DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

PROA: 23/1400-0008814-6
Assunto: Contratação de Serviços de Central de Operações de Segurança (SOC) e Serviços Gerenciados de Segurança da Informação (MSS)

ANEXO II

TERMO DE REFERÊNCIA - TR

1. OBJETO

1.1. Contratação do **Serviço de Central de Operações de Segurança** (*Security Operations Center – SOC*) e contratação de **Serviços Gerenciados de Segurança** (*Managed Security Services - MSS*).

1.2. O prazo de vigência da contratação é de 12 meses, prorrogável até o limite da lei.

2. FUNDAMENTAÇÃO

Esta contratação tem como finalidade prover a Secretaria da Fazenda do Rio Grande do Sul – SEFAZ RS – serviços técnicos especializados em segurança da informação necessários para manter disponibilidade contínua dos serviços de TIC, detectando e impedindo acessos não autorizados, vasculhando o ambiente para identificar vulnerabilidades e correlacionando todos os eventos de segurança de forma unificada, mantendo a integridade das informações.

A infraestrutura de TIC da SEFAZ RS dispõe de uma série de ativos heterogêneos agrupados em: soluções de segurança, rede de comunicação de dados, telefonia, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup e recursos de armazenamento de dados que, dada a criticidade dos sistemas hospedados, devem operar em alta disponibilidade e em resiliência a falhas.

Com o crescente uso de recursos tecnológicos, os sistemas e dados da SEFAZ RS tornaram-se essenciais para o funcionamento institucional, transformando a informação em um dos bens mais valiosos. Com planejamento e uso correto de recursos, a segurança da informação impede o acesso não autorizado, roubo e destruição de informações, não apenas no contexto de sistemas tecnológicos e seus dispositivos, mas em todo e qualquer ativo que contenha uma informação de valor.

Considerando a importância que os sistemas e serviços de Tecnologia da Informação e Comunicações – TIC – adquiriram para as organizações e a constante diversificação e desenvolvimento de novas ameaças cibernéticas, são mandatórios a constante evolução, o aprimoramento dos mecanismos de segurança, bem como o desenvolvimento de equipes e de métodos de segurança cada vez mais eficazes e complexos. Considerando o grande e crescente volume de acessos, a disponibilização de novos serviços e a complexidade das atividades executadas pelas áreas de TIC da SEFAZ, conjugados com o crescimento de novas ameaças cibernéticas, tentativas de invasão a partir de técnicas avançadas, ataques de negação de serviço, além do crescimento de ataques direcionados às instituições, gerando um impacto negativo na manutenção da qualidade dos serviços prestados.

Ademais, é primordial aprimorar a atuação preventiva, elevar a capacidade de detecção de comportamentos anômalos agregado ao processo de gestão de incidentes de segurança, agilizando o tratamento e resposta a incidentes e por sua vez, melhorando a percepção de segurança perante os usuários internos e a sociedade. Esses objetivos serão perseguidos nesta contratação pela criação e revisão dos níveis de serviço, para que estes estejam condizentes com a importância que a segurança da informação possui para a Secretaria.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

Portanto, considerando a importância dos serviços de segurança de TIC para a manutenção da disponibilidade e qualidade nos diversos serviços e sistemas da SEFAZ RS, aliado à escassez de profissionais especializados nos quadros de servidores efetivos, com a qualificação necessária para o atendimento dessa demanda, torna-se essencial a contratação de Serviços de Central de Operações de Segurança (SOC) e Serviços Gerenciados de Segurança da Informação (MSS).

3. ESPECIFICAÇÃO DOS SERVIÇOS

3.1. Central de Operações de Segurança (Security Operations Center – SOC):

3.1.1. Monitoração de Serviços de Segurança da Informação, por meio de Central de Operações de Segurança (Security Operations Center – SOC), abrangendo a totalidade de infraestrutura de segurança e usuários da CONTRATANTE;

3.1.2. O serviço prestado deverá ocorrer em harmonia com as atividades administrativas da CONTRATANTE;

3.1.3. Os serviços monitorados pelo SOC deverão abranger, mas não se limitar, ao gerenciamento dos seguintes pontos:

3.1.3.1. Serviço de Firewall de Próxima Geração (Next Generation Firewall - NGFW);

3.1.3.2. Serviços de Segurança de Mensageria;

3.1.3.3. Serviço de Gestão de Pontos de Extremidade;

3.1.3.4. Serviço de Gestão de Vulnerabilidades;

3.1.3.5. Serviço de Gestão de Acessos Privilegiados;

3.1.3.6. Serviço de Detecção e Resposta de Rede (Network Detection and Response – NDR);

3.1.3.7. Serviço de SIEM (Security Information and Event Management); e

3.1.3.8. Serviço de Detecção e Respostas a Incidentes de Segurança (Blue Team).

3.1.4. A CONTRATADA deverá fazer uso do conjunto de soluções existente no parque da CONTRATANTE;

3.1.4.1. A CONTRATADA poderá fazer uso de soluções complementares na prestação dos serviços, desde que aprovado pela CONTRATANTE e que não resulte em custo adicional à CONTRATANTE.

3.2. Serviços Gerenciados de Segurança (Managed Security Services - MSS):

3.2.1. Administração, gerenciamento dos Serviços de Segurança da Informação, por meio de equipe especializada de segurança, abrangendo a totalidade de infraestrutura de segurança e usuários da CONTRATANTE;

3.2.2. O serviço prestado deverá ocorrer em harmonia com as atividades administrativas da CONTRATANTE;

3.2.3. Os serviços compreendidos no MSS deverão abranger, mas não se limitar, ao gerenciamento dos seguintes pontos:

3.2.3.1. Serviço de Firewall de Próxima Geração (Next Generation Firewall - NGFW);

3.2.3.2. Serviços de segurança de mensageria;

3.2.3.3. Serviço de Gestão de Pontos de Extremidade;

3.2.3.4. Serviço de Gestão de Vulnerabilidades; e

3.2.3.5. Serviço de Gestão de Acessos Privilegiados;

3.2.4. CONTRATADA deverá fazer uso do conjunto de soluções existente no parque da CONTRATANTE;

3.2.4.1. A CONTRATADA poderá fazer uso de soluções complementares na prestação dos serviços, desde que aprovado pela CONTRATANTE e que não resulte em custo adicional à CONTRATANTE.

4. LOCAL E HORÁRIO DE PRESTAÇÃO DOS SERVIÇOS

4.1. Os serviços de SOC e MSS poderão ser prestados ser prestados de forma remota pela CONTRATADA, podendo ser prestados on-site, de comum acordo entre CONTRATANTE e CONTRATADO, nos casos de impossibilidade de acesso remoto ou em que a situação assim o demande, abrangendo a totalidade de infraestrutura de segurança e usuários da CONTRATANTE e observadas as seguintes disposições:

4.1.1. A estrutura de operação de Nível 1 deverá ser dentro das instalações físicas da CONTRATADA, em território nacional;

4.1.2. As estruturas de operação de Nível 2 e Nível 3 poderão ser prestadas a partir das instalações do prestador ou de forma remota;

4.1.3. Os custos de viagem em casos de incidentes que necessitarem de deslocamento dos agentes da contratada ocorrerão às custas da CONTRATADA, sem a possibilidade de reembolsos.

4.1.4. O SOC será prestado no regime de é 24x7 (vinte e quatro horas por dia, sete dias por semana);

4.1.5. O Serviço de MSS será prestado segunda a sexta feira das 7:00 às 19:00, podendo, em casos de urgência, sofrer alterações mediante comum acordo.

5. REQUISITOS DA CONTRATAÇÃO

5.1. **Requisitos de Segurança e Privacidade:**

5.1.1. A CONTRATADA deverá atender aos princípios e procedimentos elencados nos instrumentos legais como Políticas, Resoluções, Normativas, Padrões de TIC e Notas Técnicas do CONTRATANTE.

5.2. **Requisitos da Arquitetura Tecnológica:**

5.2.1. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da CONTRATANTE;

5.2.2. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela CONTRATANTE. Caso não seja autorizada, é vedado à CONTRATADA adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela CONTRATANTE;

5.2.3. As ferramentas em uso pela CONTRATANTE para a prestação dos serviços poderão ser alteradas durante a vigência do contrato, sempre respeitando os requisitos técnicos mínimos definidos nesta especificação. Neste caso a CONTRATADA participará do processo de implantação da nova ferramenta, devendo providenciar treinamento aos seus profissionais para a continuidade da prestação dos serviços.

ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

5.3. **Equipe da CONTRATADA:**

5.3.1. O dimensionamento das equipes para execução adequada dos Serviços Gerenciados de Segurança é de responsabilidade exclusiva da CONTRATADA, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos e indicadores constantes neste Caderno de Especificação Técnica, no entanto, cada um dos profissionais designados para a realização dos serviços deve possuir, no mínimo, 1 (uma) certificação na área de segurança da informação conforme abaixo:

5.3.2. São consideradas certificações válidas:

5.3.2.1. Certified Information Systems Security Professional (CISSP);

5.3.2.2. Certified Information Security Manager (CISM);

5.3.2.3. CompTIA Security Plus Certification (Security+);

5.3.2.4. Certified Ethical Hacker (CEH);

5.3.2.5. CompTIA Advanced Security Practitioner (CASP+);

5.3.2.6. EC-Council Certified Security Analist (ECSA);

5.3.2.7. Global Information Assurance Certification (GIAC); e

5.3.2.8. CompTIA Cybersecurity Analyst+ (CySA+).

5.3.3. São consideradas obrigatórias na composição da equipe, profissionais com os seguintes certificados:

5.3.3.1. Microsoft Cerfified:

5.3.3.1.1. Azure Security Engineer Associate;

5.3.3.1.2. Identity and Access Administrator Associate; e

5.3.3.1.3. Security Operations Analyst Associate.

5.3.3.2. Fortinet:

5.3.3.2.1. NSE 6;

5.3.3.2.2. NSE 5; e

5.3.3.2.3. NSE 4.

5.3.4. Os certificados apresentados devem estar válidos e terem sido obtidos ou renovados em data não superior a 5 anos contados da data do pregão;

5.3.5. Requisitos mínimos de experiência profissional:

5.3.5.1. Os profissionais designados para realização do serviço devem possuir no mínimo 03 (três) anos de experiência em serviços de Sustentação de Infraestrutura e Soluções de Segurança ou em gestão e resposta a incidentes de segurança da informação, contados da data do pregão;

5.3.5.1.1. Para comprovação deverá ser apresentado atestado de prestação de serviço ou contrato constando data de início e término da prestação;

5.3.5.1.2. A comprovação poderá se dar pela soma de atestados e contratos.

5.3.6. Deverá ser nominado e indicado por parte da CONTRATADA um profissional que atuará como ponto de contato para assuntos relacionados a gestão do contrato. Este profissional precisará ter certificação PMP, visto suas funções estarem relacionadas a parte administrativa do contrato;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

5.3.7. Os profissionais designados pela CONTRATADA deverão possuir vínculo empregatício ou societário junto à empresa;

5.3.8. Antes da assinatura do Contrato, a CONTRATADA deverá apresentar relação com todos os profissionais pertencentes à equipe de trabalho, além de comprovar que atende a todos os requisitos estabelecidos no tópico 6.5 deste Termo de Referência;

5.3.8.1. Em não atendimento ao item 5.3.3, a CONTRATADA deverá apresentar plano de capacitação da equipe, com apresentação dos certificados faltantes em até 45 dias.

5.4. **Requisitos do ambiente da contratada:**

5.4.1. Os Serviços de Central de Operação de Segurança deverão ser prestados por meio de estrutura de SOC - Security Operation Center;

5.4.2. O MSS poderá ser prestado em estrutura de NOC ou SOC, atendendo os seguintes requisitos mínimos:

5.4.3. Infraestrutura mínima da CONTRATADA para prestação dos serviços de SOC e MSS:

5.4.3.1. O SOC deve estar ativo e deverá atender aos seguintes requisitos mínimos:

5.4.3.1.1. Utilizar sistema de gerenciamento de Circuito fechado de televisão - CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;

5.4.3.1.2. Filmar toda a área, mantendo as imagens armazenadas por no mínimo 90 (noventa) dias;

5.4.3.1.3. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC por no mínimo 90 dias;

5.4.3.1.4. Possuir solução de monitoramento de disponibilidade e desempenho;

5.4.3.1.5. O perímetro deve estar protegido contra intrusão e acesso indevido;

5.4.3.1.6. Ser vigiado de forma ininterrupta por segurança especializada em regime de 24x7;

5.4.3.1.7. Ter controle de acesso físico, preferencialmente, com pelo menos 2 (dois) fatores de autenticação;

5.4.3.1.8. Ser configurado de forma que a falha de equipamentos isolados NÃO interrompa a prestação dos serviços;

5.4.3.1.9. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPS (unidades de alimentação elétrica contínua) para garantir a transição entre o fornecimento normal de energia e o grupo gerador;

5.4.3.1.10. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;

5.4.3.1.11. Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001;

5.4.3.1.12. O ambiente dever dispor de alta disponibilidade, dispondo de link contingenciado, para a execução das atividades de SOC;

5.4.3.1.13. A CONTRATADA será responsável pela aplicação de controles de segurança adequados para garantir a confidencialidade de qualquer dado ou informação do CONTRATANTE que receber em seu ambiente;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

5.4.3.1.13.1. Essa regra também deverá ser observada caso a CONTRATADA faça uso de ferramentas complementares que não são utilizadas no parque do CONTRATANTE.

5.4.4. O ambiente da CONTRATADA poderá ser objeto de diligência, para fins de verificação do atendimento ao item 5.4.

5.5. **Informações relevantes para o dimensionamento da proposta:**

5.5.1. Ambiente de Infraestrutura e Serviços de TIC da SEFAZ tem as seguintes características:

5.5.1.1. **Infraestrutura de Armazenamento e Processamento**:

5.5.1.1.1. Windows Servers: 342;

5.5.1.1.2. Windows Server: 83 (sem agente);

5.5.1.1.3. Linux: 70;

5.5.1.1.4. Estações VDI: 2000;

5.5.1.1.5. Storages: 5; e

5.5.1.1.6. Fitotecas: 2.

5.5.1.2. **Infraestrutura de Segurança:**

5.5.1.2.1. Firewall NGFW (_SD-wan, WAF, Firewall, Fortimanager, Fortiauthenticator) Solução Fortinet

5.5.1.2.2. Appliances (Datacenter): 4;

5.5.1.2.3. Azure: 4; e

5.5.1.2.4. Appliances Físicos (Interior): 47.

5.5.1.3. **Infraestrutura de Microinformática:**

5.5.1.3.1. Desktops: 1930;

5.5.1.3.2. Impressoras: 300;

5.5.1.3.3. Infraestrutura de Rede – LAN:

5.5.1.3.4. Switch core: 04

5.5.1.3.5. Switches de acesso: 130;

5.5.1.3.6. Controladoras Wireless: 2; e

5.5.1.3.7. Access Point: 265.

5.5.1.4. **Infraestrutura de Rede – WAN:**

5.5.1.4.1. Redes PROCERGS: 02.

5.5.1.5. **Infraestrutura de Software:**

5.5.1.5.1. AD Federation Services: 02;

5.5.1.5.2. Web Application Proxy: 02;

5.5.1.5.3. Sistemas Web SEFAZ-RS: 80;

5.5.1.5.4. Qlik Server: 04;

5.5.1.5.5. Moodle: 03;

5.5.1.5.6. TraceGP: 01;

5.5.1.5.7. 4biz: 01;

5.5.1.5.8. Netbackup 8.1: 02;

5.5.1.5.9. File Server: 40;

5.5.1.5.10. AD, DHCP, DNS, DFS: 70;

5.5.1.5.11. System Center (SCOM, SCVMM, SCCM, SCSM, SCORCH): 10;

5.5.1.5.12. Exchange Server: 06;

5.5.1.5.13. SQL Server: 28;

5.5.1.5.14. Hyper-V: 50; e

5.5.1.5.15. OPMON: 03.

5.5.1.6. **Serviços Azure:**

5.5.1.7. Microsoft Sentinel;

5.5.1.8. Microsoft 365 Defender;

5.5.1.9. Score de Segurança está na faixa de 70% a 74% ;

5.5.1.10. Score de Exposição está na faixa de 20 a 16 pontos; e

5.5.1.11. Microsoft Purview.

5.5.2. **Usuários AD:**

5.5.2.1. Usuários : 2511;

5.5.2.2. Usuários Azure: 47;

5.5.2.3. Aplicações: 225.

5.6. **Vistoria:**

5.6.1. Para a obtenção de informações e condições necessárias à correta elaboração da proposta e execução dos serviços, a licitante poderá realizar vistoria técnica para tomar conhecimento dos principais softwares, aplicativos, sistemas e ferramentas auxiliares em utilização na Secretaria;

5.6.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo até o dia útil anterior à data prevista para a abertura da sessão pública;

5.6.3. Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria;

5.6.4. O agendamento deverá ser realizado de segunda a sexta, 9:00 – 12:00 e 13:30 – 17:00, por meio eletrônico e-mail: fredericob@sefaz.rs.gov.br E gustavok@sefaz.rs.gov.br;

5.6.4.1. A CONTRATANTE recomenda que esta marcação seja feita com no mínimo 48 horas de antecedência do horário pretendido.

5.6.5. Quando da vistoria ao local dos serviços, as LICITANTES devem se inteirar de todos os aspectos referentes à execução do fornecimento;

5.6.6. Para todos os efeitos, considerar-se-á que a LICITANTE, optante pela realização de vistoria ou não, tem pleno conhecimento da natureza e do escopo dos serviços, não se admitindo, posteriormente, qualquer alegação de desconhecimento dos serviços e de dificuldades técnicas não previstas.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

5.6.7. Efetuada a vistoria será lavrado, por representante da equipe técnica designado para tanto, o respectivo Termo de Vistoria, conforme modelo do ANEXO A MODELO DE DECLARAÇÃO DE VISTORIA, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando, oportunamente, à sua habilitação;
5.6.8. Caso a LICITANTE renuncie à vistoria técnica, deverá entregar a Declaração de Renúncia à Vistoria, conforme modelo do ANEXO B, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando, oportunamente, à sua habilitação.

6. MODELO DE EXECUÇÃO DO OBJETO

6.1. Todas as operações realizadas deverão ser registradas e documentadas na ferramenta de ITSM da CONTRATANTE, seguindo as boas práticas do ITIL;

6.2. Os acessos necessários ao ambiente da CONTRATANTE para a execução dos serviços serão concedidos somente para os profissionais designados e avaliados pela equipe da CONTRATANTE. Eventuais substituições na equipe designada deverão ser comunicadas ao CONTRATANTE, que procederá a avaliação relativa às certificações e experiência do novo profissional designado;

6.3. A CONTRATADA deverá monitorar permanentemente e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média de acessos e identificando comportamentos não usuais, visando antecipar a identificação de incidentes segurança, antes mesmo de impacto nos serviços;

6.4. **Requisitos para o Planejamento e Metodologia de Trabalho:**

6.4.1. As manutenções programadas, preventivas ou corretivas, que representem risco de interrupção do(s) serviço(s) ou em parada do(s) ambiente(s) deverão ser realizadas fora do horário regular ou em dia não útil, mediante aprovação de pessoa designada pela CONTRATANTE, sendo que a solicitação de manutenção deverá ser solicitada com antecedência mínima de 48 horas;

Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção;

6.4.2. A CONTRATADA deverá seguir o processo de mudança estabelecido pelo CONTRATANTE. Sempre que solicitado, a CONTRATADA deverá estar disponível para participar das reuniões com o Gestores do DETIC através de videoconferência, para prestar informações sobre os ambientes e serviços por elas executados. Mudanças que impliquem em um conjunto de procedimentos complexos, que envolvam várias equipes ou empresas CONTRATADAS e que implicarem em riscos de paralisação de quaisquer serviços considerados prioritários, deverão ser tratadas como um Projeto conduzido pela CONTRATADA;

6.4.3. A CONTRATADA deverá apresentar aos Gestores do DETIC a proposta de todas as mudanças no ambiente, conforme níveis de controle estabelecidos. Para todas as mudanças apresentadas, será necessário acompanhar dentre outras informações, as análises de risco relativas às mudanças, descrevendo o impacto da sua realização;

6.4.4. A CONTRATADA deverá comunicar formalmente o CONTRATANTE sempre que identificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável à indisponibilidade;

6.4.5. Instrumentos Formais de solicitação dos serviços:

6.4.5.1. Os serviços deverão ser executados após a emissão de Ordens de Servicos, com a obrigatória autorização pelo CONTRATANTE, ou após abertura de chamado na central de serviços da CONTRATANTE;
6.4.5.2. Solicitações por meio da central de serviços da CONTRATANTE:

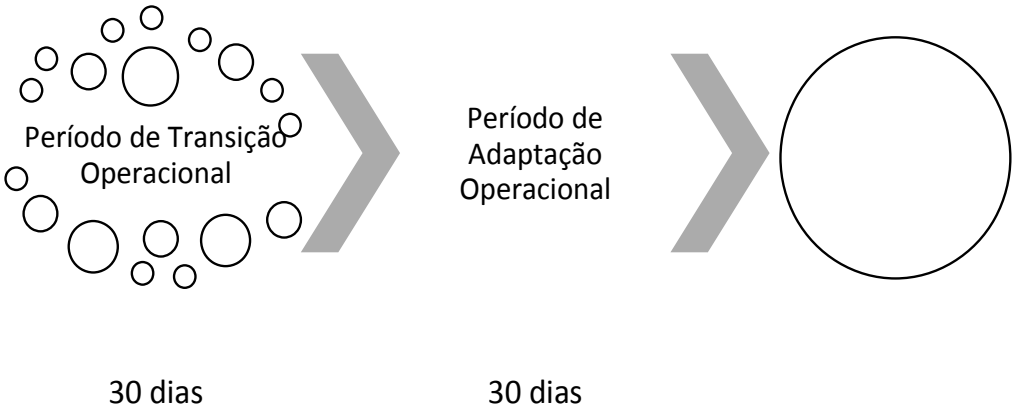
DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

6.4.5.2.1. Todos os serviços objetos desta contratação, excetuando-se os realizados por meio de Ordens de Serviço, deverão ser solicitados através de abertura de chamados por meio de sistema de acompanhamento de chamados (central de serviços), provido pela CONTRATANTE;
6.4.5.2.2. Os chamados poderão ser abertos a qualquer hora do dia ou da noite, tanto em dia úteis, como nos finais de semana, feriados e pontos facultativos, e devem ser executados de acordo com os níveis de serviços estabelecidos neste termo de referência;
6.4.5.2.3. Os chamados, especialmente os incidentes, podem ser abertos automaticamente na central de serviços pelas ferramentas de monitoramento existentes no ambiente da CONTRATANTE;
6.4.5.2.4. Ao abrir um chamado, a CONTRATANTE poderá agendar data e hora para início do atendimento para a prestação do serviço;
6.4.5.2.5. Os chamados deverão ser gerenciados exclusivamente por meio de chamado técnico, contendo, no mínimo, as seguintes informações: número de identificação exclusivo; data e hora do início da ocorrência; descrição da ocorrência; nível de severidade; providências adotadas para o diagnóstico; indicação de solução provisória e/ou definitiva; data e hora do término da ocorrência, com solução definitiva; identificação do técnico da CONTRATANTE que solicitou e validou o chamado técnico; identificação do técnico da contratada responsável pela execução do chamado técnico, bem como outras informações pertinentes.

6.4.6. Transição dos serviços:

6.4.6.1. Visando minimizar os impactos da transição do serviço, é apresentado um período de transição operacional (PTO) seguido de um período de adaptação operacional (PAO); e

6.4.6.2. A operação continua, com o serviço completo e com averiguação dos SLAs, começa após período inicial de 60 dias.



6.4.7. **Período de Transição Operacional (PTO):**

6.4.7.1. O Período de Transição Operacional terá a duração de 30 dias, abrangendo o intervalo de tempo desde o recebimento da ordem de início dos serviços até o trigésimo dia de prestação efetiva deles. Neste período, a CONTRATADA deverá conduzir o levantamento da abordagem para a execução das atividades, modelar e ajustar seus processos e alinhar os procedimentos em cooperação com a

CONTRATANTE, com o propósito de assegurar o sucesso da transição sem causar impactos negativos no negócio;

6.4.7.2. Durante este período, será franqueado à CONTRATADA o acesso às instalações do Departamento de Tecnologia da Informação e Comunicação – DETIC - e demais locais de prestação de serviços, podendo esta visitar as dependências físicas e, junto à atual prestadora de serviços, caso haja contrato ativo, para entendimento, assimilação, estudo e levantamento de todas as questões que julgar necessários para o início de sua operação;

6.4.7.3. Este período também deverá ser utilizado para que a CONTRATADA possa absorver os conhecimentos necessários para operação e continuidade dos serviços que ficarão sob sua responsabilidade minimizando a probabilidade de impacto sobre os serviços ou sua interrupção;

6.4.7.4. Com base nas informações recolhidas durante o PERÍODO DE TRANSIÇÃO OPERACIONAL (PTO), a CONTRATADA deverá produzir e entregar em até 05 (cinco) dias úteis após o início da data da prestação do serviço, PROJETO DE IMPLANTAÇÃO DOS SERVIÇOS, que contemplará não só as atividades necessárias ao início da prestação dos serviços, bem como o seguinte:

6.4.7.4.1. Diagnóstico do Catálogo de Serviços, bem como propostas de possíveis melhorias, inclusive automatizações, ou acréscimos;

6.4.7.4.2. O detalhamento da estratégia de acompanhamento e cumprimento dos requisitos de nível de atendimento;

6.4.7.4.3. Os controles e tratamentos relativos a cada fator de risco à plena execução do contrato;

6.4.7.4.4. Relação de todos os serviços de segurança da CONTRATANTE, indicando o estado do serviço quanto à criticidade e estado da monitoria;

6.4.7.4.5. Cronograma detalhado de todas as outras atividades a serem executadas pela CONTRATADA; e

6.4.7.4.6. Eventuais problemas identificados durante o PERÍODO DE TRANSIÇÃO OPERACIONAL, que possam vir a comprometer o bom andamento dos serviços ou o alcance dos níveis de serviço estabelecidos neste Termo de Referência, deverão ser comunicados à CONTRATANTE, que colaborará com a CONTRATADA na busca da melhor solução para o problema.

6.4.8. **Período de Adaptação Operacional (PAO):**

6.4.8.1. O PERÍODO DE ADAPTAÇÃO OPERACIONAL (PAO) da CONTRATADA terá a duração de 30(trinta) dias, contados a partir do final do Período de Transição Operacional. Durante este período a CONTRATADA deverá realizar todos os ajustes que se mostrarem necessários no dimensionamento e qualificação das equipes, bem como nos procedimentos adotados e demais aspectos da prestação dos serviços, de modo a assegurar o alcance das metas estabelecidas. Caso haja prorrogação da vigência contratual, não haverá novo período de Adaptação;

6.4.8.2. Durante o PERÍODO DE ADAPTAÇÃO OPERACIONAL (PAO) a CONTRATADA deverá executar o Plano de Implantação de Serviços elaborado e aprovado no Período de Transição Operacional, além de:

6.4.8.2.1. Revisar e configurar, caso necessário, as ferramentas de monitoramento de infraestrutura de segurança;

6.4.8.2.2. Revisar e, se for o caso, propor melhorias nos Catálogos de Serviços existentes, bem como sua configuração nas ferramentas de gestão de TIC;

6.4.8.2.3. Revisar e, se for o caso, propor melhorias nos processos de gestão de TIC existentes no ambiente computacional da CONTRATANTE;

6.4.8.2.4. Validar os modelos operacionais, modelos de relatórios e matrizes de responsabilidade;

6.4.8.3. As metas de nível de serviço serão implementadas gradualmente durante o período de adaptação, de modo a permitir à CONTRATADA realizar a adequação progressiva de seus serviços e alcançar, ao término desse período, o desempenho pleno requerido pela CONTRATANTE. Para tanto, serão consideradas as seguintes metas:

6.4.8.3.1. Para o 1º mês de execução contratual: 65% da meta de SLA estabelecido;

6.4.8.3.2. Para o 2º mês de execução contratual: 80% da meta de SLA estabelecido;

6.4.8.3.3. Para o 3º mês de execução contratual: 100% da meta de SLA estabelecida; e

6.4.9. A execução dos serviços durante o período de adaptação será realizada pela CONTRATADA e gerenciada pela CONTRATANTE, que fará o acompanhamento diário da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções de direção; e

6.4.10. Ao término do PERÍODO DE ADAPTAÇÃO OPERACIONAL (PAO), todos os requisitos relacionados com o Sistema de Gerenciamento de Serviços de Segurança deverão estar devidamente operacionais.

6.5. **Operação contínua nos serviços de SOC:**

6.5.1. Após o período de adaptação operacional, inicia-se o período de Operação contínua, em que a prestação do serviço, objeto deste termo de Referência, deverá estar disponível conforme os indicadores, níveis de prioridade e prazos detalhados abaixo;

6.5.2. Indicadores:

Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Meta Exigida
Tempo máximo para triagem e notificação de incidentes de segurança	Tempo = Hora de triagem – Hora de entrada do evento de segurança Onde: Hora Entrada de evento de segurança é horário em que qualquer incidente é identificado nas ferramenta de análise de segurança Hora da triagem é a momento da classificação do incidente.	<=30 minutos
Tempo máximo para instauração de comitê de crise (war room)	Tempo = Hora da instauração do comitê de crise – Hora da triagem Onde: Hora da instauração do comitê de crise é horário em que é instaurado uma reunião com os interessados ao incidente Hora da triagem é a momento da classificação do incidente.	<=30 minutos

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

Tempo máximo para abertura de chamados de suporte com terceiros	Tempo = Hora da abertura do chamado – hora da triagem Onde: Hora da abertura do chamado é horário em que é aberto o chamado com fornecedores através das plataformas oficiais Hora da triagem é a momento da classificação do incidente.	<= 60 minutos
Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço	Prazo Real em dias/Prazo acordado em dias Onde: Prazos serão decididos através de um planejamento em conjunto entre CONTRATADA E CONTRATANTE.	<= 1,25
Tempo máximo para resolução das requisições de serviços	Tempo = Hora da resolução da requisição – hora da requisição Onde: Hora da requisição é o momento da abertura da requisição. Hora da resolução é o momento da conclusão da requisição.	<= 16 horas
Tempo máximo para resposta para esclarecimentos requisitados	Dias totais de resolução = Dia da resposta - Dia da requisição Onde: Dia da requisição é o momento da abertura da requisição. Dia da resposta é o momento do retorno do questionamento.	<= 1 dia útil
Tempo máximo para resolução das requisições de serviços não padrão	Dias totais de resolução = Dia da resposta - Dia da requisição Onde: Dia da requisição é o momento da abertura da requisição. Dia da resolução da requisição é momento de conclusão da requisição	<= 5 dias
IAP – ÍNDICE DE ATENDIMENTO NO PRAZO **(Incidentes)**	IAP = 100 * (ΣQtap / ΣQtr) Onde: IAP = Indicador de atendimento aos prazos do serviço; ΣQtap = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência; ΣQtr = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.	85% <= IAP < 95% 75% <= IAP < 85% IAP < 70%

6.5.3. Os níveis de serviço são medidos mensalmente, sendo apresentados nos relatórios à CONTRATANTE.

6.5.4. Níveis de Prioridade:

Prioridade	Descrição

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

Emergencial	O serviço está fora de operação ou há um impacto crítico nas operações da CONTRATANTE
Alta	Perda ou comprometimento relevante de informação sensível, exposição pública ou disseminação nos meios de comunicação causados por ataques cibernéticos ou indisponibilidade de serviços da CONTRATANTE.
Média	Perda, comprometimento ou divulgação não autorizada de informação sensível que gerem perdas financeiras para a CONTRATANTE causadas por ataques cibernéticos.
Baixa	Perda, comprometimento ou divulgação não autorizada de informação sensível causadas por ataques cibernéticos, mas sem impacto financeiro para a CONTRATANTE.

6.5.5. Prazos para detecção, análise e resposta de incidente de segurança:

Item	**SLA (Prazo)**
Triagem e Notificação de incidente de segurança	30 min
Instauração de comitê de crise	30 min

6.5.6. Prazo de atendimento:

Serviço	**Prioridade do chamado**	**Nível de serviço (Tempo)**
Atendimento a requisições de serviço	SSR	16h úteis
Atendimento a requisições de serviço não padrão	NSSR	Conforme planejamento (5 dias úteis para resposta)
Resolução do Incidente	Emergencial	4h
	Alta	8h
	Média	12h
	Baixa	48h

6.5.7. A CONTRATADA deverá notificar a CONTRATANTE em até 60 minutos de um incidente de segurança ocorrido no ambiente. Esse prazo é contabilizado pela diferença entre o horário de abertura do incidente e o horário em que a CONTRATADA define a sua prioridade, podendo a CONTRATANTE reclassificar sua prioridade caso julgue necessário;

6.5.8. O prazo para resolução dos incidentes começa a contabilizar a partir da classificação feita pela CONTRATADA;

6.5.9. O prazo para resolução poderá ser prorrogado, excepcionalmente, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

6.5.10. A CONTRATADA deverá ter a capacidade de, após a classificação de um incidente com prioridade EMERGENCIAL, instaurar um comitê de crise e notificar a CONTRATANTE do impacto ao negócio. Esse prazo é contabilizado pela diferença entre o horário em que o Analista do SOC notifica a CONTRATANTE de um incidente com prioridade alta e o horário em que a CONTRATADA notifica a CONTRATANTE de que um Comitê de Crise foi instaurado e está trabalhando na resolução do incidente;

6.5.11. Todos os prazos citados serão considerados em horas corridas, ressaltando que serão contados as horas a partir do momento em que ocorrer o incidente, conforme os prazos;

6.6. **Operação contínua para os serviços de MSS:**

6.6.1. Após o período de adaptação operacional, inicia-se o período de Operação contínua, em que a prestação do serviço, objeto deste termo de Referência, deverá estar disponível conforme os indicadores, níveis de prioridade e prazos detalhados abaixo:

6.6.2. Níveis de serviços:

Indicadores de Níveis de Serviço	**Fórmula de Cálculo com base no mês calendário**	**Descumprimento da Meta**
Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço	Prazo Real em dias / Prazo acordado em dias Onde: Prazos serão decididos através de um planejamento em conjunto entre CONTRATADA E CONTRATANTE.	> 1,25
Tempo máximo para resposta para esclarecimentos requisitados	Dias totais de resolução = Dia da resposta - Dia da requisição Onde: Dia da requisição é o momento da abertura da requisição. Dia da resposta é o momento do retorno do questionamento.	> 1 dia útil
Tempo máximo para resolução das requisições de serviços não padrão	Dias totais de resolução = Dia da resposta - Dia da requisição Onde: Dia da requisição é o momento da abertura da requisição. Dia da resolução da requisição é momento de conclusão da requisição	> 5 dias úteis
IAP – ÍNDICE DE ATENDIMENTO NO PRAZO	IAP = 100 * (ΣQtap / ΣQtr) Onde: IAP = Indicador de atendimento aos prazos do serviço; ΣQtap = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência; ΣQtr = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.	85% >= IAP < 95% 75% >= IAP < 85% IAP < 70%
Score de Segurança	Avaliação mensal do Score na ferramenta MS-Defender	1 Ano Score<75% 2 Ano Score<76%

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

		3 Ano Score <77% 4 Ano Score<78% 5 Ano Score<79%
Score de Exposição	Avaliação mensal do Score na ferramenta MS-Defender	70 >= Score 30 >= Score < 69

6.6.3. Nível de prioridade:

Prioridade	**Descrição**
1- Emergencial	O serviço está fora de operação ou há um impacto crítico nas operações dos negócios.
2- Alta	O serviço está degradado ou aspectos significativos das operações de negócio sofreram impactos negativos pelo desempenho inadequado.
3- Média	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4- Baixa	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionalidade ou de operação
5- Planejado	Um incidente e/ou evento que não causa interrupção ou degradação dos serviços ao cliente

6.6.4. Prazo de atendimento:

Serviço	**Prioridade de Chamado**	**Nível de serviço(tempo)**
Resolução de Incidente	1. Emergencial	4h
	2. Alta	8h
	3. Média	12h
	4. Baixa	48h
	5. Planejados	60h
Serviço	**Prioridade de Chamado**	**Nível de serviço(tempo)**
Resolução de Requisições	1. Emergencial	8h
	2. Alta	12h
	3. Média	16h
	4. Baixa	52h
	5. Planejados	64h
Atendimento a requisições de serviço não padrão	NSSR	Conforme planejamento (5 dias

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

		úteis para resposta)
Hora corrida: Contagem ininterrupta do período. Hora útil: Contagem do período somente durante o horário de segunda a sexta-feira das 8:30h às 18:00h		

6.6.5. A CONTRATANTE estabeleceu critérios para classificação dos chamados em níveis de "prioridade" e "prazo", seguindo as diretrizes estabelecidas nas tabelas anteriores;

6.6.6. O Catálogo de Serviços de TIC deverá ser elaborado em conjunto entre CONTRATANTE e CONTRATADA.;

6.7. **Formas de transferência de conhecimento para os serviços de SOC e MSS:**

6.7.1. Sempre que solicitado pela CONTRATANTE, os chamados para resolução de problemas ou esclarecimento de dúvidas deverão ensejar elaboração de script padronizado que permita aplicar a mesma solução a futuros problemas de mesma natureza que venham a acontecer;

6.7.2. A CONTRATANTE poderá solicitar, sem ônus adicional, correção ou refazimento dos documentos que não estiverem de acordo com os padrões definidos ou que não corresponderem, na prática, aos procedimentos adotados. Este serviço será visto como uma garantia da qualidade do serviço prestado e poderá ser demandada até noventa dias após o encerramento do contrato;

6.7.3. O tempo gasto na elaboração da documentação deverá estar previsto no dimensionamento das atividades correlatas;

6.7.4. Os direitos autorais e patrimoniais e a propriedade intelectual dos produtos gerados pela CONTRATADA, na execução deste contrato, são propriedade da CONTRATANTE, não sendo necessário nenhum pagamento extracontrato para a sua transferência;

6.8. **Procedimentos de transição futura e finalização do contrato:**

6.8.1. A CONTRATADA fará o repasse de todo o conhecimento à CONTRATANTE e à futura empresa contratada que irá assumir os serviços descritos no Termo de Referência;

6.8.2. Considerando-se o término do contrato entre CONTRATANTE e CONTRATADA, obriga-se a CONTRATADA, signatária do acordo em fase de expiração, independentemente do motivo, repassar para a nova empresa prestadora de serviço, por intermédio de eventos formais, os documentos, procedimentos e conhecimentos necessários à continuidade da prestação dos serviços, incluindo a base de conhecimento, bem como esclarecer dúvidas a respeito de procedimentos no relacionamento entre a CONTRATANTE e a nova Contratada.;

6.8.3. A CONTRATADA deverá entregar, ao final da execução contratual, toda documentação relacionada com o objeto do contrato. A entrega da referida documentação no final do contrato não exime a CONTRATADA do repasse mensal.

7. DESCRIÇÃO DA SOLUÇÃO – SERVIÇO SOC

7.1. A execução dos serviços de SOC, utilizando as ferramentas apresentadas no item 5.5, se dará observando os seguintes dispositivos:

7.1.1. **Serviço de Firewall de Próxima Geração (Next Generation Firewall - NGFW):**

7.1.1.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de Serviço de Firewall de Próxima Geração durante a vigência do contrato para prestação do serviço;

7.1.1.2. A CONTRATADA deverá realizar as seguintes operações de monitoração da solução de Gerência do Serviço de Firewall de Próxima Geração que inclui, mas não se limita, utilizando o modelo ITIL como referência:

7.1.1.2.1. **Serviço de VPN** (com funcionalidade SSL– Secure Sockets Layer, IPsec e PPTP);

7.1.1.2.2. **Serviço de IDS/IPS** (Sistemas de Detecção e Prevenção de Intrusão)**;**

7.1.1.2.3. **Serviço de Firewall de Aplicação** (WAF);

7.1.1.2.4. **Serviço de Proxy/Filtro de Conteúdo WEB; e**

7.1.1.2.5. **Serviço de filtro de DNS** (Domain Name System).

7.1.1.3. A CONTRATADA deverá realizar as seguintes operações referentes a segurança quanto a monitoração da solução de Firewall, utilizando o modelo ITIL como referência, incluindo, mas não se limitando:

7.1.1.3.1. Guarda e recuperação de logs em serviço do tipo SIEM; e

7.1.1.3.2. Análise de logs, com consequente detecção de problemas gerais ou de segurança da informação.

7.1.1.4. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 7.1.9. deste termo de referência;

7.1.1.5. No Período de Transição Operacional, a CONTRATADA realizará análise de segurança em todo o sistema de Firewall utilizado pela CONTRATANTE e recomendará a melhor configuração, incluindo, mas não se limitando:

7.1.1.5.1. Serviço de VPN;

7.1.1.5.2. Serviço de IDS/IPS;

7.1.1.5.3. Serviço de Firewall de Aplicação;

7.1.1.5.4. Serviço de Proxy/Filtro de Conteúdo WEB;

7.1.1.5.5. Serviço de filtro de DNS;

7.1.1.5.6. Serviço de registro, análise e geração de relatórios em tempo real; e

7.1.1.5.7. Serviço de gerenciamento centralizado.

7.1.1.6. Após aprovação da CONTRATANTE, o serviço gerenciado de segurança implementará as alterações.

7.1.2. **Serviços de Segurança de Mensageria:**

7.1.2.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de segurança de mensageria durante a vigência do contrato para prestação do serviço;

7.1.2.2. A CONTRATADA deverá realizar as seguintes operações referentes a segurança quanto a monitoração da solução mensageria, utilizando o modelo ITIL como referência, incluindo, mas não se limitando:

7.1.2.2.1. Guarda e recuperação de logs em serviço do tipo SIEM;e

7.1.2.2.2. Análise de logs, com consequente detecção de problemas gerais ou de segurança da informação.

7.1.2.3. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 7.1.9. termo de referência;

7.1.2.4. No Período de Transição Operacional, a CONTRATADA realizará análise de segurança em todo o sistema de serviço de tratamento de segurança de mensageria utilizado pela CONTRATANTE e recomendará a melhor configuração, incluindo, mas não se limitando:

7.1.2.4.1. Proteção do Exchange;

7.1.2.4.2. Política de Anti-Spam, Anti-Malware e Anti-Phishing; e

7.1.2.4.3. Links seguros.

7.1.2.5. Após aprovação da CONTRATANTE, o serviço gerenciado de segurança implementará as alterações;

7.1.2.6. A CONTRATANTE poderá adicionar ao Serviço de Tratamento a E-mails Maliciosos o serviço de Governança de Dados Unificados em que a própria CONTRATANTE fornecerá a solução que será utilizada.

7.1.3. **Serviço de Gestão de Pontos de Extremidade:**

7.1.3.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de Gestão de Pontos de Extremidade durante a vigência do contrato para prestação do serviço;

7.1.3.2. A CONTRATADA deverá realizar as seguintes operações referentes a segurança quanto a monitoração das soluções de gestão de Pontos de Extremidade ativos do tipo Desktop e Servidor, utilizando o modelo ITIL como referência, incluindo, mas não se limitando:

7.1.3.2.1. Guarda e recuperação de logs em serviço do tipo SIEM; e

7.1.3.2.2. Análise de logs, com consequente detecção de problemas gerais ou de segurança da informação.

7.1.3.3. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 7.1.9. deste termo de referência;

7.1.3.4. No Período de Transição Operacional, a CONTRATADA realizará análise de segurança em todas as soluções de Gestão de Pontos de Extremidade utilizado pela CONTRATANTE e recomendará a melhor configuração e planos de ação ordenados para execução, incluindo, mas não se limitando:

7.1.3.4.1. Priorização baseada em risco;

7.1.3.4.2. Exceções para recomendações de segurança; e

7.1.3.4.3. Mitigação de vulnerabilidades;

7.1.3.5. Após aprovação da CONTRATANTE, o serviço gerenciado de segurança implementará as alterações;

7.1.3.6. A CONTRATADA deverá efetuar análise de impacto das solicitações de configuração de regras, no que se refere à segurança e desempenho dos equipamentos;

7.1.3.7. A CONTRATADA deverá monitorar todos os computadores internos e externos das soluções de gestão de Pontos de Extremidade, entre estações de trabalho e servidores;

7.1.3.8. A CONTRATADA deverá agir de forma proativa quanto a disseminação ou ação de algum código malicioso dentro da rede a partir dos dispositivos monitorados, informando o responsável da unidade atingida do evento e a ação de correção;

7.1.3.9. A CONTRATADA deverá notificar toda irregularidade detectada pela solução em qualquer servidor corporativo, informando a ação do código malicioso e ação de reparo;

7.1.3.10. A CONTRATADA deverá informar qualquer anomalia na atualização dos agentes da gestão de Pontos de Extremidade Corporativos de qualquer desktop ou servidor;

7.1.3.11. A CONTRATADA deverá monitorar de forma proativa ação de códigos maliciosos disseminadas pelo mundo e prover ações para minimizar a ação destes sobre os ativos da CONTRATANTE;

7.1.3.12. A CONTRATADA deverá analisar códigos suspeitos, identificando-os ou não como código malicioso e quando necessário encaminhá-los ao fabricante quando necessário;

7.1.3.13. A CONTRATADA deve acompanhar toda manutenção requerida das soluções de gestão de Pontos de Extremidade, seja em seu software de gerenciamento ou nos agentes instalados; e

7.1.3.14. A CONTRATANTE poderá adicionar ao Serviço de gestão de Pontos de Extremidade o serviço de Governança de dados unificado em que a própria CONTRATANTE fornecerá a solução que será utilizada.

7.1.4. **Serviço de Gestão de Vulnerabilidades:**

7.1.4.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de gestão de vulnerabilidades durante a vigência do contrato para prestação do serviço;

7.1.4.2. A CONTRATADA deverá realizar as seguintes operações referentes a segurança quanto a monitoração na solução de Gestão de Vulnerabilidades fornecida, utilizado o modelo ITIL como referência, incluindo, mas não se limitando:

7.1.4.2.1. Guarda e recuperação de logs em serviço do tipo SIEM; e

7.1.4.2.2. Análise de logs, com consequente detecção de problemas gerais ou de segurança da informação.

7.1.4.3. A CONTRATADA entregará relatório mensal, utilizando para identificação das vulnerabilidades o Framework MITRE ATT&CK como uma forma de descrever e categorizar os comportamentos identificados. O relatório deverá considerar a predição de ameaças baseadas em fundamentos técnicos e teóricos, incluindo e não se limitando a notícias, fóruns e tendências de segurança cibernética mundiais para colaborar com a CONTRATANTE na definição de estratégias de priorização do tratamento de vulnerabilidades;

7.1.4.4. No Período de Transição Operacional, a CONTRATADA recomendará o plano de ação, a partir da análise do sistema de Gestão de Vulnerabilidades incluindo, mas não se limitando:

7.1.4.4.1. Priorização baseada em risco;

7.1.4.4.2. Classificar softwares que terão tratamento excepcional de segurança;

7.1.4.4.3. Estratégia de gerenciamento das vulnerabilidades; e

7.1.4.4.4. Procedimentos de boas práticas de acesso dos usuários.

7.1.4.5. Após aprovação da CONTRATANTE, o serviço gerenciado de segurança implementará as alterações;

7.1.4.5.1. A CONTRATADA deverá prover inteligência de proteção contra-ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra-ataques cibernéticos, sendo responsável por:

7.1.4.5.1.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATANTE; e

7.1.4.5.1.2. Criar e revisar periodicamente regras (casos de uso) para detecção de ataques no sistema de monitoramento e visibilidade de ataques cibernéticos e sistema de SIEM, realizando as adaptações e evoluções necessárias.

7.1.4.5.1.3. A CONTRATADA deverá, ao final do contrato, manter todas as regras de negócios, correlações e casos de uso na plataforma SIEM da CONTRATANTE

7.1.4.6. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 7.1.9. termo de referência;

7.1.4.7. A Contratada poderá adicionar ao Serviço de Gestão de Vulnerabilidade a prestação do serviço de Governança de dados unificado em que a CONTRATANTE fornecerá a solução que será utilizada.

7.1.5. **Serviço de Gestão de Acessos Privilegiados:**

7.1.5.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de gestão de acessos privilegiados durante a vigência do contrato para prestação do serviço;

7.1.5.2. A CONTRATADA deverá realizar as seguintes operações de monitoração da solução de Serviço de gestão de acessos privilegiados fornecida, utilizado o modelo ITIL como referência, incluindo, mas não se limitando:

7.1.5.2.1. Guarda e recuperação de logs em serviço do tipo SIEM; e

7.1.5.2.2. Análise de logs, com consequente detecção de problemas gerais ou de segurança da informação.

7.1.5.3. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 7.1.9. deste termo de referência;

7.1.5.4. No Período de Transição Operacional, a CONTRATADA recomendará o plano de ação, a partir da análise do serviço de gestão de acessos privilegiados incluindo, mas não se limitando:

7.1.5.4.1. Workflows de aprovação;

7.1.5.4.2. Boas práticas; e

7.1.5.4.3. Revisão da concessão das permissões dos usuários.

7.1.5.5. Após aprovação da CONTRATANTE, o serviço gerenciado de segurança implementará as alterações.

7.1.6. **Serviço de Detecção e Resposta de Rede (Network Detection and Response - NDR):**

7.1.6.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de Detecção e Resposta de Rede durante a vigência do contrato para prestação do serviço;

7.1.6.2. A CONTRATADA deverá realizar as seguintes operações referentes a segurança quanto a monitoração da ferramenta de Detecção e Resposta de Rede durante a vigência do contrato para prestação do serviço utilizando o modelo ITIL como referência, incluindo, mas não se limitando:

7.1.6.2.1. Guarda e recuperação de logs em serviço do tipo SIEM; e

7.1.6.2.2. Análise de logs e fluxos de rede com consequente detecção de problemas gerais ou de segurança da informação.

7.1.6.2.3. Interação com os fabricantes das soluções;

7.1.6.2.4. Backup e restore de configurações;

7.1.6.2.5. Resolução de problemas;

7.1.6.2.6. Suporte técnico;

7.1.6.2.7. Instalação de serviços adicionais;

7.1.6.2.8. Atualizações, de acordo com as recomendações do fabricante; e

7.1.6.2.9. Ativação de licenças a serem disponibilizadas pela CONTRATANTE.

7.1.6.3. Os comportamentos anômalos de aplicações, serviços e infraestrutura detectados pelo monitoramento contínuo e ininterrupto do ambiente da CONTRATANTE, relacionados à segurança da informação, deverão ser transformados em incidentes de segurança da informação, conforme definido em processo de gestão de incidentes;

7.1.6.4. Os comportamentos anômalos de aplicações, serviços e infraestrutura detectados pelo monitoramento contínuo e ininterrupto do ambiente da CONTRATANTE, relacionados à qualidade operacional, deverão ser informados através de relatórios mensais. Caso o impacto do comportamento anômalo seja considerado grave, deverá ser gerado um incidente de segurança da informação, conforme definido em processo de gestão de incidentes;

7.1.6.4.1. A CONTRATADA deverá prover inteligência de proteção contra-ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra-ataques cibernéticos, sendo responsável por:

7.1.6.4.1.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATANTE; e

7.1.6.4.1.2. Criar e revisar periodicamente regras (casos de uso) para detecção de ataques no sistema de monitoramento e visibilidade de ataques cibernéticos e sistema de SIEM, realizando as adaptações e evoluções necessárias.

7.1.6.5. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 7.1.9. deste termo de referência;

7.1.6.6. No Período de Transição Operacional, a CONTRATADA recomendará o plano de ação, a partir da análise do Serviço de Detecção e Resposta de Rede incluindo, mas não se limitando:

7.1.6.6.1. Revisão das configurações dos equipamentos;

7.1.6.6.2. Revisão da concessão das permissões dos usuários; e

7.1.6.6.3. Classificação de riscos da rede e recomendar as regras de acesso.

7.1.6.7. Após aprovação da CONTRATANTE, o serviço gerenciado de segurança implementará as alterações.

7.1.7. **Serviço de SIEM (Security Information and Event Management):**

7.1.7.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de SIEM durante a vigência do contrato para prestação do serviço;

7.1.7.2. A CONTRATADA deverá realizar as seguintes operações de administração, gerenciamento e monitoração da CONTRATANTE, utilizado o modelo ITIL como referência, incluindo, mas não se limitando:

7.1.7.2.1. Criação e manutenção de regras de correlação;

7.1.7.2.2. Criação, manutenção e refinação de regras para geração de alertas;

7.1.7.2.3. Realização de configurações;

7.1.7.2.4. Criar e realizar manutenção de regras de automação para tratamento de incidentes;

7.1.7.2.5. Adição e remoção de ativos da base do SIEM;

7.1.7.2.6. Geração de novos dashboards e relatórios de acompanhamento;

7.1.7.2.7. Backup e restore de configurações;

7.1.7.2.8. Resolução de problemas;

7.1.7.2.9. Suporte técnico;

7.1.7.2.10. Instalação de serviços adicionais;

7.1.7.2.11. Atualizações, de acordo com as recomendações do fabricante; e

7.1.7.2.12. Ativação de licenças a serem disponibilizadas pela CONTRATANTE.

7.1.7.3. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 7.1.9. deste termo de referência;

7.1.7.4. A CONTRATADA deverá acompanhar e notificar a CONTRANTANTE sobre os gastos previstos planejados, bem como otimizá-los, para que possam ser eficientes em seu armazenamento, sem prejudicar seu correto funcionamento previsto;

7.1.7.5. Registros detalhados dos sistemas deverão estar disponíveis na CONTRATANTE on-premisse, sendo enviados apenas os logs relevantes para detecção de incidentes à central de logs do SIEM da CONTRATANTE;

7.1.7.6. A CONTRATADA deverá avaliar e propor a otimização de envio de dados dos sistemas para a central de logs do SIEM;

7.1.7.7. A CONTRATADA deverá ter autorização da CONTRATANTE para adicionar novos conectores à ferramenta de SIEM;

7.1.7.8. A base de conhecimento da CONTRATANTE deverá ser utilizada como base para a implementação de regras de automação no sistema de SIEM da CONTRATADA;

7.1.7.9. A CONTRATADA deverá, durante o Período de Transição Operacional, elaborar um plano de ação, a partir da análise do SIEM, incluindo, mas não se limitando:

7.1.7.9.1. Uso de conectores;

7.1.7.9.2. Aplicação de regras de análises; e

7.1.7.9.3. A CONTRATADA documentará a configuração do sistema de SIEM, e será a principal responsável pela manutenção e atualização dele, até o final do contrato.

7.1.8. **Serviço de Detecção e Respostas a Incidentes de Segurança (Blue Team)**:

7.1.8.1. Tem por objetivo analisar, documentar e indicar como conter e remediar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal

serviço deverá ser executado obedecendo aos frameworks NIST e SANS de resposta a incidente de segurança da informação e boas práticas de mercado;

7.1.8.1.1. Manter logs de auditoria de todas as ações realizadas em sistemas da CONTRATANTE. Esses dados poderão ser requisitados pela CONTRATANTE a qualquer momento

7.1.8.2. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, podendo levar, ou não, a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade e Privacidade;

7.1.8.3. O início do processo de resposta a incidente de segurança se dará das seguintes formas:

7.1.8.3.1. Sempre que um evento adverso for submetido à CONTRATADA, pelo corpo técnico da CONTRATANTE, a qualquer tempo;

7.1.8.3.2. A partir de consultas diárias ao sistema de monitoramento e visibilidade de ataques cibernéticos, deve identificar situações em que os pontos de extremidade, sistemas ou usuários apresentem comportamentos comprovadamente ou potencialmente nocivos a segurança dos dados;

7.1.8.3.3. Após o incidente de segurança ser aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs, pacotes, flows e demais artefatos coletados, a fim de no primeiro instante, identificar do que se trata o incidente e avaliar o risco dele;

7.1.8.3.3.1. Uma vez realizadas as análises iniciais do incidente, o grupo de resposta a incidente de segurança da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE;

7.1.8.3.3.2. Como próximo passo, o grupo de resposta a incidente de segurança da CONTRATADA, deverá comunicar ao time de segurança da informação do CONTRATANTE as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente; e

7.1.8.3.3.3. Caso identifique ações que possam afetar muitos dispositivos e/ou serviços considerados críticos pela CONTRANTE, deverá elaborar plano de ação com abertura de chamados junto a equipe de Serviços Gerenciados de Segurança.

7.1.8.3.4. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente e urgência referindo-se à velocidade necessária para resolver um incidente;

7.1.8.4. Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e todos os seus artefatos coletados;

7.1.8.5. Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança da CONTRATADA deverá definir uma estratégia para a mitigação e contenção do ataque em questão;

7.1.8.6. Ao longo do processo de resposta ao incidente de segurança, a CONTRATADA através do grupo de resposta a incidente de segurança, deve documentar toda e quaisquer evidências e identificação dos serviços e usuários envolvidos. Tais evidências serão utilizadas até a finalização do processo pela CONTRATADA, para execução de análise forense do caso. A análise deve ser realizada com o objetivo de identificar pessoas, locais e/ou eventos relacionados, correlacionando todas as informações reunidas, gerando como produto final um laudo sobre o incidente de segurança em questão;

7.1.8.7. Toda e qualquer atividade relacionada com análise forense deverá ser realizada por parceiro subcontratado pela CONTRATADA a fim de manter a visão agnóstica ao serviço prestado com uma quantidade determinada de acionamentos

7.1.8.8. Para análise forense, caso seja necessária a reconstrução do ataque, este deverá ser realizado pela CONTRATADA em ambiente controlado, usando-se, por exemplo, de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). A CONTRATADA deve dispor de ambiente controlado que suporte os testes;

7.1.8.8.1. O escopo de análise forense digital se limitará às seguintes atividades, devendo elas serem realizadas através de empresa subcontratada visando manter a isenção sobre o processo até 2 (duas) vezes por ano sob demanda através do envio de ordens de serviços:

7.1.8.8.1.1. No processo de coleta de evidências, especialistas em análise forense utilizam métodos adequados para preservar a integridade dos dados, garantindo que nenhuma informação crucial seja comprometida ou corrompida. Isso pode envolver a criação de cópias forenses de dispositivos, aquisição de dados em mídias digitais ou extração de informações de sistemas em rede.

7.1.8.8.1.2. Na fase de análise técnica, deverão ser aplicadas técnicas forenses básicas para identificar e examinar os dados coletados. Isso pode incluir a busca por arquivos relevantes, análise de registros de atividades, recuperação de dados apagados, identificação de padrões de uso e análise de metadados. Os especialistas também podem utilizar ferramentas forenses básicas para examinar documentos, e-mails, histórico de navegação e comunicações em redes sociais, a fim de reconstruir eventos e relacionamentos digitais relevantes.

7.1.8.8.1.3. Ao concluir a análise, um laudo técnico deverá ser elaborado, descrevendo as descobertas, os métodos utilizados e as conclusões tiradas com base nas evidências digitais examinadas. O laudo técnico deve ser objetivo, detalhado e claro, fornecendo informações essenciais para apoiar investigações e processos judiciais.

7.1.8.8.1.4. A Entrevista Forense é uma etapa crucial que deverá envolver a interação com indivíduos relacionados ao caso, como vítimas, suspeitos, testemunhas ou responsáveis pelo sistema afetado, limitado à 3 pessoas indicadas pela CONTRATANTE. Os especialistas deverão conduzir entrevistas estruturadas para obter informações relevantes sobre o incidente, identificar potenciais fontes de evidências digitais, compreender o contexto do caso e determinar os objetivos da investigação.

7.1.8.8.1.5. A Coleta Forense é uma atividade essencial para obter evidências digitais de maneira precisa, legalmente admissível e forensicamente sólida. Os especialistas em análise forense digital deverão empregar técnicas avançadas de coleta, utilizando ferramentas e metodologias adequadas para extrair dados de dispositivos e sistemas sem comprometer a integridade das evidências. Isso pode envolver a coleta de mídias de armazenamento, como discos rígidos, dispositivos móveis ou servidores, bem como a captura de dados em tempo real de sistemas em rede limitado à até 3 dispositivos como laptops, estações de trabalho, servidores e dispositivos de armazenamento de dados, preservando a cadeia de custódia.

7.1.8.8.1.6. Ao adicionar essas atividades, espere-se que a análise forense digital aprimore a abrangência e a profundidade da investigação, permitindo uma compreensão mais completa dos eventos digitais relevantes. Essas etapas adicionais devem reforçar a robustez do processo forense, fornecendo informações adicionais para a análise técnica e enriquecendo o laudo técnico final.

7.1.8.9. O grupo de resposta a incidente de segurança da CONTRATADA deve documentar as lições aprendidas no incidente de segurança em questão na base de conhecimentos da CONTRATANTE, formando durante todo o período de vigência do contrato, uma base de conhecimento sobre ataques adversos;

7.1.8.10. A base de conhecimento deverá ser utilizada para a implementação de solução de SOAR (Security Orchestration, Automation and Response) da CONTRATANTE, que deverá ser utilizada para agilizar e otimizar o processo de resposta a incidentes de segurança da informação;

7.1.8.11. A solução de SOAR, deverá ser operada pela CONTRATADA de forma conjunta com a solução de SIEM existente da CONTRATANTE;

7.1.8.12. Poderá ser utilizada ferramenta complementar da CONTRATADA, sem custos adicionais a CONTRATANTE, para auxiliar na resposta rápida a incidentes. No entanto, as ações adotadas deverão ser implementadas na solução de SOAR da CONTRATANTE, promovendo sua autonomia;

7.1.8.13. Qualquer automação para defesa realizada pela CONTRATADA deverá ser implantada nas ferramentas de automação da CONTRATANTE, estando sujeitas a ajustes, que quando necessários, deverão serem justificados;

7.1.8.14. O serviço de resposta a incidentes será responsável por monitorar, configurar e operar o sistema de monitoramento e visibilidade de ataques cibernéticos e o sistema de SIEM, visando a análise de logs, correlações, flows e pacotes das redes envolvidas;

7.1.8.15. A CONTRATADA deverá prover inteligência de proteção contra-ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra-ataques cibernéticos, sendo responsável por:

7.1.8.15.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATANTE;

7.1.8.15.2. A CONTRATADA deverá executar semestralmente exercícios de melhoria contínua do time de defesa considerando no mínimo 10 TTPs (Técnicas, Tácicas e Procedimentos) elencados no M1tre &ttack, também conhecidos como exercícios de Purple Team.

7.1.8.15.3. Criar e revisar periodicamente regras (casos de uso) para detecção de ataques no sistema de monitoramento e visibilidade de ataques cibernéticos e sistema de SIEM, realizando as adaptações e evoluções necessárias;

7.1.8.15.4. O serviço deve ser capaz de gerar detecções baseadas no framework do MITREATTACK possuindo no mínimo 15 regras de detecções para as fases previstas no framework e que as detecções sejam atualizadas regularmente

7.1.8.15.5. Implementar procedimentos para triagem de alertas e resposta a incidentes; e

7.1.8.15.6. A CONTRATADA deverá oferecer periodicamente exercícios de melhoria contínua dos times do SOC.

7.1.8.16. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 7.1.9. deste termo de referência

7.1.8.17. O relatório deverá considerar a predição de ameaças baseadas em fundamentos técnicos e teóricos, incluindo e não se limitando a notícias, fóruns e tendências de segurança

cibernética mundiais para colaborar com a CONTRATANTE na definição de estratégias para prevenção de incidentes de segurança;

7.1.8.18. A CONTRATADA deverá realizara apresentação do relatório mensal dos incidentes de segurança, contendo planos de ação para melhorias nos ambientes;

7.1.8.19. A CONTRATANTE poderá adicionar ao Serviço de Gestão de Incidentes de Segurança o serviço de Governança de Dados Unificado em que a própria CONTRATANTE fornecerá a solução que será utilizada;

7.1.9. **Relatórios da prestação de serviços de SOC:**

7.1.9.1. A CONTRATADA deverá entregar relatórios mensais com, pelo menos, as seguintes informações:

Item	Título	Descrição
1	Serviço de Serviço de Firewall de Próxima Geração (Next Generation Firewall - NGFW)	Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Oportunidades pontuais de melhoria do serviço. Gráfico de aplicações utilizadas; principais aplicações por utilização de largura de banda de entrada e saída; principais aplicações por taxa de transferência de bytes; Principais hosts por número de ameaças identificadas; atividades de um usuário específico e grupos de usuários, incluindo aplicações acessadas, categorias de URL e as ameaças (IPS, Anti-Malware, Antivírus e Anti-spyware) vinculadas a este tráfego; visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-spyware), URLs e filtro de arquivos (quando aplicável).
2	Serviços de segurança de mensageria	Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Oportunidades pontuais de melhoria do serviço. Exchange: Quarentena Uso de rótulo de confidencialidade
3	Serviço de Gestão de Pontos de Extremidade;	Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Oportunidades pontuais de melhoria do serviço. Relatório de regras de redução de superfície de ataque Relatório de firewall Relatório de proteção da Web Relatório de integridade do dispositivo Relatório de incidentes Relatório de proteção contra ameaças
4	Serviço de Gestão de Vulnerabilidades	Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Relatório de inteligência contra ameaças, baseado em previsões de probabilidade de violação, contextos de negócios e avaliações de dispositivo; Oportunidades pontuais de melhoria do serviço.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

		Relatório de dispositivos vulneráveis Relatório de regras de redução de superfície de ataque
5	Serviço de Gestão de Acessos Privilegiados	Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Oportunidades pontuais de melhoria do serviço. Relatório de acompanhamento de trocas; Relatório de erros de trocas;
6	Serviço de Detecção e Resposta de Rede (Network Detection and Response - NDR)	Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Oportunidades pontuais de melhoria do serviço. Relatório de incidentes Relatório de anomalias e atividades maliciosas de redes
7	Serviço de SIEM (Security Information and Event Management	Gráficos com Eventos e alertas por tempo Tempo médio de resposta do SOC Status dos Incidentes Total de incidentes identificados Tipos de incidentes encontrados Top 10 de usuários relacionados a incidentes Top 10 de dispositivos relacionados a incidentes Relatório de atividades de mensageria Relatório das atividades do Office 365 Oportunidades pontuais de melhoria do serviço. Quadro-resumo dos chamados registrados no período; Análise dos pontos de atenção;
8	Serviço de Detecção e Respostas a Incidentes de Segurança (Blue Team).	Gráficos de Indicadores do serviço; Resumo das operações relacionadas a análise de logs Volumetria de Logs Oportunidades pontuais de melhoria do serviço. Quadro-resumo dos chamados registrados no período; Análise dos pontos de atenção; Deverá apresentar semestralmente relatório dos exercícios de melhoria contínua do time de defesa considerando no mínimo 10 TTPs (Técnicas, Tácicas e Procedimentos) elencados no M1tre &ttack, também conhecidos como exercícios de Purple Team

7.1.9.2. Além dos relatórios (mensais, semestrais) previstos em cada um dos itens que compõem os lotes, deverá ser fornecido um Relatório gerencial de serviços (RGS) que deverá possuir, no mínimo, os Indicadores de Níveis de Serviço listados neste termo de referência;

8. DESCRIÇÃO DA SOLUÇÃO – SERVIÇO MSS

8.1. A execução dos serviços de MSS, utilizando as ferramentas apresentadas no item 5.5, se dará observando os seguintes dispositivos:

8.1.1. **Serviço de Firewall de Próxima Geração (Next Generation Firewall - NGFW):**

8.1.1.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de Next Generation Firewall durante a vigência do contrato para prestação do serviço.

8.1.1.2. A CONTRATADA deverá realizar as seguintes operações de administração, gerenciamento da solução de Gerência dos Next Generation Firewall que inclui, utilizando o modelo ITIL como referência, mas não se limitando:

8.1.1.2.1. Serviço de VPN (com funcionalidade SSL– Secure Sockets Layer, IPsec e PPTP);

8.1.1.2.2. Serviço de IDS/IPS (Sistemas de Detecção e Prevenção de Intrusão);

8.1.1.2.3. Serviço de Firewall de Aplicação (WAF);

8.1.1.2.4. Serviço de Proxy/Filtro de Conteúdo WEB; e

8.1.1.2.5. Serviço de filtro de DNS (Domain Name System).

8.1.1.3. A CONTRATADA deverá realizar as seguintes operações referentes a segurança quanto a monitoração da solução mensageria utilizando o modelo ITIL como referência, incluindo, mas não se limitando a:

8.1.1.3.1. Realização de configurações;

8.1.1.3.2. Interação com os fabricantes das soluções;

8.1.1.3.3. Backup e restore de configurações;

8.1.1.3.4. Resolução de problemas;

8.1.1.3.5. Suporte técnico;

8.1.1.3.6. Instalação de serviços adicionais;

8.1.1.3.7. Atualizações, de acordo com as recomendações do fabricante; e

8.1.1.3.8. Ativação de licenças a serem disponibilizadas pela CONTRATANTE.

8.1.1.4. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 8.1.6. deste mesmo termo de referência;

8.1.1.5. A CONTRATADA documentará as configurações dos sistemas de Firewall utilizados pela CONTRATANTE, e será a principal responsável pela manutenção e atualização dele, até o final do contrato;

8.1.1.6. A CONTRATADA deverá efetuar análise de impacto das solicitações de configuração de regras, no que se refere à segurança e desempenho dos equipamentos; e

8.1.1.7. Deverá implementar as configurações aprovadas pela CONTRATANTE.

8.1.2. **Serviços de segurança de mensageria:**

8.1.2.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de segurança de mensageria durante a vigência do contrato para prestação do serviço;

8.1.2.2. A CONTRATADA deverá as seguintes operações referentes a segurança quanto a administração, gerenciamento da solução mensageria, utilizando o modelo ITIL como referência, incluindo, mas não se limitando:

8.1.2.2.1. Administração de regras;

8.1.2.2.2. Atualização de assinaturas;

8.1.2.2.3. Realização de configurações;

8.1.2.2.4. Interação com os fabricantes das soluções;

8.1.2.2.5. Backup e restore de configurações;

8.1.2.2.6. Resolução de problemas;

8.1.2.2.7. Suporte técnico;

8.1.2.2.8. Instalação de serviços adicionais;

8.1.2.2.9. Atualizações, de acordo com as recomendações do fabricante; e

8.1.2.2.10. Ativação de licenças a serem disponibilizadas pela CONTRATANTE.

8.1.2.3. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 8.1.6. deste termo de referência;

8.1.2.4. Deverá implementar as configurações aprovadas pela CONTRATANTE;

8.1.2.5. A CONTRATADA documentará a configuração do sistema de tratamentos de e-mails maliciosos utilizado pela CONTRATANTE, e será a principal responsável pela manutenção e atualização dele, até o final do contrato;

8.1.2.6. A CONTRATADA deverá efetuar análise de impacto das solicitações de configuração de regras, no que se refere à segurança e desempenho dos equipamentos;

8.1.2.7. A CONTRATANTE poderá adicionar ao Serviço de Tratamento a E-mails Maliciosos o serviço de Governança de Dados Unificados em que a própria CONTRATANTE fornecerá a solução que será utilizada.

8.1.3. **Serviço de Gestão de Pontos de Extremidade:**

8.1.3.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de Gestão de Pontos de Extremidade durante a vigência do contrato para prestação do serviço;

8.1.3.2. A CONTRATADA deverá realizar as seguintes operações referentes a segurança quanto a administração, gerenciamento das soluções de gestão de Pontos de Extremidade ativos do tipo Desktop e Servidor, utilizando o modelo ITIL como referência, incluindo, mas não se limitando:

8.1.3.2.1. Administração de regras;

8.1.3.2.2. Atualização de assinaturas;

8.1.3.2.3. Configuração de exceções;

8.1.3.2.4. Realização de configurações;

8.1.3.2.5. Interação com os fabricantes das soluções;

8.1.3.2.6. Backup e restore de configurações;

8.1.3.2.7. Resolução de problemas;

8.1.3.2.8. Suporte técnico;

8.1.3.2.9. Instalação de serviços adicionais;

8.1.3.2.10. Atualizações, de acordo com as recomendações do fabricante; e

8.1.3.2.11. Ativação de licenças a serem disponibilizadas pela CONTRATANTE;

8.1.3.3. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 8.1.6. deste termo de referência;

8.1.3.4. Deverá implementar as configurações aprovadas pela CONTRATANTE;

8.1.3.5. A CONTRATADA documentará a configuração do sistema de Gestão de Pontos de Extremidade utilizado pela CONTRATANTE, e será a principal responsável pela manutenção e atualização dele, até o final do contrato;

8.1.3.6. A CONTRATANTE poderá adicionar ao Serviço de gestão de Pontos de Extremidade o serviço de Governança de dados unificado em que a própria CONTRATANTE fornecerá a solução que será utilizada.

8.1.4. **Serviço de Gestão de Vulnerabilidades:**

8.1.4.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de gestão de vulnerabilidades durante a vigência do contrato para prestação do serviço;

8.1.4.2. A CONTRATADA deverá realizar as seguintes operações referentes a segurança quanto a administração, gerenciamento na solução de Gestão de Vulnerabilidades fornecida, utilizado o modelo ITIL como referência, incluindo, mas não se limitando:

8.1.4.2.1. Realização de scans;

8.1.4.2.2. Detecção e identificação de ativos;

8.1.4.2.3. Atualização de base de vulnerabilidades;

8.1.4.2.4. Realização de configurações;

8.1.4.2.5. Interação com os fabricantes das soluções;

8.1.4.2.6. Backup e restore de configurações;

8.1.4.2.7. Resolução de problemas;

8.1.4.2.8. Suporte técnico;

8.1.4.2.9. Instalação de serviços adicionais;

8.1.4.2.10. Atualizações, de acordo com as recomendações do fabricante; e

8.1.4.2.11. Ativação de licenças a serem disponibilizadas pela CONTRATANTE.

8.1.4.3. Deverá implementar as configurações aprovadas pela CONTRATANTE.

8.1.4.4. A CONTRATADA documentará a configuração do sistema de Gestão de Vulnerabilidades fornecido, e será a principal responsável pela manutenção e atualização dele, até o final do contrato.

8.1.4.5. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 8.1.6. deste termo de referência;

8.1.4.6. A Contratada poderá adicionar ao Serviço de Gestão de Vulnerabilidade a prestação do serviço de Governança de dados unificado em que a CONTRATANTE fornecerá a solução que será utilizada.

8.1.5. **Serviço de Gestão de Acessos Privilegiados:**

8.1.5.1. A CONTRATADA deverá fazer uso da solução que a CONTRATANTE fornecer como ferramenta de gestão de acessos privilegiados durante a vigência do contrato para prestação do serviço;

8.1.5.2. A CONTRATADA deverá realizar as seguintes operações de administração, gerenciamento da solução de Serviço de gestão de acessos privilegiados fornecida, utilizado o modelo ITIL como referência, incluindo, mas não se limitando:

8.1.5.2.1. Realização de configurações;

8.1.5.2.2. Backup e restore de configurações;

8.1.5.2.3. Resolução de problemas;

8.1.5.2.4. Suporte técnico;

8.1.5.2.5. Instalação de serviços adicionais;

8.1.5.2.6. Atualizações, de acordo com as recomendações do fabricante; e

8.1.5.2.7. Ativação de licenças a serem disponibilizadas pela CONTRATANTE.

8.1.5.3. A CONTRATADA entregará relatório mensal, específico para este serviço, de acordo com o item 8.1.6. deste termo de referência

8.1.5.4. A CONTRATADA documentará a configuração do sistema Gestão de Acessos Privilegiados fornecido, e será a principal responsável pela manutenção e atualização dele, até o final do contrato;

8.1.6. **Relatórios para os serviços de MSS:**

8.1.6.1. A CONTRATADA deverá entregar relatórios mensais com, pelo menos, as seguintes informações:

Item	Título	Descrição
1	Serviço de Next Generation Firewall (NGFW)	Resumo gráfico de aplicações utilizadas; principais aplicações por utilização de largura de banda de entrada e saída; principais aplicações por taxa de transferência de bytes; situação do dispositivo e do cluster; administradores autenticados na gerência da plataforma de segurança; número de sessões simultâneas;utilização dos recursos por aplicações, URL, ameaças IPS, Anti-spyware, entre outros. ; status das interfaces e consumo de recursos do appliance.
2	Serviços de segurança de mensageria	Exchange: Atividade de email Uso do aplicativo de email Uso de caixa de correio Office 365: Atividades de grupos Quadro-resumo dos chamados registrados no período; Oportunidades pontuais de melhoria do serviço.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3	Serviço de Gestão de Pontos de Extremidade;	Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Oportunidades pontuais de melhoria do serviço. Relatório de regras de redução de superfície de ataque Relatório de firewall Relatório de proteção da Web Relatório de integridade do dispositivo Relatório de incidentes Relatório de proteção contra ameaças
4	Serviço de Gestão de Vulnerabilidades	Score de Segurança Score de Exposição Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Relatório de inteligência contra ameaças, baseado em previsões de probabilidade de violação, contextos de negócios e avaliações de dispositivo; Oportunidades pontuais de melhoria do serviço. Relatório de dispositivos vulneráveis pendentes de correção Relatório de regras de redução de superfície de ataque
5	Serviço de Gestão de Acessos Privilegiados	Gráficos de Indicadores do serviço; Análise dos pontos de atenção; Quadro-resumo dos chamados registrados no período; Oportunidades pontuais de melhoria do serviço. Relatórios PCI; Relatórios de Gestão de Eventos; Relatórios de Auditoria; Relatórios de Alertas;

8.1.6.2. Além dos relatórios mensais previstos em cada um dos itens que compõem os lotes, deverá ser fornecido um Relatório gerencial de serviços (RGS) que deverá possuir, no mínimo, os Indicadores de Níveis de Serviço listados neste termo de referência.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

9. MODELO DE GESTÃO DO CONTRATO

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

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

9.1.3. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim;

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

9.1.5. Preposto

9.1.6. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

9.1.7. Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade

9.1.8. Reunião Inicial

9.1.9. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

9.1.10. A pauta desta reunião observará, pelo menos:

9.1.11. Presença do representante legal da contratada, que apresentará o seu preposto;

9.1.12. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

9.1.13. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

9.1.14. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

10. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO:

10.1. **Relativo ao Serviço SOC:**

10.1.1. Faturamento e Pagamento:

10.1.1.1. Os pagamentos serão efetuados mensalmente. Os trâmites de faturamento terão início, mensalmente, com o envio pela CONTRATADA dos Relatórios Gerenciais de Serviços (RGS), que serão validados pelo fiscal do contrato, que avaliará os níveis de qualidade do serviço para fins de pagamento. Após o aceite formal dos RGS a CONTRATADA poderá emitir o documento credor relativo aos serviços prestados;

10.1.2. Níveis Mínimos de Serviço Exigidos (NMSE):

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

10.1.2.2. A meta exigida representa o parâmetro de valor exato (=), limite máximo (<=) ou limite mínimo (>=) que deve ser alcançado pela CONTRATADA para cada um dos indicadores que deverão ser medidos do primeiro ao último dia de cada mês.

10.1.2.3. A CONTRATADA sofrerá glosa de 1% (um ponto percentual), sobre o valor mensal do contrato, a cada 15 pontos ou percentual proporcional ao número de pontos, levando em consideração a relação: glosa de 1% a cada 15 pontos.

10.1.2.4. Os tempos serão contados a partir do recebimento de incidente / requisição / ordem de serviço. No caso da contagem em dias, a contagem é efetuada dia a dia, incluindo o primeiro e o último dia.

10.1.2.5. No caso da resolução de incidentes, se o mesmo não tiver a sua causa raiz conhecida, ou seja, existe um problema a ser resolvido, a CONTRATADA é obrigada a aplicar uma solução de contorno na resolução do incidente para que o serviço volte à sua operação padrão.

10.1.2.6. Os níveis de serviço serão mensurados de forma automatizada e não poderão ser manipulados pela empresa CONTRATADA.

10.1.3. A CONTRATADA se responsabilizará somente pelos índices que reflitam as requisições de serviços e incidentes designados a ela, não poderá ser responsabilizada por chamados pendentes de fornecedores/prestadores de serviços externos ou encaminhados a outros níveis, ou situações que dependam de terceiros, que, desta forma, não poderão ser computados.

10.1.4. Por requisições de serviço e incidentes reabertos entende-se que são requisições de serviço ou incidentes que foram dados como resolvidos, porém os mesmos ainda permanecem pendentes de resolução.

10.1.5. Os serviços serão medidos com base em indicadores e níveis mínimos de serviço, vinculados a fórmulas de cálculo específicas, e deverão ser executados pela CONTRATADA, e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela adiante.

10.1.6. A CONTRATADA deverá manter os seguintes níveis de qualidade para a prestação dos Serviços escopo desta contratação:

Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Meta Exigida	Glosa por inadimplemento
Tempo máximo para triagem e notificação de incidentes de segurança	Tempo = Hora de triagem – Hora de entrada do evento de segurança Onde: Hora Entrada de evento de segurança é	<=30 minutos	10 pontos (+ 3 Pontos a cada 5 minutos excedentes), por ocorrência

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

	horário em que qualquer incidente é identificado nas ferramenta de análise de segurança Hora da triagem é a momento da classificação do incidente.		
Tempo máximo para instauração de comitê de crise (war room)	Tempo = Hora da instauração do comitê de crise – Hora da triagem Onde: Hora da instauração do comitê de crise é horário em que é instaurado uma reunião com os interessados ao incidente Hora da triagem é a momento da classificação do incidente.	<=30 minutos	15 pontos (+ 3 Pontos a cada 5 minutos excedentes) ,por ocorrência
Tempo máximo para abertura de chamados de suporte com terceiros	Tempo = Hora da abertura do chamado – hora da triagem Onde: Hora da abertura do chamado é horário em que é aberto o chamado com fornecedores através das plataformas oficiais Hora da triagem é a momento da classificação do incidente.	<= 60 minutos	5 pontos (+2 pontos a cada 5 minutos excedentes), por ocorrência
Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço	Prazo Real em dias/Prazo acordado em dias Onde: Prazos serão decididos através de um planejamento em conjunto entre CONTRATADA E CONTRATANTE.	<= 1,25	15 pontos, por ocorrência
Tempo máximo para resolução das requisições de serviços	Tempo = Hora da resolução da requisição – hora da requisição Onde: Hora da requisição é o momento da abertura da requisição. Hora da resolução é o momento da conclusão da requisição.	<= 16 horas	10 pontos (+3 pontos a cada hora excedente), por ocorrência

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

Tempo máximo para resposta para esclarecimentos requisitados	Dias totais de resolução = Dia da resposta - Dia da requisição Onde: Dia da requisição é o momento da abertura da requisição. Dia da resposta é o momento do retorno do questionamento.	<= 1 dia útil	10 pontos (+3 pontos a cada dia excedente) ,por ocorrência
Tempo máximo para resolução das requisições de serviços não padrão	Dias totais de resolução = Dia da resposta - Dia da requisição Onde: Dia da requisição é o momento da abertura da requisição. Dia da resolução da requisição é momento de conclusão da requisição	<= 5 dias	10 pontos (+3 pontos a cada hora excedente) ,por ocorrência
IAP – ÍNDICE DE ATENDIMENTO NO PRAZO **(Incidentes)**	IAP = 100 * (ΣQtap / ΣQtr) Onde: IAP = Indicador de atendimento aos prazos do serviço; ΣQtap = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência; ΣQtr = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.	85% <= IAP < 95% 75% <= IAP < 85% IAP < 70%	150 Pontos 300 pontos 450 pontos

10.1.7. Serão aplicadas as referidas pontuações para efeito de glosa, no caso de:

Nº	Descrição	Referência	Glosa por inadimplemento
1	Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução.	Por ocorrência	10 pontos
2	Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação.	Por ocorrência	5 pontos

3	Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução.	Por ocorrência	5 pontos
4	Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada.	Por ocorrência	5 pontos
5	Alterar indicadores/metas de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado.	Por ocorrência	100 pontos
6	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, ainda que em casos de substituição temporária.	Por ocorrência	30 pontos
7	Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais.	Por ocorrência	50 pontos
8	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	200 pontos
9	Deixar de comunicar ao CONTRATANTE a substituição de profissionais responsáveis pela execução das atividades.	Por ocorrência	10 pontos
10	Deixar de atuar tempestivamente no caso de incidentes graves	Por ocorrência	15 pontos
11	Deixar de cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato.	Por ocorrência	10 pontos
12	Deixar de atuar proativamente em caso de identificação de situação de desconformidade com boas práticas de segurança.	Por ocorrência	10 pontos
13	Deixar de apresentar os relatórios consolidados conforme exigências do Termo de Referência.	Por ocorrência	5 pontos
14	Deixar de apresentar mensalmente proposta de melhorias no ambiente.	Por ocorrência	5 pontos
15	Deixar de elaborar plano de capacitação caso não possua as certificações exigidas.	Por ocorrência	50 pontos
16	Deixar de cumprir quaisquer obrigações estabelecidas no contrato e anexos, não previstas nesta tabela, após reincidência formalmente notificada pela CONTRATANTE.	Por ocorrência	15 pontos

10.1.8. Os primeiros 60 (noventa) dias após o início da execução dos serviços serão considerados como período de estabilização, durante o qual os resultados esperados e os níveis de qualidade exigidos poderão ser implementados gradualmente, de modo a permitir à CONTRATADA realizar a

adequação progressiva de seus serviços e alcançar, ao término desse período, o desempenho requerido. Essa flexibilização, porém, será restrita aos limites destacados a seguir:

10.1.8.1. Para o 1º (primeiro) mês de execução: serão considerados 65% (setenta e cinco por cento) do total de pontos dos níveis de qualidade para o cálculo de glosa sobre o valor da fatura;

10.1.8.2. Para o 2º (segundo) mês de execução: serão considerados, 80% (oitenta por cento) do total de pontos dos níveis de qualidade para o cálculo de glosa sobre o valor da fatura;

10.1.8.3. Para o 3º (terceiro) mês de execução: serão considerados, 100% (cem por cento) do total de pontos dos níveis de qualidade para o cálculo de glosa sobre o valor da fatura;

10.1.9. Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização.

10.2. **Relativo ao Serviço MSS:**

10.2.1. Faturamento e Pagamento

10.2.1.1. Os pagamentos serão efetuados mensalmente. Os trâmites de faturamento terão início, mensalmente, com o envio pela CONTRATADA dos Relatórios Gerenciais de Serviços (RGS), que serão validados pelo fiscal do contrato, que avaliará os níveis de qualidade do serviço para fins de pagamento. Após o aceite formal dos RGS a CONTRATADA poderá emitir o documento credor relativo aos serviços prestados.

10.2.2. Níveis Mínimos de Serviço Exigidos (NMSE)

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

10.2.2.2. A meta exigida representa o parâmetro de valor exato (=), limite máximo (<=) ou limite mínimo (>=) que deve ser alcançado pela CONTRATADA para cada um dos indicadores que devem ser medidos do primeiro ao último dia de cada mês.

10.2.2.3. A CONTRATADA sofrerá glosa de 1% (um por cento), sobre o valor mensal do contrato, a cada 15 pontos ou percentual proporcional ao número de pontos, levando em consideração a relação: glosa de 1% a cada 15 pontos.

10.2.2.4. Os tempos serão contados a partir do recebimento de incidente / requisição / ordem de serviço. No caso da contagem em dias, a contagem é efetuada dia a dia, incluindo o primeiro e o último dia.

10.2.2.5. No caso da resolução de incidentes, se o mesmo não tiver a sua causa raiz conhecida, ou seja, existe um problema a ser resolvido, a CONTRATADA é obrigada a aplicar uma solução de contorno na resolução do incidente para que o serviço volte à sua operação padrão.

10.2.2.6. Os níveis de serviço serão mensurados de forma automatizada e não poderão ser manipulados pela empresa CONTRATADA.

10.2.3. A CONTRATADA se responsabilizará somente pelos índices que reflitam as requisições de serviços e incidentes designados a ela, não poderá ser responsabilizada por chamados pendentes de fornecedores/prestadores de serviços externos ou encaminhados a outros níveis, ou situações que dependam de terceiros, que, desta forma, não poderão ser computados.

10.2.4. Por requisições de serviço e incidentes reabertos entende-se que são requisições de serviço ou incidentes que foram dados como resolvidos, porém os mesmos ainda permanecem pendentes de resolução.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

10.2.5. Os serviços serão medidos com base em indicadores e níveis mínimos de serviço, vinculados a fórmulas de cálculo específicas, e deverão ser executados pela CONTRATADA, e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela adiante.

10.2.6. A CONTRATADA deverá manter os seguintes níveis de qualidade para a prestação dos Serviços escopo desta contratação:

Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Descumprimento da Meta	Glosa por inadimplemento
Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço	Prazo Real em dias / Prazo acordado em dias Onde: Prazos serão decididos através de um planejamento em conjunto entre CONTRATADA E CONTRATANTE.	> 1,25	15 pontos , por ocorrência
Tempo máximo para resposta para esclarecimentos requisitados	Dias totais de resolução = Dia da resposta - Dia da requisição Onde: Dia da requisição é o momento da abertura da requisição. Dia da resposta é o momento do retorno do questionamento.	> 1 dia útil	10 pontos (+3 pontos a cada dia excedente) ,por ocorrência
Tempo máximo para resolução das requisições de serviços não padrão	Dias totais de resolução = Dia da resposta - Dia da requisição Onde: Diada requisição é o momento da abertura da requisição. Dia da resolução da requisição é momento de conclusão da requisição	> 5 dias úteis	10 pontos (+3 pontos a cada dia excedente), por ocorrência
IAP – ÍNDICE DE ATENDIMENTO NO PRAZO	IAP = 100 * (ΣQtap / ΣQtr) Onde: IAP = Indicador de atendimento aos prazos do serviço; ΣQtap = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência; ΣQtr = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.	85% >= IAP < 95% 75% >= IAP < 85% IAP < 70%	150 Pontos 300 pontos 450 pontos

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

Score de Segurança	Avaliação mensal do Score na ferramenta MS-Defender	1 Ano Score<75% 2 Ano Score<76% 3 Ano Score <77% 4 Ano Score<78% 5 Ano Score<79%	100 pontos(+10 pontos a cada 1% a menos)
Score de Exposição	Avaliação mensal do Score na ferramenta MS-Defender	70 >= Score 30 >= Score < 69	300 Pontos 150 pontos

10.2.7. Serão aplicadas as referidas pontuações para efeito de glosa, após passado o período de notificação e período de defesa por parte da CONTRATADA, no caso de:

Nº	Descrição	Referência	Glosa por inadimplemento
1	Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução.	Por ocorrência	10 pontos
2	Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação.	Por ocorrência	5 pontos
3	Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução.	Por ocorrência	5 pontos
4	Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada.	Por ocorrência	5 pontos
5	Alterar indicadores/metas de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado.	Por ocorrência	100 pontos
6	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, ainda que em casos de substituição temporária.	Por ocorrência	30 pontos
7	Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais.	Por ocorrência	50 pontos
8	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares) ou utilizar equipamento particular, salvo em situação excepcional e devidamente autorizado pelo CONTRATANTE.	Por ocorrência	10 pontos

9	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	200 pontos
10	Deixar de comunicar ao CONTRATANTE a substituição de profissionais responsáveis pela execução das atividades.	Por ocorrência	10 pontos
11	Deixar de atuar tempestivamente no caso de incidentes graves	Por ocorrência	15 pontos
12	Deixar de cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato.	Por ocorrência	10 pontos
13	Deixar de cumprir ou implementar as rotinas em conformidade com os Planos de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres das soluções de segurança.	Por ocorrência	10 pontos
14	Deixar de atuar proativamente em caso de identificação de situação de desconformidade com boas práticas de segurança.	Por ocorrência	10 pontos
15	Deixar de apresentar os relatórios consolidados conforme exigências do Termo de Referência.	Por ocorrência	5 pontos
16	Deixar de apresentar relatórios, levantamentos ou inventários conforme demanda.	Por ocorrência	5 pontos
17	Deixar de apresentar mensalmente proposta de melhorias no ambiente.	Por ocorrência	5 pontos
18	Deixar de elaborar plano de capacitação caso não possua as certificações exigidas.	Por ocorrência	100 pontos
19	Deixar de cumprir as exigências quanto às experiencias profissionais de seus colaboradores após início da prestação de serviço.	Por ocorrência	150 pontos
20	Deixar de cumprir quaisquer obrigações estabelecidas no contrato e anexos, não previstas nesta tabela, após reincidência formalmente notificada pela CONTRATADA	Por ocorrência	10 pontos

10.2.8. Os primeiros 90 (noventa) dias após o início da execução dos serviços serão considerados como período de estabilização, durante o qual os resultados esperados e os níveis de qualidade exigidos poderão ser implementados gradualmente, de modo a permitir à CONTRATADA realizar a adequação progressiva de seus serviços e alcançar, ao término desse período, o desempenho requerido. Essa flexibilização, porém, será restrita aos limites destacados a seguir:

10.2.8.1. Para o 1º (primeiro) mês de execução: serão considerados 65% (setenta e cinco por cento) do total de pontos dos níveis de qualidade para o cálculo de glosa sobre o valor da fatura;

10.2.8.2. Para o 2º (segundo) mês de execução: serão considerados,80% (oitenta por cento) do total de pontos dos níveis de qualidade para o cálculo de glosa sobre o valor da fatura;

10.2.8.3. Para o 3º (terceiro) mês de execução: serão considerados, 100% (cem por cento) do total de pontos dos níveis de qualidade para o cálculo de glosa sobre o valor da fatura;

10.2.9. Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

TERMO DE REFERÊNCIA

Anexo A

DECLARAÇÃO DE VISTORIA TÉCNICA

Declaro, em atendimento ao previsto no Edital xx/xxxx e seus anexos do PREGÃO ELETRÔNICO Nº XX/XXXX, que eu, _____, portador(a) da CI/RG nº _____ e do CPF nº _____, representante da empresa _____, estabelecida no(a) _____ como seu representante legal, para os fins da presente declaração, compareci perante o representante do SEFAZ em Porto Alegre/RS e vistoriei o ambiente computacional do mesmo, assim como inteirei-me sobre as condições e grau de dificuldades existentes envolvendo o parque tecnológico da CONTRATANTE e os serviços a serem executados com apoio dos profissionais, tomando plena ciência das condições e grau de dificuldade existentes e das condições para prestação dos serviços, estando satisfeita com as informações e esclarecimentos obtidos durante a visita, estando plenamente capaz de elaborar proposta para a licitação em tela, de modo a não incorrer em omissões que jamais poderão ser alegadas em favor de eventuais pretensões de inclusão de serviços ou acréscimos de preços.

Local e data

_____

Assinatura

(Responsável da empresa)

Visto:

_____

Representante da SEFAZ-RS

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

TERMO DE REFERÊNCIA

ANEXO B

DECLARAÇÃO DE RENÚNCIA DA VISTORIA TÉCNICA

Declaro, em atendimento ao previsto no Edital xx/xxxx e seus anexos do PREGÃO ELETRÔNICO Nº XX/XXXX, que eu, _____, portador(a) da CI/RG nº _____ e do CPF nº _____, representante da empresa _____, estabelecida no(a) _____ como seu representante legal, para os fins da presente declaração, optamos pela não realização de vistoria técnica assumindo inteiramente a responsabilidade ou consequências por essa omissão, mantendo as garantias que vincularem nossa proposta ao presente processo licitatório, em nome da empresa que represento, estando plenamente capaz de elaborar proposta para a licitação em tela, de modo a não incorrer em omissões que jamais poderão ser alegadas em favor de eventuais pretensões de inclusão de serviços ou acréscimos de preços.

Local e data

_____

Assinatura

(Responsável da empresa)

Visto:

_____

Representante da SEFAZ-RS