Sumário

1 OBJETO

1.1 Contratação de prestação contínua e ininterrupta de Centro de Operações de Segurança – COS (em inglês SOC – Security Operation Center) da CONTRATADA, unidade centralizadora dos serviços de segurança cibernética, voltada para a prevenção, detecção e respostas a incidentes e monitoração da segurança da informação.

2 OBJETIVO

2.1 Garantir ampla segurança aos sistemas, aplicações e dados dos sistemas hospedados no centro de dados e da rede CONTRATANTE, na monitoração em serviços de investigação e inteligência de segurança da informação. O serviço de SOC abrange duas modalidades:

2.1.1 Monitoração de Segurança; e

2.1.2 Monitoração de inteligência de segurança da informação em fontes abertas.

3 REQUISITOS

3.1 A prestação do serviço se dará da seguinte forma:

3.1.1 Os ativos (recursos computacionais, ferramentas, *playbooks* etc.) do SOC serão 24x7, o que significa dizer que a monitoração de segurança e envio de alertas de incidentes serão prestados de forma contínua.

3.1.2 A janela de manutenção para as mudanças planejadas ocorrerá entre 22h e 7h em dias úteis e, a qualquer tempo, em feriados e/ou fins de semana.

3.1.3 A execução de paradas programadas para a manutenção preventiva será negociada com, no mínimo, 15 (quinze) dias corridos de antecedência.

3.1.4 A execução de parada emergencial, deverá ser negociada tempestivamente.

3.1.5 Paradas emergenciais são as que envolvem tratamento de vulnerabilidades de segurança, atualização de hardware e/ou software, redimensionamento e/ou reconfiguração do ambiente para garantia de disponibilidade dos serviços.

3.1.6 A equipe técnica do SOC atuará na modalidade 14x5, catorze horas por dia, das 7h às 21h, em dias úteis.

3.1.6.1 Fora de horário descrito no item anterior, a equipe ficará disponível sob regime de sobreaviso, ou seja, é feita escala dos empregados e estes são acionados pontualmente em casos de alerta de incidentes de segurança de alta severidade.

3.1.7 A equipe técnica do SOC realizará procedimentos de acionamento e comunicação dos registros de incidentes ou eventos de segurança da informação abertos pela CONTRATANTE na Central de Serviços da

CONTRATADA (CSS) ou de eventos de incidentes de segurança da informação, registrados em ferramenta definida pela CONTRATADA, ou por meio de alertas gerados pela monitoração, conforme Plano de Comunicação, aprovado em comum acordo com a CONTRATANTE.

3.1.7.1 O Plano de Comunicação deverá ser produzido pela CONTRATADA e aprovado pela CONTRATANTE contendo todos os tipos de eventos que devem ser comunicados, periodicidade, forma de comunicação, interessados e demais detalhes necessários para que a comunicação aconteça de acordo com os requisitos definidos pela CONTRATANTE.

3.1.8 A CONTRATADA deverá entregar mensalmente à CONTRATANTE relatório de prestação de contas e ateste para todos os serviços contratados.

3.1.9 O serviço SOC não abrange as atividades e funcionalidades de segurança que são realizadas por outros serviços de segurança da informação da CONTRATADA, a saber:

3.1.9.1 Tratamento de incidentes – atendimento a incidentes 24x7; analisar, classificar, rastrear, registrar e encaminhar alertas de incidentes; aplicar técnicas de tratamento (mitigação) do incidente (resposta a ataque);

3.1.9.2 Firewall – Proteção Exclusivo – monitoração do tráfego de entrada e saída de redes e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto bem definido de regras de segurança;

3.1.9.3 *AntiDDoS* Proteção URL – proteção a sítio a contra ataques de negação de serviços distribuídos (DDoS), ao uso dos protocolos de acesso Internet de forma indevida e à otimização do uso da banda para publicação dos sítios;

3.1.9.4 Filtro de Conteúdo – Proteção Exclusiva - monitoração e gerenciamento de acesso a URL com aplicação de políticas de acesso a sítios Internet, como monitoramento e controle de acesso;

3.1.9.5 *GovShield* – o serviço de segurança em nuvem para tratamento e proteção de sítios Web com CDN que conta com um conjunto de ferramentas de proteção contra-ataques, interrompendo o tráfego malicioso antes que ele atinja o sítio do cliente;

3.1.9.6 *Pentest* – detecção e exploração de vulnerabilidades existentes nos sistemas do cliente, realizando simulações de ataques com a ótica de hackers;

3.1.9.7 SERPRO *Multicloud* – conjunto de serviços profissionais especializados em nuvem;

3.1.9.8 Sala de Crise – montar e/ou gerenciar salas de crise, espaços que podem reunir áreas técnicas envolvidas em uma crise, sejam elas presenciais ou virtuais;

3.1.9.9 Quaisquer outros serviços descritos em outro anexo deste contrato ou que sejam objetos de outro tipo de contratação diversa à descrita neste anexo.

4 DESCRIÇÃO DO SERVIÇO

4.1 CARACTERÍSTICAS DO SERVIÇO

4.1.1 Monitoração de Segurança

4.1.1.1 Este serviço, de prestação contínua e ininterrupta, compreende a monitoração dos ativos de TI da CONTRATANTE, especialmente servidores WEB, de aplicação, de bancos de dados, ativos de infraestrutura (servidores de autenticação MS AD, Ldap, etc.) e ativos de segurança (*firewall*, IPS, IDS, Antivírus, etc.), por meio de criação de coletores de eventos e casos de usos implementados em ferramenta da CONTRATADA.

4.1.1.2 A CONTRATADA deverá correlacionar eventos de equipamentos de segurança, de *endpoints* e *Antimalware* para servidores e para estações de trabalho, de correio, de autenticação, de servidores Web e de servidores de aplicação.

4.1.1.3 A CONTRATADA deverá criar, implementar, sustentar, revisar, atualizar casos de usos aplicados às correlações contratadas e comunicar a CONTRATANTE para conhecimento.

4.1.1.4 A CONTRATANTE poderá sugerir alterações ou novos casos de uso a CONTRATADA, que deverá avaliá-los considerando os fatores de risco, urgência, ameaça antes da aplicação na ferramenta.

4.1.1.5 A CONTRATADA deverá fornecer os requisitos necessários para configuração dos dispositivos a serem coletados, bem como os agentes de coleta.

4.1.1.6 A CONTRATANTE disponibilizará um servidor de coleta quando a arquitetura requerer que seja feita coleta no ambiente da CONTRATANTE.

4.1.1.7 A CONTRATADA disponibilizará um servidor de coleta quando a arquitetura indicar que a coleta poderá ser enviada diretamente a CONTRATADA.

4.1.1.8 A CONTRATADA deverá elaborar e disponibilizar painel corporativos para CONTRATANTE

4.1.1.9 A CONTRATADA deverá garantir o funcionamento da coleta de eventos.

4.1.1.10 Criar os casos de uso na ferramenta da CONTRATADA para correlação de eventos com base em regras indicativas de comportamento suspeito.

4.1.1.11 Gerar alertas com encaminhamento automatizado para a equipe da CONTRATANTE para tratamento de incidentes de segurança, conforme definição da CONTRATANTE para o caso de uso descrito.

4.1.1.12 CONTRATADA poderá indicar as recomendações de tratamento ou mitigação para cada alerta/incidente.

4.1.1.13 Disponibilizar em lista de reputação para que a CONTRATANTE possa gerar configurações de bloqueio em seus ativos de segurança (IPS e *firewall*).

4.1.1.14 Para realização das atividades deste item, a CONTRATANTE realizará o levantamento dos ativos que serão monitorados, tais como:

4.1.1.14.1 Servidores WEB;

4.1.1.14.2 Servidores de aplicação;

4.1.1.14.3 Servidores de Bancos de Dados;

4.1.1.14.4 Ativos de Infraestrutura (servidores de autenticação MS AD, Ldap, gerência etc.);

4.1.1.14.5 Ativos de segurança (firewall, IPS, IDS, Antivírus, etc.).

4.1.1.14.6 A manutenção da lista de ativos é de responsabilidade da CONTRATANTE que poderá, a qualquer momento, realizar alterações na lista de ativos monitorados.

4.1.2 Monitoração de inteligência de segurança da informação em fontes abertas

4.1.2.1 Esse serviço, de prestação contínua e ininterrupta e sob demanda, é realizado com base nas ferramentas de inteligência do SOC, que fazem a busca em fontes abertas na Internet (incluindo *deep/dark web*) de informações suspeitas. As ferramentas trazem continuamente conteúdo associado aos argumentos de pesquisa.

4.1.2.2 A monitoração do serviço compreende:

4.1.2.2.1 Monitorar vazamento de Marcas e VIPs;

4.1.2.2.2 Monitorar vazamento de documentos, credenciais de acesso e contas comprometidas;

4.1.2.2.3 Monitorar Endereços IP e Blocos corporativos e individualizados por cliente;

4.1.2.2.4 *Takedown* de sites maliciosos/fraude.

4.1.2.3 A CONTRATANTE deverá indicar quais dados devem ser tratados, que podem ser: nomes de marcas, pessoas VIPs, endereços IP, domínios, e-mails, credenciais de usuários, entre outros.

4.1.2.4 A partir do resultado do serviço pode-se obter informações sensíveis em relação aos ativos analisados, que permitem conhecer previamente/posteriormente:

4.1.2.4.1 Identificação de grupos hacker envolvidos com atividades criminosas;

4.1.2.4.2 Ataques a imagem de marcas da organização;

4.1.2.4.3 Preparação de ataques de negação de serviços (DoS e DdoS);

4.1.2.4.4 Vulnerabilidades exploradas, roubo de informações;

4.1.2.4.5 Deformação/abuso/comprometimento de website e aplicações expostas na internet;

4.1.2.4.6 Vazamento de credenciais de acesso;

4.1.2.4.7 Vazamento de dados pessoais; e

4.1.2.4.8 Difamação e calúnia (VIPs) das organizações.

4.2 FORMA DE EXECUÇÃO DO SERVIÇO

4.2.1 Demandas

4.2.1.1 Demandas objeto desse anexo são aquelas relativas as eventuais necessidades em que a CONTRATANTE solicitará à CONTRATADA a sua implementação ou alteração, tais como, novos relatórios, novos Casos de Uso, ou qualquer outra nova implementação, alteração, definição etc.

4.2.1.2 As demandas terão cronograma apresentado pela CONTRATADA em até 15 (quinze) dias úteis a partir da data do envio da demanda para a CONTRATADA.

4.2.1.3 A demanda e o cronograma deverão ser acordados entre ambas as partes.

4.2.2 Monitoração de Segurança

4.2.2.1 Relacionar ativos da CONTRATANTE que serão monitorados.

4.2.2.2 Criar o conjunto de coletores necessários para receber o redirecionamento dos logs dos ativos selecionados.

4.2.2.3 Realizar os testes de funcionamento da coleta de eventos e criar os casos de uso na ferramenta de correlação de evento para geração dos alertas de segurança.

4.2.2.4 Reter os eventos na ferramenta de correlação de eventos deve ser de 90 (noventa) dias.

4.2.3 Correlação de eventos dos equipamentos de segurança (firewall, Ips etc.):

4.2.3.1 Coletar os eventos gerados pelos equipamentos de segurança da CONTRATANTE;

4.2.3.2 Estabelecer casos de uso de monitoração que permitam identificar comportamento suspeito e tentativas de ataques aos ativos da CONTRATANTE.

4.2.4 Correlação de eventos de endpoints e Antimalware para servidores:

4.2.4.1 Receber os eventos gerados pelas ferramentas de endpoints e antimalware da CONTRATANTE.

4.2.4.2 Estabelecer casos de uso de monitoração que permitam identificar comportamento suspeito e tentativas de ataques aos ativos da CONTRATANTE.

4.2.5 Correlação de eventos de autenticação (AD, Ldap, etc):

4.2.5.1 Receber os eventos gerados pelos servidores de autenticação (AD, LDAP) da CONTRATANTE.

4.2.5.2 Estabelecer casos de usos que permitam identificar comprometimentos de credenciais, tentativas de acessos não autorizados ou indevidos.

4.2.6 Correlação de eventos Web Server (apache, IIS etc.):

4.2.6.1 Receber os eventos gerados pelos servidores Web.

4.2.6.2 Estabelecer casos de usos que permitam identificar comprometimento de aplicação, tentativas de intrusão e outros ataques que exploram vulnerabilidades do serviço WEB.

4.2.7 Correlação de eventos de Servidores (Windows/Linux):

4.2.7.1 Receber os eventos gerados pelos servidores Windows e Linux.

4.2.7.2 Estabelecer casos de usos que permitam identificar eventos suspeitos e comandos maliciosos executados sob o sistema operacional.

4.2.8 Criação de coletores de log para SIEM – Especializado Cliente:

4.2.8.1 Identificar a quantidade e perfil dos servidores de coleta de acordo com as necessidades de correlação de eventos definidos pela CONTRATANTE, conforme lista de funcionalidades de correlação de eventos contratados.

4.2.9 Aplicação de bloqueio de tentativas suspeitas/maliciosas – Equipamento CONTRATADA – Reputation SERPRO:

4.2.9.1 Realizar bloqueios de endereços IP que originaram tentativas de acessos suspeitos e maliciosos, de forma automatizada.

4.2.9.2 Para a aplicação da funcionalidade, o equipamento de segurança (firewall, IPS) da CONTRATANTE precisa ser administrado pela CONTRATADA.

4.2.10 Fornecimento de listas de reputação de tentativas suspeitas/maliciosas – *Reputation* SERPRO:

4.2.10.1 Disponibilizar para CONTRATANTE e manter atualizada a lista de reputação de endereços IP suspeitos e maliciosos.

4.2.11 Criação de relatórios sob demanda:

4.2.11.1 Elaborar, sob demanda, relatórios de análise com dados de monitoração com base em casos de uso e ativos selecionados pela CONTRATANTE.

4.2.12 Criação de Painel sob demanda:

4.2.12.1 Disponibilizar painéis com dados de monitoração customizados para os casos de uso e ativos da CONTRATANTE.

4.2.13 Monitoração de Inteligência de Segurança da Informação em fontes abertas

4.2.13.1 Monitoração de vazamento de Marcas e VIPS:

4.2.13.1.1 Realizar monitoramento de inteligência em fontes externas de nome/url de sistemas, nome de órgãos e pessoas VIP com objetivo de antecipar informações e gerar alertas sobre uso indevido dessas informações.

4.2.13.2 Monitoração de palavras-chaves:

4.2.13.2.1 Realizar monitoramento de inteligência de palavras-chaves relacionadas ao domínio do cliente com objetivo de antecipar informações e gerar alertas sobre do uso indevido dessas informações.

4.2.13.3 Monitoração de vazamento de documentos, credenciais de acesso e contas comprometidas:

4.2.13.3.1 Realizar monitoramento de inteligência em fontes abertas em documentos, credenciais de acesso e contas comprometidas com objetivo de antecipar informações e gerar sobre o uso indevido dessas informações.

4.2.13.4 Monitoração de vazamentos de cartões de crédito:

4.2.13.4.1 Realizar monitoramento de inteligência de vazamentos de cartões de crédito com objetivo de antecipar informações e gerar alertas sobre o uso indevido dessas informações.

4.2.13.5 Monitoração de Endereços IP e Blocos de endereços:

4.2.13.5.1 Realizar monitoramento de inteligência em endereços IP e Blocos de endereços IP individualizados com objetivo antecipar informações e alertas sobre vulnerabilidades, intenção de invasão e demais tipos de incidentes com origem ou destino desses ativos.

4.2.13.6 Solicitação de *Takedown* para sites maliciosos/fraude:

4.2.13.6.1 Identificar sites como maliciosos ao negócio da CONTRATANTE.
4.2.13.6.2 Criar solicitação de retirada junto a provedores e órgãos competentes.
4.2.13.6.3 Atender solicitação da CONTRATANTE de retirada de sites junto a provedores e órgãos competentes.

4.2.13.7 Relatório sob demanda de monitoramento de Inteligência:

4.2.13.7.1 Disponibilizar para relatório mensal com informações do monitoramento de inteligência contratada.
4.2.13.7.2 Em caso de outras solicitações de relatórios, a CONTRATANTE deverá abrir demandas em sistema informatizado de controle de demanda. Caso as informações fornecidas na demanda sejam insuficientes, A CONTRATADA poderá devolvê-la para inclusão de informações complementares.
4.2.13.7.3 A estimativa de prazo de atendimento da demanda será definida conforme o tipo do serviço.
4.2.13.7.4 As demandas, em que a CONTRATANTE der causa ao descumprimento do prazo de atendimento da demanda, não serão computadas para desconto de nível mínimo de serviço e as evidências deverão constar no relatório de ateste de Nível Mínimo de Serviço.

5 ESTRATÉGIA DE CONTRATAÇÃO

5.1 DISPONIBILIZAÇÃO

5.1.1 O serviço do SOC será disponibilizado em cronograma a ser combinado entre as partes, e apresentado a partir da data da assinatura do contrato.

5.1.2 O início do pagamento dos serviços será a partir do momento em que o SOC estiver disponibilizado para a CONTRATANTE.

5.1.3 É pré-requisito para início da configuração do SOC que a CONTRATANTE forneça dados sobre rede e infraestrutura da CONTRATANTE para criação de conectividade/integração/convergência com o SOC.

6 METODOLOGIA DE AVALIAÇÃO

6.1 PROCESSO DE AVALIAÇÃO DOS INDICADORES AFERIDOS POR INSTRUMENTOS DE MENSURAÇÃO DE RESULTADO

6.1.1 Durante a prestação mensal dos serviços, a CONTRATANTE acompanhará as ocorrências na prestação dos serviços, registrando todas as informações em controle próprio. Nessa apuração, a CONTRATANTE utilizar-se-á, além de todas as outras fontes de informação, da solução de controle de demandas para apuração do indicador de tempestividade de entrega de demanda.

6.1.2 A CONTRATADA informará para ateste da CONTRATANTE mensalmente relatório contendo informações sobre os alertas de indisponibilidade gerados, comunicados e os comunicados encaminhados em atraso para apuração do indicador de tempo máximo de comunicação.

6.1.2.1 Durante o período de ateste, a CONTRATADA proverá instrumentos para que a CONTRATANTE possa validar as informações registradas no relatório, por meio de relatórios de apoio, extrações de dados ou acesso à ferramenta de gestão de alertas de incidentes.

6.1.2.2 Caberá a CONTRATADA a emissão e encaminhamento dos relatórios do IMR.

6.1.3 Quando um período apuração for diferente do período de aferição mensal, os serviços deverão ser recebidos e atestados de maneira proporcional e os IMR avaliados também de maneira proporcional, nos casos em que couber.

6.1.4 Durante o período de aferição da prestação do serviço da competência, caso a CONTRATADA decida contestar algum indicador apurado pela CONTRATANTE, deverá enviar evidências, com a indicação das cláusulas contratuais que embasaram a contestação e argumentações para análise da CONTRATANTE.

6.1.4.1 Em caso de recusa às contestações feitas pela CONTRATADA em relação aos indicadores apurados e informados, a CONTRATANTE deverá apresentar à CONTRATADA uma resposta por escrito motivando o ato administrativo.

6.1.5 Após a conclusão do ateste da competência e autorização de faturamento pela CONTRATANTE, caso a CONTRATADA apresente contestação, essa deverá seguir o rito de processo administrativo junto à CONTRATANTE sendo sempre observados o devido processo legal, a ampla defesa e o contraditório.

6.1.5.1 Caso a contestação apresentada pela CONTRATADA seja considerada procedente pela CONTRATANTE, total ou parcialmente, o faturamento do valor correspondente à parcela incontroversa será autorizado até a competência seguinte à notificação da decisão, pela Fiscalização Administrativa, à CONTRATADA e ao Gestor do Contrato, salvo mediante justificativa da CONTRATANTE, hipótese em que este prazo poderá ser prorrogado em até 6 (seis) competências.

6.1.5.2 Caso a contestação seja considerada parcial ou totalmente improcedente, a CONTRATANTE deverá apresentar os fundamentos por escrito, os quais poderão ser objeto de recurso pela CONTRATADA, observando o respectivo rito de processo administrativo, com ampla defesa e contraditório.

6.1.6 Quando um período apuração for diferente do período de aferição mensal, os serviços deverão ser recebidos e atestados de maneira proporcional e os IMR avaliados também de maneira proporcional.

7 ITEM FATURÁVEL

7.1 A lista completa dos itens faturáveis objetos deste anexo está discriminada seguir:

CÓDIGO – NOME IFA	
04.03.01 – SOC – Pacote Básico para 5.000 EPS	
DESCRIÇÃO	Prestação de serviço contínuo de monitoração com direito a média mensal a 5.000 EPS* dos ativos de TI da CONTRATANTE, e monitoração de inteligência.
UNIDADE DE MEDIDA	Parcela Mensal
04.03.02 SOC – Pacote Adicional para 1.000 EPS	
DESCRIÇÃO	Adicional de 1.000 EPS
UNIDADE DE MEDIDA	Valor Mensal

*EPS – Eventos por segundo é quantidade de eventos que ocorrem em ativos de tecnologia de informação.

7.2 O faturamento do serviço considerará o consumo do período de apuração e será definido de acordo com os pacotes de IFA;

7.2.1 Para consumo no período de apuração do faturamento de até 5.000 EPS, será considerada a parcela mensal IFA 04.03.01;

7.2.2 Para consumo no período de apuração do faturamento de até 6.000 EPS, será considerada a parcela mensal IFA 04.03.01 acrescido do valor mensal do IFA 04.03.02;

7.2.3 Para consumo no período de apuração do faturamento de até 7.000 EPS, será considerada a parcela mensal IFA 04.03.01 acrescido de duas vezes o valor mensal do IFA 04.03.02;

7.2.4 Para consumo no período de apuração do faturamento de até 8.000 EPS, será considerada a parcela mensal IFA 04.03.01 acrescido de três vezes o valor mensal do IFA 04.03.02;

7.2.5 Para consumo acima de 8.000 EPS o pacote básico deverá ser revisado e, seu preço, alterado, bem como os pacotes adicionais, se necessário.

8 DO VOLUME E VALOR ESTIMADO PARA O SERVIÇO

8.1 O volume, valor mensal e valor anual proposto para o serviço estão descritos no Anexo VI do Contrato.

9 SUPORTE

9.1 A solicitação de suporte técnico será realizada durante o período de vigência do contrato, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

9.2 Será aberto um acionamento nos canais de atendimento para cada situação reportada.

9.3 Cada acionamento receberá um número de identificação para comprovação por parte da CONTRATANTE e para acompanhamento.

10 CANAIS

10.1 O canal de atendimento será definido no Plano de Comunicação, acordado entre as partes.

11 DO ATESTE DOS SERVIÇOS

11.1 Os serviços serão atestados formalmente pela CONTRATANTE a partir do recebimento dos relatórios de comprovação dos serviços prestados, referente ao período especificado com descriminação dos itens faturáveis, quantitativos, preços unitários e totais.

12 INDICADORES APURADOS POR INSTRUMENTOS DE MENSURAÇÃO DE RESULTADOS

12.1 A seguir, os indicadores que deverão ser apurados para fins de mensuração de resultados:

IMR 01 – TED –TEMPESTIVIDADE DE ENTREGA DA DEMANDA	
ITEM	**DESCRIÇÃO**
Finalidade	Medir a tempestividade de entrega do serviço das demandas do SOC.
Meta a cumprir	Demandas entregues no prazo, conforme cronograma aprovado pela CONTRATANTE.
Instrumento de medição	Cronograma de atendimento da demanda gerado pela solução de controle de demandas com base em informações fornecidas pela CONTRATADA.

Forma de acompanhamento	Relatório com os registros na solução de controle de demandas.
Periodicidade	Mensal.
Início de vigência	A partir da disponibilização do serviço, devidamente aprovada pela CONTRATANTE.
Mecanismo de cálculo	TED = (Da)/Tc onde: Da = Média dos dias de atraso (data da entrega da demanda menos a data do cronograma da demanda) das demandas concluídas do período. Tc = Média do total de dias dos cronogramas das demandas concluídas do período.
Faixas de ajuste no pagamento	Fator de ajuste no pagamento: Se TED <= 10%, FAP = 0,0% Se TED > 10% e TED <= 25%, FAP = 0,02% Se TED > 25% e TED <= 50%, FAP = 0,04% Se TED > 50% e TED <= 75%, FAP = 0,06% Se TED > 75%, FAP = 0,08% % de ajuste no pagamento= FAP*Da Vdsc = Vs * % de ajuste no pagamento onde: FAP = Fator de ajuste no pagamento Vdsc = Valor do Desconto Vs = Valor mensal do Serviço de SOC O percentual de ajuste no pagamento é limitado a 2%.
Sanções	1. Na ocorrência de prestação de serviços que extrapole o limite máximo deste Instrumentos de Medição de Resultado (IMR): TED > 75%, por 3 (três) meses consecutivos ou não, num período de 12 (doze) meses a partir do mês inicial da vigência do contrato, configura prestação de serviço em desacordo com o Contrato, passível de sanção conforme definido na respectiva cláusula do Contrato. 2. Na ocorrência de prestação de serviços cuja demanda esteja em

	mora por mais de 60 dias da data estimada para entrega, e que não haja justificativa aceita pela CONTRATANTE, configura prestação de serviço em desacordo com o Contrato, passível de sanção conforme definido na respectiva cláusula do Contrato.
Observação	Para cálculo dos dias de atraso, leva-se em consideração o tempo decorrido entre a data prevista para conclusão da demanda, que consta no cronograma da demanda, e a data em que a CONTRATADA registrar a entrega da demanda.

IMR 02 - TMC – TEMPO MÁXIMO DE COMUNICAÇÃO	
ITEM	**DESCRIÇÃO**
Finalidade	Medir a tempestividade para comunicação dos alertas de incidentes de segurança do SOC, conforme definido no plano de comunicação
Meta a cumprir	90% dos alertas de incidentes comunicados em até 2h 100% dos alertas de incidentes comunicados em até 24h
Instrumento de medição	Alertas de incidentes detectados pelo SOC.
Forma de acompanhamento	Análise de relatório de TMC enviado pela CONTRATANTE, comparando com os registros das ferramentas de gestão de alertas de incidentes, registros da central de serviços e os relatórios do serviço de monitoração de segurança.
Periodicidade	Mensal.
Início de vigência	A partir da disponibilização do serviço, devidamente aprovada pela CONTRATANTE.
Mecanismo de cálculo	Se TP1/T >= 90%, FA=0% Senão FA = 90% - TP1/T TMC = [(TP1+TP2)/T] x 100% - FA onde: TMC: indicador de tempo de máximo de comunicação TP1: Total de alertas de incidentes de segurança gerados no período

	com tempo de comunicação menor ou igual a 2h. TP2: Total de alertas de incidentes de segurança gerados no período com tempo de comunicação menor ou igual a 24h menos o Total de alertas de incidentes de segurança gerados no período com tempo de comunicação menor ou igual a 2h. T: Total de alertas de incidentes de segurança gerados que deveriam ter sido comunicados no período. FA = fator de ajuste
Faixa de ajuste no pagamento	Se houver descumprimento injustificado de TMC e % de ajuste no pagamento for maior do que 0 (0%), aplica-se % de ajuste sobre o valor correspondente mensal do Serviço de SOC (IFA SOC e SOC Adicional), ou seja: Vdsc = Vs * % de ajuste no pagamento onde: Vdsc = Valor do Desconto. Vs = Valor mensal do Serviço de SOC. Faixas de ajuste no pagamento: TMC >= 95%, % ajuste no pagamento = 0% TMC < 95%, % ajuste no pagamento = (95% - TMC) O percentual de ajuste no pagamento é limitado a 30%.
Sanções	01) Na ocorrência de prestação de serviços que extrapole o limite máximo deste Instrumentos de Medição de Resultado (IMR): TMC < 95%, por 3 (três) meses consecutivos ou não, num período de 12 (doze) meses a partir do mês inicial da vigência do contrato, configura prestação de serviço em desacordo com o Contrato, passível de sanção conforme definido na respectiva cláusula do Contrato. 02) Na constatação pela CONTRATANTE de falta de comunicação de alerta de incidente de segurança objeto desse anexo e previsto ou contidos no Plano de Comunicação, artefatos, relatórios e registros nas ferramentas da CONTRATADA, configura prestação de serviço em desacordo com o Contrato, passível de sanção conforme definido na respectiva cláusula do Contrato. 03) Na ocorrência de prestação de serviços cujo TMC < 70%, configura prestação de serviço em desacordo com o Contrato, passível de sanção conforme definido na respectiva cláusula do Contrato.
Observação	Para cálculo do TMC não deve ser considerado o período referente às ocorrências fora do horário definido no item 3.7. Os incidentes de alta severidade considerará o período de 24x7, e os

	demais incidentes o período do item 3.7.

12.2 O nível mínimo de serviço para demandas de serviço de solicitação de *Takedown* para Sites Maliciosos/Fraude por se tratar de serviço que depende do envolvimento e acionamentos de terceiros – provedores de serviços de internet, que a Contratada não tem governança, será considerado o prazo até o acionamento de terceiros.

13 CANCELAMENTO E SUSPENSÃO DOS SERVIÇOS

13.1 Em caso de cancelamento ou suspensão dos serviços, no todo ou em parte, por iniciativa da CONTRATANTE, estes serão considerados parcialmente entregues e caberá à CONTRATANTE efetuar o pagamento proporcional aos serviços até então prestados.

13.2 A solicitação do cancelamento ou da suspensão dos serviços, será feita pela CONTRATANTE, por solicitação formal emitida por autoridade com competência igual ou superior à que firmou o referido contrato.