Os seguintes anexos integram este Termo de Consulta:

ANEXO I-A - Formulário de precificação

ANEXO I-B – Especificação Técnica – Serviços SOC

ANEXO I-C – Especificação Técnica – Serviços Técnicos Especializados

ANEXO I-D – Relatório de Níveis de serviços

ANEXO I-E - Laudo técnico de execução de serviços

ANEXO I-F- Ordem de Serviço para Serviços Especializados

ANEXO I-G – Glossário

ANEXO I-H – Níveis de Serviços

ANEXO I-i – Especificação técnica da plataforma de busca na Deep/DarkWeb

ANEXO I-J – Especificação técnica da plataforma NDR

ANEXO I-K – Equipe técnica

As proponentes deverão preencher as tabelas abaixo, com os preços segmentados por lote, item e cenários, em Reais, com todos impostos, taxas, seguros e demais despesas inclusas.

1. LOTE 1

1.1. Item único - Serviços Continuados de SOC

Lote 1 - Cenário 1 – Serviços Continuados de SOC REMOTO com solução de busca Deep/DarkWeb – 36 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 1 Cenário 1	Serviços Continuados de Centro de Operações de Segurança (Security Operation Center – SOC), na modalidade **REMOTO**, com disponibilização de plataforma tecnológica para realizar buscas contínuas em Deep/DarkWeb	meses	**36**		

Lote 1 - Cenário 2 – Serviços Continuados de SOC REMOTO com solução de busca Deep/DarkWeb e solução NDR – 36 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 1 Cenário 2	Serviços Continuados de Centro de Operações de Segurança (Security Operation Center – SOC), na modalidade **REMOTO**, com disponibilização de plataforma tecnológica para realizar buscas contínuas em Deep/DarkWeb e **plataforma tecnológica de NDR.**	meses	**36**		

Lote 1 - Cenário 3 – Serviços Continuados de SOC PRESENCIAL com solução de busca Deep/DarkWeb – 36 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 1 Cenário 3	Serviços Continuados de Centro de Operações de Segurança (Security Operation Center – SOC), na modalidade **PRESENCIA**L, com disponibilização de plataforma tecnológica para realizar buscas contínuas em Deep/DarkWeb	meses	**36**		

Lote 1 - Cenário 4 – Serviços Continuados de SOC PRESENCIAL com solução de busca Deep/DarkWeb e solução NDR– 36 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 1 Cenário 4	Serviços Continuados de Centro de Operações de Segurança (Security Operation Center – SOC), na modalidade **PRESENCIA**L, com disponibilização de plataforma tecnológica para realizar buscas contínuas em Deep/DarkWeb e **plataforma tecnológica de NDR.**	meses	**36**		

Lote 1 - Cenário 5 – Serviços Continuados de SOC REMOTO com solução de CTI – 48 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 1 Cenário 5	Serviços Continuados de Centro de Operações de Segurança (Security Operation Center – SOC), na modalidade **REMOTO,** com disponibilização de plataforma tecnológica para realizar buscas contínuas em Deep/DarkWeb	meses	**48**		

Lote 1 - Cenário 6 – Serviços Continuados de SOC REMOTO com solução de busca Deep/DarkWeb e solução NDR – 48 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 1 Cenário 6	Serviços Continuados de Centro de Operações de Segurança (Security Operation Center – SOC), na modalidade **REMOTO**, com disponibilização de plataforma tecnológica para realizar buscas contínuas em Deep/DarkWeb e **plataforma tecnológica de NDR.**	meses	**48**		

Lote 1 - Cenário 7 – Serviços Continuados de SOC PRESENCIAL com solução de busca Deep/DarkWeb – 48 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 1 Cenário 7	Serviços Continuados de Centro de Operações de Segurança (Security Operation Center – SOC), na modalidade **PRESENCIAL**, com disponibilização de plataforma tecnológica para realizar buscas contínuas em Deep/DarkWeb	meses	**48**		

Lote 1 - Cenário 8 – Serviços Continuados de SOC PRESENCIAL com solução de busca Deep/DarkWeb e solução NDR – 48 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 1 Cenário 8	Serviços Continuados de Centro de Operações de Segurança (Security Operation Center – SOC), na modalidade **PRESENCIAL**, com disponibilização de plataforma tecnológica para realizar buscas contínuas em Deep/DarkWeb e **plataforma tecnológica de NDR.**	meses	**48**		

2. LOTE 2

2.1. Item 1 – Serviços Técnicos Especializados de Segurança da Informação, **com atendimento em horário comercial**

Lote 2 - Cenário 9 - Serviços Técnicos Especializados de Segurança da Informação, com atendimento em horário comercial – 36 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 02 Item 1 Cenário 9	Serviços Técnicos Especializados de Segurança da Informação, **com atendimento em horário comercial (8 x 5**), em dias úteis e **vigência de 36 meses.**	horas	**3.000**		

Lote 2 - Cenário 10 - Serviços Técnicos Especializados de Segurança da Informação, com atendimento em horário comercial – 48 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 02 Item 1 Cenário 10	Serviços Técnicos Especializados de Segurança da Informação, **com atendimento em horário comercial (8 x 5),** em dias úteis e **vigência de 48 meses**.	horas	**4.000**		

2.2. Item 2 – Serviços Técnicos Especializados de Segurança da Informação, **com atendimento 24 x 7 x 365**

Lote 2 - Cenário 9 - Serviços Técnicos Especializados de Segurança da Informação, com atendimento 24 x 7 x 365 – 36 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 02 Item 2 Cenário 11	Serviços Técnicos Especializados de Segurança da Informação, **com atendimento 24 x 7 x 365** (24 horas por dia, sete dias por semana, 365 dias por ano) e **vigência de 36 meses.**	horas	**1.500**		

Lote 2 - Cenário 10 - Serviços Técnicos Especializados de Segurança da Informação, com atendimento 24 x 7 x 365 – 48 meses

Lote/ Item	Serviços	Unidade	Quantidade	Valor Unitário	Valor Total
Lote 02 Item 2 Cenário 10	Serviços Técnicos Especializados de Segurança da Informação, **com atendimento 24 x 7 x 365** (24 horas por dia, sete dias por semana, 365 dias por ano) e **vigência de 48 meses.**	horas	**2.000**		

_____

Local e data **Proposta válida até: DD / MM / AA**

_____x_____

1. Serviços Continuados de SOC (Lote 01)

1.1. Os serviços serão prestados de acordo com as especificações, padrões técnicos de qualidade, desempenho, arquitetura, processos e plataformas tecnológicas estabelecidas pela CONSULENTE, conforme requisitos e exigências estabelecidas neste anexo. A unidade de medida para a prestação destes serviços será em meses, na forma de serviços continuados, durante toda vigência contratual.

1.2. Para execução dos serviços a PROPONENTE deverá utilizar as plataformas de soluções de TIC relacionadas à segurança da informação, implementadas no ambiente de TIC da CONSULENTE. Estas plataformas cobrem tanto os ambientes on-premises quanto na nuvem, garantindo uma abordagem abrangente e integrada.

1.2.1. A tabela abaixo detalha as plataformas de soluções de TIC que serão utilizadas durante a prestação dos serviços, assim como a responsabilidade pela disponibilização e manutenção da infraestrutura de hardware e software de cada uma:

Plataforma de soluções de TIC	**Responsabilidade pela disponibilização e manutenção da infraestrutura de hardware e software**
SIEM (IBM QRadar)	CONSULENTE em todos os cenários
WAF (ModSecurity e F5)	CONSULENTE em todos os cenários
Gestão de Vulnerabilidades (Tenable.IO)	CONSULENTE em todos os cenários
ZABBIX Comunity	CONSULENTE em todos os cenários
Prometheus	CONSULENTE em todos os cenários
SonarQube	CONSULENTE em todos os cenários
Dynatrace	CONSULENTE em todos os cenários
Firewall Checkpoint	CONSULENTE em todos os cenários
IDS/IPS	CONSULENTE em todos os cenários
Antivirus (Kaspersky)	CONSULENTE em todos os cenários
Mainview	CONSULENTE em todos os cenários

Plataforma de soluções de TIC	Responsabilidade pela disponibilização e manutenção da infraestrutura de hardware e software
NDR	Cenários 1, 3, 5 e 7 Responsável: CONSULENTE Cenários 2, 4, 6 e 8 Responsável: PROPONENTE, conforme especificações definidas no item 2 deste anexo.
Motor de busca contínua de Deep/DarkWeb	Todos oito cenários Responsável: PROPONENTE, conforme especificações definidas no item 2 deste anexo.

Tabela 1 – Plataformas de soluções de TIC

1.2.2. A PROPONENTE deve garantir que o conhecimento sobre novas tecnologias de cibersegurança, que venham ser implantadas pela CONSULENTE, sejam rapidamente absorvidas por suas equipes de profissionais que operam na prestação de serviços da presente contratação, em um prazo máximo de 30 (trinta) dias corridos, após a CONSULENTE formalizar junto à PROPONENTE, a implantação da nova plataforma.

1.2.2.1. Esse contexto também se aplica quanto às inovações, capacitação contínua e acompanhamento de tendências do mercado de cibersegurança.

1.3. **Detalhamento das atividades**

1.3.1. Para execução do serviço a PROPONENTE deverá atuar de forma preventiva e reativa, compreendendo, mas não se restringindo, nas seguintes atividades:

1.3.2. **Na Gestão de Vulnerabilidades**

1.3.2.1. Identificar, de forma proativa e recorrente, possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações da CONSULENTE, com o intuito de evitar que ataques cibernéticos sejam realizados com sucesso contra seu ambiente e ativos por ela mantidos. Deve contemplar também a gestão de vulnerabilidade e seus respectivos atributos.

1.3.3. **No serviço de monitoramento de ataques cibernéticos:**

1.3.3.1. Monitorar, de forma contínua e ininterrupta, ataques cibernéticos direcionados ao ambiente da CONSULENTE, mediante solução de correlacionamento de logs (SIEM), pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura, compreendendo, mas não se limitando, a servidores WEB, de aplicação, banco de dados, mail server, office 365 na nuvem, ativos de infraestrutura (AD, LDAP, DNS, DHCP etc) e ativos de segurança (Firewall, IPS, IDS, Antivirus, WAF etc).

1.3.3.2. Registrar e tratar eventos de segurança da informação, os quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo a um processo cíclico e rigoroso de gestão de incidentes, conforme os principais frameworks de mercado ISO, NIST, SAMS

1.3.3.3. Disponibilizar lista de reputação para que a CONSULENTE possa gerar configurações de bloqueio em seus ativos de segurança.

1.3.4. **No acompanhamento de liberação de Sistemas Críticos**

1.3.4.1. Acompanhar a homologação e a liberação para produção, de aplicações críticas e atualizações.

1.3.4.2. As atividades de acompanhamento deverão ser detalhadas, em modo passo a passo, em documento fornecido pela PROPONENTE e poderão ocorrer também nos finais de semana, feriados e fora do horário comercial.

1.3.4.3. A PROPONENTE não poderá alegar indisponibilidade de profissionais para a execução dos trabalhos programados, desde que comunicada pela CONSULENTE com até 2 (dias) dias corridos antes do início da execução das atividades.

1.3.5. **Na resposta a incidentes de segurança e problemas e privacidade**

1.3.5.1. Analisar, remediar, conter e documentar os eventos/incidentes de segurança da informação, como ainda, prover a devida orientação técnica à CONSULENTE na obtenção da solução para incidentes, bem como implementar respostas automatizadas a determinados eventos. O processo de tratamento de incidentes deve seguir os principais frameworks de mercado ISO, NIST ou SAMS

1.3.5.2. Realizar as tratativas de resposta a incidentes, obedecendo os normativos e políticas da CONSULENTE, principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas, oferecer as respostas (preferencialmente automatizadas) aos incidentes de segurança da informação, nos quais se incluem eventos relacionados à quebra da privacidade de informações pessoais e sensíveis, com a conseguinte restauração do ativo/serviço/processo.

1.3.5.3. Promover o gerenciamento de Incidente e problemas, realizando a comunicação, identificação, tratamento, resolução e/ou escalonamentos de todos os alertas oriundos do ambiente tecnológico de TIC da CONSULENTE, integrando as equipes necessárias pelo atendimento.

1.3.5.4. Escalar os incidentes cibernéticos que não sejam de sua alçada de acordo com os normativos definidos pela CONSULENTE.

1.3.5.5. Sugerir melhorias nos normativos da CONSULENTE e alterações em regras e controles de prevenção e detecção, quando for o caso. O processo de tratamento de incidentes deve seguir os principais frameworks de mercado ISO, NIST ou SAMS

1.3.5.6. Enriquecer os dados dos eventos e incidentes cibernéticos a partir das fontes de dados disponibilizadas pela CONSULENTE, em especial com buscas em registros do SIEM e dados oriundos dos serviços realizados pelo SOC.

1.3.5.7. Solicitar bloqueios e criação de regras de segurança à equipe de operação da CONSULENTE, e acompanhar a conclusão das solicitações.

1.3.5.8. Encerrar os eventos após sua solução.

1.3.6. **No serviço de gestão de Endpoint**

1.3.6.1. Verificar o status do gerenciador do antivirus, para certificar-se do correto funcionamento dos servidores de rede e estações de trabalho.

1.3.6.2. Verificar as definições de vacina do antivirus, fazendo o acompanhamento diário das atualizações.

1.3.6.3. Verificar os logs e alertas do gerenciador do antivirus, com especial atenção aos logs gerados, acionando a Gerência de Segurança de Informação da CONSULENTE, através de chamados, caso o mesmo não consiga remover alguma ameaça detectada.

1.3.6.4. Verificar se o backup da base de dados do antivirus foi concluído com sucesso.

1.3.6.5. Acompanhar o resultado do scan de rede, em especial o recurso de descoberta no gerenciador com a finalidade de encontrar computadores com o antivírus sem gerenciamento, máquinas sem antivírus e computadores que estão com IPs e nomes duplicados e gerar relatório para envio Gerência de Segurança de Informação da CONSULENTE, conforme detalhado na tabela 3 deste anexo.

1.3.6.6. Identificar no relatório do gerenciador quais são os equipamentos que estão com o Auto-Protect e o Network Threat Protection desativados e gerar relatório para envio Gerência de Segurança de Informação da CONSULENTE, conforme detalhado na tabela 3 deste anexo.

1.3.6.7. Gerar relatórios mensais com os quantitativos de endpoints que apresentaram problemas e tiveram que ser resolvidos através de chamados, conforme detalhado na tabela 3 deste anexo.

1.3.7. **No serviço de inteligência aplicado a segurança da informação (Cyber Threat Intelligence - CTI)**

1.3.7.1. Realizar buscas contínuas em Deep/DarkWeb sobre a CONSULENTE, pessoas e domínos por ela definidos, de forma eficaz e proativa, em busca de informações acerca dessas pessoas, links falsos, documentos falsos, IPs, hashes, credenciais, emails, URLs parecidas com os oficiais, que possam induzir fraudes, como principalmente a retirada “takedown” (independentemente da localidade em que se situa) dos respectivos endereços, endpoints, links, domínios e congêneres junto às empresas e aos órgãos competentes.

1.3.7.1.1. Os serviços de monitoramento de informações na Deep/DarkWeb serão realizados por meio de plataforma de busca automatizada, disponibilizada pela PROPONENTE, conforme requisitos definidos no ANEXO I-i e no item 2 deste anexo.

1.3.7.2. Monitorar ameaças contidas na internet aberta, Deep/DarkWeb, em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC da CONSULENTE, do ponto de vista da segurança cibernética. O monitoramento nestes 3 ambientes compreende, mas não se limita, às mídias como: domínios, sites, blogs, vlogs, fóruns e IRCs;

1.3.7.3. Monitorar as lojas de aplicativos Apple Store e Google Play com o objetivo de detectar aplicativos maliciosos que estejam

relacionados com a CONSULENTE. É de responsabilidade da PROPONENTE providenciar a remoção de aplicações falsas e maliciosas através de parcerias com as lojas de aplicativos, quando solicitadas pela CONSULENTE;

1.3.7.4. Monitorar fontes de informações como Shodan, BinaryEdge, Zone-H, Bases de CVE, entre outras, bem como sites que compartilhem informações sobre TTPs utilizados para ataques como phishing, ransomware, entre outros;

1.3.7.5. Monitorar ameaças cibernéticas contidas nas redes sociais em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC da CONSULENTE, do ponto de vista da segurança cibernética. As mídias sociais, compreendem, mas não se limitam à: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, Pastebin, Ghostbin, Scribd, Reclame Aqui, Apple Store, 4Shared, Google Play, Vimeo e Github, Gitlab e feeds RSS;

1.3.7.6. Monitorar ameaças representadas por domínios suspeitos ou fraudulentos e em seguida, para estes domínios, informar a CONSULENTE, o mais breve possível (máximo de 1 hora após a detecção). A PROPONENTE se obriga a apoiar a Gerência de Segurança de Informação da CONSULENTE no processo de takedown, para retirada do ar desses sites que contenham phishing ou sites que disparem spam utilizando-se do nome, da marca ou da imagem da CONSULENTE, mesmo que similar, (com intuito de confundir e aplicar fraudes ou golpes nos usuários dos serviços prestados pela CONSULENTE).

1.3.7.7. Prover serviço de monitoramento de domínios nacionais e internacionais, incluindo Top-Level Domain (TLDs) e Generic Top-Level Domain (gTLDs) e Country Code Top-Level Domain (ccTLD), que verifique a utilização do uso indevido das marcas da CONSULENTE no nome do domínio ou na URL, a empresa que administra o registro do domínio, e os dados do proprietário do domínio.

1.3.7.8. Emitir um alerta, atualizado conforme andamento do atendimento, para acompanhamento do processo de takedown de cada ocorrência. No caso de perfis falsos, pode ser necessário removê-los, desde que estejam relacionados com os ativos de informação monitorados.

1.3.7.8.1. Será obrigação da PROPONENTE estabelecer parcerias com as principais redes sociais para os procedimentos de desativação desses perfis falsos. O procedimento de desativação deverá ser

autorizado formalmente (via e-mail) pela Gerência de Segurança de Informação da CONSULENTE;

1.3.7.9. Monitorar ameaças, ataques e vulnerabilidades contidas em aplicativos de mensagens, como por exemplo WhatsApp e Telegram, em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC da CONSULENTE, do ponto de vista da segurança cibernética;

1.3.7.10. Monitorar às ameaças cibernéticas, proteção de marcas ou tentativas de fraudes envolvendo produtos e/ou serviços que constarão em listagem fornecida pela CONSULENTE após a assinatura do contrato, definida na fase de inserção (item 5.50 do termo de consulta). Esta listagem pode ser alterada a qualquer tempo pela CONSULENTE;

1.3.7.11. Classificar as descobertas categorias críticas, médias, baixas ou informacionais levando em consideração o risco associado e a tabela de Classificação de Riscos Cibernéticos definida na fase de inserção (item 5.50 do termo de consulta). Esta tabela poderá ser alterada a qualquer tempo pela CONSULENTE.

1.3.7.11.1. Para as classificações críticas e médias, elaborar planos de ação para mitigação e plano de resposta a incidentes para casos confirmados.

1.3.7.12. Reportar as descobertas, por meio de e-mail e ligação telefônica em tempo real, se a urgência de medidas mitigatórias ao risco assim o exigirem, conforme definido na tabela de Classificação de Riscos Cibernéticos. Para esse fim a CONSULENTE irá fornecer uma listagem de, pelos menos, 3 (três) contatos telefônicos, na fase de inserção (item 5.50 do termo de consulta), para a PROPONENTE.

1.3.7.13. **Reportar no mínimo, mas não se limitando as descobertas relacionadas na tabela 2, abaixo:**

Item	Descobertas Deep/DarkWeb
a	Sites utilizados para realizar, ou tentar realizar, golpes e fraudes que envolvam ou remetam de qualquer forma aos ativos de informação monitorados;
b	Anomalias nos registros “WhoIS” dos domínios monitorados;
c	Serviços que devem ser somente de consumo interno, sistemas e páginas internas (intranet) relacionados ao CONSULENTE e que estejam expostas na internet, podendo ou não ser exploradas para eventuais ataques cibernéticos;

Item	Descobertas Deep/DarkWeb
d	Vulnerabilidades dos domínios monitorados que foram tornadas públicas, mesmo que essa exposição esteja disponível apenas na Deep/DarkWeb;
e	Novas vulnerabilidades que tenham sido recentemente divulgadas.
f	Identificação de possíveis intenções de ataques a sistemas, serviços, ativos de informação e pessoas de interesse da CONSULENTE que serão fornecidas a PROPONENTE na fase de Inserção (item 5.50 do termo de consulta).
g	Intenções de ataque que tenham como objetivo os ativos monitorados
h	Campanhas relevantes de "hacktivismo", como por exemplos ataques crescentes cujos alvos são em sua maioria órgão públicos ou de governo, ou ainda campanhas de ataques em que a vulnerabilidade explorada possa estar presente nas tecnologias implantadas na CONSULENTE;
i	Comercialização online de informações sensíveis, informações pessoais, entre outras, das pessoas de interesse ou vinculadas à CONSULENTE;
j	Atividades fraudulentas relacionadas aos ativos monitorados (utilização indevida de nome e marca, por exemplo);
k	Endereços de correio eletrônico (e-mails) de domínios monitorados em listas de spam;
l	Credenciais de acesso aos ativos e Nuvem privada da CONSULENTE que estejam, ou não, à venda na web aberta, Deep/DarkWeb;
m	Credencias de correio eletrônico dos domínios monitorados que estejam, ou não, à venda na web aberta, Deep/DarkWeb;
n	Códigos maliciosos (malwares) direcionados para os ativos e sistemas de informação monitorados;
o	Intenções diretas de ataques aos ativos e sistemas de informação monitorados;
p	Discussões online maliciosas que divulguem ou acompanhem informações dos ativos de informação monitorados;
q	Perfis falsos que utilizem os nomes e/ou fotos das pessoas de interesse da CONSULENTE;
r	Documentos ou informações confidenciais, sensíveis ou sigilosas vazadas dos ativos de informação monitorados;

Item	Descobertas Deep/DarkWeb
s	Aplicações (dispositivos móveis, softwares e aplicações web) falsas que utilizem o nome, a marca ou identidade visual dos ativos de informação monitorados;
t	Desfiguração de páginas (defacement) hospedadas nos domínios monitorados;
u	Indicativos de que qualquer um dos fornecedores de serviços de TIC da CONSULENTE teve suas operações comprometidas por ataques cibernéticos. Para esse fim será fornecida uma listagem de até 50 (cinquenta) fornecedores que devem ser monitorados na fase de inserção (item 5.50 do termo de consulta). Esta listagem poderá ser alterada a qualquer tempo pela CONSULENTE.

Tabela 2 – Descobertas Deep/DarkWeb

2. Disponibilização de Plataformas de Tecnologia de Soluções de TIC

2.1. Plataforma de Busca Contínua de Deep/DarkWeb

2.1.1. A PROPONENTE deverá disponibilizar esta plataforma, **para todos os cenários do lote 1**, conforme requisitos e exigências detalhados no **ANEXO I-i**, deste Termo de Consulta.

2.1.2. A PROPONENTE deverá informar também as condições de hospedagem e responsabilidades das partes, para instalação no data center da CONSULENTE.

2.2. Plataforma de NDR

2.2.1. A PROPONENTE deverá disponibilizar esta plataforma, para os **cenários 2, 4, 6 e 8 do lote 1**, conforme requisitos e exigências detalhados no **ANEXO I-J**, deste Termo de Consulta.

2.2.2. A PROPONENTE deverá informar também as condições de hospedagem e responsabilidades das partes, para instalação no data center da CONSULENTE.

2.2.3. Outras Plataformas

2.2.3.1. Para o serviço de SOC, se for necessária, além das duas plataformas supracitadas, a implantação de hardware e/ou

software adicional (exemplo, instalação de uma ferramenta SOAR, caso a PROPONENTE julgue necessário), no ambiente da CONSULENTE, a PROPONENTE terá duas opções:

2.2.3.1.1. **Opção 1** - A PROPONENTE irá prover todo software necessário, mas caberá a CONSULTANTE prover os recursos de hardware, limitado aos quantitativos abaixo:

2.2.3.1.1.1. Maquinas virtuais com Linux Red Hat ou Windows Server

2.2.3.1.1.2. Limite de 32 vCPUs, tendo um máximo de 8 vCPUs por servidor virtual.

2.2.3.1.1.3. Limite de 256 GB de vRAM, tendo um máximo de 64 GB por servidor virtual.

2.2.3.1.1.4. Limite de 3 TB líquido de área de armazenamento.

2.2.3.1.1.5. Toda necessidade de hardware que ultrapassarem estes limites deverá ser fornecido pela PROPONENTE.

2.2.3.1.2. **Opção 2** - A PROPONENTE irá prover todo hardware e software, sem custo adicional para a CONSULENTE.

2.3. Suporte, Apoio técnico e Manutenção para as Plataformas

2.3.1. A PROPONENTE deverá:

2.3.1.1. Instalar, gerir e manter (atualizações e evoluções inclusive) a infraestrutura das plataformas fornecidas por ela, sem ônus a CONSULENTE.

2.3.1.1.1. Se houver necessidade de upgrade na solução implementada, incluindo adição ou substituição de hardware e software, a PROPONENTE será responsável pelo custo adicional, sem ônus para a CONSULENTE.

2.3.1.2. Providenciar que os softwares não estejam, quando aplicável, em listas dos respectivos fabricantes que indiquem que não serão mais desenvolvidos, atualizados, suportados ou comercializados durante a vigência do contrato.

2.3.1.3. Prover acesso às plataformas para a CONSULENTE.

2.3.2. **Monitoramento**

2.3.2.1. Independente do cenário adotado para implantação das plataformas, todas deverão ser monitoradas pela PROPONENTE para resolução de problemas de mau funcionamento e/ou baixo desempenho.

2.3.2.2. A monitoração deverá ser efetuada durante toda vigência do contrato, 24 horas por dia, 7 dias por semana, 365 dias por ano.

2.3.2.3. Em caso de paralisação da plataforma ou degradação dos serviços da plataforma a PROPONENTE deverá entrar em contato imediato com a CONSULENTE, informando o ocorrido com informações detalhadas e as medidas de mitigação que serão tomadas.

2.3.3. **Prazo para entrega e instalação das plataformas:**

2.3.3.1. O prazo para disponibilização das plataformas tecnológicas está definido no item “Requisitos Temporais”, detalhado no termo de Consulta.

2.3.4. **Workshops**

2.3.4.1. Após a implantação das plataformas nas instalações da CONSULENTE, a PROPONENTE deverá realizar workshops e sessões práticas (hands-on) regulares para a transferência de conhecimento sobre os processos e as funcionalidades das plataformas disponibilizadas.

2.3.4.2. Os workshops e hands-on serão realizados por um período mínimo de três dias úteis, com duração de quatro horas por dia, para cada plataforma, em dias distintos.

2.3.4.3. Na fase de inserção (item 5.50 do termo de consulta) a PROPONENTE deverá elaborar um cronograma prevendo a quantidade de dias necessários para a transferência de conhecimento, respeitando os prazos mencionados anteriormente.

2.3.5. **Níveis de Serviços**

2.3.6. Os níveis de serviços e os indicadores de disponibilidade de cada plataforma e da realização dos workshops, estão definidos no ANEXO I-H deste Termo de Consulta.

3. Da categorização e priorização dos Incidentes Cibernéticos

3.1. Os incidentes deverão ser categorizados e priorizados para seguirem os fluxos de trabalhos dos níveis N1, N2 e N3 do Serviço Continuado de SOC.

3.1.1. As etapas de Recebimento, Registro, Análise, Enriquecimento e Tratamento de Incidentes serão baseadas nessa categorização e priorização.

3.2. A PROPONENTE irá designar um Gestor de SOC, profissional alocado exclusivamente à gestão e supervisão técnicas das equipes de N1 e N2 da prestação dos serviços continuados de SOC e garantindo a atuação conjunta, de sua equipe com a equipe N3 da CONSULENTE.

3.3. Em cada turno a PROPONENTE deverá designar um supervisor, que, a critério da PROPONENTE, poderá ser o N2.

3.4. As responsabilidades, perfis e tarefas de cada um dos integrantes do SOC estão descritas no ANEXO I-K, deste Termo de Consulta.

3.5. A categorização dos eventos e incidentes pode ser baseada em modelos como o “Reference Incident Classification Taxonomy”, o “A good practice guide of using taxonomies in incident prevention and detection” elaborados pela The European Union Agency for Cybersecurity (ENISA), ou em outros modelos similares, desde que mantenham a estrutura de níveis de atendimento supracitados (N1, N2 e N3).

3.5.1. A priorização dos eventos e incidentes cibernéticos pode ser baseada na Instrução Normativa de Gestão de Incidente de Segurança da Informação da PRODEMGE, em modelos de priorização que considerem os níveis de sensibilidade e de criticidade das pessoas de interesse, dos ativos de informação e dos sistemas de TIC da CONSULENTE que possam ser comprometidos pelos incidentes cibernéticos, ou ainda em uma combinação de ambos.

3.5.1.1. A Instrução Normativa de Gestão de Incidente de Segurança da Informação da PRODEMGE será fornecida à PROPONENTE, após a assinatura do contrato, durante a fase de inserção (item 5.50 do termo de consulta)

3.5.2. Como exemplo espera-se a implementação de um modelo como o previsto no documento CSIRT Case Classification, elaborado pelo FIRST. Nesse sentido deve-se implementar 2 níveis de prioridade para os incidentes que envolvam criticidade: N1 e N2. Cada nível estabelece um tempo limite para que seja iniciado o tratamento do incidente denominado Tempo Máximo para Tratamento Inicial (TMTI).

3.5.2.1. A PROPONENTE deverá, com apoio da CONSULENTE e tendo a Instrução Normativa de Tratamento de Incidentes da CONSULENTE como referência, aprimorar a Instrução Normativa e definir um Plano de Tratamento de Incidentes Cibernéticos (PTIC), em até 12 (doze) meses após a assinatura do contrato.

3.6. Uma listagem inicial de Ativos e Sistemas de TIC será fornecida à PROPONENTE, após assinatura do contrato, durante a fase de inserção, (item 5.50 do termo de consulta), para a prestação dos serviços contratados, mas ressaltando que esta lista é dinâmica e será sempre atualizada, formalmente, pela CONSULENTE, durante a vigência do contrato.

4. Condições de prestação dos Serviços Continuados de SOC

4.1. A equipe técnica da PROPONENTE, que será alocada no SOC, deve ser capacitada tecnicamente e dimensionada pela PROPONENTE de modo a atender os serviços técnico, as exigências e as qualificações definidas neste Termo de Consulta e seus anexos.

4.2. A especificação completa relativas aos perfis, quantidades mínimas de profissionais e regimes e janelas de trabalho estão detalhadas no **ANEXO I-K** – Equipe Técnica, deste Termo de Consulta.

4.3. A PROPONENTE deverá manter a escala dos profissionais em serviço por turno (profissionais N1, N2, Supervisor e Gestor) e os contatos atualizados junto à CONSULENTE.

4.3.1. Não haverá remuneração adicional para a PROPONENTE nos casos em que os profissionais da PROPONENTE estiverem em regime de sobreaviso e/ou horas extras.

4.4. O horário e local de prestação dos serviços está detalhado no item 7 do Termo de Consulta.

4.5. **O tratamento aos incidentes e eventos cibernéticos deve respeitar os seguintes prazos:**

4.5.1. **Tempo Máximo para Registro do Incidente (TMRI)**

4.5.1.1. Tem como meta estabelecida trinta (30) minutos para todos os eventos e alertas.

4.5.1.2. Esse tempo inclui a detecção, a triagem, a classificação, a priorização e o registro dos eventos e incidentes cibernéticos nas ferramentas apropriadas.

4.5.2. **Tempo Máximo para Tratamento Inicial do incidente (TMTI-1)**

4.5.2.1. Para os incidentes de criticidade nível 1 o Tempo Máximo para Tratamento Inicial (TMTI-1) tem meta estabelecida em sessenta (60) minutos corridos desde a identificação do incidente (manualmente ou pelas ferramentas/plataformas de monitoração).

4.5.3. **ITMTI2 - Tempo Máximo para Tratamento Inicial do incidente (TMTI-2)**

4.5.3.1. Para os incidentes de criticidade nível 2 o Tempo Máximo para Tratamento Inicial (TMTI-2) tem meta estabelecida em quatro (4) horas corridas desde a identificação do incidente (manualmente ou pelas ferramentas/plataformas de monitoração)

4.6. Os valores acima serão utilizados como indicadores de qualidade que serão utilizados para aferir a qualidade dos serviços prestados, conforme definido nos níveis de serviços detalhados no ANEXO I-H, neste Termo de Consulta.

4.6.1. Os valores definidos para os TMTI-1, TMTI-2 e TMRI poderão, em comum acordo, basearem-se em novas lógicas de cálculo, à medida que haja avanço na maturidade do SOC, evolução da prestação do Serviço e integração com o Service Manager.

4.6.2. Considera-se tratamento inicial as ações de responsabilidade do N1 e N2.

4.6.3. A CONSULENTE utilizará o Service Manager como instrumento para aferição do TMRI, e do TMTI para os diferentes tipos de incidentes e seus respectivos níveis de criticidade.

4.6.4. Importante que fique claro para a PROPONENTE que os tempos de atendimentos dos incidentes TMTI-1 e TMTI-2, definidos no glossário (ANEXO I-G), não se alteram, independente do horário de atendimento, ou seja, o tempo continua sendo contabilizado quando do acionamento do perfil N2, não sendo, em nenhuma hipótese, zerado para uma nova contagem para fins de apuração de atendimento aos indicadores de níveis de serviços estabelecidos.

4.7. **Local de prestação dos serviços**

4.7.1. Conforme detalhado no item “Modelo de Execução do Objeto” do Termo de Consulta.

4.7.2. Independentemente dos cenários, dada a sensibilidade das informações tratadas no contexto dos trabalhos do SOC, é vedado o desempenho dessas tarefas em ambientes de trabalho compartilhados, tal como cafés e coworking;

4.7.3. A prestação do serviço de SOC, quando executada nas dependências da PROPONENTE deve se limitar às estruturas de Data Center e estruturas de CSOC localizadas dentro do território brasileiro;

4.8. Reuniões de acompanhamento

4.8.1. Forma de Acompanhamento: A CONSULENTE e a PROPONENTE realizarão reuniões de acompanhamento, que podem ser presenciais ou remotas, para discutir os detalhes da prestação dos serviços sempre que necessário. No entanto, essas reuniões ocorrerão no mínimo uma vez por semana, de acordo com um calendário definido em conjunto na fase de inserção (item 5.50 do termo de consulta).

4.8.1.1. Na primeira segunda feira útil de cada mês, as reuniões deverão ser realizadas presencialmente, nas instalações da CONSULENTE, sem ônus adicional para a CONSULENTE.

4.8.1.1.1. Esta reunião mensal poderá ser remota, desde que a CONSULENTE, explicitamente, solicitar que a reunião seja remota.

4.8.1.2. As datas poderão ser reagendadas em comum acordo entre CONSULENTE e a PROPONENTE, durante a vigência do contrato.

4.8.2. A PROPONENTE enviará para o e-mail equipe_soc@prodemge.gov.br as atas das reuniões em até 2 (dois) úteis após a realização de cada reunião.

4.9. Workshops

4.9.1. A PROPONENTE deverá realizar workshops e sessões práticas (hands-on) regulares para a transferência de conhecimento sobre os processos e as ferramentas utilizadas, sejam elas disponibilizadas pela CONSULENTE ou pela própria PROPONENTE.

4.9.1.1. Será obrigatório um workshop com hands-on de, no mínimo, três dias úteis, com duração de quatro horas por dia, no 6º, 12º, 18º, 24º e 30º mês do contrato.

4.9.1.2. O tema será definido pela CONSULTANTE em até 2 meses anteriores à realização do Workshop. Os prazos serão definidos em cronograma a ser elaborado entre as partes durante a fase de inserção (item 5.50 do termo de consulta)

5. Canais de Atendimento para o SOC:

5.1. Deverá ser disponibilizado, pela PROPONENTE, no mínimo, um canal de atendimento com a equipe do SOC, em regime integral, 24 (vinte e quatro) horas em 7 (sete) dias na semana e em feriados, 365 dias por ano.

5.2. O Canal de Atendimento deverá ser implementado por meio de ferramentas de comunicação disponibilizadas pela PROPONENTE de modo a garantir a disponibilidade de contato, sendo, no mínimo:

5.2.1. Via aplicativo WhatsApp.

5.2.2. Via E-mail.

5.2.3. Via telefone, com a disponibilização de 2 (dois) números de contato.

5.2.4. Via vídeo conferencia, com plataforma fornecida pela PROPONENTE

5.3. Outros canais de comunicação poderão ser também disponibilizados pela PROPONENTE, desde que com a anuência da CONSULENTE e sem prejuízo ao regime de atendimento especificado neste Termo de Consulta.

6. Relatórios

6.1. A PROPONENTE deverá, durante a vigência do contrato, emitir os seguintes relatórios, que serão avaliados de acordo com indicadores de qualidade, conforme detalhado no ANEXO I-H, deste Termo de Consulta:

Relatório	Periodicidade	Conteúdo
Relatórios Técnicos de	Periodicidade Semanal. Deverão ser entregues às segundas-feiras até às 20:00,	O relatório deve ser composto por informações técnicas detalhadas dos Incidente Verdadeiros Positivos de criticidade nível 1 da semana anterior

Relatório	Periodicidade	Conteúdo
Incidentes (RT-I)	independentemente de ser dia útil ou não. Todas informações serão relativas à semana anterior, de segunda-feira a domingo.	incluindo os relacionados a monitoração do Endpoint da CONSULENTE. O objetivo é aferir os detalhes técnicos das respostas dadas no tratamento inicial aos incidentes de maior criticidade, bem como avaliar a efetividade das soluções encaminhadas pelo N1 e N2 para esse tipo de incidente. Maiores detalhes sobre o Relatório estão detalhados no ANEXO I-H, no indicador de qualidade específico deste relatório.
Relatórios Técnicos de CTI - (RT-CTI)	Periodicidade Semanal. Deverão ser entregues às segundas-feiras até às 20:00, independentemente de ser dia útil ou não. Todas informações serão relativas à semana anterior, de segunda-feira a domingo.	O relatório deve ser composto por informações gerais dos Eventos de Informação e por informações técnicas detalhadas dos Eventos de Aviso e Eventos de Exceção organizados por grupo de ativos de TIC e ativos de informação monitorados. Uma análise contextualizada de tendências deve ser apresentada para os Eventos de Aviso e Eventos de Exceção. O objetivo é aferir os detalhes técnicos do serviço de CTI e utilizar essas informações no processo de tratamento de incidentes do CSOC, bem como na antecipação de ações para enfrentamento de ameaças cibernéticas Maiores detalhes sobre o Relatório estão detalhados no ANEXO I-H, no indicador de qualidade específico deste relatório.
Relatórios Executivos de incidentes (RE-I)	Periodicidade Mensal e Anual. Deverão ser entregues em uma versão mensal, até o 5º (quinto) dia corrido do mês seguinte à prestação dos serviços, e uma versão anual que deverá ser disponibilizada até o 10º (décimo) dia corrido do ano seguinte, independentemente de ser dia útil ou não.	Os RE-I devem trazer as informações consolidadas relativas ao período: Total de Alertas que o SOC recebeu, Número de Incidente Verdadeiros Positivos, Número de Incidente Falso Positivo, Média de Eventos por dia, Média de Incidentes por dia, Número Total de Incidentes organizados por categoria e criticidade, Taxa de cobertura do SIEM em relação aos comportamentos do Mitre ATT&CK, casos de Uso relacionados aos principais comportamentos maliciosos e quantitativos de endpoints que apresentaram problemas e tiveram que ser resolvidos através de chamados. O objetivo é aferir os detalhes gerenciais do serviço de SOC e utilizar essas informações na tomada de decisão com o objetivo de aprimorar os serviços da equipe de SOC forma global.

Relatório	Periodicidade	Conteúdo
		A PROPONENTE poderá ser demandada a apresentar, no RE-I, os valores dos seguintes: Key Performance Indicator (KPI): Mean Alarm Time to Triage (MTTT), Mean Alarm Time to Qualify (MTTQ), Mean Threat Time to Investigate (MTTI), Mean Time to Mitigate (MTTM), Mean Time to Recover (MTTV), Mean Incident Time to Detect (MTTD), Mean Incident Time to Response (MTTR). Maiores detalhes sobre o Relatório estão detalhados no ANEXO I-H, no indicador de qualidade específico deste relatório.
Relatórios Executivos de CTI (RE-CTI)	Periodicidade Mensal e Anual. Deverão ser entregues em uma versão mensal, até o 5º (quinto) dia corrido do mês seguinte à prestação dos serviços, e uma versão anual que deverá ser disponibilizada até o 10º (décimo) dia corrido do ano seguinte, independentemente de ser dia útil ou não.	Os RE-CTI devem trazer as informações consolidadas relativas ao período. São informações importantes para compor esses Relatórios: Média Diária e Mensal de Eventos de Aviso e Eventos de Exceção, Nº de Eventos de Aviso e de Eventos de Exceção por Ativos de TIC e Ativos de Informação monitorados, Tendências Globais de Ataques Cibernéticos para a área de atuação da CONSULENTE. Uma análise contextualizada das tendências baseada nos dados históricos dos Eventos de Aviso e Eventos de Exceção deve ser fornecida no RE-CTI. O objetivo é aferir os detalhes gerenciais do serviço de CTI e utilizar essas informações no processo de tratamento de incidentes do SOC, bem como na antecipação de ações para enfrentamento de ameaças cibernéticas. Maiores detalhes sobre o Relatório estão detalhados no ANEXO I-H, no indicador de qualidade específico deste relatório.
Relatórios de Tendências (RTend)	Periodicidade Mensal e Anual. Deverão ser entregues em uma versão mensal, até o 5º (quinto) dia corrido do mês seguinte à prestação dos serviços, e uma versão anual que deverá ser disponibilizada até o 10º (décimo) dia corrido do ano	As informações que devem constar no RTend são de uma visão de análise de dados das métricas definidas nos RE-I e deve ser apresentado a partir do 2º mês de execução efetiva do serviço de SOC. O objetivo é aferir as tendências das informações definidas no RE-I e, assim, utilizar essas informações na tomada de decisão com o objetivo de aprimorar os serviços da equipe de SOC,

Relatório	Periodicidade	Conteúdo
	seguinte, independentemente de ser dia útil ou não.	inclusive propiciando a antecipação de ações como gestão da capacidade, gestão de compras e contratações de ferramentas aplicáveis à segurança cibernética, bem como o dimensionamento dos recursos humanos vis a vis com as necessidades e as tendências demonstradas no RTend. Maiores detalhes sobre o Relatório estão detalhados no ANEXO I-H, no indicador de qualidade específico deste relatório.
Relatórios Detalhados de Incidentes (RDI)	Periodicidade Mensal. Deverão ser entregues em uma versão mensal, até o 5º (quinto) dia corrido do mês seguinte à prestação dos serviços, independentemente de ser dia útil ou não.	Irá detalhar as atividades prestadas pelo serviço de SOC na gestão de incidentes de segurança cibernética. O RDI deverá conter, obrigatoriamente, as seguintes informações, segregadas por Perfil de Atendimento (N1 e N2): Quantidade de Eventos tratados (somente para o N1), Quantidade de Incidentes tratados, Data/hora do início do incidente de segurança, Nome do responsável pelo atendimento, Descrição do incidente de segurança, Categoria e Criticidade do incidente, Número de identificação do chamado, Descrição da solução oferecida, Data/hora de finalização do incidente de segurança, Detalhamento do tempo em que o incidente ficou registrado em cada status nas ferramentas, Consolidado dos incidentes que não foram atendidos dentro dos prazos estabelecidos na, com suas devidas justificativas fundamentadas O objetivo é aferir a capacidade da PROPONENTE em autogerenciar os três indicadores, quais sejam: Tempo Máximo para Registro do Incidente (TMRI), Tempo Máximo para Tratamento Inicial do evento/incidente de criticidade nível 1 (TMTI-1) e Tempo Máximo para Tratamento Inicial do evento/incidente de criticidade nível 2 (TMTI-2). O instrumento de medição será o prazo definido para a entrega do RDI. A apuração será mensal e irá considerar, individualmente, cada grupo de informação que está definida para constar no RTend. Maiores detalhes sobre o Relatório estão detalhados no ANEXO I-H, no indicador de qualidade específico deste relatório.

Relatório	Periodicidade	Conteúdo
Relatório de Efetividade de Reporte – RER - exclusivo do serviço de CTI	Periodicidade Mensal. Será elaborado pela CONSULENTE, relativo aos serviços de CTI prestados pela PROPONENTE no mês anterior, até o 5º dia útil do mês seguinte à prestação dos serviços e encaminhado para a PROPONENTE, que terá 3 dias úteis para justificar e contestar as discrepâncias apontadas. A CONSULENTE irá avaliar e emitir o relatório final até o final do mês.	Irá evidenciar o descumprimento de níveis de serviços se a PROPONENTE deixar de reportar a CONSULENTE a ocorrência de quaisquer dos eventos listados na tabela 2 do anexo I-B, caso tal evento seja detectado pela CONSULENTE por outros meios. O objetivo é aferir a efetividade da monitoração e reporte das informações de inteligência e contrainteligência de ameaças cibernética que a PROPONENTE se obriga a informar aa CONSULENTE em regime 24x7x365 Essas informações são imprescindíveis para o processo de enriquecimento do tratamento de incidentes cibernéticos do SOC, bem como na antecipação de ações para enfrentamento de ameaças cibernéticas, sendo assim a CONSULENTE carece de se resguardar quanto a inefetividade do monitoramento e reporte dessas informações. Para evidenciar uma ocorrência não relatada pela PROPONENTE, a CONSULTENTE irá registrar um chamado, para análise e justificativa. A PROPONENTE, após a emissão do RER pela CONSULENTE, poderá apresentar suas justificativas para análise da CONSULENTE. Maiores detalhes sobre o Relatório estão detalhados no ANEXO I-H, no indicador de qualidade específico deste relatório.

Tabela 3 – Relatórios do SOC

7. Acesso às plataformas tecnológicas instaladas na CONSULENTE

7.1. **Controle de Acesso**: Todo acesso às plataformas tecnológicas instaladas na CONSULENTE, necessárias para a prestação dos serviços, será restrito apenas ao pessoal autorizado. Este acesso será realizado exclusivamente por meio de acesso remoto às estações de trabalho da CONSULENTE, utilizando credenciais de login e autenticação multifator para garantir a segurança.

7.2. **Comunicação Segura:** Toda comunicação entre o centro de operações e as plataformas do SOC deverá ser criptografada. Isso inclui, mas não se limita a comunicações via rede, transferência de arquivos e quaisquer dados trocados entre as partes. A criptografia deve atender aos padrões de segurança mais rigorosos, garantindo a confidencialidade e a integridade das informações.

___x___

1. Serviços Técnicos Especializados de Segurança da Informação (Lote 2)

1.1. O Lote 2 define um banco de horas de serviços técnicos especializados de segurança da informação, com utilização sob demanda, durante a vigência contratual, sem garantia de execução em sua totalidade.

1.2. Os serviços técnicos deverão ser executados por profissionais qualificados e sempre considerando as melhores práticas do mercado, incluindo normas e regulamentações. O ANEXO I-K detalha o perfil, experiência, formação e conhecimento destes profissionais.

1.3. A PROPONENTE deverá, no mínimo, realizar as seguintes atividades, sem se limitar a elas:

1.3.1. **Análise de Regras e Políticas de Segurança:**

1.3.1.1. Objetivo: Avaliar e revisar regras, normativos e políticas de segurança em vigor na CONSULENTE.

1.3.1.2. Descrição: Conduzir análises de políticas e regras aplicadas a firewall, WAF, IPS, NDR etc, realizar análises forenses e de tráfego de rede para identificar e mitigar riscos e apoiar a CONSULTENTE na elaboração de um Playbook de Segurança da Informação Cibernética.

1.3.2. **Elaboração de Pareceres em Segurança da Informação:**

1.3.2.1. Objetivo: Produzir relatórios detalhados e fundamentados sobre segurança da informação e analisar o nível de maturidade da estratégia de cibersegurança da CONSULTANTE (gestão de segurança e segurança cibernética).

1.3.2.2. Descrição: Realizar estudos e análises aprofundadas sobre aspectos de segurança da informação no ambiente de TIC da CONSULTENTE (on-premises e nuvem), gerar pareceres técnicos que ofereçam recomendações estratégicas baseadas em normas e melhores práticas, além de gap analysis para identificar áreas de melhoria.

1.3.3. **Planos de Melhoria de Infraestrutura de Segurança:**

1.3.3.1. Objetivo: Apoiar a melhoria contínua da infraestrutura de segurança.

1.3.3.2. Descrição: Auxiliar na elaboração de planos de melhoria que otimizem a segurança da infraestrutura existente. Prestar suporte na implementação de novas medidas de segurança.

1.3.4. **Elaboração de Projetos Técnicos:**

1.3.4.1. Objetivo: Desenvolver projetos técnicos destinados a mitigar vulnerabilidades na implantação de novos sistemas de informação, novas plataformas, atualizações de software ou vulnerabilidades detectadas pela CONSULENTE.

1.3.4.2. Descrição: Envolver-se na análise e gestão de vulnerabilidades, com foco em ações preventivas e/ou de remediação. Criar documentação técnica detalhada que aborde as vulnerabilidades identificadas, propondo soluções adequadas.

1.3.5. **Definição e Implementação de Mecanismos de Monitoramento:**

1.3.5.1. Objetivo: Estabelecer e implementar novos mecanismos de monitoramento e recursos de segurança.

1.3.5.2. Descrição: Propor e integrar novos sistemas de monitoramento que se alinhem com as plataformas de segurança da CONSULENTE. Garantir a vigilância contínua e a pronta resposta a incidentes.

1.3.6. **Desenvolvimento de Indicadores de Segurança:**

1.3.6.1. Objetivo: Desenvolver e implantar novos indicadores de desempenho em segurança da informação.

1.3.6.2. Descrição: Criar métricas de segurança que permitam a avaliação contínua do ambiente de TI. Implementar indicadores não previstos anteriormente para cobrir novas ameaças.

1.3.7. **Procedimentos de Auditoria Forense:**

1.3.7.1. Objetivo: Fornecer orientações sobre auditorias forenses no ambiente de TIC.

1.3.7.2. Descrição: Estabelecer procedimentos padronizados para a realização de auditorias forenses. Treinar a equipe da CONSULENTE para conduzir investigações detalhadas e precisas.

1.3.8. **Resposta a Incidentes de Segurança:**

1.3.8.1. Objetivo: Apoiar na resposta eficaz a incidentes de segurança.

1.3.8.2. Descrição: Oferecer suporte especializado na gestão de incidentes de grande vulto. Coordenar ações de contenção, análise e remediação.

1.3.9. **Workshops para transferência de conhecimento**

1.3.9.1. Objetivo: Capacitar a equipe da CONSULENTE através de transferência de conhecimento, via workshops e hands-on.

1.3.9.2. Descrição: Organizar e conduzir workshops e sessões práticas (hands-on) sobre o uso e gerenciamento das principais funcionalidades das plataformas de segurança da CONSULENTE.

2. Processo de emissão da Ordem de Serviço

2.1. Todos serviços serão solicitados por meio de ordem de serviço (OS), que serão avaliadas de acordo com os níveis de serviços definidos no ANEXO I-H.

2.2. O processo de aprovação dos serviços dependerá do tipo de ordem de serviço, de acordo com o objetivo da solicitação:

2.2.1. **Item 1 -** Serviços Técnicos Especializados de Segurança da Informação, **com atendimento em horário comercial (8 x 5), em dias úteis**, sob demanda.

2.2.1.1. São serviços contratados para elaborar diagnósticos, projetos, transferência de conhecimento, consultorias e apoio no uso de plataformas, otimizações de processos.

2.2.2. **Item 2 -** Serviços Técnicos Especializados de Segurança da Informação, **com atendimento 24 x 7 x 365** (24 horas por dia, sete dias por semana, 365 dias por ano), sob demanda.

2.2.2.1. São serviços contratados para apoiar a equipe de segurança da informação da CONSULENTE, nas respostas a incidentes de grande vulto.

2.3. Toda ordem de serviço será formalizada através do preenchimento do formulário definido no Anexo I-F e assinado pela CONSULENTE e PROPONENTE.

2.3.1. A PROPONENTE não poderá iniciar qualquer tipo de atividade sem o recebimento da ordem de serviço, devidamente assinada pela CONSULENTE.

2.3.2. A CONSULENTE poderá abrir mais de uma ordem de serviço, paralela às ordens em execução, a seu critério.

3. Prazos

3.1. **Item 1** - Serviços Técnicos Especializados de Segurança da Informação, com atendimento em horário comercial (8 x 5), em dias úteis, sob demanda**.**

3.1.1. A PROPONENTE terá até **2 (dois) dias úteis**, contados a partir da data de convocação, para agendar a reunião de entendimento da ordem de serviço e a data desta reunião não poderá exceder **4 (quatro) dias úteis** da data de convocação.

3.1.2. Na reunião de entendimento a PROPONENTE e CONSULENTE irão elaborar, em conjunto, um plano de trabalho detalhando o serviço a ser realizado, as entregas previstas, os prazos de execução, perfis dos profissionais envolvidos, planejamento de horas necessárias para o atendimento, critérios de aceite das entregas e se o pagamento será por entrega parcial ou somente após a última entrega.

3.1.3. A PROPONENTE terá **até 2 (dois) dias úteis**, contados a partir da reunião de entendimento para aceitar e assinar a ordem de serviço.

3.1.4. As horas trabalhadas pela PROPONENTE, nesta etapa de aprovação e aceite para execução da ordem de serviço não serão contabilizadas no banco de horas.

3.2. **Item 2** - Serviços Técnicos Especializados de Segurança da Informação, com atendimento 24 x 7 x 365 (24 horas por dia, sete dias por semana, 365 dias por ano), sob demanda.

3.2.1. A PROPONENTE terá até **1 (uma) hora corrida**, contada a partir da data/hora de convocação, para agendar a reunião de entendimento da ordem de serviço e a data/hora desta reunião **não poderá exceder 2 (duas) horas corridas** da data/hora de convocação.

3.2.2. Na reunião de entendimento a PROPONENTE e CONSULENTE irão elaborar, em conjunto, um plano de trabalho detalhando o serviço a ser realizado, as entregas previstas, os prazos de execução, perfis dos

profissionais envolvidos, planejamento de horas necessárias para o atendimento, critérios de aceite das entregas e se o pagamento será por entrega parcial ou somente após a última entrega.

3.2.3. A PROPONENTE irá iniciar o atendimento da ordem de serviço conforme plano de trabalho definido na reunião de entendimento. O aceite da ordem de serviço pela PROPONENTE é imediato, na reunião.

3.2.4. As horas trabalhadas pela PROPONENTE, nesta etapa de aprovação e aceite para execução da ordem de serviço não serão contabilizadas no banco de horas.

4. Execução da Ordem de Serviço

4.1. No início da execução de cada ordem de serviço, a PROPONENTE deverá detalhar e incluir no plano de trabalho as Atividades a serem realizadas, impactos na infraestrutura e arquitetura do ambiente e recomendações para mitigação, caso seja necessário.

4.1.1. A PROPONENTE deverá iniciar a prestação do serviço no prazo estabelecido na própria ordem de serviço.

4.2. Os serviços serão contratados sob demanda, não havendo obrigatoriedade ou compromisso prévio da CONSULENTE na utilização do total ou de parte das horas estimadas para sua realização, competindo exclusivamente a CONSULENTE a decisão sobre suas demandas, conforme sua necessidade e estratégia, sempre condicionada uma entrega, quaisquer que sejam a complexidade das atividades, e sempre com metas, prazos e resultados objetivamente definidos, podendo inclusive haver demandas a serem executadas simultaneamente.

4.2.1. Os serviços serão e remunerados de acordo com preço previamente estabelecido na Ordem de Serviço, independentemente do número de profissionais alocados ou do tempo efetivamente gasto na execução dos serviços.

4.3. Após o término de cada entrega prevista na ordem de serviço, a PROPONENTE deverá:

4.3.1. Apresentar relatório de conclusão dos serviços prestados detalhando todas atividades realizadas.

4.3.2. Entregar toda documentação referente aos serviços prestados, em português, contendo todos os documentos produzidos e gerados no contexto da sua execução.

4.4. O serviço será considerado concluído após a emissão pela CONSULENTE do “laudo técnico de execução de serviços”, definido no Anexo I-E, atestando a execução dos serviços especificados na ordem de serviço.

4.4.1. As horas utilizadas serão deduzidas do total do banco de horas.

4.4.2. Ao final do contrato, as horas não consumidas não poderão ser faturadas.

4.5. Os serviços serão prestados pela PROPONENTE remotamente.

4.5.1. Os serviços podem ser prestados nas dependências da CONSULENTE, mediante comum acordo entre CONSULENTE e PROPONENTE, sem ônus adicional para a CONSULENTE.

4.5.2. Aqueles serviços que demandarem a presença física de profissionais da PROPONENTE nas dependências da CONSULENTE deverão ser combinados em comum acordo e agendados previamente.

5. Local de prestação dos serviços

5.1. Conforme detalhado no item “Modelo de Execução do Objeto” do Termo de Consulta.

5.2. Independentemente dos cenários, dada a sensibilidade das informações tratadas no contexto dos trabalhos do SOC, é vedado o desempenho dessas tarefas em ambientes de trabalho compartilhados, tal como cafés e coworking;

5.2.1. A prestação do serviço de SOC, quando executada nas dependências da PROPONENTE deve se limitar às estruturas de Data Center e estruturas de CSOC localizadas dentro do território brasileiro;

6. Acesso às plataformas tecnológicas instaladas na CONSULENTE

6.1.1.1. **Controle de Acesso**: Todo acesso às plataformas tecnológicas instaladas na CONSULENTE, necessárias para a prestação dos serviços, será restrito apenas ao pessoal autorizado. Este acesso será realizado exclusivamente por meio de acesso

remoto às estações de trabalho da CONSULENTE, utilizando credenciais de login e autenticação multifator para garantir a segurança.

6.1.1.2. **Comunicação Segura:** Toda comunicação entre os especialistas da PROPONENTE e as plataformas serão criptografadas. Isso inclui, mas não se limita a comunicações via rede, transferência de arquivos e quaisquer dados trocados entre as partes. A criptografia deve atender aos padrões de segurança mais rigorosos, garantindo a confidencialidade e a integridade das informações.

___x___

ANEXO I-D – Relatório de apuração de níveis de serviços

Identificação do contrato:

Código do indicador de qualidade:

Período de apuração: ___ /___ /___ a ___ /___ /___

Valor apurado: _____

Desconto no (pagamento) : SIM ou NÃO

( ) desconto de R$_____ (_____) na parcela devida do serviço, conforme estipulado no contrato supracitado.

Detalhamento das infrações dos indicadores de níveis de serviço:

ANEXO I-E – Laudo Técnico de Execução de Serviços **- LOTE 1**

Identificação do contrato:

Lote 1 – Serviços continuados de Centro de Operações de Segurança (Security Operation Center – SOC

- Plataforma em operação:
  - Plataforma Deep/DarkWeb / NDR)
  - Data da instalação: ___/___/___
  - Data do aceite: ___/___/___
  - Descrição dos serviços executados:

- Perfis profissionais para execução dos serviços:
  - Relação dos profissionais das Equipes N1, N2 e/ou supervisores alocados, por turno e Gestor de contrato.
  - Data da entrega de toda documentação: ___/___/___
  - Data do aceite: ___/___/___

- Reuniões realizadas na fase de inserção (item Requisitos Temporais do Termo de Consulta):
  - Minimo de 10 reuniões realizadas
  - Aceite do processo de inserção: ___/___/___

- Relatórios e plano de tratamento de incidentes (PTIC) entregues:
  - Relatório (RTI, RCTI, REI, RECTI, RTEND, RDI), PTIC.
  - Data planejada: __/___/__
  - Data da entrega: ___/___/___

- Workshops de transferência de conhecimento e reuniões de acompanhamento do serviço de SOC realizadas:
  - Workshop / Reunião
  - Data planejada: __/___/__
  - Data da entrega: ___/___/___

- Serviço continuado de SOC executado de acordo com os requisitos de contrato (**SIM/NÃO**)
  - Mês e Ano de execução: MM / AAAA (se pro rata, informar)
  - Descrição dos relatórios entregues e data da entrega:

- Problemas na execução dos serviços:
  - Número do chamado:
  - Data da ocorrência: ___/___/___
  - Data do encerramento: ___/___/___
  - Ações tomadas para regularização e/ou penalização

_____

Nome do responsável técnico da PROPONENTE

_____

ANEXO I-E – Laudo Técnico de Execução de Serviços **– LOTE 2**

Identificação do contrato:

- Perfis profissionais para execução dos serviços:
  - Relação dos profissionais das Equipes N1, N2 e/ou supervisores alocados, por turno e Gestor de contrato.
  - Data da entrega de toda documentação: ___/___/___
  - Data do aceite: ___/___/___

- Serviços Técnicos Especializadas de Segurança da Informação
  - Número da OS:
  - **Item do lote: (1 ou 2)**
  - Entrega(s) realizada(s):
    - Quantidade de horas por entrega:
    - Descrição detalhada dos serviços executados:
    - Data de início da entrega: ___/___/___
    - Data do aceite da entrega: ___/___/___

_____

Nome do responsável técnico da PROPONENTE

_____

Nome do Fiscal do contrato

ANEXO I-F – Solicitação - Ordem de Serviço – Serviços Técnicos Especializados de segurança da informação

Identificação do contrato:

Identificação da Ordem de Serviço

1. Descrição do serviço a ser realizado:
2. Número de horas
3. Descrição das entregas e prazos
4. Outras informações

_____

Nome do responsável técnico da PROPONENTE

_____

Nome do Fiscal do contrato

-----X -----

1. Glossário

1.1. Ambiente mainframe (plataforma alta) – Neste Termo de Consulta é uma plataforma de infraestrutura, constituída por um equipamento mainframe IBM e aplicações desenvolvidas, principalmente, em Natural, Cobol, PL, ADABAS, VSAM e DB2, entre outros softwares.

1.2. Ambiente open (plataforma open) – Neste Termo de Consulta é um ambiente de infraestrutura constituído por servidores da plataforma x86, físicos (Baremetal) e virtuais (VMs), com sistema operacional Linux, plataforma Java e banco de dados Oracle, MySQL, PostgreSQL, SQLServer, MongoBD, mas não se limitando a estes.

1.3. Aplicações Web: São aplicações acessíveis por meio de navegadores web, utilizando uma arquitetura distribuída em camadas. Este conjunto inclui não apenas as aplicações web tradicionais, mas também os Web Services e microsserviços (microservices). São exemplos de Aplicações Web: Sites da Internet e da Intranet.

1.4. Archiving - Arquivamento de dados - Processo de mover arquivos, pouco utilizados do armazenamento primário de sistemas de informações para áreas seguras e de custo reduzido que farão a retenção dessas informações por um longo prazo.

1.5. Assistência técnica – São as atividades de apoio técnico da PROPONENTE com vistas a solucionar problemas, nas sugestões de melhorias, ajustes nas configurações e esclarecimentos de dúvidas.

1.6. Ativos de Informação: Conjunto de pessoas, tecnologias, marcas, nomes de domínios, entre outras informações, que será monitorado pelo serviço de Inteligência de Ameaças Cibernéticas;

1.7. Ativos de TIC: Os meios de armazenamento, transmissão e processamento de dados e informações em meio digital;

1.7.1. São exemplos de Ativos de TIC: Estações de trabalho (Desktops, Laptops etc.), Servidores, Switches, Roteadores, Dispositivos Móveis (Smartphones e Tablets), dispositivos IOT (Impressoras, Câmeras de Monitoramento, Totens etc.), Sistemas Operacionais, Imagens para contêineres hospedadas nas plataformas de gerenciamento de repositórios e Contêineres em execução nas plataformas de gerenciamento de contêineres.

1.8. Backup - Cópia de segurança de dados de uma instância computacional para um ambiente de armazenamento distinto com vistas à recuperação em caso de perda dos dados originais (vide Recovery neste glossário).

1.9. Backup site – É um local alternativo ao data center principal de uma organização, onde são replicados os sistemas mais críticos com o objetivo de mantê-los em operação, mesmo após um incidente que indisponibilize o data center principal (vide Disaster Recovery neste glossário).

1.10. Batch – São programas executados (JOB) sem interação com o usuário final e podem ser agendados para serem ativados conforme os recursos do ambiente operacional permitirem.

1.11. Console de CTI: Interface de consulta amigável para consumo das informações disponibilizadas pela PROPONENTE para o serviço de Inteligência de Ameaças Cibernéticas, atividade prevista nos Serviços Continuados de SOC.

1.12. **CTI (Cyber Threat Intelligence)** - Abrange uma série de práticas que incluem a pesquisa, análise e modelagem de ameaças cibernéticas. O objetivo do CTI é identificar, compreender e mitigar as ameaças antes que elas possam causar danos. Isso é realizado através do monitoramento contínuo de diversas fontes de informações, análise de comportamentos suspeitos e padrões de ataque, e desenvolvimento de estratégias proativas para prevenir e detectar ataques cibernéticos.

1.13. Correção de erro - Qualquer alteração que se fizer no software, inclusive alterações feitas para manter a compatibilidade do sistema, melhoria de operação aprimorada e segurança, bem como soluções de contingência que estabeleçam ou ajudem a restabelecer a funcionalidade substancial com as especificações na documentação referente a esse software.

1.13.1. Em geral, é uma solução provisória para um problema específico do cliente e, normalmente, é fornecida por meio de point patch específico ou hot fix. Uma “Correção” também incluirá quaisquer recomendações ou avisos feitos a um cliente, inclusive recomendações para que um cliente migre para uma versão atual ou novo release, análise do problema no desenvolvimento de uma versão futura do software ou outras medidas para encerrar um atendimento aberto.

1.14. CSP – (Cloud Service Provider) – Provedor de Serviços de Nuvem – São empresas especializadas em disponibilizar, em data centers (públicos ou privados), com redundância, serviços de TIC sob demanda (servidores, armazenamento, rede, de plataformas de software serviços cognitivos e outros serviços especializados (comunicação, desktop, voz, etc). São responsáveis

pelas operações de data center, que dão suporte aos serviços de nuvem (vide Nuvem neste glossário).

1.15. Data center - Instalação construída com o objetivo de alojar recursos de infraestrutura de TIC, como servidores, dispositivos de rede, storage e outros equipamentos. Um datacenter é uma infraestrutura que centraliza as operações e os equipamentos de tecnologia da informação.

1.15.1. Data Center Privado – Instalação alocada para uso exclusivo de uma organização e de suas unidades vinculadas. Sua propriedade e gerenciamento de seus recursos, segurança e operação podem ser realizados pela própria organização, bem como por terceiros ou ambos;

1.15.2. Data Center Público – Instalação onde diversas empresas compartilham os recursos de infraestrutura de TIC. É um modelo no qual os recursos de computação pertencem a uma empresa (vide CSP e Nuvem neste glossário) e são operados por ela, que os compartilha entre vários locatários, com uma separação lógica por cliente.

1.15.3. DDL - Data Definition Language – Artefato que disponibiliza um conjunto de comandos para criação, alteração e remoção de tabelas e outras estruturas em um banco de dados.

1.16. Disaster Recover (DR) – É a capacidade de resposta e recuperação de uma empresa em caso de incidentes em sua infraestrutura de TIC. Os incidentes podem ter origem em acidentes (tempestades, inundações, incêndios etc.) ou atém mesmo em ataques cibernéticos (hackers).

1.16.1. Como prevenção muitas empresas adotam um ambiente de backup site (vide Backup site neste glossário), replicando os sistemas considerados críticos para a organização em outro data center (ou em uma nuvem pública), que, em caso de incidentes darão uma capacidade de resposta rápida e efetiva aos problemas, reduzindo o tempo recuperação dos ambientes de TIC. Importante ressaltar que falhas em sistemas podem levar a contratempos que vão desde a perda de dados até prejuízos financeiros.

1.17. Documentação – Compreende as especificações, a documentação, os manuais e os guias técnicos.

1.18. Evento Cibernético: Qualquer ocorrência identificada em um sistema de TIC, serviço ou Nuvem privada da CONSULENTE, que indique possíveis falhas na aplicação, ou das salvaguardas das informações processadas, armazenadas ou transmitidas, ou ainda, uma situação até então desconhecida, que possa se tornar relevante em termos de segurança cibernética.

1.19. Incidente - Uma interrupção não planejada de um serviço de TI ou uma redução da qualidade de um serviço de TI ou uma falha de um componente de hardware ou software.

1.20. Incidente Cibernético - Ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá, também, ser caracterizada pela tentativa de exploração de vulnerabilidade de um Sistema de TIC da CONSULENTE.

1.21. Instrução Normativa de Gestão de Incidente de Segurança da Informação da PRODEMGE - Define estruturas, meios e formas operativas para segurança no contexto organizacional de forma a garantir a total proteção de informações, pessoas, bens e instalações, assegurando técnicas, conhecimentos, sistemas, processos, produtos ou meios, à integridade e continuidade dos negócios.

1.22. NDR - Network Detection and response (Detecção e Resposta de Rede). É uma ferramenta de cibersegurança que analisa o tráfego de redes corporativas

1.23. **Níveis de Atendimento no SOC** - O atendimento do SOC é classificado em 3 categorias, cada uma com um nível de especialização e responsabilidade na gestão de incidentes de segurança.

1.23.1. **N1 – Primeiro Nível de Suporte** - Realizar a triagem inicial de incidentes de segurança.

1.23.2. **N2 – Segundo Nível de Suporte -** Lidar com incidentes de segurança que requerem um conhecimento técnico mais aprofundado.

1.23.3. **N3 – Terceiro Nível de Suporte -** Gerenciar incidentes altamente técnicos e complexos que exigem conhecimento especializado.

1.24. Nuvem - Plataforma de serviços de hardware e software que permite acesso universal e sob demanda, operados por CSP (vide CSP neste glossário) por intermédio da Internet e/ou links dedicados, a um conjunto de recursos de infraestrutura de TIC configuráveis por um portal (por exemplo: redes, servidores, armazenamento, aplicações, banco de dados), que podem ser rapidamente provisionados e disponibilizados, substituindo e/ou integrando a infraestrutura de TIC tradicional, on-premises (hospedada em data centers próprios).

1.25. Online - São programas executados (JOB) através de interação com o usuário final.

1.26. On-Premises - corresponde a instalação e uso de recursos de infraestrutura de TIC dentro do data center da PRODEMGE (vide Data Center neste glossário).

1.27. Pacote de serviço - conjunto de CORREÇÕES DE ERRO cumulativas para uma determinada VERSÃO ou RELEASE da solução proposta. Um Pacote de Serviços estará disponível na forma de download por meio do Portal Online ou kit de mídia.

1.27.1. Em geral, é instalado como sobreposição do produto (também conhecido como patch). A nomenclatura do Pacote de Serviço está vinculada a versão ou release correspondente. Por exemplo, um Pacote de Serviço relativo à Versão 1.0 será designado como 1.0 SP 1, 1.0 SP 2 etc., e um Pacote de Serviço relativo ao release 2.1 será designado como 2.1 SP1, 2.1 SP2 etc.

1.27.2. Playbook: Para os fins deste edital, entende-se como o conjunto de ações necessárias para realizar o tratamento e a resposta a um determinado incidente. Esse conjunto de ações deve ser o mais automatizado possível.

1.28. Release – Compreende a liberação de um produto de software que pode conter uma pequena funcionalidade da próxima VERSÃO do software, código ou compatibilidade e incorpora todos os PACOTES DE SERVIÇOS e CORREÇÕES DE ERRO anteriores (se houver) desde a última VERSÃO.

1.28.1. Geralmente a liberação requer uma nova instalação, em vez de uma sobreposição para o software já instalado. Salvo disposição em contrário, a liberação está ligada à versão anterior e é designada por um número à direita do ponto decimal, como 1.1, 1.2, 1.3 etc.

1.29. Retenção - Período em que os backups ficam retidos e guardados em um dispositivo de armazenamento.

1.30. Recovery - Restauração de dados e informações de um backup retido em um dispositivo de armazenamento.

1.31. Sistemas de TIC: Aplicativos, Aplicações (Web ou não), Softwares e Sistemas que são executados nos Ativos de TIC;

1.32. São exemplos, mas não se limitando a estes, de Sistemas de TIC: Aplicações Web, Web Services, WebSocket, Aplicações em Contêineres, Gerenciadores de Repositórios de Imagens-Base de Contêineres, Contêineres e Gerenciadores de Contêineres, Banco de Dados (BD) e Sistemas Gerenciadores de Banco de Dados (SGBD), Aplicações de Inteligência Artificial (Machine Learning e Deep Learning), Aplicações Cliente-Servidor e Aplicativos desenvolvidos pelo, ou para a CONSULENTE para dispositivos móveis.

1.33. SOAR: Security Orchestration, Automation and Response é um processo de orquestração, automação e respostas aos eventos e incidentes de segurança cibernética. A CONSULENTE não possui solução dessa natureza implementada.

1.34. **SOC (Security Operations Center)** – Estrutura organizacional, centralizada, responsável pelo monitoramento contínuo de ameaças, pela análise dessas ameaças e pela prevenção e mitigação de incidentes de cibersegurança.

1.35. Solução de Contingência - significa uma solução provisória de um problema e poderá incluir modificações específicas ao software para tratar de problemas críticos (podendo ser denominada também como “hot fixes”).

1.35.1. Em alguns casos, o problema tratado por uma solução de contingência será definitivamente solucionado quando o usuário realizar o próximo upgrade (atualização). A Solução Alternativa em si poderá ser considerada final caso estabeleça uma forma diferente de uso do software pelo usuário, de modo a reduzir substancialmente o impacto de um erro ou defeito.

1.36. Suporte de autoatendimento – Suporte com acesso às ferramentas de autoajuda oferecidas no suporte online, tais como informações sobre compatibilidade de produto, correções publicadas anteriormente, soluções alternativas, documentos informativos e outras soluções de produto.

1.37. Tempo Máximo para Registro do Incidente (TMRI): Compreende a meta estabelecida em minutos para todos os eventos e alertas que serão recebidos pelo SOC N1. Esse tempo inclui a detecção, a triagem, a classificação, a priorização e o registro dos eventos e incidentes cibernéticos.

1.38. Tempo Máximo de Tratamento Inicial (TMTI): Compreende o tempo máximo que o N1 e N2 terão para iniciar o tratamento dos incidentes, de acordo com a categoria e nível de criticidade previamente definidas para os incidentes cibernéticos. Esse tempo começa a contar após o N1 ter transformado determinado Evento Cibernético em Incidente Cibernético.

1.39. TTPs: São as Técnicas, Táticas e Procedimentos utilizados pelos hackers para realizarem seus ataques e alcançarem seus objetivos.

1.40. Upgrade (Atualizações) - incluem revisões de Documentação, correções de erro, pacotes de serviço, versões e releases da solução proposta para o qual é fornecido o suporte técnico, e não incluem opções ou produtos que sejam licenciados separadamente.

1.40.1. Estas Atualizações poderão ser denominadas como “atualizações de produto” ou “atualizações de software”.

1.41. Usuário Administrador - Grupo de usuários com permissão para definir funções e permissões de acesso, parametrizações das tabelas, validação das integrações, acesso aos relatórios de auditoria, execução de backup e recovery.

1.42. Versão – Compreende um RELEASE de um produto de software que contém grandes mudanças na funcionalidade do produto de software, código ou compatibilidade e incorpora as liberações anteriores (se tiverem ocorrido).

1.42.1. Normalmente, a versão requer uma nova instalação, em vez de uma sobreposição para o software já instalado. Salvo disposição em contrário, a Versão é designada pelo número à esquerda do ponto decimal, como 1.0, 2.0, 3.0 etc.

1.43. VPN - Virtual Private Network - Rede privada virtual - é uma rede de comunicações privada, virtual, construída sobre qualquer outra rede de comunicações, utilizando protocolos padrões.

_____x_____

1. Níveis de Serviços

1.1. Suporte técnico:

1.1.1. A PROPONENTE oferecerá, dentro do período de contrato, os serviços de suporte técnico por meio de telefone e e-mail, em idioma Português do Brasil, durante a vigência do contrato.

1.2. Indicadores de Qualidade

1.2.1. Os serviços prestados pela PROPONENTE serão avaliados conforme o quadro com o sumário dos indicadores de qualidade, abaixo relacionado.

#	Indicador	Objeto	Definição	Entrega prevista
01	**ICPR**	Lote 2 - item 2	Indicador de cumprimento de prazo previsto para a reunião de entendimento (item 3 do ANEXO I-C) referente a solicitação de horas técnicas especializadas em regime 24x7x365 (item 2 do lote 2).	Reunião de entendimento da demanda para abertura de uma ordem de serviço
02	**ICPH**	Lote 2 - item 2	Indicador de cumprimento de prazo previsto para início da prestação dos serviços de horas técnicas especializadas (item 3 do ANEXO I-C) referente a solicitação de horas técnicas especializadas em regime 24x7x365 (item 2 do lote 2).	Início de execução de uma ordem de serviço
03	**ICPP**	Lote 2 - itens 1 e 2	Indicador de cumprimento de prazo previsto para execução da Ordem de Serviço técnico **(itens 1 e 2 do lote 2),** conforme detalhado no anexo I-C.	Entregas definidas em uma ordem de serviço
04	**ICPD**	Lote 1 - item único	Indicador de cumprimento de prazo previsto para disponibilização (entrega, instalação e customização) da(s) plataformas de soluções de TIC (Deep/DarkWeb e NDR), referentes aos serviços prestados no lote 1, conforme detalhado no anexo I-B. O indicador será calculado independentemente por plataforma	Plataforma de soluções de TIC instaladas e em produção
05	**ICPM**	Lote 1 - item único	Indicador de cumprimento do percentual de disponibilidade mensal da(s) plataformas de soluções de TIC (Deep/DarkWeb e NDR), relacionadas aos serviços prestados no lote 1, conforme detalhado no anexo I-B. O indicador será calculado independentemente por plataforma	Disponibilidade mensal das plataformas de soluções de TIC
06	**IE-RTI**	Lote 1 - item único	Indicador de cumprimento de prazo de entrega do Relatórios Técnicos de Incidentes (RT-I)	Relatórios Técnicos de Incidentes (RT-I)

#	Indicador	Objeto	Definição	Entrega prevista
07	**IE-RTCTI**	Lote 1 - item único	Indicador de cumprimento de prazo de entrega do Relatórios Técnicos de CTI - (RT-CTI)	Relatórios Técnicos de CTI - (RT-CTI)
08	**IE-REI**	Lote 1 - item único	Indicador de cumprimento de prazo de entrega do Relatórios Executivos de incidentes (RE-I)	Relatórios Executivos de incidentes (RE-I)
09	**IE-RECTI**	Lote 1 - item único	Indicador de cumprimento de prazo de entrega do Relatórios Executivos de CTI (RE-CTI)	Relatórios Executivos de CTI (RE-CTI)
10	**IE-RTEND**	Lote 1 - item único	Indicador de cumprimento de prazo de entrega do Relatórios de Tendências (RTend)	Relatórios de Tendências (RTend)
11	**IE-RDI**	Lote 1 - item único	Indicador de cumprimento de prazo de entrega do Relatórios Detalhados de Incidentes (RDI)	Relatórios Detalhados de Incidentes (RDI)
12	**IE-RER**	Lote 1 - item único	Indicador de qualidade e efetividade da monitoração do serviço de CTI	Relatório de Efetividade de Reporte (RER) - exclusivo do serviço de CTI
13	**IE-PTIC**	Lote 1 - item único	Indicador de cumprimento de prazo de entrega do Plano de Tratamento de Incidentes Cibernéticos	Plano de Tratamento de Incidentes Cibernéticos
14	**ICKNOW**	Lote 1 - item único	Indicador de cumprimento de meta de transferência de conhecimento. O indicador irá considerar a quantidade de workshops não realizados no ano em relação aos definidos nos itens 2 e 4 do ANEXO I-B para cada período de 12 meses de prestação de serviços continuados de SOC.	Workshops realizados
15	**INOT**	Lote 1 - item único	Indicador de cumprimento de meta de reuniões de acompanhamento do serviço continuado de SOC	Reuniões realizadas
16	**ITMRI**	Lote 1 - item único	Indicador de cumprimento de meta para Registro de Incidente no Service Manager	Registro de todos eventos no prazo
17	**ITMTI1**	Lote 1 - item único	Indicador de cumprimento de meta para tratamento de incidente N1	Tratamento de todos incidentes N1 no prazo
18	**ITMTI2**	Lote 1 - item único	Indicador de cumprimento de meta para tratamento de incidente N2	Tratamento de todos incidentes N2 no prazo

1.3. Os mecanismos de cálculo, início de vigência, faixa no ajuste no pagamento, bem como observações aplicáveis constam do detalhamento dos indicadores, abaixo relacionados:

2. Detalhamento dos indicadores de Qualidade

#01 – ICPR – Item 2 do lote 2

ICPR - Indicador de cumprimento de prazo previsto para a reunião de entendimento (item 3 do ANEXO I-C) referente a solicitação de horas técnicas especializadas em regime 24x7x365 (item 2 do lote 2).	
Tópico	Descrição
Finalidade	Mede a quantidade de horas corridas de atraso para a realização da reunião de entendimento, conforme prazos definidos no item 3 do ANEXO I-C exclusivamente para o item 2 do lote 2
Meta a cumprir	ICPR ≤ prazo previsto - Prazo menor ou igual ao prazo previsto no ANEXO I-C.
Instrumento de medição	Data e hora da solicitação para a reunião de entendimento e data e hora da realização da reunião.
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos no item 3 do ANEXO I-C.
Periodicidade	Mensal, para todas reuniões solicitadas no mês para entendimento de uma ordem de serviço
Mecanismos de Cálculo (métrica)	ICPR = PRZ, Onde: PRZ – Prazo para a Reunião – corresponde ao período entre a data/hora da solicitação e data/hora da realização da reunião inicial, entre a CONSULENTE e a PROPONENTE, conforme detalhado no item 3 do ANEXO I-C desse Termo de Consulta.
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.
Início da vigência	Na solicitação do serviço pela CONSULENTE.

ICPR - Indicador de cumprimento de prazo previsto para a reunião de entendimento (item 3 do ANEXO I-C) referente a solicitação de horas técnicas especializadas em regime 24x7x365 (item 2 do lote 2).	
Tópico	Descrição
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para a ordem de serviço. O cálculo do desconto referente a este indicador de qualidade, seguirá as regras abaixo: - Sem desconto, se ICPR menor ou igual a 2 horas corridas - Desconto de 1%, se ICPR maior que 2 horas corridas e menor que 3 horas corridas - Desconto de 1,5%, se ICPR maior que 3 horas corridas e menor que 4 horas corridas - Desconto de 2%, se ICPR maior que 4 horas corridas. Além disto, poderão ser aplicadas sanções conforme estabelecidas no item “Sanções Administrativas” do Termo de Consulta.

#02 – ICPH – Item 2 do lote 2

ICPH - Indicador de cumprimento de prazo previsto para início da prestação dos serviços de horas técnicas especializadas (item 3 do ANEXO I-C) referente a solicitação de horas técnicas especializadas em regime 24x7x365 (item 2 do lote 2).	
Tópico	Descrição
Finalidade	Mede a quantidade de horas corridas de atraso para a início dos serviços da PROPONENTE, conforme prazos definidos na Ordem de Serviço – OS exclusivamente para o item 2 do lote 2.
Meta a cumprir	ICPH ≤ prazo previsto - Prazo menor ou igual ao prazo previsto.
Instrumento de medição	Ordem de serviço e termo de aceite dos serviços prestados
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos na OS.
Periodicidade	Mensal, para todas ordens de serviços iniciadas no mês

ICPH - Indicador de cumprimento de prazo previsto para início da prestação dos serviços de horas técnicas especializadas (item 3 do ANEXO I-C) referente a solicitação de horas técnicas especializadas em regime 24x7x365 (item 2 do lote 2).	
Tópico	Descrição
Mecanismos de Cálculo (métrica)	ICPH = PRI Onde: PRI – Prazo para iniciar os serviços – corresponde ao período entre a data/hora da solicitação e data/hora de início da prestação dos serviços, conforme definido na OS.
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE, ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.
Início da vigência	Na solicitação do serviço pela CONSULENTE.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para a ordem de serviço. O cálculo do desconto referente a este indicador de qualidade, seguirá as regras abaixo: - Sem desconto, se ICPH menor ou igual a 1 hora corrida. - Desconto de 1%, se ICPH maior que 1 hora corrida e menor que 2 horas corridas - Desconto de 1,5%, se ICPH maior que 2 horas corridas e menor que 3 horas corridas - Desconto de 2%, se ICPH maior que 3 horas corridas. Além disto, poderão ser aplicadas sanções conforme estabelecidas no item “Sanções Administrativas” do Termo de Consulta.

#03 – ICPP – Lote 2 (itens 1 e 2)

ICPP - Indicador de cumprimento de prazo previsto para execução da Ordem de Serviço técnico (itens 1 e 2 do lote 2), conforme detalhado no anexo I-C.	
Tópico	Descrição
Finalidade	Mede a quantidade de dias úteis de atraso na execução da Ordem de Serviço (OS) dos itens 1 e 2 do lote 2.

ICPP - Indicador de cumprimento de prazo previsto para execução da Ordem de Serviço técnico (itens 1 e 2 do lote 2), conforme detalhado no anexo I-C.	
Tópico	Descrição
Meta a cumprir	ICPP ≤ prazo previsto - Prazo da execução do serviço menor ou igual aos prazos previstos no cronograma do projeto, definido na reunião de planejamento para execução de uma ordem de serviço, com o objetivo de reduzir o risco de atrasos
Instrumento de medição	Ordem de serviço e termo de aceite dos serviços prestados
Forma de Acompanhamento	A avaliação será feita conforme linha de base do cronograma registrado na OS.
Periodicidade	Mensal, para todas entregas realizadas com aceite de uma ordem de serviço
Mecanismos de Cálculo (métrica)	ICPP = TEX - TEST, Onde: TEX – Tempo de Execução – corresponde ao período de execução da OS, em dias úteis (para o item 1 do lote 2 e em dias corridos para o item 2 do lote 2), da sua data de início até a data de entrega. A data de início será aquela constante na OS. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Consulta. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OS continua a correr, findando-se apenas quanto a PROPONENTE entrega os produtos da OS e haja aceitação por parte do fiscal técnico. TEST – Tempo definido para a execução da OS – conforme estipulado no Termo de Consulta.
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE, ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso. Para cálculo de dias úteis no cômputo do indicador, os dias com expediente parcial na PROPONENTE serão considerados.
Início da vigência	Conforme cronograma definido na OS.

ICPP - Indicador de cumprimento de prazo previsto para execução da Ordem de Serviço técnico (itens 1 e 2 do lote 2), conforme detalhado no anexo I-C.	
Tópico	Descrição
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para a ordem de serviço. O cálculo do desconto referente a este indicador de qualidade, seguirá as regras abaixo: Para as ordens de serviços referentes ao item 1 do lote 2, o prazo será contabilizado em dias úteis. Para as ordens de serviços referentes ao item 2 do lote 2, o prazo será contabilizado em dias corridos. - Sem desconto, se ICPP ≤ prazo previsto (dias) - Desconto de 1%, se prazo previsto + 1 dia ≤ ICPP < prazo previsto + 11 dias - Desconto de 2%, se prazo previsto + 11 dias ≤ ICPP < prazo previsto + 21 dias - Desconto de 3%, se prazo previsto + 21 dias ≤ ICPP < prazo previsto + 31 dias - Desconto de 4%, se ICPP > prazo previsto + 30 dias. Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#04 – ICPD – Lote 1

ICPD - Indicador de cumprimento de prazo previsto para disponibilização (entrega, instalação e customização) da(s) plataformas de soluções de TIC (Deep/DarkWeb e NDR), referentes aos serviços prestados no lote 1, conforme detalhado no anexo I-B. O indicador será calculado independentemente por plataforma	
Tópico	Descrição
Finalidade	Mede a quantidade de dias corridos de atraso na instalação e disponibilização, para cada uma das plataformas (Deep/DarkWeb e NDR), conforme detalhado no ANEXO I-B, deste Termo de Consulta
Meta a cumprir	ICPD ≤ prazo previsto - Prazo da execução do serviço menor ou igual aos prazos previstos no cronograma do projeto, com o objetivo de reduzir o risco de atrasos.

ICPD - Indicador de cumprimento de prazo previsto para disponibilização (entrega, instalação e customização) da(s) plataformas de soluções de TIC (Deep/DarkWeb e NDR), referentes aos serviços prestados no lote 1, conforme detalhado no anexo I-B. O indicador será calculado independentemente por plataforma	
Tópico	Descrição
Instrumento de medição	Termo de aceite da disponibilização por plataforma, emitido pela CONSULENTE.
Forma de Acompanhamento	A avaliação será feita conforme linha de base do cronograma, por plataforma.
Periodicidade	Mensal, até o aceite da disponibilização de cada plataforma.
Mecanismos de Cálculo (métrica)	ICPD = TEX - TEST, Onde: TEX – Tempo de Execução – corresponde ao período entre a assinatura do contrato e a data da disponibilidade da plataforma. A data de disponibilização deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Consulta. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução continua a correr, findando-se apenas quando a PROPONENTE disponibilizar a plataforma e haja aceitação por parte do fiscal técnico. TEST – Tempo definido para a disponibilização da plataforma conforme cronograma definido pelas partes.
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE, ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.
Início da vigência	Conforme cronograma definido entre as partes, por plataforma.

ICPD - Indicador de cumprimento de prazo previsto para disponibilização (entrega, instalação e customização) da(s) plataformas de soluções de TIC (Deep/DarkWeb e NDR), referentes aos serviços prestados no lote 1, conforme detalhado no anexo I-B. O indicador será calculado independentemente por plataforma	
Tópico	Descrição
Faixas de ajuste no pagamento e sanções	Meta não atingida, por plataforma, implicará em desconto no valor do pagamento previsto para o mês de entrega e aceite e todos demais meses seguintes até o aceite da disponibilização da plataforma. O cálculo do desconto referente a este indicador de qualidade, seguirá as regras abaixo, por plataforma: - Sem desconto, se ICPD ≤ prazo previsto (dias corridos) - Desconto de 2%, se prazo previsto + 1 dia ≤ ICPD < prazo previsto + 11 dias corridos - Desconto de 5%, se prazo previsto + 11 dias ≤ ICPD < prazo previsto + 21 dias corridos - Desconto de 8%, se prazo previsto + 21 dias ≤ ICPD < prazo previsto + 31 dias corridos - Desconto de 10%, se ICPD > prazo previsto + 30 dias corridos. Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#05 – ICPM – Lote 1

ICPM - Indicador de cumprimento do percentual de disponibilidade mensal da(s) plataformas de soluções de TIC (Deep/DarkWeb e NDR), relacionadas aos serviços prestados no lote 1, conforme detalhado no anexo I-B. O indicador será calculado independentemente por plataforma	
Tópico	Descrição
Finalidade	Mede o percentual de disponibilidade mensal, por plataforma, conforme requisitos detalhados no ANEXO I-B, deste Termo de Consulta.
Meta a cumprir	ICPM ≤ Percentual de disponibilidade mensal prevista
Instrumento de medição	Relatórios de monitoramento e registros de chamado.

ICPM - Indicador de cumprimento do percentual de disponibilidade mensal da(s) plataformas de soluções de TIC (Deep/DarkWeb e NDR), relacionadas aos serviços prestados no lote 1, conforme detalhado no anexo I-B. O indicador será calculado independentemente por plataforma	
Tópico	Descrição
Forma de Acompanhamento	Cada tempo de falha (downtime) será calculado considerando a data e hora de registro do chamado da CONSULENTE e de seu contingenciamento/finalização ou por paralisações registradas pelo sistema de monitoramento da plataforma. O somatório dos tempos de falha (Sdown) será dado pela soma de todos os tempos de falha ocorridos no mês de medição, sejam eles concluídos ou em estando ainda em aberto.
Periodicidade	Mensal, após o aceite da disponibilização da plataforma.
Mecanismos de Cálculo (métrica)	ICPM = ((Tdisp - Sdown) / Tdisp) * 100 Onde: ICPM = Disponibilidade mensal da plataforma, medida em %. Tdisp = Tempo acordado para funcionamento do equipamento em horas, referente ao mês de medição considerando o horário de 24 x 7, todos os dias, inclusive feriados e finais de semana. Sdown = Somatório dos tempos de falha (downtime), em horas, considerando o horário de 24 x 7, todos os dias, inclusive feriados e finais de semana.
Observações	Importante ressaltar que no cálculo da variável “Sdown” não serão consideradas as paradas planejadas: • Paradas planejadas são manutenções previamente agendadas, através de comunicação formal entre a CONSULENTE e a PROPONENTE, para manutenções na solução. • Estas paralisações devem ser solicitadas com um mínimo de 5 (cinco) dias úteis de antecedência, ou de comum acordo entre as partes. • Somente serão consideradas como gravidades se excederem os prazos pactuados para a manutenção e a responsabilidade por esta falha for comprovadamente da PROPONENTE Também não serão considerados no cálculo da variável “Sdown”, os problemas decorrentes de falhas ocasionadas comprovadamente pela CONSULENTE ou de comum acordo entre as partes.
Início da vigência	Este indicador somente será aferido após o aceite da disponibilização da plataforma (entrega, instalação e customização).

ICPM - Indicador de cumprimento do percentual de disponibilidade mensal da(s) plataformas de soluções de TIC (Deep/DarkWeb e NDR), relacionadas aos serviços prestados no lote 1, conforme detalhado no anexo I-B. O indicador será calculado independentemente por plataforma	
Tópico	Descrição
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade, será feito por plataforma e seguirá as regras abaixo: - Sem desconto, se 98% ≤ ICPM - Desconto de 1%, se 95% ≤ ICPM < 98% - Desconto de 1,5%, se 90% ≤ ICPM < 98% - Desconto de 2%, se ICPM < 90%. Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#06 – IE-RTI – Lote 1

IE-RTI - Indicador de cumprimento de prazo de entrega do Relatórios Técnicos de Incidentes (RT-I)	
Tópico	Descrição
Finalidade	Aferir os detalhes técnicos das respostas dadas no tratamento inicial aos incidentes de maior criticidade, bem como avaliar a efetividade das soluções encaminhadas pelo N1 e N2 para esse tipo de incidente.
Meta a cumprir	IE-RTI ≤ prazo previsto - Prazo menor ou igual ao prazo previsto.
Instrumento de medição	Será o prazo definido para a entrega do RT-I. O relatório é semanal e a apuração irá considerar cada incidente cibernético, de criticidade nível 1, individualmente. A entrega somente será considerada com o termo de aceite dos serviços prestados.
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos.
Periodicidade	Mensal. A apuração irá considerar todos relatórios semanais, que deverão ser entregues às segundas-feiras até às 20:00, independentemente de ser dia útil ou não. Todas informações serão relativas à semana anterior, de segunda-feira a domingo.

IE-RTI - Indicador de cumprimento de prazo de entrega do Relatórios Técnicos de Incidentes (RT-I)	
Tópico	Descrição
Mecanismos de Cálculo (métrica)	QTAZ (em horas) = Quantidade de horas de atraso na entrega do relatório. Calcular apenas quando DER1 > DER2 (calcular em minutos, dividir por 60 e desconsiderar quando menor que 0,5) DER1 = data, horas e minutos na entrega do relatório DER2 = data, horas e minutos previstos para a entrega do relatório IE-RTI = Somatório das horas de atrasos da entrega dos relatórios previstos no mês (Somatório de todos QTAZ >0,5 ocorridos no mês).
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se IE-RTI = 0 - Desconto de 0,0008% de desconto por cada hora de atraso (IE-RTI) Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#07 – IE-RTCTI – Lote 1

IE-RTCTI - Indicador de cumprimento de prazo de entrega do Relatórios Técnicos de CTI - (RT-CTI)	
Tópico	Descrição
Finalidade	Aferir os detalhes técnicos do serviço de CTI e utilizar essas informações no processo de tratamento de incidentes do SOC, bem como na antecipação de ações para enfrentamento de ameaças cibernéticas.
Meta a cumprir	IE-RTCTI ≤ prazo previsto - Prazo menor ou igual ao prazo previsto.

IE-RTCTI - Indicador de cumprimento de prazo de entrega do Relatórios Técnicos de CTI - (RT-CTI)	
Tópico	Descrição
Instrumento de medição	Será o prazo definido para a entrega do RT-CTI. O relatório é semanal e irá considerar, individualmente, cada grupo de ativos de TIC e de ativos de informação para constar no RT-CTI. A entrega somente será considerada com o termo de aceite dos serviços prestados.
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos.
Periodicidade	Mensal. A apuração irá considerar todos relatórios semanais, que deverão ser entregues às segundas-feiras até às 20:00, independentemente de ser dia útil ou não. Todas informações serão relativas à semana anterior, de segunda-feira a domingo.
Mecanismos de Cálculo (métrica)	QTAZ (em horas) = Quantidade de horas de atraso na entrega do relatório. Calcular apenas quando DER1 > DER2 (calcular em minutos, dividir por 60 e desconsiderar quando menor que 0,5) DER1 = data, horas e minutos na entrega do relatório DER2 = data, horas e minutos previstos para a entrega do relatório IE-RTCTI = Somatório das horas de atrasos da entrega dos relatórios previstos no mês (Somatório de todos QTAZ >0,5 ocorridos no mês).
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se IE-RTCTI = 0 - Desconto de 0,0008% de desconto por cada hora de atraso (IE-RCTI) Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#08 – IE-REI – Lote 1

IE-REI - Indicador de cumprimento de prazo de entrega do Relatórios Executivos de incidentes (RE-I)	
Tópico	Descrição
Finalidade	Aferir os detalhes gerenciais do serviço de SOC e utilizar essas informações na tomada de decisão com o objetivo de aprimorar os serviços da equipe de SOC forma global A PROPONENTE poderá ser demandada a apresentar, no RE-I, os valores dos seguintes: Key Performance Indicator (KPI): Mean Alarm Time to Triage (MTTT), Mean Alarm Time to Qualify (MTTQ), Mean Threat Time to Investigate (MTTI), Mean Time to Mitigate (MTTM), Mean Time to Recover (MTTV), Mean Incident Time to Detect (MTTD), Mean Incident Time to Response (MTTR).
Meta a cumprir	IE-REI ≤ prazo previsto - Prazo menor ou igual ao prazo previsto.
Instrumento de medição	Será o prazo definido para a entrega do relatório mensal e anual. A entrega somente será considerada com o termo de aceite dos serviços prestados.
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos.
Periodicidade	Mensal. Deverão ser entregues em uma versão mensal, até o 5º (quinto) dia corrido do mês seguinte à prestação dos serviços, e uma versão anual que deverá ser disponibilizada até o 10º (décimo) dia corrido do ano seguinte, independentemente de ser dia útil ou não.
Mecanismos de Cálculo (métrica)	Para cada relatório, mensal e anual, calcular: QTAZ (em horas) = Quantidade de horas de atraso na entrega do relatório. Calcular apenas quando DER1 > DER2 (calcular em minutos, dividir por 60 e desconsiderar quando menor que 0,5) DER1 = data, horas e minutos na entrega do relatório DER2 = data, horas e minutos previstos para a entrega do relatório IE-REI = Somatório das horas de atrasos da entrega dos relatórios previstos para o mês (Somatório de todos QTAZ >0,5 ocorridos no mês).
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.

IE-REI - Indicador de cumprimento de prazo de entrega do Relatórios Executivos de incidentes (RE-I)	
Tópico	Descrição
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se IE-REI = 0 - Desconto de 0,0008% de desconto por cada hora de atraso (IE-REI) Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#09 – IE-RECTI – Lote 1

IE-RECTI - Indicador de cumprimento de prazo de entrega do Relatórios Executivos de CTI (RE-CTI)	
Tópico	Descrição
Finalidade	Aferir os detalhes gerenciais do serviço de CTI e utilizar essas informações no processo de tratamento de incidentes do SOC, bem como na antecipação de ações para enfrentamento de ameaças cibernéticas.
Meta a cumprir	IE-RECTI ≤ prazo previsto - Prazo menor ou igual ao prazo previsto.
Instrumento de medição	Será o prazo definido para a entrega do relatório mensal e anual. A apuração será mensal e anual e irá considerar, individualmente, cada grupo de ativos de TIC e de ativos de informação para constar no RE-CTI. A entrega somente será considerada com o termo de aceite dos serviços prestados.
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos.
Periodicidade	Mensal. Deverão ser entregues em uma versão mensal, até o 5º (quinto) dia corrido do mês seguinte à prestação dos serviços, e uma versão anual que deverá ser disponibilizada até o 10º (décimo) dia corrido do ano seguinte, independentemente de ser dia útil ou não.

IE-RECTI - Indicador de cumprimento de prazo de entrega do Relatórios Executivos de CTI (RE-CTI)	
Tópico	Descrição
Mecanismos de Cálculo (métrica)	Para cada relatório mensal e anual calcular: QTAZ (em horas) = Quantidade de horas de atraso na entrega do relatório. Calcular apenas quando DER1 > DER2 (calcular em minutos, dividir por 60 e desconsiderar quando menor que 0,5) DER1 = data, horas e minutos na entrega do relatório DER2 = data, horas e minutos previstos para a entrega do relatório IE-RECTI = Somatório das horas de atrasos da entrega dos relatórios previstos para o mês (Somatório de todos QTAZ >0,5 ocorridos no mês).
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se IE-RECTI = 0 - Desconto de 0,0008% de desconto por cada hora de atraso (IE-RECTI) Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#10 – IE-RTEND – Lote 1

IE-RTEND - Indicador de cumprimento de prazo de entrega do Relatórios de Tendências (RTend)	
Tópico	Descrição
Finalidade	Aferir as tendências das informações definidas no RE-I e, assim, utilizar essas informações na tomada de decisão com o objetivo de aprimorar os serviços da equipe de SOC, inclusive propiciando a antecipação de ações como gestão da capacidade, gestão de compras e contratações de ferramentas aplicáveis à segurança cibernética, bem como o dimensionamento dos recursos humanos vis a vis com as necessidades e as tendências demonstradas no RTend.
Meta a cumprir	IE-RTEND ≤ prazo previsto - Prazo menor ou igual ao prazo previsto.

IE-RTEND - Indicador de cumprimento de prazo de entrega do Relatórios de Tendências (RTend)	
Tópico	Descrição
Instrumento de medição	Será o prazo definido para a entrega do RTend. A apuração será mensal. A entrega somente será considerada com o termo de aceite dos serviços prestados
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos.
Periodicidade	Mensal. Deverão ser entregues em uma versão mensal, até o 5º (quinto) dia corrido do mês seguinte à prestação dos serviços, e uma versão anual que deverá ser disponibilizada até o 10º (décimo) dia corrido do ano seguinte, independentemente de ser dia útil ou não.
Mecanismos de Cálculo (métrica)	Para cada relatório mensal e anual calcular: QTAZ (em horas) = Quantidade de horas de atraso na entrega do relatório. Calcular apenas quando DER1 > DER2 (calcular em minutos, dividir por 60 e desconsiderar quando menor que 0,5) DER1 = data, horas e minutos na entrega do relatório DER2 = data, horas e minutos previstos para a entrega do relatório IE-RTEND = Somatório das horas de atrasos da entrega dos relatórios previstos para o mês (Somatório de todos QTAZ >0,5 ocorridos no mês).
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se IE-RTEND = 0 - Desconto de 0,0008% de desconto por cada hora de atraso (IE-RTEND) Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#11 – IE-RDI – Lote 1

IE-RDI - Indicador de cumprimento de prazo de entrega do Relatórios Detalhados de Incidentes (RDI)	
Tópico	Descrição
Finalidade	Aferir a capacidade da PROPONENTE em autogerenciar os três indicadores, quais sejam: Tempo Máximo para Registro do Incidente (TMRI), Tempo Máximo para Tratamento Inicial do evento/incidente de criticidade nível 1 (TMTI-1) e Tempo Máximo para Tratamento Inicial do evento/incidente de criticidade nível 2 (TMTI-2).
Meta a cumprir	IE-RDI ≤ prazo previsto - Prazo menor ou igual ao prazo previsto.
Instrumento de medição	Será o prazo definido para a entrega do RDI. A apuração será mensal e irá considerar, cada grupo de ativos de TIC e de ativos de informação para constar no RTend. A entrega somente será considerada com o termo de aceite dos serviços prestados
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos.
Periodicidade	Mensal. Deverão ser entregues em uma versão mensal, até o 5º (quinto) dia corrido do mês seguinte à prestação dos serviços, independentemente de ser dia útil ou não.
Mecanismos de Cálculo (métrica)	QTAZ (em horas) = Quantidade de horas de atraso na entrega do relatório. Calcular apenas quando DER1 > DER2 (calcular em minutos, dividir por 60 e desconsiderar quando menor que 0,5) DER1 = data, horas e minutos na entrega do relatório DER2 = data, horas e minutos previstos para a entrega do relatório IE-RDI = Somatório das horas de atrasos da entrega dos relatórios previstos para o mês (Somatório de todos QTAZ >0,5 ocorridos no mês).
Observações	Atrasos decorrentes de atividades de responsabilidade da CONSULENTE ou de comum acordo entre as partes e devidamente documentados, deverão ser desprezados no cálculo de atraso.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.

IE-RDI - Indicador de cumprimento de prazo de entrega do Relatórios Detalhados de Incidentes (RDI)	
Tópico	Descrição
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se IE-RDI = 0 - Desconto de 0,0008% de desconto por cada hora de atraso (IE-RDI) Além disto, poderão ser aplicadas sanções conforme previstas no item "Sanções Administrativas" do Termo de Consulta.

#12 – IE-RER – Lote 1

IE-RER - Indicador de qualidade e efetividade da monitoração do serviço de CTI	
Tópico	Descrição
Finalidade	Aferir a efetividade da monitoração e reporte das informações de inteligência e contrainteligência de ameaças cibernética que a PROPONENTE se obriga a informar à CONSULENTE em regime 24x7x365. Essas informações são imprescindíveis para o processo de enriquecimento do tratamento de incidentes cibernéticos do SOC, bem como na antecipação de ações para enfrentamento de ameaças cibernéticas, sendo assim a CONSULENTE irá se resguardar avaliando a efetividade dos serviços de monitoramento e reporte dessas informações, pela PROPONENTE.
Meta a cumprir	IE-RER = ZERO
Instrumento de medição	Análise das informações contidas no RT-CTI, bem como no RE-CTI, vis a vis com informações de inteligência cibernética obtidas por outros meios e que sejam relevantes para o ambiente cibernético da CONSULENTE. Cada ocorrência detectada pela CONSULENTE, para qualquer um dos eventos listados na tabela 2 do anexo I-B e que não tiver sido reportado pela PROPONENTE, será considerado uma falha. Consideram-se relevantes aquelas informações de inteligência cibernéticas que devam constar nos reportes por estarem relacionadas aos grupos de ativos de TIC e ativos de informação especificados nesse Termo de Consulta. A apuração será mensal e irá considerar, individualmente, cada grupo de ativos de TIC e de ativos de informação no RT-CTI e RE-CTI. A PROPONENTE terá 5 dias úteis após o recebimento do relatório para apresentar suas justificativas em relação às evidências detalhadas no relatório.

IE-RER - Indicador de qualidade e efetividade da monitoração do serviço de CTI	
Tópico	Descrição
Forma de Acompanhamento	A avaliação será feita conforme meta a cumprir e irá considerar cada evento cibernético detectado pela CONSULENTE individualmente
Periodicidade	Mensal. O relatório será elaborado pela CONSULENTE, comparando os serviços de CTI prestados pela PROPONENTE vis a vis com os eventos detectados pela CONSULENTE, relativos ao mês anterior da emissão do relatório.
Mecanismos de Cálculo (métrica)	IE-RER = Quantidade de eventos cibernéticos do serviço de CTI, não detectados pela PROPONENTE no mês.
Observações	Eventos discrepantes resultantes de atividades de responsabilidade da CONSULENTE, ou acordadas em comum entre as partes e devidamente documentadas, não deverão ser consideradas no cálculo
Início da vigência	A partir do 2o. mês da disponibilização da plataforma de buscas Deep/DarkWeb, pela PROPONENTE e aceite pela CONSULENTE.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês de emissão do relatório (que trata das discrepâncias registradas no mês anterior). O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se IE-RER= 0 - Desconto de 0,25% por evento discrepante do serviço CTI listado no relatório de efetividade de reporte (RER) após o aceite do relatório pela PROPONENTE. Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#13 – IE-PTIC – Lote 1

IE-PTIC - Indicador de cumprimento de prazo de entrega do Plano de Tratamento de Incidentes Cibernéticos	
Tópico	Descrição
Finalidade	Aferir se o plano de tratamento de incidentes cibernéticos foi entregue até o 12º Mês de contrato, conforme previsto no ANEXO I-B deste Termo de Consulta.
Meta a cumprir	Entrega o Plano de tratamento de incidentes cibernéticos no prazo acordado
Instrumento de medição	Laudo técnico de aceite da entrega do PTIC

IE-PTIC - Indicador de cumprimento de prazo de entrega do Plano de Tratamento de Incidentes Cibernéticos	
Tópico	Descrição
Forma de Acompanhamento	A avaliação será feita conforme prazos definidos.
Periodicidade	Uma única vez. No 13o. mês de vigência do contrato e todos meses subsequentes, até o aceite da entrega pela CONSULENTE.
Mecanismos de Cálculo (métrica)	DEE = Data de entrega do PTIC DEP = Data máxima prevista para a entrega do PTIC Se DEE < DEP então IE-PTIC = ZERO caso contrário, IE-PTIC = DEE - DEP
Observações	O relatório será elaborado pela PROPONENTE, em conjunto com a CONSULENTE e entregue em até 12 meses após a assinatura do contrato, conforme detalhado no ANEXO I-B. Atrasos decorrentes da CONSULENTE e devidamente documentados serão descontados no cálculo do indicador.
Início da vigência	a partir da assinatura do contrato
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto do mês da entrega do PTIC. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se IE-PTIC = ZERO - Desconto de 0,04 % por dia corrido de atraso na entrega do PTIC. Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#14 – ICKNOW – Lote 1

ICKNOW - Indicador de cumprimento de meta de transferência de conhecimento. O indicador irá considerar a quantidade de workshops não realizados no ano em relação aos definidos nos itens 2 e 4 do ANEXO I-B para cada período de 12 meses de prestação de serviços continuados de SOC.	
Tópico	Descrição
Finalidade	Aferir o nível de capacitação contínua com o qual os profissionais de segurança cibernética são requeridos, com vistas a fazerem frente a contínua evolução do cenário de ameaças cibernéticas a que a organização está exposta.
Meta a cumprir	Efetuar todos workshops planejados, conforme detalhado no Anexo I-B por ano.
Instrumento de medição	Laudo técnico de realização do WorkShop.
Forma de Acompanhamento	A avaliação será feita conforme metas previstas. O indicador será calculado com o somatório dos workshops realizados, sem distinção dos itens 2 e 4 versus a quantidade de workshops planejados para o ano.
Periodicidade	Anual, no 13o. mês, no 25o. mês e no 36o. mês de prestação de serviços continuados de SOC.
Mecanismos de Cálculo (métrica)	QWP = Quantidade de Workshops planejados nos 12 meses anteriores, exceto a última avaliação que será realizada no último mês de vigência do contrato. QWR = Quantidade de Workshops realizados nos 12 meses anteriores, exceto a última avaliação que será realizada no último mês de vigência do contrato. ICKNOW = QWP - QWR
Observações	O planejamento dos workshops, base de referência da métrica, pode ser alterado de comum acordo entre as partes.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se ICKNOW = ZERO - Desconto de 0,5% por workshop não realizado (ICKNOW) no valor do pagamento previsto no mês de apuração. Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#15 – INOT – Lote 1

INOT - Indicador de cumprimento de meta de reuniões de acompanhamento do serviço continuado de SOC	
Tópico	Descrição
Finalidade	Aferir se as reuniões gerenciais entre CONSULENTE e PROPONENTE, definidas no ANEXO I-B, foram realizadas de acordo com a agenda estabelecida, garantindo a participação de todos os membros relevantes e a conclusão dos objetivos propostos.
Meta a cumprir	Efetuar todas reuniões planejadas no mês.
Instrumento de medição	Atas das reuniões
Forma de Acompanhamento	A avaliação será feita conforme meta a cumprir e comparar o planejamento de reuniões acordado versus reuniões realizadas
Periodicidade	Mensal, considerando todas reuniões semanais e mensal planejada para cada mês.
Mecanismos de Cálculo (métrica)	QNP = Quantidade de reuniões planejados no mês anterior. QNR = Quantidade de reuniões realizadas no mês anterior. INOT = QNP - QNR = Quantidade de reuniões planejadas não realizadas no mês
Observações	O planejamento das reuniões, base de referência da métrica, pode ser alterado de comum acordo entre as partes.
Início da vigência	A partir da assinatura do contrato
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se INOT = ZERO - Desconto de 0,5% por reunião não realizada (INOT) Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#16 – ITMRI – Lote 1

ITMRI – Indicador de cumprimento de meta para Registro de Incidente no Service Manager	
Tópico	Descrição
Finalidade	Aferir a agilidade e assertividade na triagem inicial dos eventos de segurança cibernética
Meta a cumprir	Tem como meta registrar todos eventos e alertas em até 5 (cinco) minutos. A tolerância mensal será de 150 minutos de atraso considerando todos eventos registrados no mês de referência. Esse tempo inclui a detecção, a triagem, a classificação, a priorização e o registro dos eventos e incidentes cibernéticos
Instrumento de medição	O instrumento de medição serão as ferramentas (ex: SIEM, Service Manager entre outras) que venham ser utilizadas.
Forma de Acompanhamento	A avaliação será feita conforme meta a cumprir e irá considerar cada evento/incidente cibernético individualmente
Periodicidade	Mensal
Mecanismos de Cálculo (métrica)	QMR (em minutos) = DHM2 – DHM1 = quantidade de minutos no registro de um evento QMR5 = Quantidade de minutos atrasados no registro de um evento. Calculado apenas quando QMR > 5 minutos. DHM1 = data, hora e minuto de coleta do log (evidência) do alerta DHM2 = data, hora e minuto do registro do incidente/evento ITMRI = Somatório dos minutos de atrasos de todos registros ocorridos no mês (Somatório de todos QMR5 ocorridos no mês).
Observações	Os eventos registrados com atraso em função da ferramenta de registro de incidentes não estar disponível ou acessível e a responsabilidade deste problema for da CONSULENTE, os atrasos não poderão ser incluídos no cálculo.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item “REQUISITOS TEMPORAIS” do Termo de Consulta.

ITMRI – Indicador de cumprimento de meta para Registro de Incidente no Service Manager	
Tópico	Descrição
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se ITMRI < 150 minutos no mês - Desconto de 0,0003% por minuto de atraso (ITMRI) Além disto, poderão ser aplicadas sanções conforme previstas no item "Sanções Administrativas" do Termo de Consulta.

#17 – ITMTI1 – Lote 1

ITMTI1 - Indicador de cumprimento de meta para tratamento de incidente N1	
Tópico	Descrição
Finalidade	Aferir a agilidade e efetividade no tratamento inicial executado pelo N1
Meta a cumprir	Tem como meta atender todos incidentes N1 em até 60 (sessenta) minutos após o registro. A tolerância mensal será de 240 minutos de atraso considerando todos incidentes N1 registrados no mês de referência. Esse tempo inclui as medidas iniciais de investigação, enriquecimento, mitigação ou elevação do incidente ao N2.
Instrumento de medição	O instrumento de medição serão as ferramentas (ex: SIEM, Service Manager entre outras) que venham ser utilizadas.
Forma de Acompanhamento	A avaliação será feita conforme meta a cumprir e irá considerar cada evento/incidente cibernético individualmente
Periodicidade	Mensal
Mecanismos de Cálculo (métrica)	QMN1 (em minutos) = DHM2 - DHM1 = quantidade de minutos para tratamento inicial de incidentes N1 QMZ1 = Quantidade de minutos atrasados no tratamento inicial de um incidente. Calculado apenas quando QMN1 > 60 minutos. DHM1 = data, hora e minuto do registro do incidente/evento DHM2 = data, hora e minuto da aplicação das medidas iniciais de tratamento e mitigação ou de elevação para o N2 ITMTI1 = Somatório dos minutos de atrasos de todos incidentes tratados no N1, ocorridos no mês (Somatório de todos QMZ1 ocorridos no mês).

ITMTI1 - Indicador de cumprimento de meta para tratamento de incidente N1	
Tópico	Descrição
Observações	Os eventos registrados com atraso em função da ferramenta de registro de incidentes não estar disponível ou acessível e a responsabilidade deste problema for da CONSULENTE, os atrasos não poderão ser incluídos no cálculo.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se ITMTI1 < 240 minutos no mês - Desconto de 0,0025% por minuto de atraso (ITMTI1) Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

#18 – ITMTI2 – Lote 1

ITMTI2 - Indicador de cumprimento de meta para tratamento de incidente N2	
Tópico	Descrição
Finalidade	Aferir a agilidade e efetividade no tratamento inicial executado pelo N2
Meta a cumprir	Tem como meta atender todos incidentes N2 em até 240 (duzentos e quarenta) minutos após o registro. A tolerância mensal será de 240 minutos de atraso considerando todos incidentes N2 registrados no mês de referência. Esse tempo inclui as medidas iniciais de investigação, enriquecimento, mitigação ou elevação do incidente ao N3.
Instrumento de medição	O instrumento de medição serão as ferramentas (ex: SIEM, Service Manager entre outras) que venham ser utilizadas.
Forma de Acompanhamento	A avaliação será feita conforme meta a cumprir e irá considerar cada evento/incidente cibernético individualmente
Periodicidade	Mensal

ITMTI2 - Indicador de cumprimento de meta para tratamento de incidente N2	
Tópico	Descrição
Mecanismos de Cálculo (métrica)	QMN2 (em minutos) = DHM2 - DHM1 = quantidade de minutos para tratamento de incidentes N2 QMZ2 = Quantidade de minutos atrasados no tratamento de um incidente N2. Calculado apenas quando QMN2 > 240 minutos. DHM1 = data, hora e minuto da transferência do incidente/evento para o N2 DHM2 = data, hora e minuto da aplicação das medidas para tratamento e mitigação do incidente ou elevação do incidente ao N3 ITMTI2 = Somatório dos minutos de atrasos de todos incidentes tratados no N2, ocorridos no mês (Somatório de todos QMZ2 ocorridos no mês).
Observações	Os eventos registrados com atraso em função da ferramenta de registro de incidentes não estar disponível ou acessível e a responsabilidade deste problema for da CONSULENTE, os atrasos não poderão ser incluídos no cálculo.
Início da vigência	Somente após o aceite da CONSULENTE para início da prestação de serviços, conforme definido no item "REQUISITOS TEMPORAIS" do Termo de Consulta.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento previsto para o mês. O cálculo do desconto referente a este indicador de qualidade seguirá as regras abaixo: - Sem desconto, se ITMTI2 < 240 minutos no mês - Desconto de 0,0025% por minuto de atraso (ITMTI2) Além disto, poderão ser aplicadas sanções conforme previstas no item “Sanções Administrativas” do Termo de Consulta.

3. Considerações gerais:

3.1. Em caso de não atingimento dos níveis de serviços por motivo de força maior, a CONSULENTE poderá analisar as justificativas fundamentadas apresentadas pela PROPONENTE, podendo, a seu critério, aceitar as justificativas, desde que embasadas em evidências razoáveis encontradas nas alegações da PROPONENTE.

3.2. O valor do desconto no pagamento será ponderado em função do desempenho mensal alcançado por cada um dos indicadores, individualmente.

3.2.1. Caso a PROPONENTE atinja todas metas de maneira integral, conforme indicadores de qualidade evidenciarem, não haverá desconto no pagamento dos serviços prestados.

3.2.2. Caso a PROPONENTE, na execução dos serviços, não atinja todas as metas, o abatimento será calculado individualmente por indicador de qualidade, e o resultado final do abatimento será a soma dos valores individuais de abatimento definidos para cada indicador de qualidade (os descontos são cumulativos).

3.3. Em caso de meta não atingida por 2 (dois) meses seguidos, sem uma justificativa plausível, a CONSULENTE poderá abrir processo punitivo contra a PROPONENTE, conforme previsto no item "Sanções Administrativas" do Termo de Consulta.

3.4. Especificamente para os serviços definidos no Lote 1 – Serviços Continuados de SOC, o limite de desconto mensal não poderá ser superior a 20% sobre o valor da prestação mensal do serviço.

3.4.1. Em caso de eventual saldo devedor, caso ultrapasse este limite supracitado, este será aplicado na fatura do mês subsequente, à exceção do último mês de vigência do contrato.

3.4.2. Para o último mês de vigência do contrato, a apuração deverá ser antecipada de maneira que os descontos sejam aplicados na última fatura do contrato.

4. Valor do desconto no pagamento dos serviços

4.1. Lote 1

4.1.1. Valor total do desconto = Somatório dos descontos previstos nos indicadores abaixo:

ID	Indicadores
#04	ICPD
#05	ICPM
#06	IE-RTI
#07	IE-RTCTI
#08	IE-REI
#09	IE-RECTI
#10	IE-RTEND
#11	IE-RDI
#12	IE-RER
#13	IE-PTIC

ID	Indicadores
#14	ICKNOW
#15	INOT
#16	ITMRI
#17	ITMTI1
#18	ITMTI2

4.2. **Lote 2**

4.2.1. Valor total do desconto = Somatório dos descontos previstos nos indicadores abaixo:

ID	Indicadores	Observações
#01	ICPR	Referente aos serviços previstos no item 2
#02	ICPH	Referente aos serviços previstos no item 2
#03	ICPP	Referente aos serviços previstos nos itens 1 e 2

5. Registro de falha na prestação do serviço

5.1. Se a CONSULENTE identificar um problema na prestação dos serviços continuados de SOC de incidentes e não conseguir entrar em contato com a PROPONENTE, a CONSULENTE irá abrir um chamado.

5.1.1. Estes chamados servirão para registrar formalmente que não houve atendimento conforme o previsto em contrato, permitindo assim documentar a situação para futuras referências e/ou sanções administrativas cabíveis conforme previsto neste Termo de Consulta.

5.1.2. Este registro incluirá detalhes como:

5.1.2.1. Data e hora do problema: Quando o problema foi identificado.

5.1.2.2. Descrição do problema: Detalhamento específico do que foi encontrado.

5.1.2.3. Tentativas de contato: Registro das tentativas de contato com a PROPONENTE, incluindo datas, horários e métodos utilizados (e-mails, telefonemas, etc.).

5.1.2.4. Consequências: Impacto do problema identificado nas operações, prazos ou resultados esperados.

5.2. Se a CONSULENTE identificar uma discrepância de seu monitoramento na Deep/DarkWeb e o monitoramento realizado pela PROPONENTE, na prestação dos serviços continuados de SOC para CTI, a CONSULENTE irá abrir um chamado.

5.2.1. Estes chamados servirão para registrar formalmente a discrepância, conforme o previsto em contrato, permitindo assim documentar a situação para futuras referências e/ou sanções administrativas cabíveis conforme previsto neste Termo de Consulta.

5.2.2. Este registro incluirá detalhes como:

5.2.2.1. Data e hora do problema: Quando o problema foi identificado.

5.2.2.2. Descrição do problema: Detalhamento específico do que foi encontrado.

5.2.3. A PROPONENTE poderá justificar a discrepância do monitoramento e a CONSULENTE irá avaliar se irá considerar a justificativa para incluí-lo ou não no Relatório de Efetividade de Reporte (RER), definido no ANEXO I-B e aplicar o indicador de qualidade IE-RER, definido neste anexo.

5.3. Ao formalizar este processo, asseguramos a transparência e a responsabilidade na comunicação e resolução de problemas, garantindo que todas as etapas e esforços sejam devidamente documentados.

5.3.1. A PROPONENTE deverá disponibilizar, para abertura (registro) de chamados, no mínimo, número de telefone, e-mail (mensagem eletrônica) ou site para contato.

5.3.1.1. No caso de ligações telefônicas, o número para contato para a abertura/registro de chamados deverá ser único.

5.3.1.2. O serviço de atendimento e gerenciamento de chamados da PROPONENTE deverá funcionar em regime 24 x 7, todos os dias, incluindo finais de semana e feriados.

5.3.1.3. O atendimento telefônico sempre que aplicável e viável, deverá ser realizado no idioma português do Brasil, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800) e deverá ter um único número de contato.

5.3.1.4. A CONSULENTE poderá efetuar um número ilimitado de chamados técnicos para a PROPONENTE, por qualquer uma das formas disponíveis, durante a vigência do contrato.

5.3.2. O contingenciamento do chamado será confirmado através do aceite pela CONSULENTE, desde que incluso as seguintes informações:

5.3.2.1. Código alfanumérico de identificação do chamado.

5.3.2.2. Data e hora de conclusão do contingenciamento.

5.3.2.3. Descrição detalhada do serviço executado.

5.3.3. Para as plataformas de soluções de TIC disponibilizadas, em caso de adoção de solução de contingência, sem prejuízo de uma solução definitiva cabível, a PROPONENTE deve emitir laudos, na periodicidade exigida pela CONSULENTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva.

5.3.3.1. O chamado deverá continuar aberto, com status de contingenciado, até sua solução definitiva, que poderá vir com correções de código, nova release ou atualização de versão.

5.3.4. A conclusão definitiva de cada chamado, será confirmada através do aceite pela CONSULENTE do atendimento correspondente, conforme formulário definido no Anexo I-E, deste Termo de Consulta.

_____x_____

1. Especificação técnica da plataforma de busca na Deep/DarkWeb

1.1. A PROPONENTE deverá disponibilizar, durante a vigência do contrato, uma plataforma de solução tecnológica, doravante denominada PLATAFORMA Deep/DarkWeb, que será utilizada para o serviço continuado de SOC, na atividade inteligência de ameaças cibernéticas entre outras, executado através de busca contínua em Deep/DarkWeb, internet aberta, páginas de compartilhamento, redes sociais e aplicativos monitorados.

1.2. A PLATAFORMA Deep/DarkWeb poderá ser disponibilizada nas dependências da CONSULENTE (on-premises) ou da PROPONENTE. (em Nuvem ou nas próprias dependências) e deverá ser implementada em uma arquitetura de infraestrutura redundante, garantindo uma disponibilidade mínima de 99,8%, 24 x 7 x 365 (24 horas, 7 dias por semana, 365 dias por ano).

1.2.1. É de responsabilidade da PROPONENTE a monitoração da PLATAFORMA Deep/DarkWeb, bem como a gestão, suporte e manutenção.

1.2.2. A PLATAFORMA Deep/DarkWeeb deverá ser integrada com o Systems Manager da CONSULENTE, registrando automaticamente alertas e eventos cibernéticos para o SOC.

1.2.3. A monitoração da PLATAFORMA Deep/DarkWeb também deverá gerar alertas para o Systems Manager da CONSULENTE.

1.2.4. Os níveis de serviços que serão avaliados durante a prestação dos serviços, estão definidos no ANEXO I-H deste Termo de Consulta.

1.3. Em qualquer um dos cenários, toda infraestrutura de hardware e software da PLATAFORMA Deep/DarkWeb será de responsabilidade da PROPONENTE e, independente do cenário adotado.

1.3.1. Todo software deve estar devidamente licenciado, em linha de produção do fabricante, com direito a suporte e atualização de versão, sem ônus para a CONSULENTE.

1.3.2. Todo hardware deve estar em linha de produção do fabricante, com direito a suporte, manutenção corretiva e substituição de peças, sem ônus para a CONSULENTE.

1.3.3. A PLATAFORMA Deep/DarkWeb também deverá atender aos requisitos do programa Energy Star ou similar, de eficiência energética.

2. Funcionalidades da PLATAFORMA

2.1. A PLATAFORMA Deep/DarkWeb irá gerar eventos que terão como produtos a detecção de citações, termos ou referências aos ativos de informação e de TIC monitorados, seja na Deep/DarkWeb, na internet aberta, em páginas de compartilhamento, redes sociais e aplicativos monitorados.

2.1.1.1. É de responsabilidade da PROPONENTE avaliar se todos os insumos para a geração dos eventos estão sendo repassados corretamente para a PLATAFORMA Deep/DarkWeb.

2.1.1.2. Caso a PROPONENTE identifique a ausência de insumos necessários para a geração dos eventos, será reponsabilidade da PROPONENTE a correção e/ou habilitação de tal insumo. A CONSULENTE, sempre que solicitada, repassará para a PROPONENTE as informações necessárias para aprimorar este processo.

2.1.1.3. Dar-se-á então o passo de classificação do evento, também de responsabilidade da PROPONENTE. A CONSULENTE fará processo de revisão e pode determinar a alteração de categorias dos eventos.

2.1.2. O serviço disponibilizado pela PLATAFORMA Deep/DarkWeb não deverá limitar a quantidade de recursos pesquisados e deverá:

2.1.2.1. Prover pesquisa direcionada através da monitoração de palavras pré-selecionadas fornecidas;

2.1.2.2. Possibilitar que se monitore ameaças emergentes e se avalie a aplicabilidade, especificamente no ambiente da CONSULENTE, com o objetivo de prevenir a exploração de alguma vulnerabilidade de segurança.

2.1.2.3. Possuir modelos de filtro de informações pré-configurados, personalizados de acordo com comportamentos conhecidos dos usuários na utilização das diferentes fontes de informação monitoradas.

2.1.2.3.1. Possibilitar salvar os resultados das pesquisas já realizadas e apresentar os dados filtrados em painéis com as principais fontes identificadas na busca.

2.1.2.4. Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas.

2.1.2.5. Prover um campo de descrição em que os analistas de segurança cibernética da CONSULENTE, ou da PROPONENTE, possam contextualizar as informações associadas aos eventos.

2.1.2.6. Apresentar a descoberta de páginas web de "*phishing*", utilizando o nome dos recursos pesquisados, a marca, identidade visual, domínios e ativos de informação que serão protegidas;

2.1.2.7. Apresentar a verificação de sites suspeitos de *phishing* para domínios solicitados pela CONSULENTE, ou que tenham sido levantados pela PROPONENTE. Para essa verificação deve-se utilizar, entre outras, as seguintes entidades reguladoras: ICANN (*Internet Corporation for Assigned Names and Numbers*) e Registro.Br (Registro de Domínios para a Internet do Brasil);

2.1.2.8. Apresentar a detecção de domínios recentemente registrados que possam oferecer riscos e serem utilizados de forma maliciosa contra a CONSULENTE como, por exemplo:

2.1.2.8.1. Variações comuns de nomes;

2.1.2.8.2. Permutações de caracteres;

2.1.2.8.3. Desvio de URL (typosquatting).

2.1.3. A PLATAFORMA Deep/DarkWeb deverá possuir interface de fácil visualização para demonstrar os resultados das buscas por cada categoria de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de mensagens instantâneas, Deep/DarkWeb);

2.1.3.1. Deverá possibilitar consultas sobre vulnerabilidades relacionadas aos ativos de TIC da CONSULENTE que retornem informações como: valor do *Common Vulnerability Scoring System* (CVSS); CVSS associado à vulnerabilidade; Nível de maturidade de *exploits*, caso existam;

2.1.3.2. Possuir facilidade de exploração da vulnerabilidade, caso existam exploits e o impacto da exploração da vulnerabilidade;

2.1.3.3. Deverá registrar os eventos cibernéticos no Systems Manager da CONSULENTE.

2.1.3.4. **Deverá permitir pesquisar nos seguintes contextos, sem se limitar a estes:**

2.1.3.4.1. Ameaças cibernéticas;

2.1.3.4.2. Resposta a incidentes**;**

2.1.3.4.3. Prevenção de perdas de dados;

2.1.3.4.4. Proteção de Marca;

2.1.3.4.5. Risco de Terceiros;

2.1.3.4.6. Fraude**;**

2.1.3.4.7. Quaisquer outras fontes disponíveis, ou que venham a se tornar disponíveis.

2.1.3.5. A Console da PLATAFORMA Deep/DarkWeb deverá permitir gerar consultas previamente cadastradas, sob demanda, reportando:

2.1.3.5.1. Intenções de ataques que tenham como objetivo os ativos de informação monitorados ou a área de atuação da CONSULENTE;

2.1.3.5.2. Campanhas relevantes de “hacktivismo”, como por exemplos ataques crescentes cujos alvos são, em sua maioria, órgão públicos ou de governo, ou ainda campanhas de ataques em que a vulnerabilidade explorada possa estar presente nas tecnologias implantadas na CONSULENTE. Bem como as campanhas de "hacktivismo" que tenham como alvo a área de atuação da CONSULENTE.

2.1.3.5.3. Intenção de executar atividades fraudulentas, ou mesmo aquelas já em curso, relacionadas aos recursos pesquisados;

2.1.3.5.4. Pessoas envolvidas em atividades criminosa, contraventora ou imoral contra a CONSULENTE e sua área de atuação;

2.1.3.5.5. Códigos maliciosos (malwares) direcionados contra os ativos de informação monitorados;

2.1.3.5.6. Discussões online que divulguem de forma primária ou repliquem informações que possam ser utilizadas para executar ataques cibernéticos, inclusive engenharia social e ciber-extorsão, contra qualquer dos ativos de informação monitorados.

2.1.3.6. As funcionalidades de pesquisa deverão permitir, no mínimo:

2.1.3.6.1. Retornar os seguintes campos: contexto pesquisado, data, idioma, endereço Deep/DarkWeb, conteúdo original completo;

2.1.3.6.2. Salvar o resultado para posterior verificação.

2.1.3.6.3. Gerar pesquisas por, no mínimo, intervalo de data, contexto, metadados e tipo da fonte.

2.1.3.6.4. Permitir que os resultados exibidos sejam ordenados conforme o interesse do usuário sendo ordenáveis por data e hora da ocorrência mais recente para a mais antiga, e por tema, ameaça, entre outros;

2.1.3.6.5. Atualizar automaticamente o resultado de pesquisas anteriormente realizadas com alertas visuais dessas atualizações;

2.1.3.6.6. Disponibilizar uma tela com informações consolidadas para visualização das pesquisas realizadas e alertas cadastrados;

2.1.3.6.7. Gerar arquivos resultantes das pesquisas, a critério da CONSULENTE, nos formatos JSON, HTML, PDF, CSV, H5, Planilha eletrônica e DOCX, ou em outros formatos aderentes ao E-Ping.

2.2. **Da Confidencialidade, Integridade e Disponibilidade dos dados.**

2.2.1. A PLATAFORMA Deep/DarkWeb deverá permitir acesso através de API e Console, por meio de login e senha, com as seguintes características:

2.2.1.1. Devem ser disponibilizados no mínimo de 7 (sete) usuários com acessos simultâneos;

2.2.1.2. Um dos acessos simultâneos deve ser disponibilizado via API, preferencialmente API REST, para integração aos demais processos do SOC;

2.2.1.3. Deve ser capaz de receber chamadas REST API via serviço web utilizando o protocolo HTTPS com TLS 1.2 com autenticação no mínimo: chave, senha e certificado;

2.2.1.4. A CONSULENTE poderá solicitar a alteração de login e senha do acesso conforme a sua necessidade;

2.2.1.5. A autenticação para acesso ao sistema deverá contar com duplo fator de autenticação (2FA), oferecendo, no mínimo, uma das opções: E-mail ou *One Time Password* (OTP).

2.2.1.6. A opção de duplo fator de autenticação por meio de SMS deverá ser completamente implementada pela PROPONENTE, e o efetivo envio de mensagens deve ocorrer sem qualquer custo adicional para a CONSULENTE.

2.2.2. A PROPONENTE deverá, no uso da PLATAFORMA Deep/DarkWeb:

2.2.2.1. Implementar os controles necessários para que apenas os seus profissionais, bem como os usuários e grupos criados pela CONSULENTE, tenham acesso às pesquisas realizadas e aos dados armazenados;

2.2.2.2. Se responsabilizar pela guarda das informações coletadas por período a ser definido pela CONSULENTE, durante toda vigência do contrato;

2.2.3. A PLATAFORMA Deep/DarkWeb deverá gerar cópias de segurança dos dados coletados em razão dos ativos de informação monitorados, de forma a permitir ao menos a restauração das pesquisas realizadas e de seus resultados.

2.2.3.1. Essas informações, quando solicitadas pela CONSULENTE, devem ser disponibilizadas pela PROPONENTE, para download pela CONSULENTE, de forma segura e criptografada, nos formatos JSON, HTML, PDF, CSV, H5, Planilha eletrônica e DOCX, ou em outros formatos aderentes ao E-Ping, à critério da CONSULENTE.

2.2.4. A PLATAFORMA Deep/DarkWeb também deverá permitir gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todas as contas de usuários.

2.2.4.1. Os registros de logs devem conter, no mínimo, a data e hora do evento, origem de acesso, usuário, hostname do equipamento e ação/pesquisa efetuada.

2.2.4.2. Os logs também poderão ser exportados conforme padrões definidos no item anterior.

_____x_____

ANEXO I-J – Especificação técnica da PLATAFORMA NDR

2.3. A PROPONENTE deverá disponibilizar, durante a vigência do contrato, uma plataforma de solução tecnológica, doravante denominada PLATAFORMA NDR, que será utilizada pelos Serviços Continuados de SOC.

2.4. A PLATAFORMA NDR poderá ser disponibilizada nas dependências da CONSULENTE (on-premises) ou em nuvem pública (CSP como SAAS), implementada em uma arquitetura de infraestrutura redundante, garantindo uma disponibilidade mínima de 99,8%, 24 x 7 x 365 (24 horas, 7 dias por semana, 365 dias por ano).

2.4.1. É de responsabilidade da PROPONENTE a monitoração da PLATAFORMA NDR, bem como a gestão, suporte e manutenção.

2.4.2. Os níveis de serviços que serão avaliados durante a prestação dos serviços, estão definidos no ANEXO I-H deste Termo de Consulta.

2.5. Em qualquer um dos cenários, toda infraestrutura de hardware e software da PLATAFORMA NDR será de responsabilidade da PROPONENTE e, independente do cenário adotado.

2.5.1. Todo software deve estar devidamente licenciado, em linha de produção do fabricante, com direito a suporte e atualização de versão, sem ônus para a CONSULENTE.

2.5.2. Todo hardware deve estar em linha de produção do fabricante, com direito a suporte, manutenção corretiva e substituição de peças, sem ônus para a CONSULENTE.

2.5.3. Se a plataforma for instalada nas dependências da CONSULENTE, o hardware utilizado deverá atender os requisitos do programa Energy Star ou similar, de eficiência energética.

2.5.4. A PLATAFORMA NDR deverá ser integrada com o Systems Manager da CONSULENTE, registrando automaticamente alertas e eventos cibernéticos para o SOC.

2.5.5. A monitoração da PLATAFORMA NDR também deverá gerar alertas para o Systems Manager da CONSULENTE.

3. Funcionalidades da PLATAFORMA NDR

3.1. A tabela abaixo relaciona os requisitos e funcionalidades da PLATAFORMA NDR. A PROPONENTE deverá informar os requisitos que são atendidos totalmente, parcialmente ou não atendidos

3.2. Para os requisitos não atendidos ou atendidos parcialmente a PROPONENTE deverá sugerir, se possível, a alteração necessária para atendimento. A CONSULENTE irá avaliar a possibilidade ou não destas alterações em reunião posterior.

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
1	**Características Gerais da Solução**	
1.1	A CONTRATADA será responsável pelo fornecimento de todo o hardware e software necessários para a completa sustentação e funcionamento da solução ofertada. Isso inclui, mas não se limita a:	
1.1.1	Hardware: equipamentos como servidores, storages, dispositivos de rede, computadores e quaisquer outros dispositivos essenciais para a operação da solução. Qualquer que seja o hardware ofertado para a operacionalização da solução, será empregado durante a vigência do contrato, com devolução à CONTRATADA em até 30 (trinta) dias úteis após o término da vigência do contrato. A CONTRATADA terá a obrigação de manter o equipamento em perfeito estado de conservação e funcionamento, garantindo a manutenção preventiva e corretiva. Quaisquer danos ao equipamento serão de responsabilidade da CONTRATADA. Além disso, a CONTRATADA será responsabilizada por quaisquer danos causados a terceiros decorrentes do uso do equipamento durante a prestação do serviço, isentando a CONTRATANTE de responsabilidades por incidentes que ocorram em função da utilização do equipamento.	
1.1.2	Software: licenças de sistemas operacionais, sistemas de gerenciamento, bancos de dados, ferramentas de segurança e quaisquer outros softwares requeridos para a instalação, operação, manutenção e gestão da solução.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
1.1.3	Garantia e Suporte Técnico: a CONTRATADA deverá assegurar que todos os equipamentos de hardware e software fornecidos terão suporte técnico especializado, além de garantir as atualizações e a manutenção de cada item pelo período de vigência do contrato.	
1.1.4	Compatibilidade e Integração: todos os componentes de hardware e software fornecidos deverão ser compatíveis e integrados entre si para assegurar o pleno funcionamento da solução conforme as especificações técnicas.	
1.2	A CONTRATADA será a única responsável por qualquer ônus adicional decorrente da necessidade de fornecimento de hardware e software além do previsto inicialmente, visando garantir o funcionamento completo e contínuo da solução ofertada.	
1.3	Deverá ser capaz de fornecer visibilidade 24 horas por dia, 7 dias por semana, para todas as atividades, dispositivos e serviços de infraestrutura de rede e transações em nível de aplicação.	
1.4	Deverá ser construída a partir da premissa de que a ameaça já está presente no ambiente da CONTRATANTE e utilizar o tráfego da rede como fonte para identificar as ameaças.	
1.5	Deverá possuir sensores físicos ou virtuais, instalados na rede da CONTRATANTE para coletar, processar e gerar metadados a partir do tráfego de rede e enviar tais metadados para a solução de análise baseada em nuvem, permitindo a rápida consulta e contextualização das ameaças.	
1.6	Deverá permitir que a CONTRATANTE implemente processo de investigação, threat hunting e forense de rede com base em metadados da solução utilizando funcionalidades de detecção e investigação.	
1.7	Deverá ser licenciada com capacidade para suportar o tráfego de 20Gbps ou monitorar em tempo real até 10.000 ativos, de acordo com o modelo de licenciamento estabelecido pelo fabricante.	
1.8	Deverá ser escalável e não sofrer degradação de desempenho em função do grande volume de dados coletados, processados e armazenados.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
1.9	Deverá implementar a detecção de anomalias utilizando machine learning, combinado com inteligência de ameaças para fornecer detecções em tempo real	
1.10	Deverá ser capaz de identificar ações de agentes maliciosos nos ativos da PRODEMGE	
1.11	Deverá alertar para comportamentos anômalos ou comportamentos suspeitos dos usuários.	
1.12	Deverá ser capaz de analisar todo o tráfego proveniente de, no mínimo, Flow de rede DNS ou Syslog.	
2	**Arquitetura**	
2.1	Deverá ser implantado por meio do monitoramento passivo do tráfego de rede.	
2.2	Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches.	
2.3	Deverá ser implantado sem agentes nos endpoints, dispositivos de rede e em cloud pública.	
2.4	Deverá ser capaz de coletar, armazenar e analisar o tráfego de rede em tempo real, por meio de inspeção das camadas 2 a 7	
2.5	Deverá realizar as análises e prover alertas em tempo real, utilizando sensores físicos ou virtuais.	
2.6	Deverá oferecer suporte técnico a recursos de SPAN modernos (VXLAN e port mirroring), para que não seja necessário implantar um dispositivo virtual em cada servidor de hypervisor físico para visibilidade.	
2.7	Deverá oferecer detecção continua de ameaças e gerar contexto visando identificar a causa raiz e realizar o bloqueio da ameaça.	
2.8	Appliances virtuais (no local ou na nuvem) deverão ter exatamente as mesmas funcionalidades e versões de software que os dispositivos físicos.	
2.9	Os sensores virtuais deverão ter suporte técnico para ambientes virtuais Vmware, Hyper-V, ESXi e KVM	
2.10	Deverá ser uma solução dedicada ao monitoramento do tráfego de rede, não serão aceitos módulos ou funcionalidades adicionais de soluções de SIEM, Firewall, EDR, XDR e outros.	
2.11	A plataforma deverá fornecer a mesma visibilidade com os sensores, independentemente das implantações, escritórios remotos, data centers físicos, nuvem privada ou nuvem pública.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
2.12	Deverá fornecer visibilidade de tráfego em nuvens públicas (GCP, AWS, Azure, Oracle e Huawei).	
2.13	Deverá ser capaz de processar o tráfego 24 horas por dia, 7 dias por semana, continuamente com 90 dias de armazenamento de todas as métricas coletadas dentro de uma única plataforma.	
3	**Gerenciamento (Dashboards) e Relatórios**	
3.1	A plataforma deverá possuir console de gerenciamento centralizada, permitindo controlar todos os elementos que compõem a solução, os sensores físicos, virtuais, implementados on premise, em nuvem privada ou pública e os componentes de armazenamento físicos ou virtuais.	
3.2	A console de monitoramento centralizada deverá possuir interface de gerenciamento acessada de forma segura via web, sendo que, para a implementação on premise, é possível instalar o componente de gerenciamento de forma virtual.	
3.3	Deverá disponibilizar dashboards com visões analíticas das detecções.	
3.4	Deverá permitir extrair relatórios de análise do tráfego.	
3.5	Deverá identificar todos os dispositivos presentes no tráfego monitorado de forma automática.	
3.6	Deverá identificar e monitorar as comunicações entre os diferentes dispositivos.	
3.7	Deverá fornecer uma lista de todos os dispositivos identificados e permitir a análise detalhada, considerando dados históricos e em tempo real (independentemente da existência de detecções).	
3.8	Deverá permitir que o usuário inclua critérios de agrupamento de ativos de forma manual.	
3.9	Não deverá depender exclusivamente da configuração de listas de endereços IP estáticos para agrupamento de dispositivos.	
3.10	Deverá permitir que sejam gerados relatórios, alertas e detalhamentos sobre os grupos de dispositivos, independentemente se os grupos foram criados dinamicamente ou manualmente.	
3.11	Deverá permitir a visibilidade de ameaças do tráfego de forma centralizada mesmo que haja muitos appliances de visibilidade distribuídos em ambientes de nuvem pública e privada.	
3.12	Deverá ter capacidade de registrar e indexar todas as comunicações de rede ocorridas sem amostragem.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
3.13	Deverá possuir interface simples de usar que suporte técnico a revisão das detecções, a triagem dos eventos, as investigações e a condução de operações de buscas por ameaças.	
3.14	**Deverá possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:**	
3.14.1	resumidos;	
3.14.2	visão geral dos incidentes de segurança;	
3.14.3	discriminação dos tipos de incidentes;	
3.14.4	top ameaças analisadas;	
3.14.5	top hosts infectados;	
3.14.6	recomendações de segurança;	
3.14.7	executivos;	
3.14.8	deverá possuir detalhes técnicos dos incidentes detectados;	
3.14.9	deverá possuir indicadores de risco do ambiente;	
3.15	**Deverá possuir relatórios customizados de todas as suas funcionalidades e conter no mínimo:**	
3.15.1	computadores infectados	
3.15.2	origem de infecções	
3.15.3	estatísticas de ameaças	
3.15.4	eventos suspeitos	
3.15.5	infecções de malware	
3.16	**A solução deverá apresentar função de pesquisa por logs contendo no mínimo:**	
3.16.1	Critérios de pesquisa por dia, mês e ano;	
3.16.2	Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos	
3.16.3	Possibilidade de pesquisa por ameaças, URL’s maliciosas, correlação de incidentes, nome de malware, protocolo e direção da detecção	
3.17	Os relatórios ou logs deverão ser exportados nos formatos PDF ou CSV.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
4	**Detecções**	
4.1	Deverá detectar todos os dispositivos na rede automaticamente e monitorar as inter-relações de comunicação por porta e protocolo entre dispositivos e servidores	
4.2	Deverá descobrir o endereço MAC L2, bem como o IP L3 correspondente ao dispositivo.	
4.3	Deverá fornecer visibilidade de ameaças avançadas para fluxos de tráfego norte-sul e leste-oeste.	
4.4	Deverá implementar machine learning não-supervisionado para detecção de anomalias de segurança.	
4.5	Deverá ser capaz de detectar atividades de comando e controle, bem como atividades de saída suspeitas, IPs e URIs suspeitas, e conexões por tunelamento DNS/SSH.	
4.6	Deverá ser capaz de detectar atividades de reconhecimento, tais como descobertas de contas, varredura de serviços na rede, compartilhamentos na rede, acessos incomuns em diretórios e arquivos e controles remoto a máquinas.	
4.7	Deverá ser capaz de detectar atividades de exploração (exploits), de força bruta sobre RDP, explorar aplicações publicadas, aplicações conhecidas e exploração de credenciais.	
4.8	Deverá ser capaz de detectar atividades de movimentação lateral e de escalação de privilégios de rede.	
4.9	Deverá ser capaz de detectar atividades de ação em objetivos com dados criptografados, exfiltração e ransomware.	
4.10	Deverá possuir recursos de machine learning (aprendizado de máquina) para rastrear, aprender o perfil comportamental de dispositivos IoT (Internet of Things) e detectar possíveis movimentações laterais de atividades maliciosas.	
4.11	Deverá permitir a pesquisa de detecções baseado nas categorias, táticas e técnicas do Framework ATT&CK do MITRE.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
4.12	Deverá ser capaz de rastrear as atividades com base no comportamento de usuários e aplicações para identificar exploração de credenciais de acesso, movimentação lateral na rede, ataques de força bruta e autenticação, manipulação de usuários, grandes transferências de arquivos, potenciais fontes de exfiltração de dados e sniffing na rede.	
4.13	Deverá se integrar com feeds de inteligência de ameaças externos para obter contexto adicional sobre IPs suspeitos, técnicas usadas por Threat Actors e outros indicadores de comprometimento.	
4.14	Deverá possuir listas de Threat Intelligence devidamente validadas e atualizadas periodicamente.	
4.15	Deverá ser capaz de detectar CVEs - vulnerabilidades e exposições comuns.	
4.16	Deverá possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques.	
4.17	A solução deverá detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP.	
4.18	Deverá possuir foco em proteção contra APTs (Advanced Persistent Threats).	
4.19	Deverá possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero).	
4.20	Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa.	
4.21	Deverá possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
4.22	Deverá possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado.	
4.23	Deverá possuir regras que identifiquem comunicações P2P, Instant Messengers e Streaming.	
5	**Investigações**	
5.1	A interface deverá possuir mecanismo de atualização automática para informar sobre novas vulnerabilidades recém-divulgadas OU oferecer recursos de monitoramento e detecção de segurança de rede para identificar possíveis vulnerabilidades e ameaças no ambiente.	
5.2	Deverá relacionar as vulnerabilidades recém-divulgadas ao ambiente existente para identificar potenciais vulnerabilidades, superfície de ataque ou violações passadas que possam já ter ocorrido, com o tráfego real observado.	
5.3	Deverá detectar em tempo real ameaças potenciais e eventuais indicadores de comprometimento (IOCs).	
5.4	Deverá apresentar um resumo das detecções ocorridas, contendo, no mínimo as detecções agregadas por categoria, por pontuação de risco e ocorrência.	
5.5	Deverá possuir mecanismo de investigação automatizada que forneça, os detalhes do ofensor, da vítima, a linha do tempo do incidente, arquivos, URLs e IPs envolvidos, portas e protocolos.	
5.6	Deverá fornecer o detalhamento sobre cada detecção ocorrida para que o analista possa entender e atuar rapidamente na resposta, com a descrição da detecção, detalhamento, sugestões de ações, fatores de risco e recomendações de mitigação.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
5.7	Deverá permitir que várias detecções sejam posicionadas na linha do tempo, permitindo o entendimento da relação entre as diferentes detecções associadas a uma mesma campanha de ataque.	
5.8	Deverá permitir que o analista inclua anotações em formato de texto aberto nas investigações em andamento.	
5.9	Deverá permitir que investigações sejam iniciadas independentemente da ocorrência de detecções, viabilizando um trabalho de threat hunting.	
6	**Integrações**	
6.1	Deverá permitir a integração com as principais nuvens públicas (Azure e AWS) para enriquecer a análise no NDR.	
6.2	Deverá permitir a integração com ambientes virtuais para obter dados de pacote entre hosts dentro desses ambientes.	
6.3	Deverá receber feeds de inteligência de ameaças para corresponder a endereços IP maliciosos e domínios observados durante uma análise, fazendo com que essas correspondências apareçam nas visualizações, métricas de transação e registros.	
6.4	Deverá permitir integração para autenticação remota por meio do SAML.	
6.5	Deverá permitir integração com soluções de single sign-on, como por exemplo: Azure AD, Google, e Okta.	
6.6	Deverá permitir a integração direcional com as soluções de SIEM dos principais fabricantes do mercado de forma nativa ou por meio de APIs, permitindo tratar o tráfego para reduzir o volume antes de enviar.	
6.7	Deverá possuir integração nativa com soluções de NGFW (Next Generation Firewall) dos principais fabricantes do mercado para contenção automatizada, como por exemplo: Checkpoint, PaloAlto e Cisco;	
6.8	Deverá possuir integração nativa com soluções de SOAR dos principais fabricantes para fornecer detecções de alta qualidade, fluxos de trabalho automatizados.	

Número do Requisito	Detalhamento técnico do requisito	Informar se atende os requisitos e caso não atenda, as sugestões de alterações
6.9	Deverá ter integração nativa para gerenciamento de tíquetes em tempo real para automatizar as filas de triagem dos analistas e receber o retorno das informações do tíquete no NDR, com os principais fabricantes do mercado.	
6.10	Deverá possuir APIs abertas para permitir integrações com soluções de terceiros utilizando API REST.	
7	**Redundância e alta disponibilidade**	
7.1	Todos os componentes que farão parte da estrutura da solução deverão suportar a operação com redundância. No caso de falha de um dos componentes do cluster, o outro deverá ser capaz de assumir as operações e funcionalidades sem interrupção dos serviços.	
7.1.1	Alternativamente, caso não seja suportado redundância dos sensores, deverá ser fornecido sensores de maneira duplicada para prover redundância. No caso de sensores virtuais, será aceito redundância através do recurso de "live-migration" do hypervisor, que permite replicar a máquina virtual do sensor em caso de falha, sem impacto no ambiente.	

_____X_____

1. Lote 1 – Serviços Continuados de SOC

1.1. Quantidade mínimas de perfis profissionais

1.1.1. As quantidades de profissionais, por perfil, informadas na tabela 1, abaixo, são consideradas mínimas. É de responsabilidade exclusiva da PROPONENTE estimar adequadamente sua capacidade de atendimento para fazer face à demanda de serviços e o atendimento aos níveis mínimos de serviços previstos neste Termo de Consulta e seus anexos.

Equipe	Tipo de Perfil	Nível Profissional mínimo	Janela de Atendimento	Quantidade de Perfis
Gestor	Gerente de SOC	Master	Presencial e Remoto das 8:00 às 18:00, conforme definido no Termo de Consulta	1
Supervisor	Supervisor de turno de SOC	Sênior	Presencial ou Remoto, em regime 24x7x365, de acordo com os cenários do lote 1.	1 por turno. A critério da PROPONENTE pode ser o N2.
N2	Analista de SOC N2	Sênior	Presencial ou Remoto, em regime 24x7x365, de acordo com os cenários do lote 1.	Mínimo de 3, mas obrigatoriamente 1 por turno
N1	Analista de SOC N1	Pleno	Presencial ou Remoto, em regime 24x7x365, de acordo com os cenários do lote 1.	2 por turno

Tabela 1 - Equipe Mínima

1.1.2. Para cada turno deverá ser designado um supervisor, que, a critério da PROPONENTE, poderá ser o N2.

1.2. Funções e responsabilidades (PROPONENTE e CONSULENTE)

1.2.1. **N1 – Primeiro Nível de Suporte:**

1.2.1.1. Responsável: **PROPONENTE**

1.2.1.2. Função: Realizar a triagem inicial de incidentes de segurança.

1.2.1.3. Atividades:

1.2.1.3.1. Monitorar alertas de segurança e identificar incidentes potenciais.

1.2.1.3.2. Coletar informações básicas sobre os incidentes, como logs e dados de eventos.

1.2.1.3.3. Aplicar soluções padronizadas para resolver problemas simples.

1.2.1.3.4. Documentar todas as atividades realizadas durante a resolução dos incidentes.

1.2.1.4. Escalonamento: Encaminhar incidentes mais complexos ou aqueles que não puderem ser resolvidos com soluções padronizadas para o N2.

1.2.2. **N2 – Segundo Nível de Suporte**

1.2.2.1. Responsável: **PROPONENTE**

1.2.2.2. Função: Lidar com incidentes de segurança que requerem um conhecimento técnico mais aprofundado.

1.2.2.3. Atividades:

1.2.2.3.1. Analisar detalhadamente os incidentes encaminhados pelo N1.

1.2.2.3.2. Realizar diagnósticos avançados para identificar a causa raiz dos problemas.

1.2.2.3.3. Implementar soluções técnicas específicas para mitigar os incidentes.

1.2.2.3.4. Fornecer orientação e suporte técnico para a equipe de N1.

1.2.2.3.5. Documentar as soluções implementadas e quaisquer ações adicionais necessárias.

1.2.2.4. Escalonamento: Encaminhar incidentes de alta complexidade ou de grande impacto para o N3.

1.2.3. **N3 – Terceiro Nível de Suporte**

1.2.3.1. Responsável: CONSULENTE ou empresa por ela indicada

1.2.3.2. Função: Gerenciar incidentes altamente técnicos e complexos que exigem conhecimento especializado.

1.2.3.3. Atividades:

1.2.3.3.1. Desenvolver e implementar soluções tecnológicas avançadas para resolver falhas graves.

1.2.3.3.2. Conduzir análises forenses detalhadas para investigar a origem e o impacto dos incidentes de segurança.

1.2.3.3.3. Trabalhar em colaboração com outras equipes de TIC (Tecnologia da Informação e Comunicação) e com especialistas externos, quando necessário.

1.2.3.3.4. Realizar testes e avaliações de segurança para identificar vulnerabilidades e propor melhorias contínuas.

1.2.3.3.5. Documentar todas as descobertas, soluções e recomendações de melhoria.

1.2.3.4. Colaboração: Atuar em incidentes críticos, muitas vezes em conjunto com diversas equipes técnica envolvidas no evento.

1.2.4. **Gestor do SOC**

1.2.4.1. Responsável: PROPONENTE

1.2.4.2. Função: Gerenciar as equipes técnicas N1 e N2 alocada para prestação dos serviços continuados de SOC. O Gerente de SOC deve possuir capacidade de liderança e coaching.

1.2.4.3. Atividades:

1.2.4.3.1. Garantir que os serviços prestados sejam executados com o máximo de rigor possível, atendendo às especificações constantes neste Termo de Consulta e seus anexos e garantindo que não haja quebras de níveis de serviços, conforme indicadores de qualidade definidos no ANEXO I-H deste Termo de Consulta.

1.2.4.3.2. Validar o conteúdo dos relatórios definidos no ANEXO I-B deste Termo de Consulta e garantir a entrega dos mesmos nos prazos pactuados.

1.2.4.3.3. Trabalhar em colaboração com outras equipes de TIC (Tecnologia da Informação e Comunicação) e com especialistas externos, quando necessário.

1.2.4.4. Escalonamento: Garantir o encaminhamento de incidentes de alta complexidade ou de grande impacto para o N3 e para a Gerencia de Segurança da Informação da CONSULENTE.

1.2.4.5. Colaboração: Atuar em incidentes críticos, garantindo a atuação conjunta e colaborativa das equipes N1 e N2 com as equipes técnicas N3.

1.2.5. **Supervisor do SOC**

1.2.5.1. Responsável: PROPONENTE

1.2.5.2. Função: Supervisionar a prestação de serviços realizadas pelas equipes técnicas N1 e N2 alocadas no SOC, mas reportando qualquer evento significativo ao Gestor do SOC.

1.2.5.3. Atividades:

1.2.5.3.1. Garantir que os serviços prestados sejam executados com o máximo de rigor possível, atendendo às especificações constantes neste Termo de Consulta e seus anexos e garantindo que não haja quebras de níveis de serviços, conforme indicadores de qualidade definidos no ANEXO I-H deste Termo de Consulta.

1.2.5.3.2. Validar o conteúdo dos relatórios definidos no ANEXO I-B deste Termo de Consulta e garantir a entrega dos mesmos nos prazos pactuados.

1.2.5.3.3. Trabalhar em colaboração com outras equipes de TIC (Tecnologia da Informação e Comunicação) e com especialistas externos, quando necessário.

1.2.5.4. Escalonamento: Garantir o encaminhamento de incidentes de alta complexidade ou de grande impacto para o N3, para o Gestor do SOC e para a Gerencia de Segurança da Informação da CONSULENTE.

1.2.5.5. Colaboração: Atuar em incidentes críticos, garantindo a atuação conjunta e colaborativa das equipes N1 e N2 com as equipes técnicas N3.

1.3. Perfis profissionais dos especialistas alocados no SOC

1.3.1. Para ocupar a função de Gestor, Supervisor, N1 e N2 do SOC os profissionais deverão atender todos os requisitos de formação, conhecimentos e experiências, especificados nas tabelas abaixo:

1.3.1.1. Gestor do SOC

Experiência profissional	Mínimo de 2 (dois) anos de experiência, ao longo dos últimos 6 (seis) anos na função de coordenação do trabalho de equipe composta de, no mínimo, 10 pessoas; Possuir experiência mínima de 1 (um) ano trabalhando como analista de segurança de SOC desenvolvendo todas as atividades inerente ao cargo de analista de SOC, ou seja, N1, N2 ou N3; - Possuir experiencia profissional na função de planejar, coordenar e acompanhar as atividades das equipes N1 e N2 de SOC.
Formação acadêmica	Curso superior completo na área de Tecnologia da Informação ou de graduação em qualquer curso superior, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
Proficiência em inglês	Possuir domínio da língua inglesa.
Conhecimentos técnicos	Possuir, pelo menos uma, certificação como (ISC)2 CISSP, Carnegie Mellon CSIH, GIAC GCIH, GIAC GSOC. Para este perfil profissional a PROPONENTE poderá solicitar o deferimento de outras certificações, desde que sejam fortemente relacionadas à área de segurança cibernética. A título de exemplificação, certificações fornecidas por organizações como CompTIA, GIAC, Offensive Security, Carnegie Mellon, (ISC)2, Cisco, EC Council, Microsoft, ISACA e F5 BIG-IP, entre outras, podem ser aceitas. No entanto, a CONSULENTE se reserva o direito de deferir ou não a solicitação.

Tabela 2a – Gestor do SOC

1.3.1.1. Supervisor e atendente N2 do SOC

Experiência profissional	Mínimo de 2 (dois) anos de experiência, ao longo dos últimos 6 (seis) anos na função de Analista de Segurança da Informação.
Formação acadêmica	Curso superior completo na área de Tecnologia da Informação ou de graduação em qualquer curso superior, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
Proficiência em inglês	Possuir domínio da língua inglesa.
Conhecimentos técnicos	Ter conhecimentos, habilidades e experiências cumulativas nas seguintes áreas: . Inteligência de Ameaças Cibernéticas; . Tratamento e Resposta a Eventos e Incidentes Cibernéticos; . Análise de Logs; . Detecção de intrusões; . Mitigação de ataques; . Forense Digital; . Verificação de vulnerabilidade; . Monitoramento de redes; . Análise de tráfego de redes; . Criptografia; . Segurança de redes; . Ferramentas de análise de malware. . Normativos de segurança da informação (todos da família ABNT/NBR ISO/IEC 27.000) Possuir, pelo menos uma, certificação como (ISC)2 CISSP, GIAC, GCFE, EC Council EC|H, EC Council ECSA, EC Council CHFI, Carnegie Mellon CSIH, (ISC)2 CCFP, Offensive Security OSCP, Offensive Security OSCE. Para este perfil profissional a CONSULENTE pode solicitar o deferimento de outras certificações, desde que sejam fortemente relacionadas à área de segurança cibernética. A título de exemplificação, certificações fornecidas por organizações como CompTIA, GIAC, Offensive Security, Carnegie Mellon, (ISC)2, Cisco, EC Council, Microsoft, ISACA e F5 BIG-IP, entre outras, podem ser aceitas. No entanto, a CONSULENTE se reserva o direito de deferir ou não a solicitação;

	Capacidade de empregar linguagens de programação como Python, Power Shell, Bash e Perl.

Tabela 2b – Supervisor e atendente N2 do SOC

1.3.1.1. Atendente N1 do SOC

Experiência profissional	Mínimo de 2 anos de experiência, ao longo dos últimos 6 (seis) anos na função de Analista de Segurança da Informação Pleno.
Formação acadêmica	Curso superior completo na área de Tecnologia da Informação ou de graduação em qualquer curso superior, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC) ou possuir, pelo menos uma, certificação como Cisco Cyber Ops, Cisco CCNA Security, EC Council EC|H, EC Council C|EH, GIAC GCIH, GIAC GMON, GIAC GDAT, GIAC GCDA, GIAC GISF, CompTIA CySA+ e CompTIA Security+. Para este perfil profissional a PROPONENTE poderá solicitar o deferimento de outras certificações, desde que sejam fortemente relacionadas à área de segurança cibernética. A título de exemplificação, certificações fornecidas por organizações como CompTIA, GIAC, Offensive Security, Carnegie Mellon, (ISC)2, Cisco, EC Council, Microsoft, ISACA e F5 BIG-IP, entre outras, podem ser aceitas. No entanto, a CONSULENTE se reserva o direito de deferir ou não a solicitação.
Proficiência em inglês	Conhecimento de nível inglês instrumental.
Conhecimentos técnicos	Ter conhecimentos, habilidades e experiências cumulativas nas seguintes áreas: . Inteligência de Ameaças Cibernéticas; . Tratamento e Resposta a Eventos e Incidentes Cibernéticos; . Análise de Logs; . Verificação de vulnerabilidade; . Monitoramento de redes; . Análise de tráfego de redes; . Criptografia; . Segurança de redes; e, . Ferramentas de análise de malware.

Tabela 2c – Atendente N1 do SOC

1.4. **Considerações sobre os perfis**

1.4.1. A critério da CONSULTANTE, poderão ser avaliadas e eventualmente aceitas comprovações adicionais de experiência ou composições de certificações em substituição às indicadas para os perfis Gerente do SOC, N1 e N2, desde que apresentadas pela PROPONENTE de forma fundamentada e justificada.

1.4.2. Quando ocorrer a substituição de perfis profissionais durante a vigência do contrato, a comprovação dos requisitos obrigatórios de qualificação deverá ser efetuada previamente à alocação do novo profissional.

1.4.3. Nos casos em que a PROPONENTE apresentar certificado ou certificação equivalente, a CONSULENTE poderá solicitar comprovações de que as disciplinas ou tecnologias atestadas são similares às originalmente previstas.

2. Lote 2 – Serviços Técnicos Especializados

2.1. **Quantidade mínimas de perfis profissionais**

2.1.1. Independentemente do tipo de atendimento (item 1: 8 x 5 e item 2: 24x7x365) é de responsabilidade exclusiva da PROPONENTE estimar adequadamente sua capacidade de atendimento para execução dos serviços para fazer face à demanda e o atendimento aos níveis mínimos de serviços previstos neste Termo de Consulta e seus anexos, mas, no mínimo, a PROPONENTE deverá indicar dois profissionais com o perfil técnico abaixo, para prestação dos serviços.

2.2. **Perfil Profissional**

2.2.1. Os profissionais deverão possuir profundo conhecimento em CTI

Experiência profissional	Mínimo de 4 (quatro) anos de experiência, ao longo dos últimos 8 (oito) anos na função de Analista de Segurança da Informação, de nível 3 (N3) de atendimento e Analista Sênior ou Master de Segurança da Informação, em empresa de médio e grande porte (mais de 500 funcionários) ou para empresa de médio ou grande porte (mais de 500 funcionários).

Formação acadêmica	Curso superior completo na área de Tecnologia da Informação ou de graduação em qualquer curso superior, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
Proficiência em inglês	Possuir domínio da língua inglesa.
Conhecimentos técnicos	Ter conhecimentos, habilidades e experiências cumulativas nas seguintes áreas: . Inteligência de Ameaças Cibernéticas; . Tratamento e Resposta a Eventos e Incidentes Cibernéticos; . Análise de Logs; . Detecção de intrusões; . Mitigação de ataques; . Forense Digital; . Verificação de vulnerabilidade; . Monitoramento de redes; . Análise de tráfego de redes; . Criptografia; . Segurança de redes; . Ferramentas de análise de malware. . Normativos de segurança da informação (todos da família ABNT/NBR ISO/IEC 27.000) Possuir, pelo menos uma, certificação como (ISC)2 CISSP, Carnegie Mellon CSIH, GIAC GCIH, GIAC GSOC. Para este perfil profissional a CONSULENTE pode solicitar o deferimento de outras certificações, desde que sejam fortemente relacionadas à área de segurança cibernética. A título de exemplificação, certificações fornecidas por organizações como CompTIA, GIAC, Offensive Security, Carnegie Mellon, (ISC)2, Cisco, EC Council, Microsoft, ISACA e F5 BIG-IP, entre outras, podem ser aceitas. No entanto, a CONSULENTE se reserva o direito de deferir ou não a solicitação; Capacidade de empregar linguagens de programação como Python, Power Shell, Bash e Perl.

Tabela 3 – Especialista de Segurança

2.3. **Considerações sobre os perfis**

2.3.1. A critério da CONSULTANTE, poderão ser avaliadas e eventualmente aceitas comprovações adicionais de experiência ou composições de certificações em substituição às indicadas para os perfis, desde que apresentadas pela PROPONENTE de forma fundamentada e justificada.

2.3.2. Quando ocorrer a substituição de perfis profissionais durante a vigência do contrato, a comprovação dos requisitos obrigatórios de qualificação deverá ser efetuada previamente à alocação do novo profissional.

2.3.3. Nos casos em que a PROPONENTE apresentar certificado ou certificação equivalente, a CONSULENTE poderá solicitar comprovações de que as disciplinas ou tecnologias atestadas são similares às originalmente previstas.