de redes ou segurança do fabricante Cisco, em ambiente com mais de 500 usuários/dispositivos de rede, em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana.

Justificativa: Tendo em vista a alta complexidade da solução e da especificidade dos profissionais técnicos alocados para a prestação dos serviços, a exigência de atestado de capacidade técnica tem por objetivo comprovar a experiência anterior na realização de serviços similares, proporcionais à dimensão e complexidade do objeto a ser executado.

5.4 Sustentabilidade

A CONTRATADA deverá observar as seguintes práticas de sustentabilidade:

5.4.1 proibir quaisquer atos de preconceito de raça, cor, sexo, orientação sexual ou estado civil na seleção de mão de obra para o quadro da empresa.

5.4.2 observar a legislação trabalhista relativa à jornada de trabalho, às normas coletivas da categoria profissional e as normas internas de segurança e saúde do trabalho.

5.4.3 treinar e capacitar periodicamente seus empregados no atendimento das Normas Internas e de Segurança e Medicina do Trabalho, bem como na prevenção de incêndio, práticas de redução do consumo de água, energia e redução da geração de resíduos para implementação das lições aprendidas durante a prestação dos serviços.

5.4.4 orientar sobre o cumprimento, por parte dos funcionários, das Normas Internas e de Segurança e Medicina do Trabalho, tais como prevenção de incêndio nas áreas da prestação de serviço, zelando pela segurança e pela saúde dos usuários e da circunvizinhança.

5.4.5 administrar situações emergenciais de acidentes com eficácia, mitigando os impactos aos empregados, colaboradores, usuários e ao meio ambiente;

5.4.6 destinar de forma ambientalmente adequada todos os materiais e equipamentos que foram utilizados na prestação de serviços.

5.5 Subcontratação

5.5.1 Não é admitida a subcontratação do objeto contratual por se entender que existem empresas no mercado que conseguem atender em sua integralidade o objeto da contratação de forma plena e sem necessidade de buscar com terceiros serviços ou bens acessórios para conseguir cumprir na integralidade as obrigações contratuais.

5.6 Garantia da contratação

5.7 Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% do valor contratual, conforme regras previstas no contrato.

5.8 Necessidade de vistoria

5.8.1 É oferecida aos licitantes a possibilidade de realizar visita técnica para conhecimento pormenorizado do serviço a ser realizado. A proponente, a fim de dirimir eventuais dúvidas, poderá, de forma facultativa, realizar visita técnica à Sede do TCE/RS, na cidade de Porto Alegre, RS, objetivando conhecer o local.

5.8.2 As visitas técnicas devem ser marcadas previamente com o TCE/RS, por intermédio do telefone 3214-9832, e ser realizada com antecedência mínima de um (01) dia útil da data estabelecida para abertura da licitação.

5.8.3 Dúvidas relativas ao objeto podem ser sanadas através do setor SITSI – Supervisão de Infra, Tecnologia e Segurança da Informação, pelo telefone 3214-9832, ou através do e-mail sitsi@tce.rs.gov.br

6 MODELO DE EXECUÇÃO DO OBJETO

6.1 Condições de execução.

A execução do objeto seguirá a seguinte dinâmica:

6.1.1 A entrega de equipamentos e os serviços de implementação das soluções referentes ao ENCARTEs I, II e III deverá ocorrer em, no máximo, 120 dias, a contar da assinatura do termo de contrato.

6.1.2 A prestação dos serviços especializados de monitoramento de segurança SOC, descritos no ENCARTE IV, deverá ser iniciado tão logo ocorra a configuração e integração das soluções descritas no ENCARTE I e ENCARTE II (EDR e XDR), ou no prazo máximo de 120 dias, o que ocorrer primeiro, a contar da assinatura do termo de contrato.

6.1.3 As subscrições de licenças que constam na tabela acima deverão ser registradas junto ao fabricante Cisco Systems especificamente para o Tribunal de Contas do Estado do Rio Grande do Sul.

6.1.4 Os serviços de implementação e configuração das licenças deverão ser executados remotamente ou no Tribunal de Contas do Estado do Rio Grande do Sul, localizado na Rua Sete de Setembro, 388 – 3º andar, nesta Capital, de segunda à sexta-feira, das 10 às 18 horas.

7 MODELO DE GESTÃO DO CONTRATO

7.1 O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2 Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3 O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

7.4 Fiscalização

7.4.1 A execução do Contrato será objeto de acompanhamento, fiscalização e avaliação pelo Tribunal através de fiscal(is) do contrato, ou pelos respectivos substitutos.

7.4.2 A fiscalização do Tribunal, em especial, terá o dever de verificar a qualidade do serviço a ser prestado, observando todas as exigências editalícias, podendo exigir sua reexecução quando este não atender os termos do que foi proposto e Contratado, sem qualquer ônus para o Tribunal e sem que assista ao Contratado qualquer indenização pelos custos daí decorrentes.

7.4.3 Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

7.4.4 O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.4.5 Identificada qualquer inexatidão ou irregularidade, o fiscal do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.5 Sanções administrativas.

Pela inexecução total ou parcial do objeto deste Termo de Referência, poderão ser aplicadas, além das previstas em Termo de Contrato, as seguintes sanções:

Referentes aos ENCARTE I, ENCARTE II e ENCARTE III:

- O atraso na entrega e execução do objeto descritos nos Encartes acima implicará multa de:
    - 0,5% (cinco décimos por cento) por dia sobre o valor total do contrato destes itens, subtraída a parte adimplida, limitada a 15 (quinze) dias;
    - 10% (quinze por cento) sobre o valor total do contrato, subtraída a parte adimplida, em caso de exceder o limite previsto na alínea anterior.

- Após o décimo quinto dia, a critério da Administração, no caso de execução com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

- Caso a CONTRATADA apresente justificativa e esta for aceita pela fiscalização, a multa de mora não será aplicada.

Referentes ao ENCARTE IV (Serviço SOC):

- Advertência por escrito: Quando do não cumprimento de quaisquer das obrigações deste Termo de Referência, conforme avaliação técnica da CONTRATANTE.

- Multa por reincidência em advertência por escrito:

  - De 1% (um por cento) do valor mensal da prestação de serviços para os casos de reincidência por 2 (duas) vezes de advertência por escrito para a mesma falta.

  - De 10% (dez por cento) do valor mensal da prestação de serviços para os casos de reincidência superior a 2 (duas) vezes de advertência por escrito para a mesma falta.

- Multa por não cumprimento de SLA Mensal:

  - De 1% (um por cento) do valor mensal da prestação de serviço SOC, para os casos de não cumprimento de SLA Mensal.

  - De 10% (dez por cento) do valor mensal da prestação de serviço SOC, para os casos de não cumprimento de SLA Mensal, por 2 (dois) meses consecutivos.

  - A partir do 4º (quarto) mês consecutivo de não cumprimento do SLA Mensal, poderá ser configurado pela CONTRATANTE a inexecução total do serviço SOC, sem prejuízo da multa.

- Multa por não cumprimento de adequação da equipe técnica:

  - De 1% (um por cento) do valor mensal da prestação de serviços referentes ao serviço SOC, por mês, para os casos de não adequação da equipe técnica, enquanto perdurar o não cumprimento.

  - A partir do 3º (terceiro) mês consecutivo de não adequação da equipe técnica, poderá ser configurado pela CONTRATANTE a inexecução total do serviço SOC, sem prejuízo da multa.

- Multa por Indisponibilidade dos serviços de SOC:

  - De 1% (um por cento) do valor mensal da prestação de serviços referentes ao serviço SOC, por dia, para os casos de total indisponibilidade dos serviços prestados, enquanto a indisponibilidade durar até 2 (dois) dias corridos.

- De 5% (um por cento) do valor mensal da prestação de serviço SOC, por dia, para os casos de total indisponibilidade dos serviços descritos, enquanto a indisponibilidade for superior à 2 (dois) dias corridos.

- A partir do 10º (décimo) dia de indisponibilidade consecutiva, poderá ser configurado pela CONTRATANTE a inexecução total do serviço SOC, sem prejuízo da multa.

8 CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

8.1
6.1 Forma de medição:
8.1.1 O fornecimento será atestado pela fiscalização.

8.2 Prazo de pagamento

8.2.1 O procedimento de pagamento e o prazo seguirão a ordem cronológica de pagamentos.

8.2.2 Para este tribunal, faz-se justo que o pagamento esteja de acordo com a vigência da subscrição e garantia das soluções, ou seja, as competências de cada ano devem ser refletidas no pagamento anual respectivo.

8.2.2.1 Relativamente ao Lote 1, item 1, subitem 2 (ENCARTE I); item 2, subitem 2 (ENCARTE II); e item 3, subitens 2, 4 e 5 (ENCARTE III), o pagamento será feito em três parcelas: a primeira em 30 dias após o recebimento do objeto, a segunda 12 e a terceira 24 meses depois.

8.2.2.1.1 No que se refere aos serviços de implementação do Lote 1 (item 1, subitem 4; item 2, subitem 4; e item 3, subitem 37), o pagamento será integral a contar da finalização dos serviços, no prazo de trinta dias.

8.2.2.1.2 Quanto aos demais subitens do item 3 do Lote 1, descritos no ENCARTE III, o pagamento será integral a contar do recebimento, no prazo de trinta dias.

8.2.3 Para o serviço SOC, objeto do lote 2, descrito no ENCARTE IV, o pagamento será mensal conforme avalição dos níveis de serviço após o envio do relatório mensal de atividades elaborado pela contratada e aprovação da fiscalização.

8.2.4 A forma como deverão ser pagos os valores relativos a cada item do contrato estão resumidos na tabela que integra o ENCARTE V.

9 FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1 Forma de seleção e critério de julgamento da proposta

9.1.1 O(s) fornecedor(es) será(ão) selecionado(s) por meio da realização de procedimento de LICITAÇÃO, na modalidade *PREGÃO, sob a forma ELETRÔNICA*, com adoção do critério de julgamento pelo *MENOR PREÇO.*

9.2 Exigências de habilitação

9.2.2 As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.

9.2.3 Os critérios de qualificação econômico-financeira a serem atendidos pelo fornecedor estão previstos no edital.

9.3 Participação de consórcio e cooperativas

9.3.1 *Não será admitida a participação de pessoas jurídicas em regime de consórcio, qualquer que seja sua forma de constituição, por não se tratar de execução contratual de dimensão de alta complexidade e grande vulto financeiro.*

10 ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1 *O custo estimado da contratação consta no documento de Pesquisa de Preços e possui caráter sigiloso, de forma a possibilitar que os licitantes ofertem propostas com valores mais condizentes aos praticados no mercado, considerando suas próprias estimativas de custos, sem que exista interferência externa. No entanto, não haverá prejuízo à transparência, visto que a informação será publicizada após o julgamento das propostas.*

11 ADEQUAÇÃO ORÇAMENTÁRIA

11.1 A contratação será atendida pela dotação orçamentária a ser informada pela SOF.

11.2 Sugestão de fiscais e suplentes:

11.2.1 Carlos Eduardo Manzoni Moreira, Auditor de Controle Externo, matrícula nº 17000520 – SITSI (Supervisão de Infra, Tecnologia e Segurança da Informação).

11.2.2 Luís Henrique Gonçalves de Oliveira, Auditor de Controle Externo, matrícula nº 17001530 – SERSI - Serviço de Rede e Segurança da Informação.

Porto Alegre, 6 de novembro de 2024.

gov.br Documento assinado digitalmente
CARLOS EDUARDO MANZONI MOREIRA
Data: 06/11/2024 16:17:55-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
DANIEL COELHO VAZ HENRIQUES
Data: 06/11/2024 16:32:46-0300
Verifique em https://validar.iti.gov.br

ENCARTE I

Especificação Técnica das Licenças e Serviços

Lote 1 - Item 1 - Renovação de solução de proteção de Endpoint EDR já existente, por 36 (trinta e seis) meses:

1. Tabela 1 – PartNumbers para Renovação do EDR por 36 (trinta e seis) meses:

Subitem	Descrição Cisco	Descrição Completa	Part Number	Contrato	Subscrição/ Serviço SKU	QTD	Data de Início da Cobertura	Data Final da Cobertura
1	Cisco Secure Endpoint XaaS Subscription	Subscrição do Gerenciador Cloud da solução de proteção para endpoints - 03 anos	**AMP4E-SEC-SUB**	202944586	Subscrição da solução Cisco Secure Endpoint Cloud por 3 anos para acesso ao dashboard em cloud.	1	05/02/2025	04/02/2028
2	Cisco Secure Endpoint Cloud subscription	Subscrição da Licença Cloud da solução de proteção para endpoints - 03 anos	**AMP4E-CL-LIC**	202944586	Subscrição da solução Cisco Secure Endpoint Essentials por 3 anos. Software EDR e antimalware para proteção de computadores e servidores.	1000	05/02/2025	04/02/2028
3	Cisco AMP for Endpoints Basic SW Service	Garantia de Software da Licença Cloud da solução de endpoint - 03 anos	**SVS-AMPE-SUP-B**	202944586	Suporte da solução Cisco Secure Endpoint Essentials fornecido pelo fabricante pelo período de 3 anos.	1	05/02/2025	04/02/2028

2. Serviços relacionados aos itens da tabela acima:

2.1. A CONTRATADA deverá realizar uma revisão do ambiente do TCE-RS com o objetivo de garantir que as melhores práticas estejam sendo aplicadas no uso da Plataforma EDR Cisco Secure Endpoint Essentials;

2.2. A CONTRATADA deverá garantir que os Endpoints estão com a versão mais atualizada possível do EDR;

2.3. A CONTRATADA deverá realizar a revisão dos grupos e políticas;

2.4. A CONTRATADA deverá realizar a revisão das regras de isolamento;

2.5. A CONTRATADA deverá realizar a integração com o XDR;

2.6. A CONTRATADA deverá garantir envio de incidentes classificados conforme a severidade do mesmo para ferramenta de comunicação colaborativa e para o XDR;

2.7. A CONTRATADA deverá, junto com a equipe técnica do TCE-RS, elaborar formas de evidenciar os Endpoints que não estão com o Cisco Secure Endpoint instalado.

ENCARTE II

Especificação Técnica das Licenças e Serviços

Lote 1 - Item 2 - Contratação de solução de proteção XDR por 36 (trinta e seis) meses:

1. Tabela 1 – PartNumbers para contratação de solução de proteção XDR por 36 (trinta e seis) meses:

Subitem	Descrição Cisco	Descrição Completa	Part Number	Subscrição/ Serviço SKU	QTD
1	Cisco XDR	Subscrição do Gerenciador Cloud da solução de proteção Cisco XDR - 03 anos	**XDR-SEC-SUB**	Subscrição da solução Cisco XDR Cloud por 3 Anos para acesso ao dashboard em cloud.	1
2	Cisco XDR Essential Tier subscription	Subscrição da Licença do Cisco XDR Essentials - 03 anos	**XDR-ESS**	Subscrição da solução Cisco XDR Essentials por 3 anos. Software XDR com módulo NDR para detecção de comportamento anormal no ambiente de TI, geração, classificação e correlação de alertas de segurança.	1000
3	Enhanced Support Service for XDR	Garantia de Software da Licença Cisco XDR Essentials - 03 anos	**SVS-XDR-SUP-E**	Suporte da solução Cisco XDR Essentials fornecido pelo fabricante pelo período de 3 anos.	1

2. Serviços relacionados aos itens da tabela acima:

a. A CONTRATADA deverá realizar o provisionamento da solução, configuração e integração com os atuais produtos de segurança existentes no ambiente do CONTRATANTE de acordo com os requisitos apresentados, conforme segue:

b. Sobre a integração com o EDR Cisco Secure Endpoint:

   i. A CONTRATADA deverá realizar a integração da solução EDR atual à plataforma XDR para centralização e correlação dos alertas de segurança, criação de incidentes e designação de recursos para atuação nas ações de resposta;

   ii. A CONTRATADA deverá criar fluxos de automação na plataforma XDR para responder aos incidentes, tais como solicitar que os dispositivos seja escaneado remotamente ou isolados

c. Sobre a integração com o Cisco Firepower (2 – duas unidades):

   i. A CONTRATADA deverá integrar o produto ao módulo NDR (Network Detection and Response) da solução XDR, enviando telemetria de rede via Netflow para análise de padrões de acesso, volumetria de banda, países e tráfego malicioso com destino ou origem a internet;

   ii. A CONTRATADA deverá efetuar a criação de incidentes automáticos na plataforma XDR com base em alertas dos sensores IPS/IDS, bem como políticas de malware a nível de rede, relacionando os artefatos ou

assinaturas maliciosas com alertas similares gerados em outros produtos como da solução antimalware EDR;

iii. A CONTRATADA deverá criar fluxos de automação para realizar o bloqueio de endereços IP, hosts, URLs e hashs para responder aos incidentes de forma mais rápida.

d. Sobre a integração com o Cisco DUO:

i. A CONTRATADA deverá integrar a atual solução MFA utilizadas pelas aplicações e desktops do CONTRATANTE ao XDR a fim de detectar e responder a tentativas consecutivas e malsucedidas de autenticação;

ii. A CONTRATADA deverá criar fluxos para automatizar bloqueios de contas com atividades suspeitas para aplicações críticas;

iii. A CONTRATADA deverá gerar incidentes e designar time para tratamento de eventos ou tentativas de login a partir de dispositivos não confiáveis ou que estejam fora da área de atuação ou pontos de conexão wifi normalmente utilizados pelos usuários, relacionando aos eventos gerados pelas outras ferramentas de segurança.

e. Sobre a integração com o Cisco ISE:

i. A CONTRATADA deverá configurar integração com solução XDR a fim de treinar a solução para detectar comportamentos de autenticação suspeitos, tais como autenticação 802.1x de usuários em estações de trabalho diferentes dos habituais ou consecutivos erros de senha.

f. Sobre a integração com o Cisco Umbrella:

i. A CONTRATADA deverá integrar a proteção DNS utilizada atualmente dentro das sedes administrativas e dispositivos remotos ao XDR a fim de centralizar a geração de alertas e incidentes, com dados enriquecidos de outras plataformas como firewall e EDR a fim de traçar perfis de ações maliciosas executadas dentro do ambiente.

g. Sobre a integração com o Balanceador de WAN (Peplink) (2 – duas unidades):

i. A CONTRATADA deverá ingerir telemetria de rede via Netflow dos balanceadores de links de internet através do módulo NDR (Network Detection and Response) da solução XDR. O objetivo é analisar padrões de acesso, volumetria de banda, países e tráfego malicioso com destino ou origem sendo a internet;

h. Sobre a integração com os Servidores de Rede Microsoft (90 - noventa unidades):

i. A CONTRADADA deverá providenciar a configuração necessária de forma que os servidores existentes na rede deverão enviar telemetria mais detalhada para o módulo NDR da solução XDR. Deverá ser instalado em todos os servidores Microsoft da rede o agente Cisco Network Analytics. Políticas para geração de alarmes e incidentes relacionados à detecção de comunicações anormais (tanto internas quanto externas) e alteração de hash de processos (PIDs) deverão ser elaboradas, não excluindo funcionalidades adicionais de segurança observadas ao decorrer do projeto.

ii. A CONTRATADA deverá cadastrar lista de servidores críticos de acordo com informações fornecidas pelo CONTRATANTE, a fim de configurar a solução para priorizar de forma visual os incidentes mais graves através do dashboard de monitoramento.

i. Sobre a integração com os Roteadores e Switches (70 - setenta unidades):

i. A CONTRADADA deverá providenciar a configuração necessária de forma a enviar telemetria de rede via Netflow para módulo NDR a fim de analisar

padrões de acesso e volumetria de banda para tráfego leste-oeste (destino ou origem redes locais);

j. Repasse de Conhecimento:

i. A CONTRATADA deverá oferecer ambiente virtual ou de demonstração para a CONTRATANTE testar a solução acima e se ambientar com o funcionamento dessa sem ônus ao ambiente de produção, mesmo que apenas em modo de leitura;

ii. A CONTRATADA deverá realizar repasse de conhecimento a equipe técnica da CONTRATANTE no formato remoto ou presencial, com carga horária de 40 (quarenta horas), discorrendo sobre as seguintes ferramentas de software e tópicos que compõem a solução Cisco XDR:

1. Introdução à solução;
2. Integrações com atuais produtos de segurança;
3. Funcionamento das automações;
4. Módulo NDR Cisco Secure Cloud Analytics e agente NVM;
5. Interpretação, administração e gerenciamento de incidentes;
6. Cadastramento de assets e definição de impactos para o negócio;
7. Melhores práticas a serem utilizadas de acordo com o fabricante.

iii. A CONTRATADA deverá realizar repasse de conhecimento a equipe técnica da CONTRATANTE no formato remoto ou presencial, demonstrando o funcionamento e configurações necessárias para realizar a integração do EDR com a solução de XDR;

iv. Sistema de gerenciamento de eventos e informações de segurança (SIEM):

1. A CONTRATADA deverá realizar repasse de conhecimento a equipe técnica da CONTRATANTE no formato remoto ou presencial de forma a demonstrar como realizar pesquisas e interpretar resultados da busca dentro do serviço de armazenamento de logs disponibilizado pela CONTRATADA.

ENCARTE III

Especificação Técnica das Licenças e Serviços

Lote 1 - Item 3 – Aquisição de equipamento Switch Core com garantia de 36 (trinta e seis) meses:

1. Tabela 1 – PartNumbers para aquisição de equipamento Switch Core com garantia de 36 (trinta e seis) meses:

Subitem	Descrição Cisco	Descrição Completa	Part Number	QTD
1	Catalyst 9400 Series 10 slot,1xSup, 2xLC, DNA-A LIC	Chassis do Switch Core Catalyst 9400 Series 10 – 10 slots.	C9410R-96U-BNDL-A	1
2	CX LEVEL 1 8X7NCDCatalyst 9400 Series 10 slotSup 2xC940	Garantia e contrato de suporte do Chassis do Switch Core por 36 (trinta e seis) meses.	CON-L1NCD-C9410R9A	1
3	Cisco Catalyst 9400 DNA Advantage Term License	Termo de Licença do Software DNA Advantage.	C9400-DNA-A	1
4	CX LEVEL 1 SW SUB Cisco Catalyst 9400	Contrato de Suporte do Software do Switch Core por 36 (trinta e seis) meses.	CON-L1SWT-C94A	1
5	Cisco Catalyst 9400 DNA Advantage 3 Year License	Subscrição da licença do Software DNA Advantage por 36 (trinta e seis) meses.	C9400-DNA-A-3Y	1
6	Cisco DNA Spaces Extend Term License for Catalyst Switches	Termos de licença de extensão do Cisco DNA Spaces.	D-DNAS-EXT-S-T	1
7	Cisco DNA Spaces Extend for Catalyst Switching - 3Year	Subscrição da licença da extensão do Cisco DNA Spaces por 36 (trinta e seis) meses.	D-DNAS-EXT-S-3Y	1
8	Cisco ThousandEyes Enterprise Agent IBN Embedded	Licença do agente ThousandEyes.	TE-EMBEDDED-T	1
9	ThousandEyes - Enterprise Agents	Subscrição da licença do agente ThousandEyes por 36 (trinta e seis) meses.	TE-EMBEDDED-T-3Y	1
10	Cisco Catalyst 9400 Network Advantage License	Licença Network Advantage do Switch Core.	C9400-NW-A	2
11	Cisco Catalyst 9400 Series Power Supply Blank Cover	Tampa de cobertura do slot da fonte do Switch Core.	C9400-PWR-BLANK	4
12	Cisco Catalyst 9400 Series Slot Blank Cover	Tampa de cobertura de slot do Switch Core.	C9400-S-BLANK	3
13	TE agent for IOSXE on C9K	Software do ThousandEyes.	TE-C9K-SW	1
14	QSFP port EMI and dust protection cover	Tampa de cobertura de slot QSFP do Switch Core.	C9400-QSFP-CVR	12
15	Cisco Catalyst 9400 XE 17.12 UNIVERSAL	Software IOS-XE do Switch Core.	S9400UK9-1712	1
16	Cisco Catalyst 9400 Series 3200W AC Power Supply	Fonte de alimentação do Switch Core.	C9400-PWR-3200AC	4
17	EL224 to IEC-C19 14ft Brazil	Cabo de alimentação da fonte do Switch Core.	CAB-EL224-C19-BR	4

18	Console Cable 6ft with RJ-45-to-RJ-45	Cabo console RJ-45.	CAB-CON-C9K-RJ45	1
19	10-SLOT CHASSIS CABLE MANAGEMENT GUIDES for 9400	Organizador de cabo.	CAB-GUIDE-10R	1
20	ADAPTER FOR DB9F TO RJ45 for 9400	Adaptador DB9 para RJ-45.	C9K-ACC-ADP-DB9	1
21	12-24 and 10-32 SCREWS FOR RACK INSTALLATION, QTY 12	Parafuso para fixação do Switch Core no Rack.	C9K-ACC-SCR-12	1
22	Cisco Catalyst 9400 Series Redundant Supervisor 2 Module	Módulo da supervisora secundária SUP2 do Switch Core.	C9400X-SUP-2/2	1
23	No SSD Memory Selected	Sem SSD.	C9400-SSD-NONE	1
24	Cisco Catalyst 9400 Series 48-Port POE+ 10/100/1000 (RJ-45)	Módulo line card de 48 portas POE+ RJ-45.	C9400-LC-48P	1
25	Cisco Catalyst 9400 Series 48-Port 10 Gigabit Ethernet(SFP+)	Módulo line card de 48 portas SFP+.	C9400-LC-48XS	1
26	Cisco Catalyst 9400 Series 12-Port 40GE/4-port 100GE	Módulo line card de 12 portas QSFP+.	C9400-LC-12QC	1
27	Catalyst 9400 Series SUP2 BUNDLE PID ONLY - NOT AN ACTUAL HW	Pacote para a supervisora primária SUP2.	C9400X-SUP-2-B	1
28	Cisco Catalyst 9400 Series Supervisor 2 Module	Supervisora primária SUP2.	C9400X-SUP-2	1
29	No SSD Memory Selected	Sem SSD.	C9400-SSD-NONE	1
30	Catalyst 9400 2xC9400-LC-48P BUNDLE PID ONLY-NOT ACTUAL HW	Pacote de dois módulos line card de 48 portas POE+ RJ-45.	C9400-LC-48P-B	1
31	Cisco Catalyst 9400 Series 48-Port POE+ 10/100/1000 (RJ-45)	Módulo line card de 48 portas POE+ RJ-45.	C9400-LC-48P	1
32	Cisco Catalyst 9400 Series 48-Port POE+ 10/100/1000 (RJ-45)	Módulo line card de 48 portas POE+ RJ-45.	C9400-LC-48P	1
33	Network Plug-n-Play Connect for zero-touch device deployment	Licença da funcionalidade Plug-n-Play.	NETWORK-PNP-LIC	1
34	10GBASE-SR SFP Module, Enterprise-Class	Conversor de fibra Multimodo (MÓDULO 48XS - 48 PORTAS)	SFP-10G-SR-S=	8
35	40GBASE-CSR QSFP+ module, Extended Reach, Duplex Fiber	Conversor de fibra Multimodo (MÓDULO 12QC= - 12 PORTAS)	QSFP-40G-CSR-S	4
36	40GBASE Active Optical Cable, 3m	Cabo com transceivers 40Gb integrado AOC (Adaptive Optical Cable) QSFP, com no mínimo 3m	QSFP-H40G-AOC3M=	2

2. Serviços relacionados aos itens da tabela acima:

a. A CONTRATADA deverá realizar a instalação física em rack, substituindo o equipamento antigo (Cisco 4510) pelo equipamento novo (9410R), envolvendo os seguintes serviços:
   i. Desconexão de cabos;
   ii. Desligamento e remoção do equipamento antigo;
   iii. Fixação do equipamento novo;
   iv. Conexão do cabos no equipamento novo;
   v. Acompanhamento presencial no dia seguinte a migração.

b. Realização de toda configuração necessária para que o novo equipamento assuma totalmente a função do anterior;

c. Atualização do software do novo switch core 9410R para a versão recomendada pelo fabricante;
d. Configuração de VLANs e protocolo VTP;
e. Configuração das credencias de acesso SSH, SNMP, NTP, Radius, entre outros;
f. Teste de alta disponibilidade das supervisoras;
g. Integração com o Cisco Catalyst Center;
h. Quaisquer alterações deverão estar sujeitas à aprovação da equipe de administradores de rede do TCE-RS;

ENCARTE IV

Especificação Técnica das Licenças e Serviços

Lote 2 - Item 1 – Contratação de Serviço Especializado de SOC (Centro de Operações de Segurança):

1. Tabela 1 – PartNumbers para aquisição de equipamento Switch Core com garantia de 36 (trinta e seis) meses:

Item	Descrição do Serviço:
1	Serviços gerenciados de detecção e resposta de incidentes através de SOC com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, incluindo feriados pelo período de 36 (trinta e seis) meses.

2. Serviços relacionados aos itens da tabela acima:

a. Centro de Operações de Segurança (SOC)

i. A CONTRATADA deve prestar o serviço de SOC, possuindo um núcleo de operação de segurança cibernética, sendo essencial para garantir a proteção contínua contra ameaças e a resposta rápida a incidentes para o CONTRATANTE;

ii. O SOC deve ser planejado pela CONTRATADA em conformidade com as melhores práticas de gerenciamento de serviços, baseados no modelo ITIL, devendo a operação estar disponível em regime contínuo e integral, 24 (vinte e quatro) horas 7 (sete) dias na semana, incluindo feriados;

iii. Essa operação contínua deve suportar a integração entre as plataformas de SIEM, Cisco XDR e ferramenta de ITSM, que juntas proporcionam uma visão abrangente do ambiente e facilitam a detecção e resposta a incidentes;

iv. A CONTRATADA deve possuir o serviço de SOC fora das dependências da CONTRATANTE, administrando os sistemas de detecção e monitorando de forma proativa os dados e as tentativas de intrusão e eventos suspeitos de forma remota;

v. A CONTRATADA deve assegurar atendimento on-site na sede do CONTRATANTE em Porto Alegre-RS em até 12 (doze) horas após a solicitação, quando o suporte remoto não for suficiente para resolução do problema:

1. Caso a CONTRATADA não possua sede ou filial em município localizado em até 100 quilômetros de Porto Alegre, deverá apresentar um plano de atendimento que garanta o cumprimento deste prazo.

vi. A empresa deverá ser capacitada de acordo com os requisitos de qualificação técnica solicitados pela CONTRATADA de modo a atender todos os requisitos técnicos para implementação da solução e execução dos serviços;

vii. A CONTRATADA deverá definir, propor e executar uma estratégia para a mitigação e contenção de ataques. Investigar e identificar no ambiente alvo de ameaças persistentes ou vetores passíveis de exploração, propondo soluções para a sua mitigação e, quando possível, realizar o tratamento das ameaças identificadas.

b. Sistema de gerenciamento de eventos e informações de segurança (SIEM)

i. Requisitos Gerais:

1. A solução SIEM deve ser disponibilizada como serviço em ambiente integralmente pela CONTRATADA no ambiente SOC;
2. A infraestrutura cloud do SIEM deve estar localizada no Brasil;
3. A solução SIEM deve ser capaz de se integrar nas seguintes soluções de nuvem:
    a. AZURE (Microsoft);
    b. AWS (Amazon);
    c. GCP (Google Cloud Plataform);
    d. OCI (Oracle Cloud).
4. O acesso à ferramenta deve ser totalmente via web browser e a conexão WEB deve ser criptografa https minimamente com TLS 1.2.
5. Todas as comunicações entre os componentes do SIEM devem ser criptografadas;
6. A solução deve ser disponibilizada em formato distribuído e escalável e para garantir a disponibilidade e a integridade dos dados;
7. A solução deve cumprir as exigências da LGPD, com políticas de retenção de dados claras e mecanismos para garantir que os dados sejam acessados apenas por usuários autorizados.
8. O sistema deve contar com rotinas de backup automatizadas e o ambiente cloud deve contar com um plano de recuperação de desastres;
9. A comunicação de rede para coleta de dados entre o ambiente da CONTRATADA e CONTRATANTE deve ser feita através de conexão IPSec, sendo também responsabilidade da CONTRATADA fornecer a tecnologia necessária, além de realizar a configuração para estabelecer o túnel VPN na cloud.
10. A solução de SIEM deve ser capaz de monitorar dispositivos por meio de agente nativo e coleta de logs via SYSLOG e APIs;
11. A coleta de logs através de arquivos do tipo csv, txt, json, yaml e xml, pode ser realizada por meio de coletor disposto na infraestrutura da CONTRANTE, caso haja necessidade;
12. A solução de SIEM deve ser capaz operar em servidores configurados em alta disponibilidade, em caso de crescimento do ambiente da CONTRATANTE;
13. A solução deve ser projetada para armazenar logs por até 90 dias em formato normalizado e disponível através de dashboard via acesso WEB seguro;
14. O sistema deve ser implementado em infraestrutura distribuída, escalável e altamente disponível;
15. É indispensável que a CONTRATADA forneça toda infraestrutura na modalidade cloud necessária para máquinas virtuais, de acordo com os requisitos indicados pelo fabricante/fornecedor de solução de SIEM;
16. Os custos de licenciamento devem estar a cargo da CONTRATADA e ofertados como serviço dentro do escopo de monitoramento proativo e reativo do serviço SOC.

ii. Quantidade de dispositivos para extração e armazenamento de LOGs para o SIEM:

1. Os logs de acesso à internet devem ser extraídos das seguintes soluções via syslog:
    a. 2 (dois) Firewall Cisco Firepower.
    b. 2 (dois) Balanceadores de Wan modelo Peplink.
2. A coleta e armazenamento dos eventos gerados pelo agente de segurança SIEM deve atender minimamente:
    a. 2 (dois) Servidores Exchange;
    b. 90 (noventa) Servidores Microsoft;
    c. 70 (setenta) Servidores Linux.
3. A CONTRADA deve garantir a retenção de logs brutos por até 1 ano;
4. A CONTRATADA deve fornecer serviço de armazenamento de logs utilizando solução SIEM;
5. Em medidas realizadas pela CONTRATANTE, estimamos que a solução de SIEM deverá ser capaz de registrar o volume de até 10 (dez) GB/log por dia;
6. A solução SIEM deverá ser capaz de registrar o volume necessário de logs dos itens acima pelo período mínimo de 1 (um) ano.

iii. Requisitos técnicos do SIEM:

1. Deve permitir a criação de políticas customizadas para retenção de dados, para gestão de espaço consumido;
2. É indispensável a criação regras customizadas para tratamento de logs não normalizados;
3. A solução de SIEM deve gerar indicadores de vulnerabilidades para dispositivos monitorados por agente nativo, organizados por CVE, Severidade, Software Vulneráveis e dispositivos vulneráveis;
4. Deve possibilitar a criação de relatórios de indicadores;
5. Deve permitir a segregação de acessos, para administradores e visualizadores;
6. A ferramenta deve disponibilizar visualização através de gráficos e dashboards;
7. Deve fornecer visualização em tempo real de eventos de coletados de dispositivos conectados via agente e/ou syslog;
8. Deve ser capaz executar a consulta de dados via acesso WEB;
9. Deve permitir a agregação de eventos;
10. Gerar alertas/incidentes com base nas regras definidas previamente;
11. Permitir a análise de eventos baseados em contexto, tais como, usuários, localização geográfica, bem como qualquer outro metadado contido no evento;
12. A plataforma deve ser capaz de correlacionar logs de acesso coletados via syslog das soluções de firewall e balanceador de wan, contendo no mínimo os seguintes itens:
    a. Endereço IP de origem (antes e após source nat);
    b. Endereço IP de destino;
    c. Porta de origem (antes e após source nat);
    d. Porta de destino;
    e. Nome do usuário;
    f. Resultado do acesso (permitido ou negado);
    g. Nome da política de acesso;
    h. URL ou FQDN do site acessado se disponível;
    i. Nome da aplicação acessada de disponível;
    j. Data e horário do acesso;

13. A plataforma deve ser capaz de correlacionar eventos relacionados ao módulo de segurança UEBA (User and entity behavior analytics);
    a. Monitorar eventos de login de usuários através de agente nativo do SIEM;
    b. Monitorar eventos de grupos de usuários através de agente nativo do SIEM;
    c. Monitorar eventos de uma lista de observação customizada de usuários e/ou grupos através de agente nativo do SIEM;
    d. Lista de exceção de usuários e grupos monitorados considerados de baixo ou nenhum risco;
    e. Gerar alertas para tentativa de acesso a contas suspensas e desabilitadas;
    f. Gerar alertas para tentativas de Força bruta;
    g. Gerar alertas para detecção de movimentação lateral;
    h. Gerar alertas para alterações realizadas em usuários que estão em uma lista de observação;
    i. Gerar alerta de acesso a máquinas Linux e Windows com contas de serviço;
14. O agente nativo deve ser compatível com sistemas Windows e Linux;
15. Deve ter a capacidade para integração e monitoramento de serviço provedores de mensageria online, via API;
16. Estar integrado a fontes ou lista de observação de Threat Intel/IoC's;
17. Realizar o monitoramento de arquivos e diretórios via agente nativo FIM (File integrity monitoring);
18. Detectar e alertas tentativa de manipulação de conta em sistemas Linux;
19. Monitorar e reportar alteração em arquivos específicos;
20. Monitorar e alertar sobre execução de comandos considerados maliciosos, como execução de scripts via monitoramento por agente nativo;
21. Gerar alertas automaticamente na ferramenta de ITSM (Sistema de Gerenciamento de Serviços de TI) da CONTRATADA;
22. Fornecer informações de inventário do host, tais como, softwares instalados, portas abertas, endereços IP, MAC Address, atualização de pacotes e hotfixes;
23. Monitorar processos de dispositivos que utilizam o monitoramento via agente nativo;
24. Regras customizadas para logs gerados a partir do balanceador de carga, bem como a normalização dos logs com o firewall;
25. Todas configurações e customizações informadas no item 2.2.3 deverão ser realizadas pela CONTRATADA.

c. Monitoramento 24x7 e Resposta a Incidentes

i. O time de SOC disponibilizado pela CONTRATADA deve ser capaz de monitorar continuamente todos os sistemas críticos da organização, utilizando tanto o SIEM quanto o Cisco XDR para detectar anomalias e potenciais ameaças;
ii. A CONTRATADA deve possuir capacidade técnica de operar o Cisco XDR, para criação de regras;

iii. Fica a cargo do time de SOC, realizar as integrações nativas do Cisco XDR com outros produtos de segurança do fabricante Cisco;
iv. É responsabilidade do time de SOC manter atualizada as plataformas de SIEM e Cisco XDR;
v. O time de SOC é responsável por conduzir a resposta a incidentes de forma ágil, reagindo imediatamente às notificações geradas por essas ferramentas, mitigando riscos e minimizando impactos;
vi. Fica a cargo do time de SOC desenvolver playbooks para resposta automática utilizando a plataforma Cisco XDR;
vii. O time de SOC deverá tomar ações corretivas para conter, erradicar e recuperar de incidentes de segurança. Isso inclui a aplicação de políticas de segurança, isolamento de sistemas comprometidos e coordenação de esforços de recuperação utilizando ferramentas integradas ao Cisco XDR;
viii. O time de SOC deverá classificar os incidentes com base em sua criticidade e priorizar as respostas de acordo com o impacto potencial sobre a organização;
ix. Fica a cargo do time de SOC comunicar incidentes críticos às partes interessadas e, se necessário, escalar o incidente para níveis superiores ou especialistas técnicos. A comunicação clara e eficaz é essencial para uma resposta coordenada;
x. O time de SOC deve documentar cada incidente detalhadamente, incluindo ações tomadas, impacto, e lições aprendidas. Esta documentação é fundamental para auditorias, conformidade e melhoria contínua dos processos;
xi. O time de SOC é responsável por ajustar as regras de detecção no SIEM e as políticas de segurança no XDR com base nas novas ameaças identificadas, garantindo que o ambiente esteja sempre protegido contra as ameaças mais recentes;
xii. O time de SOC deverá estar envolvido na identificação de vulnerabilidades através de ativos monitorados e sugerindo correções a CONTRATANTE.

d. Documentação e Desenvolvimento de Processos

i. A CONTRATADA deverá prever até 40h o serviço de aperfeiçoamento da Política de Resposta à Incidente do TCE-RS, já levando em consideração o cenário de softwares e ferramentas contidas nesse edital para a prestação de serviço SOC.
    1. A política especificada acima deverá ser totalmente aderente às ferramentas de segurança utilizadas pelo TCE-RS.
ii. O time de SOC deverá desenvolver e documentar processos e procedimentos de resposta a incidentes, garantindo a consistência e a melhoria contínua das operações;
iii. A documentação deve ser desenvolvida utilizando indicadores como ativos monitoradores, incidentes x mês, severidades, principais ativos relacionados a alertas, principais tipos de alertas, principais fontes de alertas e outros KPIs;
iv. Fica sob responsabilidade do time e SOC da CONTRATADA, evidenciar documentações com procedimentos operacionais, documentação sobre regras de detecção;
v. A operação de SOC pode ser realizada na estrutura remota da CONTRATADA;

vi. A CONTRATADA deve evidenciar que monitora sua infraestrutura, bem como disponibilidade e saúde do ambiente fornecido para operação de SOC;
vii. A CONTRATADA deve evidenciar a presença de controle de acesso e monitoramento em seu ambiente de execução de SOC;
viii. A CONTRATADA deverá preparar uma apresentação do ambiente final do SOC de pelo menos 8h.

e. Mapeamento de Áreas Críticas e Análise de Riscos

i. O time de SOC em conjunto com a CONTRATADA e com o TCE-RS deverá realizar um mapeamento das áreas críticas da organização;
ii. Fica a cargo da CONTRATADA informar sobre ativos e processos essenciais, permitindo que o monitoramento e a resposta sejam priorizados de forma adequada. Além disso, o time de SOC deve conduzir uma análise de riscos abrangente, sugerindo medidas mitigatórias que protejam os ativos críticos contra potenciais ameaças.

f. Frameworks de Segurança e Conformidade

i. O time de SOC deve alinhar suas operações com frameworks de segurança consagrados, como NIST, MITRE ATT&CK e CIS, utilizando essas diretrizes para a formulação de políticas, desenvolvimento de processos e resposta a incidentes;
ii. A conformidade com regulamentações como a LGPD deve ser mantida em todos os momentos, com o SOC garantindo que os dados da organização sejam tratados e protegidos em conformidade com os requisitos legais e regulatórios.

g. Níveis de serviço

i. Os Níveis de Serviço estão relacionados aos Níveis de Severidade que se baseiam na relação entre Urgência e Impacto, sendo:
    1. **URGÊNCIA**: classificada de acordo com seu impacto nos componentes de segurança monitorados pelo sistema XDR e impacto nos negócios do cliente de acordo com o componente afetado, sendo:

        a. **Crítica**: Incidente de segurança significativo que causa a interrupção da função primária da organização ou perda significativa, vazamento, corrupção ou criptografia não autorizada de dados confidenciais. Pode haver ter um impacto financeiro significativo e imediato nos negócios do Cliente;
        b. **Maior**: A função primária da organização está gravemente degradada devido à perda de funcionalidade, de dados, vazamento, corrupção ou criptografia não autorizada de dados. Existe um provável significativo impacto financeiro nos negócios do Cliente;
        c. **Menor**: A função não crítica da organização está interrompida ou gravemente degradada. Existe um possível impacto financeiro nos negócios do Cliente;
        d. **Baixo/Aviso**: A função pública não crítica do tribunal está degradada. Não há impacto material. A CONTRATANTE percebe o problema como baixa urgência.

2. **IMPACTO**: classificado de acordo com a amplitude do seu impacto nos negócios do CONTRATANTE (o tamanho, escopo e complexidade do Incidente):

    a. **Generalizado**: Todos os serviços, áreas e locais são afetados;
    b. **Grande**: Vários locais ou áreas são afetados;
    c. **Localizado**: Um único local ou um usuário em vários locais são afetados;
    d. **Individualizado**: Um único usuário é afetado.

ii. **Tabela de Prioridade**: o cruzamento das variáveis **URGÊNCIA** e **IMPÁCTO** duas variáveis provê a Tabela de Prioridade, conforme a tabela abaixo:

Tabela de Prioridade		IMPÁCTO			
		Generalizado	**Grande**	**Localizado**	**Individualizado**
URGÊNCIA	**Crítica**	P1	P1	P2	P2
	Maior	P1	P2	P2	P3
	Menor	P2	P3	P3	P3
	Baixa/Aviso	P4	P4	P4	P4

iii. Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, quais sejam: qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança.

iv. As metas devem ser medidas do primeiro ao último dia de cada mês.
v. Os prazos de atendimento baseiam-se no tipo de **PRIORIDADE,** conforme a tabela abaixo:

PRIORIDADE	**TEMPO DE RESPOSTA INICIAL:**
P1	15 Minutos
P2	30 Minutos
P3	4 Horas
P4	8 Horas

vi. O tempo de resposta inicial ao incidente se diz respeito às atividades de contenção, isolamento e investigação. Além das atividades destacadas, a resposta inicial ao incidente também inclui o acionamento das equipes e fornecedores terceiros responsáveis pelo gerenciamento e administração das soluções afetadas pelos incidentes;
vii. Os prazos de atendimento são contados a partir do registro das requisições na solução XDR, sendo suspensos em situações que dependam de algum fator externo a CONTRATADA;
viii. Fica acordado entre a CONTRATANTE e a CONTRATADA o cumprimento de 95% dos atendimentos dentro dos tempos especificados;

h. Relatório de Atividades:

i. Deverá ser confeccionado mensalmente um Relatório de Atividades elencando detalhadamente todos os eventos ocorridos e as ações adotadas pela equipe ao longo do mês – do primeiro ao último dia do mês – relacionando eventos de PRIORIDADE classificados como P1, P2, P3 e P4;

ii. O relatório será apresentado, mensalmente, em reunião realizada remotamente, sendo posteriormente enviado por e-mail aos participantes e pontos focais do projeto.

iii. O relatório apresentado deverá possuir, no mínimo, os seguintes itens:

1. Evidências de que as principais ameaças estão sendo mitigadas através de trabalho preventivo a ser realizado;
2. Sugestões de melhorias;
3. Principais ofensores;
4. Tempo que serviços críticos ficaram fora;
5. Relação com relatórios passados que permita visualizar tendências de impacto e severidade.

ENCARTE V - Tabela de Especificação de Pagamentos

Lote	Item	Subitem	Descrição	Valor Unitário (R$)	QTD	Valor Total (R$)	Ano 1		Ano 2		Ano 3	
							(%)	Valor (R$)	(%)	Valor (R$)	(%)	Valor (R$)
1	1	2	AMP4E-CL-LIC - Cisco Secure Endpoint Cloud subscription*		1000		34		33		33	
		4	Serviços de Implementação da solução EDR		1		100		/		/	
	2	2	XDR-ESS - Cisco XDR Essential Tier subscription*		1000		34		33		33	
		4	Serviços de Implementação da solução XDR		1		100		/		/	
	3	1	C9410R-96U-BNDL-A - Catalyst 9400 Series 10 slot,1xSup, 2xLC, DNA-A LIC **		1		100		/		/	
		2	CON-L1NCD-C9410R9A - CX LEVEL 1 8X7NCDCatalyst 9400 Series 10 slotSup 2xC940		1		34		33		33	
		4	CON-L1SWT-C94A - CX LEVEL 1 SW SUB Cisco Catalyst 9400		1		34		33		33	
		5	C9400-DNA-A-3Y - Cisco Catalyst 9400 DNA Advantage 3 Year License		1		34		33		33	
		16	C9400-PWR-3200AC - Cisco Catalyst 9400 Series 3200W AC Power Supply		4		100		/		/	
		22	C9400X-SUP-2/2 - Cisco Catalyst 9400 Series Redundant Supervisor 2 Module		1		100		/		/	
		24	C9400-LC-48P - Cisco Catalyst 9400 Series 48-Port POE+ 10/100/1000 (RJ-45)		1		100		/		/	
		25	C9400-LC-48XS - Cisco Catalyst 9400 Series 48-Port 10 Gigabit Ethernet(SFP+)		1		100		/		/	
		26	C9400-LC-12QC - Cisco Catalyst 9400 Series 12-Port 40GE/4-port 100GE		1		100		/		/	
		27	C9400X-SUP-2-B - Catalyst 9400 Series SUP2 BUNDLE PID ONLY - NOT AN ACTUAL HW		1		100		/		/	
		34	SFP-10G-SR-S= - 10GBASE-SR SFP Module, Enterprise-Class		8		100		/		/	
		35	QSFP-40G-CSR-S - 40GBASE-CSR QSFP+ module, Extended Reach, Duplex Fiber		4		100		/		/	
		36	QSFP-H40G-AOC3M= - 40GBASE Active Optical Cable, 3m		2		100		/		/	
		37	Serviços de Implementação do CORE DE REDE		1		100		/		/	
							SUBTOTAL:		SUBTOTAL:		SUBTOTAL:	
2	1	1	Serviços gerenciados de detecção e resposta de incidentes através de SOC com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, incluindo feriados pelo período de 36 (trinta e seis) meses.		36		Pagamento Mensal					

*** Compõem os itens 1 e 2 do Lote 1 os seguintes PNs:**

Lote	Item	Subitem	Descrição	QTD
1	1	1	AMP4E-SEC-SUB - Cisco Secure Endpoint XaaS Subscription	1
		3	SVS-AMPE-SUP-B - Cisco AMP for Endpoints Basic SW Service	1
	2	1	XDR-SEC-SUB - Cisco XDR	1
		3	SVS-XDR-SUP-E - Enhanced Support Service for XDR	1

**** ITEM 3 - SUBITEM 1,TODOS OS PNs deverão compor os BUNDLE C9410R-96U-BNDL-A, CONFORME ABAIXO:**

Lote	Item	Subitem	Descrição	QTD
1	3	3	C9400-DNA-A - Cisco Catalyst 9400 DNA Advantage Term License	1
		6	D-DNAS-EXT-S-T - Cisco DNA Spaces Extend Term License for Catalyst Switches	1
		7	D-DNAS-EXT-S-3Y - Cisco DNA Spaces Extend for Catalyst Switching - 3Year	1
		8	TE-EMBEDDED-T - Cisco ThousandEyes Enterprise Agent IBN Embedded	1
		9	TE-EMBEDDED-T-3Y - ThousandEyes - Enterprise Agents	1
		10	C9400-NW-A - Cisco Catalyst 9400 Network Advantage License	2
		11	C9400-PWR-BLANK - Cisco Catalyst 9400 Series Power Supply Blank Cover	4
		12	C9400-S-BLANK - Cisco Catalyst 9400 Series Slot Blank Cover	3
		13	TE-C9K-SW - TE agent for IOSXE on C9K	1
		14	C9400-QSFP-CVR - QSFP port EMI and dust protection cover	12
		15	S9400UK9-1712 - Cisco Catalyst 9400 XE 17.12 UNIVERSAL	1
		17	CAB-EL224-C19-BR - EL224 to IEC-C19 14ft Brazil	4
		18	CAB-CON-C9K-RJ45 - Console Cable 6ft with RJ-45-to-RJ-45	1
		19	CAB-GUIDE-10R - 10-SLOT CHASSIS CABLE MANAGEMENT GUIDES for 9400	1
		20	C9K-ACC-ADP-DB9 - ADAPTER FOR DB9F TO RJ45 for 9400	1
		21	C9K-ACC-SCR-12 - 12-24 and 10-32 SCREWS FOR RACK INSTALLATION, QTY 12	1
		23	C9400-SSD-NONE - No SSD Memory Selected	1
		28	C9400X-SUP-2 - Cisco Catalyst 9400 Series Supervisor 2 Module	1
		29	C9400-SSD-NONE - No SSD Memory Selected	1
		30	C9400-LC-48P-B - Catalyst 9400 2xC9400-LC-48P BUNDLE PID ONLY-NOT ACTUAL HW	1
		31	C9400-LC-48P - Cisco Catalyst 9400 Series 48-Port POE+ 10/100/1000 (RJ-45)	1
		32	C9400-LC-48P - Cisco Catalyst 9400 Series 48-Port POE+ 10/100/1000 (RJ-45)	1
		33	NETWORK-PNP-LIC - Network Plug-n-Play Connect for zero-touch device deployment	1