LOTE 2

Serviços de SOC/MDR

Resposta a Incidentes e Gestão de Vulnerabilidades

Elaborado por:

SENAC
Elcio Bodart – Gerente de TI
Yan Porto - Analista de Segurança

SESC
Bruno Ferraço – Gerente de TI
Alisson Schmidt – Coord. de TI
Lucas Colaça – Analista de Segurança

1. OBJETO 3
2. ESCOPO 3
2.1. Planilha de preços 3
2.2. Definições e Conceitos 5
3. REQUISITOS TÉCNICOS MÍNIMOS DOS SERVIÇOS 6
3.1. Serviços de SOC/MDR (Security Operation Center/Managed Detection and Response) 6
3.2. Serviços de Resposta a Incidentes de Segurança da Informação 10
3.3. Serviços de Gestão de Vulnerabilidades de Servidores, Estações de Trabalho e Ativos de Rede 13
3.4. Serviços de Gestão de Vulnerabilidades de Aplicações WEB 16
3.5. Serviços de Monitoramento de Deep e Dark Web 19
4. REQUISITOS TÉCNICOS MÍNIMOS DAS SOLUÇÕES OFERTADAS PARA A PRESTAÇÃO DOS SERVIÇOS 20
4.1. Requisitos Gerais das Soluções Ofertadas 20
4.2. Solução de Monitoramento, Detecção, Investigação, Notificação e Resposta a Ataques Cibernéticos 21
4.3. Solução de Gestão de Vulnerabilidades de Servidores e Estações de Trabalho e Ativos de Rede 29
4.4. Solução de Gestão de Vulnerabilidades de Aplicações WEB 36
4.5. Solução de Monitoramento de Deep & Dark Web 40
5. REQUISITOS TÉCNICOS GERAIS DOS SERVIÇOS 41
5.1. Fornecimento e Ativação das Soluções Ofertadas 41
5.2. Implantação, Ativação e Transição dos Serviços 42
5.3. Acordo de Nível de Serviços (SLA) 44
6. IMPEDIMENTO DE CONTRATAÇÃO DA MESMA EMPRESA PARA DATACENTER E SOC 46
7. QUALIFICAÇÃO TÉCNICA 47
7.1. Da Contratada 47
7.2. Do Quadro Profissional da Contratada 48
7.3. Do Fabricante 49
8. PAGAMENTO SOB MEDIÇÃO 49
8.1. Relatórios de Medição e documentação de atividades realizadas 49
9. PRAZOS 50
9.1. Prazo de Vigência do Contrato 50
9.2. Prazo de Implantação, Ativação e Transição 50
10. ANEXO I – SOLUÇÕES DE SEGURANÇA DA INFORMAÇÃO DA CONTRATANTE 50
11. ANEXO II - PROVA DE CONCEITO 52
12. ANEXO III – COMPROVAÇÃO DE ATENDIMENTO AOS ITENS DA ESPECIFICAÇÃO TÉCNICA 53
13. ANEXO IV - TERMO DE COMPROMISSO DE MANUTENÇÃO, SIGILO E SEGURANÇA 54
14. ANEXO V - TERMO DE ACORDO DE SIGILO, CONFIDENCIALIDADE E PRIVACIDADE DE DADOS - LGPD 56

1. OBJETO

Contratação de serviços especializados em Segurança da Informação e Operações de Rede, abrangendo SOC/MDR (Security Operation Center / Managed Detection and response), Resposta a Incidentes, Gestão de Vulnerabilidades, Inteligência de Ameaças para o parque tecnológico e FQDN, além de serviços de monitoramento da Deep & Dark Web para o SESC e SENAC.

2. ESCOPO

2.1. Tabela de preços

2.1.1. A tabela seguinte apresenta os serviços, quantitativos e demais condições de contratação.

OBS: Conforme o modelo de precificação da tabela 1, a proponente deverá preencher o preço unitário (F) da **Linha 1 ou Linha 2,** além das demais linhas.

O pagamento será efetuado mensalmente, conforme quantitativo indicado no relatório de medição aprovado pela contratada.

Obrigatoriamente a proposta comercial deve conter a tabela de preços a seguir:

TABELA 1 – Tabela de preços

Item	Serviço	Descrição	Fabricante/Marca da solução	Unidade de Contratação	(A) Quant. Estimada Contratada Senac	(B) Quant. Estimada Contratada Sesc	(C) Quant. Total Estimada Sesc & Senac	Valor Total MENSAL Estimado SENAC	Valor Total MENSAL estimado SESC	(E) Preço Unitário Estimado	(F) Valor Total MENSAL Estimado Geral SESC + SENAC
1	**SOC (Licenciamento Ativos ou LOG)**	**Serviço de SOC/MDR (Security Operation Center/Managed Detection and Response), em regime remoto 24x7, com base no monitoramento de ativos e análise de logs de segurança. <Modo de precificação> A precificação deverá considerar como unidade de contratação a quantidade de ativos monitorados em blocos de 100 ativos. Caso a proponente opte por precificar por quantidade de LOG, deve considerar 200 GB ingeridos/mês para cada bloco de 100 ativos contratados. Obs.: Caso este item seja preenchido não poderá preencher o item 2**		Pacotes de 100 Ativos Gerenciados	7	9	16				= C x E
2	**SOC (Licenciamento por fonte eventos)**	**Serviço de SOC/MDR (Security Operation Center/Managed Detection and Response), em regime remoto 24x7, com base no monitoramento de ativos e análise de logs de segurança. <Modo de precificação> Quantidade de fontes de eventos, conforme item 11 - ANEXO I Nessa modalidade, o número de ativos monitorados deve ser ilimitado com agentes nativos do SIEM instalados em todos os ativos do item 1. Obs.: Caso este item seja preenchido não poderá preencher o item 1**		Fonte de eventos	9	9	18				= C x E
3	**Serviço de reposta de incidente (Banco de horas)**	**Serviços de Resposta a Incidentes de Segurança da Informação, em Regime Remoto e Presencial 24x7 Horas acumulativas durante a vigência do contrato)**		Banco de Horas de 20 Horas/Mês	1	1	2				= C x E
4	**Serviços de Gestão de Vulnerabilidades (Ativos)**	**Serviços de Gestão de Vulnerabilidades de Segurança da Informação de Servidores, Estações de Trabalho e ativos de rede**, em Regime Remoto 8x5		Pacotes de 100 Ativos Gerenciados	7	9	16				= C x E
5	**Serviços de Gestão de Vulnerabilidade de WEB/API**	**Serviços de Gestão Riscos e Vulnerabilidades de Aplicações WEB e APIs**, em Regime Remoto 8x5		FQDN (Full Qualified Domain Name)	2	1	3				= C x E
6	**Serviço Monitoramento Deep/Dark Web**	**Serviços de Monitoramento de Deep & Dark Web**, em Regime Remoto 24x7		01 FQDN Monitorado; 600 Termos Monitorados por FQDN Monitorado.	2	2	4				= C x E
PREÇO TOTAL ESTIMADO MENSAL											= SOMA COLUNA F
PREÇO GLOBAL ESTIMADO ANUAL											

O pagamento à CONTRATADA será efetuado sob o regime de medição, com base nos quantitativos efetivamente demandados/autorizados pela CONTRATANTE e executados pela CONTRATADA e nos critérios previamente estabelecidos na planilha de preços contratual.

2.1.2. O detalhamento do ambiente tecnológico da CONTRATANTE a ser contemplando pelos serviços contratados, encontra-se no Anexo I desta especificação técnica.

2.1.3. Em caso de rescisão contratual, encerramento da prestação dos serviços ou substituição da empresa contratada, a CONTRATADA deverá entregar à CONTRATANTE, de forma organizada e

documentada, todas as informações, dados, configurações, registros de logs, relatórios, documentação técnica, históricos de incidentes e demais evidências produzidas ou coletadas durante a vigência do contrato.

2.1.4. A CONTRATADA também deverá fornecer apoio técnico na transição para o novo fornecedor, assegurando a continuidade dos serviços de segurança da informação e integridade dos dados, inclusive disponibilizando acesso temporário à plataforma por no mínimo 30 dias após o encerramento contratual, caso necessário.

2.2. Definições e Conceitos

2.2.1. A modalidade de trabalho em REGIME REMOTO deverá ser executada nas dependências da CONTRATADA.

2.2.2. A modalidade de trabalho em REGIME PRESENCIAL deverá ser executada pela CONTRATADA exclusivamente nas dependências da CONTRATANTE.

2.2.3. A modalidade de trabalho em REGIME REMOTO E PRESENCIAL deverá ser executada nas dependências da CONTRATADA e, quando requisitado pela CONTRATANTE ou necessário, presencialmente nas dependências da CONTRATANTE.

2.2.4. Define-se ATIVO como sendo uma estação de trabalho, notebook, dispositivo móvel, servidor, container, firewall, ativo de rede ou qualquer equipamento similar ao listado que possua endereço IP próprio e distinto. Poderá ser físico ou virtual e poderá estar hospedado em ambiente local (on-premise) ou em nuvem.

2.2.4.1. No caso de container, deverá ser contabilizado como “Ativo monitorado” o host que hospeda o(s) container(s), para efeito de subscrição.

2.2.4.2. Caso o ativo possua mais de um endereço IP, será contabilizado um único “Ativo monitorado” para efeito de subscrição.

2.2.5. Para os Serviços de SOC/MDR, o licenciamento da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada pela CONTRATADA, deverá ser baseada em quantidade de ATIVOS ou Fonte de eventos, conforme definições desta especificação técnica.

2.2.5.1. Para o caso de solução cujo licenciamento e/ou subscrição seja baseada em volumetria de logs ingeridos, a CONTRATADA deve ofertar licenciamento para uma quantidade mínima de Área de Armazenamento em modalidade SaaS, suficiente para atender 100% do(s) pacote(s) de ativos monitorados contratados, independentemente do volume de logs, dados de telemetria e de rede gerados pelo total de ativos monitorados, observando-se o limite **mínimo de Gigabytes Ingeridos por Mês igual a 2 vezes a referida quantidade de pacote(s) de ativos** monitorados contratados. **Deste modo, para cada bloco de 100 Ativos Monitorados contratados, a CONTRATADA deve ofertar subscrição/licenciamento para no mínimo 200 Gigabytes Ingeridos por Mês. Portanto, para pacotes que totalizem 700 Ativos Monitorados, a subscrição/licenciamento deverá ser de, no mínimo, 1.400 Gigabytes Ingeridos por Mês. A unidade de contratação “fonte de eventos” também pode ser utilizada para precificação com base no parque computacional presente no anexo I. Para fins de escopo e precificação, entende-se como fonte de eventos são os componentes que geram informações para serem enviadas a ferramenta que irá correlacionar os eventos, tais como soluções de Endpoint que gerenciam todas as estações de trabalho, gerenciadores centrais de firewall que concentram a gestão de múltiplos dispositivos, servidores de Syslog que centralizam os logs de diversos servidores, além de soluções de e-mail, Active Directory (AD), switches gerenciáveis e outros**

componentes capazes de gerar e concentrar eventos relevantes para segurança. No caso do Firewall, cada equipamento individual deverá ser considerado como uma fonte de eventos.

2.2.5.2. EPS significa Events Per Second, ou "Eventos por Segundo". No contexto de soluções de monitoramento e segurança cibernética (como SOC/MDR), o EPS é uma métrica que indica a quantidade de eventos gerados e processados por segundo pela solução contratada. Esses eventos são geralmente logs ou alertas gerados por sistemas, aplicações, firewalls, endpoints ou outros ativos monitorados. Quando o licenciamento é baseado em EPS, significa que o custo será calculado conforme a volumetria dos eventos gerados em tempo real. O SENAC e o SESC não aceitarão esse parâmetro para precificação.

2.2.5.3. Define-se “Área de Armazenamento” como sendo a área disponibilizada por meio da solução contratada para armazenamento dos logs de eventos de segurança, em ambiente SaaS, coletados pela solução.

2.2.5.4. O licenciamento da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada pela CONTRATADA deve ser flexível e permitir a operação em até 10% acima da capacidade contratada, pelo prazo de até 30 dias, sem a incidência de custos adicionais, comportando assim picos esporádicos de eventos de segurança da informação.

2.2.6. A CONTRATANTE aferirá mensalmente a quantidade de ativos ou volumetria licenciada para certificar que a CONTRATADA está em conformidade com os requisitos desta especificação técnica.

3. REQUISITOS TÉCNICOS MÍNIMOS DOS SERVIÇOS

3.1. Serviços de SOC/MDR (Security Operation Center/Managed Detection and Response)

3.1.1. Os serviços de SOC/MDR deverão ser prestados por meio do Centro de Operações de Segurança Cibernética da CONTRATADA, em regime 24x7x365, abrangendo o Monitoramento, Detecção, Investigação, Notificação e a Resposta a Ataques Cibernéticos ao ambiente tecnológico da CONTRATANTE.

3.1.2. A plataforma deve incluir os agentes para a coleta de eventos em Windows e Linux, esses agentes devem ser da mesma marca da solução proposta.

3.1.3. A ingestão de eventos de atividade do usuário através da integração com active directory, se forem necessários agentes, estes devem ser da mesma marca da solução proposta, não são permitidos agentes de terceiros.

3.1.4. Requisitos para Monitoramento abrangente de Vulnerabilidades nos Ativos:

3.1.4.1. Para garantir uma postura de segurança eficaz e uma visão completa do ambiente de Infraestrutura, o licenciamento baseado em fontes de eventos deve atender a um requisito fundamental: todos os ativos precisam ser monitorados de forma que todas as vulnerabilidades sejam identificadas e analisadas. PORTANTO, É OBRIGATÓRIA A INSTALAÇÃO DE AGENTES NATIVOS DA PLATAFORMA DE SIEM OFERTADA EM TODOS OS ATIVOS. O SESC e SENAC não aceitarão um modelo de monitoramento que dependa exclusivamente de fontes de eventos sem um complemento que permita uma visibilidade completa das ameaças existentes, tal como agentes de terceiros que não sejam nativos da plataforma de SIEM. Além disso, quando a coleta de eventos for feita de maneira centralizada, o número de ativos monitorados deve ser ilimitado, garantindo que todas as estações de trabalho, servidores, Firewalls e demais dispositivos de infraestrutura sejam contemplados. O fornecedor deverá se adequar ao nosso parque tecnológico e não poderá cobrar valores adicionais por ativo,

devendo garantir que toda a arquitetura seja monitorada. Cada firewall, individualmente, deve ser considerado com uma fonte de eventos.

3.1.5. O escopo dos serviços deve incluir as seguintes macros atividades:

3.1.5.1. Monitoramento e coleta de eventos (coletas e logs), direcionando incidentes a serem tratados pela equipe responsável.

3.1.5.2. A solução de SIEM não deverá ser um software proprietário da CONTRATADA. A exigência de que a solução de SIEM não seja um software proprietário da CONTRATADA visa garantir neutralidade, continuidade operacional e independência tecnológica. Essa medida evita a dependência exclusiva de um fornecedor específico, facilita a transferência do serviço para outro prestador em caso de rescisão contratual e assegura que a plataforma utilizada possua suporte direto do fabricante, com atualizações regulares, documentação pública e aderência a padrões de mercado.

3.1.5.3. O agente instalado nos ativos deverá ser do mesmo fabricante do SIEM, não será aceito agentes de terceiros. O objetivo é assegurar que a ferramenta atenda a padrões reconhecidos internacionalmente de desempenho, escalabilidade, inovação e liderança de mercado, NÃO SENDO ACEITA BASEADA EM SOFTWARE OPEN SOURCE.

3.1.5.4. Configuração da recepção de eventos (coletas, logs e informações) de acordo com a lista de ativos tecnológicos a serem monitorados.

3.1.5.5. Análise dos eventos monitorados, mitigação de falsos-positivos e falsos-negativos eventualmente associados e aplicação de melhores práticas relacionadas à revisão e manutenção das regras de correlação e alertas, com a definição e documentação de procedimentos operacionais para tal.

3.1.5.6. Caça a ameaças, com pesquisa e análise proativa através dos ativos informacionais, visando detectar ameaças que escaparam às medidas de segurança tradicionais.

3.1.5.7. Gestão de incidentes, com foco na priorização e escalonamento, baseado em tabela de riscos e na definição de ativos informacionais críticos para a operação.

3.1.5.8. Criação de base de conhecimento com a concentração das informações advindas de resultados e andamentos de pesquisas e investigações de ataques detectados, para fins de referência futura.

3.1.5.9. Geração de relatórios, dashboards e perfis de acesso, de forma a relacionar eventos e determinar sua relevância face às políticas existentes.

3.1.5.10. Monitoramento e resposta a incidentes, inclusive com auxílio na criação, definição, implementação e documentação de processos e atividades relacionadas, visando aumentar a eficiência na detecção de ameaças e promovendo agilidade na mitigação e resolução de possíveis incidentes.

3.1.5.11. Foco na prevenção de ameaças, aplicando boas práticas de segurança que minimizem o risco no ambiente tecnológico monitorado.

3.1.5.12. Análise, detecção e apoio na correção de problemas relacionados aos processos de segurança da CONTRATANTE.

3.1.6. As ameaças de segurança da informação consistem em eventos de segurança identificados em ativos e redes monitoradas, tais como: ataques de movimentação lateral, escalação de privilégios, acessos indevidos, instalações de códigos maliciosos, ataques por força bruta, ou qualquer outra ação passível de monitoramento e que possa comprometer a confidencialidade, disponibilidade, integridade ou privacidade das informações da CONTRATANTE.

3.1.7. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação da CONTRATANTE, que pode levar à perda de um ou mais princípios básicos de segurança cibernética: confidencialidade, integridade, disponibilidade ou privacidade.

3.1.8. Os serviços devem ser realizados por meio de Solução de Monitoramento, Detecção, Investigação, Notificação e Resposta a Ataques Cibernéticos, disponibilizada pela CONTRATADA para a CONTRATANTE, e devidamente licenciada para o escopo de serviços e a quantidade de ativos definidos nesta especificação, durante toda a vigência do contrato.

3.1.9. A solução deverá atender aos requisitos técnicos mínimos estabelecidos na seção "REQUISITOS TÉCNICOS MÍNIMOS DAS SOLUÇÕES UTILIZADAS PARA A PRESTAÇÃO DOS SERVIÇOS" desta especificação.

3.1.10. Os serviços de SOC/MDR deverão contemplar, no mínimo, as seguintes etapas: Planejamento, Implantação, Validação e Monitoramento.

Planejamento

3.1.11. Nesta fase ocorrerá a reunião inicial (kick-off meeting), durante a qual é efetuado o levantamento necessário para o planejamento e elaboração de Statement of Work (SOW), a ser entregue no final desta fase do serviço.

3.1.12. Esta fase será iniciada no primeiro dia útil após a assinatura do contrato e terá duração máxima de 15 (quinze) dias.

3.1.13. O SOW deverá ser elaborada pela CONTRATADA, validada pela CONTRATANTE e contemplar, minimamente, os seguintes itens:

3.1.13.1. Planejamento e diretrizes da implantação do serviço e da solução ofertada até sua operação.

3.1.13.2. Responsabilidades e papéis das equipes da CONTRATANTE e da CONTRATADA.

3.1.13.3. Plano de monitoramento, com o levantamento do ambiente a ser monitorado.

3.1.13.4. Definição do plano/protocolo de comunicação entre a CONTRATANTE e a CONTRATADA.

3.1.13.5. Definição da classificação e priorização dos ativos a serem monitorados, de acordo com seu risco e criticidade.

3.1.13.6. Definição do processo de escalonamento de incidentes de segurança cibernética.

3.1.13.7. Modelos de relatórios técnicos e gerenciais mensais.

Implantação

3.1.14. Nesta fase serão executadas as ações necessárias para a implantação do serviço a ser prestado.

3.1.15. Esta fase será iniciada imediatamente após a entrega do Statement of Work (SOW) e terá duração máxima de 15 (quinze) dias após a entrega daquele documento.

3.1.16. Deverão ser criados, estabelecidos, elaborados ou entregues até o final desta fase:

3.1.16.1. Comunicação segura entre as redes corporativa da CONTRATANTE e da CONTRATADA, através de Rede Privada Virtual (VPN site-to-site), caso seja necessário.

3.1.16.2. Instalação, configuração e pleno funcionamento das ferramentas a serem utilizadas para a prestação do serviço no ambiente tecnológico da CONTRATANTE.

3.1.16.3. Ratificação do ambiente tecnológico da CONTRATANTE a ser monitorado de acordo com o parque computacional.

3.1.16.4. Classificação e priorização dos ativos a serem monitorados, de acordo com seu risco e criticidade, conforme definição estabelecida no SOW.

3.1.16.5. Ativação das fontes de informações para uso pelas ferramentas a serem utilizadas para a prestação do serviço.

3.1.16.6. Criação das regras de coletas de eventos (logs e datasources) e de alertas nas ferramentas a serem utilizadas para a prestação do serviço.

3.1.16.7. Criação dos alertas associados a correlacionamento de eventos na ferramenta de SIEM, UEBA e SOAR ofertadas.

3.1.16.8. Definição e adequação de criticidade de incidentes conforme a necessidade da CONTRATANTE.

3.1.16.9. Criação dos critérios para priorização preditiva das ações ou planos a serem aplicados.

3.1.16.10. Integração das ferramentas a serem utilizadas para a prestação do serviço com o ambiente tecnológico da CONTRATANTE.

3.1.16.11. Testes das ferramentas a serem utilizadas para a prestação do serviço.

Validação

3.1.17. Nesta fase serão efetuados os ajustes, validações ou redefinições ora necessárias.

3.1.18. Esta fase será iniciada no primeiro dia útil após a implantação do serviço, e terá duração máxima de 15 (quinze) dias.

3.1.19. Deverão ser efetuados, até o final desta fase:

3.1.19.1. Validação da comunicação entre as ferramentas a serem utilizadas para a prestação do serviço e os ativos informacionais ou tecnológicos sendo monitorados.

3.1.19.2. Definição de políticas e limites (thresholds) que se façam necessários.

3.1.19.3. Validação das regras de correlação de eventos na ferramenta de SIEM que se façam necessárias.

3.1.19.4. As validações e definições concluídas no final desta fase não serão impeditivos para o aprimoramento contínuo do serviço sendo prestado, bem como para a implementação das melhorias e aprimoramentos que se façam necessários no decorrer da prestação do serviço.

Monitoramento

3.1.20. Esta fase será iniciada após a implantação do serviço e reúne todas as atividades e requisitos elencados no presente instrumento.

3.1.21. A equipe da CONTRATADA deve atuar em regime 24x7x365 no monitoramento dos incidentes detectados pelas soluções e serviços propostos, sendo responsável pela identificação, classificação e análise de eventos que possam comprometer a segurança da informação da CONTRATANTE, incluindo as seguintes atividades mínimas:

3.1.21.1. Supervisão: Avaliação dos eventos de segurança e geração de alertas para atividades suspeitas, tentativas de intrusão e padrões anômalos.

3.1.21.2. Análise e Validação de Alertas: Análise dos alertas para validar ameaças e minimizar falsos positivos, assegurando que apenas eventos relevantes sejam escalados para resposta.

3.1.21.3. Automação de Respostas: Configuração de respostas automatizadas para eventos, sempre que possível, como bloqueio de IPs maliciosos, liberando recursos da equipe para focar em incidentes mais críticos.

3.1.21.4. Detecção de Padrões Suspeitos: Identificação de padrões de comportamento que possam indicar atividades maliciosas, como movimentações laterais, escaneamento de portas e exfiltração de dados.

3.1.21.5. Relatórios de Eventos Suspeitos: Geração de relatórios sobre eventos suspeitos e atividades anômalas, com informações detalhadas para apoiar a tomada de decisão de segurança.

3.1.21.6. Agrupamento e Correlação de Eventos: Consolidação de eventos relacionados para identificar padrões de ataque e ameaças que poderiam passar despercebidas em eventos isolados.

3.1.21.7. Enriquecimento de Dados de Segurança: Integração com outras ferramentas de segurança e bases de dados (threat intelligence) para adicionar contexto aos eventos, ajudando a priorizar e entender melhor as ameaças.

3.1.21.8. Relatórios Mensais de Atividade: Elaboração de relatórios detalhados sobre as atividades monitoradas, eventos detectados, resposta a incidentes e efetividade das regras de segurança.

3.1.21.9. Documentação de Procedimentos e Boas Práticas: Criação de documentação com procedimentos recomendados, fluxos de trabalho e melhores práticas para uso e manutenção das ferramentas utilizadas.

3.1.22. Todos os incidentes, chamados e demandas de serviço deverão ser registradas pela CONTRATADA em um sistema de gerenciamento de serviços (ITSM – IT Service Management) disponibilizado pela mesma e acessível pela CONTRATANTE para acompanhamento de SLAs, registros e tratamentos dos incidentes de segurança da informação e demais atendimentos, cujas especificações mínimas encontram-se listadas no item de Resposta a Incidentes de Segurança da Informação.

3.1.23. O sistema de gerenciamento de incidentes deverá ser integrado ao ITSM da CONTRATADA.

3.2. Serviços de Resposta a Incidentes de Segurança da Informação

3.2.1. Os serviços de Resposta a Incidentes de Segurança da Informação têm por objetivo analisar, remediar, conter e documentar 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 ou SANS de resposta a incidente de segurança da informação e boas práticas de mercado.

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

3.2.3. A equipe da CONTRATADA deve atuar em regime 24x7x365 no processo de resposta a incidentes detectados, sendo responsável por:

3.2.3.1. Analisar e recomendar ações de remediação e contenção, em seguida, documentar os eventos de segurança que, após analisados, demonstraram ser um ataque ao ambiente da CONTRATANTE, tendo sido categorizados como "Eventos de Exceção" e, portanto, acionado o processo de resposta a incidentes cibernéticos.

3.2.3.2. Analisar, após um incidente de segurança ser aberto, os logs e artefatos enviados/coletados a fim de, no primeiro instante, identificar as fontes geradoras de tais eventos.

3.2.3.3. Identificar, uma vez realizadas as análises iniciais do incidente, quais foram os principais vetores de ataque ao ambiente da CONTRATANTE.

3.2.3.4. Definir, junto à equipe de segurança cibernética da CONTRATANTE, a severidade do incidente de segurança.

3.2.3.5. Apoiar a equipe técnica da CONTRATANTE nos processos de mitigação, contenção de ataques e restauração do seu ambiente tecnológico.

3.2.3.6. Realizar, após análises iniciais do incidente e a definição de severidade, uma análise aprofundada do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

3.2.3.7. Definir e documentar, uma vez identificado o comportamento e os principais vetores de ataque, uma estratégia para a mitigação e contenção do ataque em questão e notificá-la à CONTRATANTE.

3.2.4. Os serviços serão contratados em regime de banco de horas, isto é, as horas contratadas estarão disponíveis e deverão ser consumidas pela CONTRATANTE ao longo de toda a vigência do contrato. A CONTRATANTE terá ao seu dispor o volume total de horas contratado para este período.

3.2.5. O consumo do banco de horas deverá ser previamente autorizado pela CONTRATANTE, e será realizado via abertura de chamado, podendo ser requisitado pelo CONTRATANTE ou pela CONTRATADA.

3.2.6. Além de serviços de resposta a incidentes cibernéticos a CONTRATANTE, a seu critério, poderá utilizar o banco de horas contratado para realizar atividades correlatas de segurança da informação, como suporte especializado e/ou remediação de vulnerabilidades em seu ambiente.

3.2.7. A CONTRATANTE poderá solicitar a realização remota ou presencial dos serviços, sem a incidência de custos adicionais de deslocamento, hospedagem ou de qualquer outra natureza.

3.2.8. Todos os incidentes, chamados e demandas de serviço deverão ser registradas pela CONTRATADA em um sistema de gerenciamento de serviços (ITSM – IT Service Management) disponibilizado pela mesma e acessível pela CONTRATANTE para acompanhamento de SLAs, registros e tratamentos dos incidentes de segurança da informação e demais atendimentos. Além disso, o ITSM da CONTRATADA deverá estar integrado à ferramenta de ITSM utilizado pela CONTRATANTE.

3.2.9. O sistema ITSM deverá ser do tipo SaaS, permitindo o registro e o acompanhamento de todos os incidentes e chamados originados pela CONTRATANTE, pela equipe da CONTRATADA, bem como pelas soluções ofertadas previstas nesta especificação técnica, com as seguintes capacidades mínimas:

3.2.9.1. Permitir registrar o sumário do incidente, incluindo título, detalhes e a fonte geradora do incidente. Também deverá incluir o status do incidente, data de criação, de modificação, de fechamento e o tempo em que o chamado está aberto;

3.2.9.2. Permitir a classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;

3.2.9.3. Possibilidade de manter o histórico de atividades realizadas pelos analistas;

3.2.9.4. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;

3.2.9.5. Permitir inserir evidências coletadas de eventual análise forense como um complemento da análise do incidente;

3.2.9.6. Permitir registrar ações de remediação que incluam contenção, erradicação, educação de usuários e melhorias no programa do SOC;

3.2.9.7. Permitir registrar os resultados de um incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;

3.2.9.8. Gerar relatórios semanais e mensais do acordo de nível de serviço (SLA – Service Level Agreement) dos alertas, incidentes e chamados;

3.2.9.9. Deve estar protegida por autenticação do tipo MFA – Multi-Factor Authentication e acesso criptografado ponto a ponto.

3.2.10. O sistema de ITSM deve ser ofertado de forma integrada a um agente de Inteligência Artificial, com interface Web para interação com analistas de segurança, permitindo consultas por parte da CONTRATANTE e analistas de segurança sobre o ambiente e incidentes detectados, com as seguintes capacidades:

3.2.10.1. Consultas sobre vulnerabilidades e incidentes: Identificação de vulnerabilidades e incidentes no ambiente com integração a bancos de dados públicos e internos (CVE, OWASP).

3.2.10.2. Categorização de incidentes com base na severidade: Análise de impacto e criticidade de cada incidente para categorização automática em níveis (baixa, média, alta, crítica).

3.2.10.3. Identificação de técnicas e táticas utilizadas nos ataques.

3.2.10.4. Prover detalhamento dos incidentes: Título do incidente, Host afetado, Usuário afetado, Hash de arquivos ou processos envolvidos.

3.2.10.5. Ser disponibilizada por meio de Interface Web com funcionalidade de chat.

3.2.10.6. Abertura automática de tickets de incidentes na ferramenta ITSM ofertada para a prestação dos serviços.

3.2.11. Após a ocorrência de incidentes de segurança, será de responsabilidade da CONTRATADA, analisar os logs, evidências, artefatos enviados/coletados, a fim de no primeiro instante identificar as fontes geradoras.

3.2.12. Uma vez realizadas as análises iniciais do incidente gerado, a CONTRATADA deve trabalhar para identificar quais foram os principais vetores de ataque ao ambiente da CONTRATANTE.

3.2.13. Como próximo passo o grupo de resposta a incidente de segurança da CONTRATADA, deve comunicar ao time de segurança da informação da CONTRATANTE detalhes sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.

3.2.14. Juntamente com a CONTRATANTE, a CONTRATADA deve definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação deve ser definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente. O atendimento ao incidente deverá ser realizado conforme os níveis mínimos de serviço estabelecidos nesta especificação técnica.

3.2.15. Após análises iniciais do incidente, a CONTRATADA deve realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

3.2.16. Todo o processo de análise e resultado deve ser documentado pela CONTRATADA, para que a equipe de segurança da informação da CONTRATANTE acompanhe os passos para a solução do incidente.

3.2.17. Uma vez identificado o comportamento e os principais vetores de ataque, a CONTRATADA deve definir e recomendar uma estratégia para a mitigação e contenção do ataque em questão. Qualquer tipo de alteração no parque computacional da CONTRATANTE, para contenção e mitigação do incidente deve ser autorizado pelo corpo técnico de segurança da CONTRATANTE.

3.2.18. Mitigado o incidente de segurança, a CONTRATADA deve iniciar o processo de recolhimento de toda e quaisquer evidências e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

3.2.19. Inicia-se então o processo de restauração dos serviços e soluções afetadas. Todo este processo deve ocorrer de forma harmoniosa entre as equipes da CONTRATADA, no que se refere as soluções

gerenciadas, e as equipes detentoras da determinada solução ou serviço afetado da CONTRATANTE.

3.2.20. O grupo de resposta a incidente de segurança da CONTRATADA, deve documentar as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

3.3. Serviços de Gestão de Vulnerabilidades de Servidores, Estações de Trabalho e Ativos de Rede

3.3.1. Os serviços de gestão de vulnerabilidades de segurança da informação devem ser realizados pela equipe técnica da CONTRATADA em conjunto com a CONTRATANTE e contemplar a identificação, avaliação, correção e/ou orientação de correção de fraquezas em servidores, estações de trabalho e aplicativos.

3.3.2. O prestador de serviços será responsável por executar avaliações de vulnerabilidades, avaliar riscos, priorizar ações de correção, implementar e/ou orientar medidas de remediação, visando manter o ambiente seguro e protegido contra ameaças.

3.3.3. Os serviços devem ser realizados por meio de solução automatizada de gestão de vulnerabilidades de servidores e estações de trabalho, disponibilizada pela CONTRATADA para a CONTRATANTE, e devidamente licenciada para a CONTRATANTE para o escopo de serviços e a quantidade de ativos definidos nesta especificação, durante toda a vigência do contrato.

3.3.4. A solução deverá atender aos requisitos técnicos mínimos estabelecidos na seção “REQUISITOS TÉCNICOS MÍNIMOS DAS SOLUÇÕES UTILIZADAS PARA A PRESTAÇÃO DOS SERVIÇOS” desta especificação.

3.3.5. A CONTRATADA deverá disponibilizar, como parte integrante da gestão de vulnerabilidades, serviços de takedown, com foco na identificação, notificação e remoção de conteúdos maliciosos, fraudulentos ou indevidos que representem risco à infraestrutura da CONTRATANTE, incluindo mas não se limitando a: páginas de phishing, domínios falsos, vazamentos de dados, perfis fraudulentos e outros ativos digitais que comprometam a integridade, confidencialidade ou disponibilidade dos sistemas de informação da CONTRATANTE. A CONTRATADA será responsável por adotar medidas técnicas, administrativas e legais, conforme aplicável, para garantir a mitigação dessas ameaças no menor tempo possível, bem como fornecer relatórios detalhados sobre as ações realizadas.

3.3.6. Os serviços devem contemplar, no mínimo, as seguintes atividades:

Ativação, Configuração e Operação

3.3.6.1. Ativação, configuração e operação da solução proposta, com avaliação contínua das vulnerabilidades detectadas, recomendação e implementação de correções, garantindo a proteção do ambiente da CONTRATANTE contra possíveis riscos.

3.3.6.2. Identificação e Inclusão de Ativos: Registro e configuração dos ativos críticos (servidores, estações de trabalho, dispositivos de rede, aplicativos) na ferramenta para que todos sejam monitorados quanto a vulnerabilidades.

3.3.6.3. Integração com Infraestrutura Existente: Configuração da ferramenta para integrar-se com a infraestrutura e sistemas existentes, como servidores, endpoints, redes e aplicativos, assegurando cobertura total, quando aplicável.

3.3.6.4. Automação das Políticas de Varredura: Configuração das políticas de varredura automáticas, definindo a frequência, tipos de escaneamento (como escaneamentos completos ou diferenciais) e horários de execução, minimizando impacto no ambiente de produção.

3.3.6.5. Configuração de Perfis de Acesso: Definição de perfis de acesso dentro da ferramenta, garantindo que apenas usuários autorizados tenham acesso a dados de vulnerabilidades.

Gerenciamento de Políticas e Regras

3.3.6.6. Criação de Perfis de Escaneamento Personalizados: Desenvolvimento de perfis de escaneamento específicos para diferentes tipos de ativos e aplicações, de acordo com as políticas de segurança da CONTRATANTE.

3.3.6.7. Configuração de Regras de Detecção de Vulnerabilidades: Personalização das regras de detecção para identificar tipos específicos de vulnerabilidades relevantes para o negócio, garantindo uma varredura alinhada aos riscos específicos.

3.3.6.8. Definição de Alertas e Notificações Automatizadas: Configuração de alertas automáticos para vulnerabilidades críticas, com notificação para a equipe de segurança em caso de detecção de falhas de alto risco.

3.3.6.9. Validação de Precisão da Detecção de Vulnerabilidades: Testes para verificar a precisão da ferramenta e garantir que as vulnerabilidades detectadas sejam reais, minimizando falsos positivos.

3.3.6.10. Documentação das Configurações e Procedimentos: Registro completo das configurações iniciais, com orientações para ajustes futuros, documentando o funcionamento da ferramenta e os parâmetros de detecção.

Varredura Contínua e Avaliação de Vulnerabilidades

3.3.6.11. Varredura Contínua e Programada de Vulnerabilidades: Execução de varreduras contínuas e agendadas para monitorar vulnerabilidades em tempo real, garantindo proteção contínua e identificação imediata de novas falhas.

3.3.6.12. Detecção de Ameaças: Identificação de vulnerabilidades críticas ou de zero-day, notificando a equipe para que possam ser priorizadas e corrigidas rapidamente.

3.3.6.13. Alertas Automáticos de Vulnerabilidades de Alto Risco: Configuração para que vulnerabilidades críticas gerem alertas automáticos, possibilitando resposta imediata por parte da equipe de segurança.

Classificação e Priorização de Vulnerabilidades

3.3.6.14. Classificação por Severidade: classificação das vulnerabilidades com base na severidade, seguindo padrões como o CVSS (Common Vulnerability Scoring System).

3.3.6.15. Priorização de Correções Baseada em Contexto: Priorização das vulnerabilidades de acordo com a criticidade dos ativos afetados e o potencial de exploração, permitindo que as correções sejam focadas onde há maior risco.

3.3.6.16. Relatórios de Priorização para Correção: Relatórios com vulnerabilidades classificadas por criticidade e recomendação de prioridade para a equipe, ajudando a planejar e gerenciar as ações de remediação.

Remediação e Correção de Vulnerabilidades

3.3.6.17. Implementação de Correções Automatizadas: A ferramenta deve aplicar automaticamente patches de segurança e atualizações em ativos específicos, com supervisão para garantir que as correções são aplicadas sem interromper os serviços, quando aplicável.

3.3.6.18. Automação de Ajustes de Configuração de Segurança: Correção de vulnerabilidades relacionadas a configurações incorretas, ajustando políticas de segurança e permissões conforme as práticas recomendadas.

3.3.6.19. Testes de Compatibilidade para Aplicação de Patches: Realização de testes antes da aplicação de patches críticos para verificar compatibilidade e evitar impactos indesejados no ambiente de produção.

3.3.6.20. Isolamento de Ativos Comprometidos: Em caso de vulnerabilidades graves, deverá ser realizado o isolamento de ativos comprometidos.

3.3.6.21. Acompanhamento e Notificação de Vulnerabilidades Remediadas: Geração de notificações e relatórios automáticos sobre vulnerabilidades corrigidas, mantendo a equipe informada sobre o status das correções aplicadas.

Validação Pós-Correção e Testes de Segurança

3.3.6.22. Validação das Correções: Após a aplicação de correções, a ferramenta deve realizar uma nova varredura para confirmar que a vulnerabilidade foi corrigida e que não há falhas adicionais.

3.3.6.23. Testes de Segurança Pós-Remediação: Realização de testes para verificar a eficácia das correções aplicadas, garantindo que os ativos estão seguros após a remediação.

3.3.6.24. Documentação de Resultados de Correções: Registro automático dos resultados das correções aplicadas, documentando as mudanças e o status das vulnerabilidades antes e após a remediação.

3.3.6.25. Revisão Contínua das Políticas de Remediação: Avaliação periódica das políticas de correção e remediação, ajustando-as conforme o surgimento de novas ameaças e a evolução do ambiente de TI.

3.3.6.26. Ajustes nas Configurações de Segurança Baseadas em Resultados: Alteração das configurações de segurança com base nos resultados das varreduras contínuas para mitigar novas falhas.

3.3.6.27. Relatórios de Varredura e Efetividade das Ações de Correção: Relatórios regulares sobre o status das ações de correção e a efetividade das medidas implementadas.

Suporte Técnico, Atualizações e Patches

3.3.6.28. Aplicação de Atualizações Críticas assistidas pela contratante: Instalação de atualizações e patches de segurança recomendados pelo fabricante para corrigir vulnerabilidades e garantir o bom funcionamento.

3.3.6.29. Testes de Compatibilidade: Antes da aplicação das atualizações, realização de testes em ambiente controlado para evitar incompatibilidades e interrupções no serviço.

3.3.6.30. Agendamento de Manutenções: Coordenação e execução das atualizações em horários de menor impacto para o negócio, com comunicação prévia à equipe interna da CONTRATANTE sobre qualquer possível interrupção de serviço.

3.3.6.31. Suporte Técnico: Registrar e acompanhar chamados técnicos abertos junto ao fabricante da solução suportada, para resolução de problemas, esclarecimento de dúvidas ou melhoria do ambiente.

Relatórios de Vulnerabilidades e Análises de Risco

3.3.6.32. Relatórios Detalhados de Vulnerabilidades Detectadas: Relatórios regulares, gerados automaticamente pela ferramenta, listando todas as vulnerabilidades identificadas, organizadas por criticidade e tipo.

3.3.6.33. Análise de Risco e Impacto Potencial: Análise automática do impacto potencial das vulnerabilidades detectadas para o ambiente de TI da CONTRATANTE, facilitando a tomada de decisão.

3.3.6.34. Painéis de Controle: Visualização do status de vulnerabilidades e nível de risco, oferecendo uma visão clara do estado de segurança dos ativos monitorados.

3.3.6.35. Relatórios Mensais de Vulnerabilidades e Correções: Relatórios automáticos mensais com resumo das vulnerabilidades detectadas, correções aplicadas e status das remediações.

3.3.6.36. Análise de Indicadores de Desempenho de Remediação: KPIs como tempo médio de correção, taxa de vulnerabilidades críticas corrigidas e taxa de falsos positivos, com sugestões de otimização.

Documentação

3.3.6.37. Documentação de políticas e configurações implementadas para as soluções gerenciadas.

3.3.6.38. Documentação com as melhores práticas, procedimentos recomendados e fluxos de trabalho para o processo de sustentação e gerenciamento das soluções.

3.3.7. Todos os incidentes, chamados e demandas de serviço deverão ser registradas pela CONTRATADA em um sistema de gerenciamento de serviços (ITSM – IT Service Management) disponibilizado pela mesma e acessível pela CONTRATANTE para acompanhamento de SLAs, registros e tratamentos dos incidentes de segurança da informação e demais atendimentos, cujas especificações mínimas encontram-se listadas no item de Resposta a Incidentes de Segurança da Informação.

3.4. Serviços de Gestão de Vulnerabilidades de Aplicações WEB

3.4.1. Os serviços de gestão de vulnerabilidades de segurança da informação devem ser realizados pela equipe técnica da CONTRATADA e contemplar a identificação, avaliação, correção e/ou orientação de correção de fraquezas em aplicações WEB.

3.4.2. O prestador de serviços será responsável por executar avaliações de vulnerabilidades, avaliar riscos, priorizar ações de correção, implementar e/ou orientar medidas de remediação, visando manter o ambiente seguro e protegido contra ameaças.

3.4.3. Os serviços devem ser realizados por meio de solução automatizada de gestão de vulnerabilidades de aplicações WEB, disponibilizada pela CONTRATANTE para a CONTRATADA, e devidamente licenciada para a CONTRATANTE para o escopo de serviços e a quantidade de FQDNs definidos nesta especificação, durante toda a vigência do contrato.

3.4.4. A solução deverá atender aos requisitos técnicos mínimos estabelecidos na seção “REQUISITOS TÉCNICOS MÍNIMOS DAS SOLUÇÕES UTILIZADAS PARA A PRESTAÇÃO DOS SERVIÇOS” desta especificação.

3.4.5. Os serviços devem contemplar, no mínimo, as seguintes atividades:

Ativação, Configuração e Operação

3.4.5.1. Ativação, configuração e operação da ferramenta proposta, avaliando continuamente as vulnerabilidades detectadas e recomendando as correções relacionadas, e garantindo que o ambiente da CONTRATANTE esteja protegido contra riscos.

3.4.5.2. Identificação e Inclusão de Aplicações: Registro e configuração os FQDNs na ferramenta para que aplicações sejam monitoradas quanto a vulnerabilidades.

3.4.5.3. Automação das Políticas de Varredura: Configuração das políticas de varredura automáticas, definindo a frequência, tipos de escaneamento (como escaneamentos completos ou diferenciais) e horários de execução, minimizando impacto no ambiente de produção.

3.4.5.4. Configuração de Perfis de Acesso: Definição de perfis de acesso dentro da ferramenta, garantindo que apenas usuários autorizados tenham acesso a dados de vulnerabilidades.

Gerenciamento de Políticas e Regras

3.4.5.5. Criação de Perfis de Escaneamento Personalizados: Desenvolvimento de perfis de escaneamento específicos para diferentes tipos aplicações, de acordo com as políticas de segurança da CONTRATANTE.

3.4.5.6. Configuração de Regras de Detecção de Vulnerabilidades: Personalização das regras de detecção para identificar tipos específicos de vulnerabilidades relevantes para o negócio, garantindo uma varredura alinhada aos riscos específicos.

3.4.5.7. Definição de Alertas e Notificações Automatizadas: Configuração de alertas automáticos para vulnerabilidades críticas, com notificação para a equipe de segurança em caso de detecção de falhas de alto risco.

3.4.5.8. Validação de Precisão da Detecção de Vulnerabilidades: Testes para verificar a precisão da ferramenta e garantir que as vulnerabilidades detectadas sejam reais, minimizando falsos positivos.

3.4.5.9. Documentação das Configurações e Procedimentos: Registro completo das configurações iniciais, com orientações para ajustes futuros, documentando o funcionamento da ferramenta e os parâmetros de detecção.

Varredura Contínua e Avaliação de Vulnerabilidades

3.4.5.10. Varredura Contínua e Programada de Vulnerabilidades: Execução de varreduras contínuas e agendadas para monitorar vulnerabilidades, garantindo proteção contínua e identificação imediata de novas falhas.

3.4.5.11. Detecção de Ameaças: Identificação de vulnerabilidades críticas ou de zero-day, notificando a equipe para que possam ser priorizadas e corrigidas rapidamente.

3.4.5.12. Alertas Automáticos de Vulnerabilidades de Alto Risco: Configuração para que vulnerabilidades críticas gerem alertas automáticos, possibilitando resposta imediata por parte da equipe de segurança.

Classificação e Priorização de Vulnerabilidades

3.4.5.13. Classificação de Severidade: classificação das vulnerabilidades com base na severidade, seguindo padrões como o CVSS (Common Vulnerability Scoring System).

3.4.5.14. Priorização de Correções Baseada em Contexto: Priorização das vulnerabilidades de acordo com a criticidade dos ativos afetados e o potencial de exploração, permitindo que as correções sejam focadas onde há maior risco.

3.4.5.15. Relatórios de Priorização para Correção: Relatórios automáticos com vulnerabilidades classificadas por criticidade e recomendação de prioridade para a equipe, ajudando a planejar e gerenciar as ações de remediação.

Validação Pós-Correção e Testes de Segurança

3.4.5.16. Validação das Correções: Após a aplicação de correções, a ferramenta deve realizar uma nova varredura para confirmar que a vulnerabilidade foi corrigida e que não há falhas adicionais.

3.4.5.17. Testes de Segurança Pós-Remediação: Realização de testes para verificar a eficácia das correções aplicadas, garantindo que os ativos estão seguros após a remediação.

3.4.5.18. Documentação de Resultados de Correções: Registro dos resultados das correções aplicadas, documentando as mudanças e o status das vulnerabilidades antes e após a remediação.

3.4.5.19. Revisão Contínua das Políticas de Remediação: Avaliação periódica das políticas de correção e remediação, ajustando-as conforme o surgimento de novas ameaças e a evolução do ambiente de TI.

3.4.5.20. Ajustes nas Configurações de Segurança Baseadas em Resultados: Alteração das configurações de segurança com base nos resultados das varreduras contínuas para mitigar novas falhas.

3.4.5.21. Relatórios de Varredura e Efetividade das Ações de Correção: Relatórios regulares sobre o status das ações de correção e a efetividade das medidas implementadas.

Suporte Técnico, Atualizações e Patches

3.4.5.22. Aplicação de Atualizações Críticas: Instalação de atualizações e patches de segurança recomendados pelo fabricante para corrigir vulnerabilidades e garantir o bom funcionamento.

3.4.5.23. Testes de Compatibilidade: Antes da aplicação das atualizações, realização de testes em ambiente controlado para evitar incompatibilidades e interrupções no serviço.

3.4.5.24. Agendamento de Manutenções: Coordenação e execução das atualizações em horários de menor impacto para o negócio, com comunicação prévia à equipe interna da CONTRATANTE sobre qualquer possível interrupção de serviço.

3.4.5.25. Suporte Técnico: Registrar e acompanhar chamados técnicos abertos junto ao fabricante da solução suportada, para resolução de problemas, esclarecimento de dúvidas ou melhoria do ambiente.

Relatórios de Vulnerabilidades e Análises de Risco

3.4.5.26. Relatórios Detalhados de Vulnerabilidades Detectadas: Relatórios regulares, gerados automaticamente pela ferramenta, listando todas as vulnerabilidades identificadas, organizadas por criticidade e tipo.

3.4.5.27. Análise de Risco e Impacto Potencial: Análise automática do impacto potencial das vulnerabilidades detectadas para o ambiente de TI da CONTRATANTE, facilitando a tomada de decisão.

3.4.5.28. Painéis de Controle: Visualização do status de vulnerabilidades e nível de risco, oferecendo uma visão clara do estado de segurança dos ativos monitorados.

3.4.5.29. Relatórios Mensais de Vulnerabilidades e Correções: Relatórios automáticos mensais com resumo das vulnerabilidades detectadas, correções aplicadas e status das remediações.

3.4.5.30. Análise de Indicadores de Desempenho de Remediação: KPIs como tempo médio de correção, taxa de vulnerabilidades críticas corrigidas e taxa de falsos positivos, com sugestões de otimização.

Documentação

3.4.5.31. Documentação de políticas e configurações implementadas para as soluções gerenciadas.

3.4.5.32. Documentação com as melhores práticas, procedimentos recomendados e fluxos de trabalho para o processo de sustentação e gerenciamento das soluções.

3.4.5.33. Todos os incidentes, chamados e demandas de serviço deverão ser registradas pela CONTRATADA em um sistema de gerenciamento de serviços (ITSM – IT Service Management) disponibilizado pela mesma e acessível pela CONTRATANTE para acompanhamento de SLAs, registros e tratamentos dos incidentes de segurança da informação e demais atendimentos, cujas especificações mínimas encontram-se listadas no item de Resposta a Incidentes de Segurança da Informação.

3.5. Serviços de Monitoramento de Deep e Dark Web

3.5.1. A CONTRATADA deverá realizar serviços de monitoramento de DEEP e DARK WEB, por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada, ou por meio de solução complementar.

3.5.2. O serviço de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas à CONTRATANTE e seus colaboradores como: credenciais roubadas, marcas, domínios e outros vazamentos de informações pessoais identificáveis.

3.5.3. Os serviços devem ser realizados por meio de solução automatizada de monitoramento de deep e dark web, disponibilizada pela CONTRATANTE para a CONTRATADA, e devidamente licenciada para a CONTRATANTE para o escopo de serviços e a quantidade de ativos definidos nesta especificação, durante toda a vigência do contrato.

3.5.4. A solução deverá atender aos requisitos técnicos mínimos estabelecidos na seção “REQUISITOS TÉCNICOS MÍNIMOS DAS SOLUÇÕES UTILIZADAS PARA A PRESTAÇÃO DOS SERVIÇOS” desta especificação.

3.5.5. O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) e deve contemplar, no mínimo, as seguintes atividades:

Identificação de Dados Sensíveis

3.5.6. Busca por informações vazadas: Monitorar fóruns, marketplaces e plataformas onde dados sensíveis podem ser comercializados ou divulgados (e.g., credenciais, dados financeiros, segredos comerciais).

3.5.7. Monitoramento de palavras-chave: Configurar buscas contínuas com termos relacionados à empresa, como nomes de domínio, IPs, marcas e produtos.

3.5.8. Análise de documentos e arquivos: Verificar se documentos internos, códigos-fonte ou informações confidenciais foram compartilhados.

Detecção de Ameaças e Planejamento de Ataques

3.5.9. Identificação de ataques direcionados: Observar discussões que mencionem campanhas contra a empresa ou seus colaboradores, como phishing, ransomware ou DDoS.

3.5.10. Rastreamento de atividades de grupos de ameaça: Acompanhar ações de grupos conhecidos de cibercriminosos e hacktivistas que possam estar planejando ataques.

3.5.11. Identificação de exploits e ferramentas: Procurar exploits, ferramentas ou métodos de ataque relacionados às vulnerabilidades dos sistemas utilizados pela organização.

Monitoramento de Atividades de Fraude

3.5.12. Detecção de phishing e sites falsos: Identificar URLs maliciosos ou cópias fraudulentas de websites da empresa.

3.5.13. Monitoramento de cartões de crédito e identidade: Buscar por dados de colaboradores e clientes em mercados que comercializam credenciais roubadas.

3.5.14. Verificação de campanhas de engenharia social: Identificar campanhas fraudulentas que utilizam o nome ou marca da empresa.

Rastreamento de Ativos Digitais

3.5.15. Domínios e IPs fraudulentos: Monitorar o registro de domínios semelhantes ao da empresa que possam ser utilizados para ataques.

3.5.16. Perfis falsos em redes sociais: Detectar contas falsas que podem ser usadas para enganar clientes ou colaboradores.

3.5.17. Monitoramento de vazamento de chaves de API e certificados: Identificar se ativos críticos estão sendo divulgados na Deep ou Dark Web.

Relatórios e Correlações

3.5.18. Análise de inteligência: Correlacionar as informações coletadas na Deep/Dark Web com incidentes ou alertas identificados em outras ferramentas de monitoramento (SIEM, EDR, etc.).

3.5.19. Produção de relatórios regulares: Criar relatórios de inteligência para a alta gestão, destacando riscos potenciais e medidas recomendadas.

3.5.20. Feedback ao plano de resposta a incidentes (IRP): Atualizar o plano de resposta com base nas ameaças detectadas na Deep/Dark Web.

Cooperação com Autoridades e Fornecedores

3.5.21. Parceria com equipes de threat intelligence: Trabalhar com empresas especializadas em monitoramento de Deep e Dark Web para ampliar a capacidade de coleta de informações.

3.5.22. Cooperação em investigações: Auxiliar em investigações relacionadas a atividades maliciosas detectadas.

4. REQUISITOS TÉCNICOS MÍNIMOS DAS SOLUÇÕES OFERTADAS PARA A PRESTAÇÃO DOS SERVIÇOS

4.1. Requisitos Gerais das Soluções Ofertadas

4.1.1.1. Deverá ser obrigatoriamente licenciada para a CONTRATANTE, possuir suporte do fabricante e não poderá ser do tipo open source (software livre).

4.1.1.2. Caso englobe a alocação de equipamentos necessários para realizar as atividades de segurança da informação e ao atendimento das especificações técnicas deste termo de referência, será de responsabilidade da CONTRATADA fornecer tais equipamentos.

4.1.1.3. Todos os eventuais equipamentos necessários à prestação dos serviços devem ser novos e de primeiro uso.

4.1.1.4. Todos os equipamentos, softwares e subscrições necessárias não podem constar, no momento da apresentação da proposta técnica, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida.

4.1.1.5. As subscrições ofertadas devem ser fornecidas em sua versão mais estável, atualizada e coberta por contratos de suporte e atualização de versão do fabricante durante toda a vigência do contrato. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante pelo período estipulado neste contrato.

4.1.1.6. Em todas as especificações técnicas elencadas devem ser respeitadas as capacidades mínimas requeridas para os serviços entregues e que, no momento de contingência ou indisponibilidade de um equipamento ou software, os produtos alocados continuem suportando a operação sem degradação ou perda de performance.

4.1.1.7. A CONTRATADA deve fornecer, durante a validade do contrato, acesso a novas versões, correções emergenciais e pacotes de correções do(s) programa(s) componentes da solução por meio de atualização, sem ônus adicional, além daqueles previstos neste contrato;

4.1.1.8. A CONTRATADA deverá prover acesso às documentações, especificações e à base de conhecimento no site do fabricante para a CONTRATANTE;

4.1.1.9. A CONTRATADA deverá garantir que as novas versões dos programas componentes da solução sejam licenciadas em nome da CONTRATANTE, que poderá a qualquer momento conferir estado dessas licenças de uso diretamente com o fabricante.

4.1.1.10. A CONTRATADA deve ser responsável por prover todos os recursos necessários à ativação, instalação, configuração e integrações das subscrições descritas.

4.1.1.11. A comprovação técnica dos requisitos das soluções ofertadas deverá ser feita por meio de apresentação de manuais, folhas de dados, especificações técnicas disponíveis via WEB, no site do fabricante ou correlatos.

4.1.1.12. Não serão aceitas Cartas de Fabricante para comprovação técnica dos requisitos mínimos das soluções ofertadas.

4.2. Solução de Monitoramento, Detecção, Investigação, Notificação e Resposta a Ataques Cibernéticos

4.2.1. A CONTRATADA deve prover uma plataforma integrada de próxima geração especializada no monitoramento, deteção, investigação e resposta a ameaças e ataques cibernéticos para a CONTRATANTE.

4.2.2. A plataforma deve ser implementada como um serviço (SaaS), fornecendo entrega segura, compressão e encriptação de dados na fonte. **NÃO SERÃO ACEITAS SOLUÇÕES BASEADAS EM SOFTWARE DE CÓDIGO ABERTO.**

4.2.3. A plataforma deve suportar e estar licenciada para coletar, correlacionar e processar o volume mínimo de ingestão de logs e volumetria de ativos previstos na seção ESCOPO DE FORNECIMENTO desta

especificação técnica, bem como, deve estar licenciada para reter 1 mês de armazenamento quente (hot logs) e 11 meses de armazenamento frio (cold logs).

Quanto às suas características gerais, a solução ofertada deverá:

4.2.4. Possuir diversas funcionalidades de segurança que irão prover a capacidade de detecção e resposta aos incidentes de segurança, alinhando das detecções com as estruturas Cyber Kill Chain e MITRE ATT&CK.

4.2.5. A plataforma deve ser unificada, podendo, no entanto, ter seus componentes fornecidos de forma separada, desde que se integrem plenamente e operem de maneira conjunta e eficiente. Abaixo, estão listados os componentes mínimos que devem compor a solução proposta.

4.2.5.1. Gerenciamento e correlação de eventos (SIEM);

4.2.5.2. Orquestração e automação de respostas aos incidentes (SOAR);

4.2.5.3. Análise do comportamento do usuário (UEBA);

4.2.5.4. Detecção e Resposta na Rede (NDR);

4.2.5.5. Sistema de detecção de intrusão (IDS);

4.2.5.6. Inteligência de Ameaças (Threat Intelligence);

4.2.5.7. Monitor de integridade de arquivos (FIM);

4.2.6. Gerenciar todos os componentes solicitados através de uma única interface gráfica Web, permitindo o gerenciamento centralizado de toda a solução;

4.2.7. SER HOSPEDADA NA NUVEM DO FABRICANTE, NO BRASIL, com leitura de dados próprios para correlação de eventos de atividades maliciosas;

4.2.8. A plataforma deve ser dimensionada dinamicamente e suportar configurações de alta disponibilidade.

4.2.9. Ser implantada de forma transparente através de sensores para fazer a coleta de informações, logs e telemetria;

4.2.10. Rastrear e detectar ameaças em qualquer fonte ou local dentro da CONTRATANTE, incluindo, mas não se limitando a:

4.2.10.1. Redes;

4.2.10.2. Servidores (físicos e virtuais);

4.2.10.3. Aplicações;

4.2.10.4. Nuvens públicas e privadas.

4.2.11. Permitir o inventário dos ativos presentes na rede, por endereços IP e o nível de risco desses ativos, contando com detalhes e evidências disso sem a necessidade de executar varreduras de rede para este fim;

4.2.12. Possuir nativamente a capacidade de correlacionar vulnerabilidades relatadas por ferramentas de terceiros, com assinaturas de ataque identificadas e exibi-las em um painel de controle a partir dos quais os relatórios são gerados;

4.2.13. Correlacionar vulnerabilidades com inteligência de ameaças para priorização.

4.2.14. Possuir mecanismos de controle de acesso e autenticação, baseado em função, para que apenas as pessoas autorizadas pela CONTRATANTE tenham acesso às informações;

4.2.15. Ser capaz de se integrar com métodos de autenticação via Active Directory e LDAP.

4.2.16. Priorizar o risco e as atividades de operação de segurança;

4.2.17. Prover toda a comunicação entre os componentes de forma criptografada;

4.2.18. Incluir mecanismos de sincronização, como NTP (Network Time Protocol) e, assim, garantir a sincronização correta das informações;

4.2.19. Possibilitar a auditoria sobre o status das ações tomadas ou pendentes.

4.2.20. A plataforma deve ser capaz de fornecer análise de dados isolada para locatários com controle centralizado.

4.2.21. Plataforma integrada de inteligência contra ameaças (TIP) que agrega e correlaciona inteligência contra ameaças proprietárias e de código aberto a alertas.

4.2.22. Oferecer suporte a modelos de aprendizado de máquina supervisionados, não supervisionados e adaptativos.

4.2.23. Normalizar automaticamente os dados de diversos formatos em um esquema comum.

4.2.24. Adicionar contexto com recursos de geolocalização de IP público.

4.2.25. Monitorar o comportamento de usuários e entidades (UEBA) usando IA/ML para detectar anomalias, como ameaças internas.

4.2.26. Ser extensível com APIs, isto é, integrar-se com ferramentas de terceiros por meio de APIs.

4.2.27. Implementar controle de acesso baseado em função: Controle granular até os níveis de linha/campo por usuário.

Quanto ao modelo de licenciamento, a solução ofertada deverá:

4.2.28. Permitir o recebimento ilimitado de eventos, tendo a capacidade de operar acima do estimado inicialmente sem perder qualquer funcionalidade/capacidade de indexação;

4.2.29. Permitir a análise do tráfego de rede completo da CONTRATADA.

Quanto ao armazenamento de logs e eventos, a solução ofertada deverá:

4.2.30. Armazenar na própria solução as informações do tráfego de rede e dos Logs durante o período, mínimo, de 30 dias, bem como o registro dos incidentes gerados pela plataforma durante o período de 365 dias;

4.2.31. Permitir a retenção do histórico de segurança da CONTRATADA, contemplando, minimamente, os seguintes dados:

4.2.31.1. Dados de eventos de segurança;

4.2.31.2. Dados das aplicações;

4.2.31.3. Dados dos sistemas operacionais;

4.2.31.4. Dados das nuvens públicas e privadas;

4.2.31.5. Dados do tráfego de rede;

4.2.31.6. Tráfego de registro (syslog).

4.2.32. Suportar o mascaramento de dados confidenciais para garantir a conformidade com os regulamentos.

Quanto à compatibilidade e integrações, a solução ofertada deverá:

4.2.33. Ser capaz de integrar-se às soluções de segurança terceiras presentes na rede, a fim de enriquecer a análise das informações coletadas e permitir ações adicionais de bloqueio contra-ataques cibernéticos;

4.2.34. Possuir uma API restful para integração com vários serviços para ingestão de logs, telemetria e tráfego para detecção e resposta a eventos de segurança;

4.2.35. Ser compatível com plataformas Windows e Linux;

4.2.36. Permitir a inspeção de plataformas como:

4.2.36.1. Amazon AWS;

4.2.36.2. Microsoft Azure;

4.2.36.3. Google G-Suite;

4.2.36.4. Microsoft Office 365;
4.2.36.5. Componentes virtuais (máquinas virtuais);
4.2.36.6. Box.
4.2.37. Deve possuir estrutura de integração aberta via API ou similar, com conectores que permitam a coleta de fontes de dados externos para, no mínimo, 100 (cem) soluções, incluindo:
4.2.37.1. Acronis Cyber Protect Cloud;
4.2.37.2. Amazon Security Lake;
4.2.37.3. AWS CloudTrail, CloudWatch, Firewall, GuardDuty e Inspector;
4.2.37.4. Barracuda WAF;
4.2.37.5. Bitdefender;
4.2.37.6. Cato Networks;
4.2.37.7. Check Point;
4.2.37.8. Cloudflare;;
4.2.37.9. CrowdStrike Streaming
4.2.37.10. Cybereason;
4.2.37.11. F5 BIG-IP ASM, Firewall e Silverline;
4.2.37.12. FortiEDR;
4.2.37.13. Fortigate;
4.2.37.14. Generic S3, Cloud Audit Logging, Cloud Security Command Center e Workspace;
4.2.37.15. Hillstone;
4.2.37.16. JumpCloud;
4.2.37.17. Microsoft Active Directory;
4.2.37.18. Microsoft Defender for Cloud Apps;
4.2.37.19. Microsoft Defender for Endpoint;
4.2.37.20. Microsoft Entra ID;
4.2.37.21. Microsoft SQL Server;
4.2.37.22. Nessus;
4.2.37.23. Netskope;
4.2.37.24. Office 365;
4.2.37.25. Palo Alto Networks XDR, Firewall e Panorama;
4.2.37.26. Qualys;
4.2.37.27. Rapid7;
4.2.37.28. SentinelOne;
4.2.37.29. SonicWall Firewall;
4.2.37.30. Tenable.io e Tenable.sc;
4.2.37.31. Trend Micro Apex Central, Cloud App Security;
4.2.37.32. Trend Micro Cloud One Workload Security;
4.2.37.33. Trend Micro Vision One;
4.2.37.34. VMware Workspace ONE.
4.2.38. Deve ter a capacidade de criar e atualizar analisadores personalizados.

Quanto ao mecanismo de gerenciamento e correlação de eventos (SIEM), a solução ofertada deverá:

4.2.39. Possuir a capacidade de realizar a coleta e a ingestão de logs de todos os componentes do ambiente tecnológico da CONTRATANTE, através do padrão syslog ou similar;

4.2.40. Correlacionar eventos, com o objetivo de identificar anomalias e incidentes automaticamente.

4.2.41. Combinar insights de endpoint, rede e nuvem para um contexto completo de ameaças.

4.2.42. Quanto ao mecanismo de detecção e resposta na rede (NDR), a solução deverá:

4.2.42.1. Analisar o tráfego TCP/UDP na rede da CONTRATANTE em camadas L2-L7 para detectar comportamentos e possíveis ameaças, gerando eventos de alerta de acordo com o tipo de tráfego;

4.2.42.2. Realizar o aprendizado do ambiente de rede e a inspeção do tráfego de forma off-line através de TAPs, providos pela CONTRATADA, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede;

4.2.43. Ter a capacidade de identificar ameaças no tráfego de rede e realizar o monitoramento proativo de forma automatizada de todo o tráfego passante na rede da CONTRATANTE, contemplando os seguintes critérios:

4.2.43.1. Utilização da largura de banda;

4.2.43.2. Tentativas de penetração e varreduras de IPs e portas;

4.2.43.3. Autenticações recusadas ou com falhas;

4.2.43.4. Ataques bem-sucedidos de autenticação de força bruta;

4.2.43.5. Presença de tráfego malicioso, como ramsomware, movimentação lateral, crypojacking, mimekatz, etc;

4.2.43.6. Análise de arquivos benignos e maliciosos e suas respectivas categorias;

4.2.43.7. Ataques de negação de serviço;

4.2.43.8. Conexões de comando e controle presentes, internamente ou de/para a Internet;

4.2.43.9. Dispositivos que representam o maior risco;

4.2.43.10. Tempos de resposta, tráfego de entrada e saída (inbytes/outbytes);

4.2.43.11. Aplicações que consomem assessoria mais recursos de rede;

4.2.43.12. Análise de DNS (tempos de resposta, comunicação, time-out, erros e desempenho);

4.2.43.13. Identificação das conexões e seu risco associado;

4.2.43.14. Uso dos servidores de banco de dados (Principais Queries, usuários, origem e destino e os detalhes de uso);

4.2.43.15. Identificação de aplicações da Camada 7;

4.2.43.16. Principais eventos críticos de segurança;

4.2.43.17. Tempo de resposta das aplicações;

4.2.44. Nos ambientes de virtualização cujo tráfego passa pela rede física monitorada, pelo menos as seguintes métricas devem ser obtidas:

4.2.44.1. Eventos críticos de segurança identificados nos servidores virtualizados;

4.2.44.2. As aplicações que são mais utilizados;

4.2.44.3. Principais eventos de segurança entre máquinas virtuais;

4.2.44.4. Risco associado entre máquinas virtuais.

4.2.45. Permitir a captura de pacotes completos para análise forense avançada.

Quanto a detecção dos incidentes, a solução ofertada deverá:

4.2.46. Ser capaz de detectar padrões de ataques sem a utilização de assinaturas, através da elaboração automatizada de um baseline comportamental dos usuários e entidades;

4.2.47. Aprender novos padrões de ataque ao longo do tempo para aumentar a precisão.

4.2.48. Possuir a capacidade de, via técnicas de Machine Learning, identificar anomalias nos comportamentos individuais dos usuários e entidades e de gerar alertas com relação, ao menos, aos seguintes casos de uso:

4.2.48.1. Horário atípico do acesso;

4.2.48.2. Número atípico de sessões de uso nos sistemas operacionais;

4.2.48.3. Volume de conexões atípico;

4.2.48.4. Volume de transferências de dados atípico;

4.2.48.5. Localização geográfica atípica da origem do acesso;

4.2.48.6. Endereço IP de origem atípico do acesso;

4.2.48.7. Acesso atípico a dados armazenados;

4.2.48.8. Criação e uso de processos (executáveis em memória) atípicos pelo usuário/entidade;

4.2.48.9. Mudança na postura de risco do usuário/entidade.

4.2.49. Possuir mais de 285 modelos de detecção para casos de uso, como, no mínimo, Ransomware, Command & Control, DGA, Cryptojacking, phishing, scripts de power shell maliciosos, UBA e ataques de zero-day;

4.2.50. Permitir a criação de novas regras de detecção e alteração das regras existentes;

4.2.51. Emitir alertas quando eventos críticos de segurança forem detectados na rede e estes se desviarem de padrões estabelecidos (anomalias), por meio de análises detalhada de cada aplicativo em execução na rede de modo nativo, gerando chamados para a equipe do SOC, automaticamente, para a sua atenção, atuação e documentação;

4.2.52. Permitir a geração de diagramas de conexões TCP mostrando como as ameaças estão associadas, bem como se movem no ambiente, baseado em capturas de tráfego, classificados e normalizadas automaticamente.

4.2.53. Usar IA/ML para correlacionar ameaças com alta precisão e reduzir a fadiga de alertas.

4.2.54. Apresentar fluxos de trabalho visuais e armários de evidências para simplificar o manuseio.

4.2.55. Priorizar os incidentes com base na gravidade para uma resolução mais rápida.

Quanto a resposta aos incidentes, a solução ofertada deverá:

4.2.56. Incluir uma solução integrada de gerenciamento de casos e incidentes;

4.2.57. Ter a capacidade de associar vários alertas recebidos a um único incidente que tem a capacidade de ser atribuído, ter uma linha do tempo, objetos associados, bem como as principais métricas MTTD e MTTR;

4.2.58. Ter a capacidade de enviar instruções de resposta através dos mesmos sensores de coleta;

4.2.59. Ter a capacidade de responder a todos os eventos de forma orquestrada e automatizada, integrando-se ao ambiente tecnológico da CONTRATANTE. As ações possíveis de resposta devem ser, pelo menos, as seguintes:

4.2.59.1. Enviar um e-mail;

4.2.59.2. Enviar mensagens para meios de comunicação do tipo SLACK;

4.2.59.3. Fazer um POST, GET ou um PUT via API;

4.2.59.4. Criar regras de bloqueio no firewall;

4.2.59.5. Desabilitar usuários no Active Directory;

4.2.59.6. Executar scripts.

4.2.60. Contemplar uma ferramenta que permita a investigação e busca de ameaças, com o objetivo de identificar as ameaças presentes na rede e automatizar os eventos de segurança para responder a elas;

4.2.61. Permitir a Caça Automatizada de Ameaças com roteiros predefinidos ou personalizados.
4.2.62. Ser capaz de realizar análise retrospectiva com base nos dados ingeridos e armazenados do tráfego TCP/UDP, apoiando uma análise forense.
4.2.63. Bloquear ameaças em tempo real sem exigir redefinições de TCP.

Quanto aos relatórios e dashboards, a solução ofertada deverá:

4.2.64. Ter a capacidade de gerar relatórios executivo e operacionais, com base em modelos pré-configurados, personalizáveis, baseados em dashboards, incluindo, pelo menos, relatórios sobre o status atual dos dispositivos, seu risco associado e tendências;
4.2.65. Gerar informações detalhadas sobre os eventos detectados, incluindo ameaças, anomalias, comportamentos e tendências de rede associadas ao risco de rede;
4.2.66. Detalhar os gráficos para aprofundar as informações apresentadas (mecanismo conhecido como Drill Down);
4.2.67. Gerar KRI (Principais Indicadores de Risco), como o número de eventos gerados em um dia, semana ou meses e compará-los com um período semelhante, o mesmo com a criticidade média dos eventos;
4.2.68. Permitir ao pessoal designado a geração de relatórios explorando todas as variáveis e funcionalidades da ferramenta, com a opção de parametrizar esses relatórios e consultá-los via Web, bem como a criação de filtros personalizados para pesquisas de eventos específicos;
4.2.69. Fornecer painéis configuráveis que possam conter diferentes gráficos com informações de, pelo menos:
4.2.69.1. Eventos anômalos e críticos, incluindo:
4.2.69.2. Detecções de segurança;
4.2.69.3. IPs de Origem e Destino;
4.2.69.4. Visão geral da atividade dos dispositivos (servidores e infraestrutura, física e virtualizada);
4.2.69.5. Táticas e técnicas do MITRE ATT&CK;
4.2.69.6. Fases do Kill Chain e os alertas associados.
4.2.69.7. Aplicações utilizadas e seus dados históricos, discriminada por:
4.2.69.8. Risco associado;
4.2.69.9. IP de Origem e Destino;
4.2.69.10. Anomalias detectadas;
4.2.69.11. Classificação de risco;
4.2.69.12. Tráfego entre hosts.
4.2.69.13. Informações de em um Host:
4.2.69.14. Aplicações utilizadas;
4.2.69.15. Tráfego de e para o Host com base em detecções de segurança e anomalias.
4.2.69.16. Informações e o status das aplicações e serviços que estão sendo executados no data center, tais como:
4.2.69.16.1.1. Quantidade e a gravidade das anomalias;
4.2.69.16.1.2. Possíveis problemas de segurança no data center.
4.2.70. Permitir a criação de relatórios por período (hora, dia, semana, mês, ano, e personalizado por datas específicas);
4.2.71. Possuir filtros pós-captura, pelo menos para:
4.2.71.1. Filtro de erro;
4.2.71.2. Filtros por tráfego entre duas estações através da seleção do nome ou endereço IP;

4.2.71.3. Filtros por protocolos;
4.2.71.4. Geolocalização;
4.2.71.5. Gravidade;
4.2.71.6. Endereço IP.
4.2.72. Suportar diagnósticos nas diferentes camadas do modelo OSI, incluindo:
4.2.72.1. Análise das anomalias da rede da camada 2 à camada 7;
4.2.72.2. Endereços IP;
4.2.72.3. Aplicações e/ou portas (TCP/UDP);
4.2.72.4. Serviços associados;
4.2.72.5. Servidores mais lentos;
4.2.72.6. Origem e destino.
4.2.73. Ser capaz de gerar um gráfico das anomalias das aplicações dentro da rede, fornecendo resultados com pelo menos as seguintes variáveis:
4.2.73.1. Movimentos laterais;
4.2.73.2. Histórico de eventos;
4.2.73.3. Anomalias de tráfego maliciosos;
4.2.73.4. Anomalias de políticas e negações de firewalls de infraestrutura;
4.2.73.5. Principais Aplicações;
4.2.73.6. Top Servidores;
4.2.73.7. Top Clientes;
4.2.73.8. Status das sessões atuais;
4.2.73.9. Origens e destinos de países com má reputação.
4.2.74. Oferecer relatórios pré-criados para ISO 27001, GDPR, HIPAA e PCI DSS.
4.2.75. Exportar as informações dos pacotes capturados em metadados para análise posterior.
4.2.76. Inclui painéis de inteligência para plataformas como Windows, Linux, MySQL, DNS e análise de tráfego.
4.2.77. A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do item sem necessidade de prévia consulta e/ou qualquer liberação por parte da empresa licitante.
4.2.78. A abertura de chamados poderá ser realizada através de Telefone ou através de endereço de e-mail do Fabricante.

Agente de Segurança de IA:

4.2.79. O SOC deverá contar com agente de segurança baseado em inteligência artificial, utilizando IA, licenciado para um número ilimitado de eventos e fontes monitoradas.
4.2.80. O agente virtual de cibersegurança baseado em inteligência artificial (IA), deverá ter como objetivo de otimizar, automatizar e evoluir as operações do Centro de Operações de Segurança (SOC) da contratante.
4.2.81. A solução deverá ser capaz de potencializar a capacidade de análise, investigação, resposta, inteligência e a automação dos processos do SOC.
4.2.82. A solução deverá atuar como agente virtual de segurança cibernética baseado em IA.
4.2.83. Estar conforme com a com a LGPD ou outras regulamentações pertinentes à proteção de dados pessoais.
4.2.84. Deverá ser capaz de operar de maneira autônoma 24 horas por dia, 7 dias por semana, sem dependência de escala humana.

4.2.85. A cada 100 ativos contratados conforme o item 1, referente aos serviços de SOC/MDR (Security Operation Center/Managed Detection and Response), a contratada deverá fornecer o agente de segurança baseado em IA, capaz de suportar e operacionalizar os ativos contratados.

4.2.86. A solução deverá realizar o monitoramento contínuo, a triagem e a resposta automática dos alertas de segurança das ferramentas em tempo real;

4.2.87. Deverá gerar de maneira automática, relatórios detalhados e contextualizados sobre incidentes de segurança;

4.2.88. A solução deverá ser capaz de reduzir o tempo de resposta a incidentes;

4.2.89. Deve ser capaz de eliminar os falsos positivos por meio de inteligência contextual;

4.2.90. Deve ser capaz de automatizar triagens, investigações e respostas através de IA;

4.2.91. A solução deverá ser capaz de:

4.2.91.1. Realizar Investigação e resposta a tentativas de engenharia social;

4.2.91.2. Realizar o monitoramento e mitigação de ameaças em ambientes de nuvem;

4.2.91.3. Detectar padrões maliciosos em tráfego de rede;

4.2.91.4. Analisar e responder a ameaças em dispositivos finais;

4.2.91.5. Realizar o monitoramento de compromissos de identidade e vazamentos;

4.2.91.6. Detectar e tratar as ameaças internas.

4.2.92. A solução deverá ser capaz de proporcionar os seguintes resultados:

4.2.92.1. Redução dos falsos positivos nos alertas processados;

4.2.92.2. Tempo médio de resposta a incidentes críticos;

4.2.92.3. Aumento na capacidade de tratamento de alertas, sem necessidade de ampliação da equipe;

4.2.92.4. Geração automatizada de relatórios técnicos e executivos;

4.2.92.5. Fortalecimento da postura proativa de segurança da informação da organização.

4.2.93. A solução deverá ser capaz de atender aos seguintes itens abaixo:

4.2.93.1. Suporte técnico especializado, com atendimento especializado para resolução de problemas críticos;

4.2.93.2. Ser capaz de fornecer atualizações contínuas da base de conhecimento e dos modelos de IA;

4.2.93.3. Painel de controle para o acompanhamento das ações realizadas pela IA.

4.3. Solução de Gestão de Vulnerabilidades de Servidores e Estações de Trabalho e Ativos de Rede

4.3.1. A CONTRATADA deve prover uma plataforma no modelo (SaaS) para a gestão de vulnerabilidades de Servidores, Estações de Trabalho e ativos de rede, gerenciamento de patches de segurança e conformidade de configurações do ambiente da CONTRATANTE, incluindo varredura de máquinas virtuais, endereços IP, ativos em nuvem, auditoria de configuração e análise de vulnerabilidades com gerência na nuvem.

4.3.2. A solução de gestão de vulnerabilidades e patches deve ser composta por software, de gerenciamento centralizado e de varredura que deverão ter a capacidade de realizar busca de vulnerabilidades, configurações incorretas e, bem como as respectivas sugestões de resolução das vulnerabilidades encontradas, permitindo a correção imediata ou agendada, quando existir.

4.3.3. A plataforma deve suportar e estar licenciada conforme volumetria prevista na seção ESCOPO DE FORNECIMENTO desta especificação técnica.

4.3.4. A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) em uma nuvem do fabricante para todos os seus serviços e aplicativos exigidos neste documento.

4.3.5. A gestão de todas as funcionalidades consideradas neste termo deve ser feita através de uma console centralizada e única.

4.3.6. Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade.

4.3.7. A solução deve permitir criação de usuários distintos.

4.3.8. Deve permitir separação de funções e permissões na console.

4.3.9. Deve permitir integração com recursos SSO Microsoft e Google.

4.3.10. A console deve ser acessível a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge ou Firefox.

Agentes

4.3.11. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede, exceto quando em download de patches.

4.3.12. A solução deve ser instalada em servidores, estações de trabalho, e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem.

4.3.13. A solução deve oferecer suporte para sua implantação, no mínimo, nos seguintes sistemas operacionais:

4.3.13.1. Windows 7, 8, 10, 11 e posteriores;

4.3.13.2. Windows Server 2008 R2, 2012, 2012R2, 2016, 2019, 2022 e posteriores;

4.3.13.3. Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64), 9,x (x64);

4.3.13.4. Ubuntu Server 16,18,20,22 (x64);

4.3.13.5. Oracle Enterprise Linux 7, Oracle Enterprise Linux 8, Oracle Enterprise Linux 9;

4.3.13.6. Debian 9 e posteriores;

4.3.13.7. Amazon Linux 2 e posteriores;

4.3.13.8. macOS 10.15 e posteriores;

4.3.13.9. macOS M Series ;

4.3.13.10. Rock Linux;

4.3.13.11. Linux Mint;

4.3.13.12. Alma Linux;

4.3.14. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente.

4.3.15. Deve ter a opção de desabilitar a atualização do agente por opção do administrador.

4.3.16. A solução deve ser capaz de coletar informações sobre o inventário de ativos.

4.3.17. As funcionalidades de gestão de ativos, gestão de vulnerabilidade e detecção de patches devem ser fornecidas pelo mesmo agente de gerenciamento, não serão aceitas soluções com múltiplos agentes.

4.3.18. A solução deve prover um recurso (software) que seja capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma.

4.3.19. O agente de gerenciamento deve suportar o uso de proxy.

4.3.20. Deve ser possível limitar o consumo de CPU do agente.

4.3.21. Deve ser possível impedir a remoção do agente pelo usuário por meio do uso de senha.

4.3.22. A solução deve permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo:

4.3.22.1. Softwares instalados;

4.3.22.2. Último usuário logado;

4.3.22.3. Nome do host;

4.3.22.4. IPv4;

4.3.22.5. Endereço MAC;

4.3.22.6. Processador;

4.3.23. A solução deve classificar automaticamente os ativos por nome do host, tipo de SO, nível de risco, quantidade de aplicações, pelo seu status e quando foi conectado pela última vez.

4.3.24. A solução deve possuir a habilidade de etiquetagem (Tags) de ativos para facilitar a identificação no momento de sua instalação e posteriormente.

4.3.25. A solução deve permitir agrupamento manual a critério do administrador da solução.

4.3.26. A solução deve atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.

4.3.27. A solução deve permitir uma interface de busca de ativos que seja baseada, no mínimo, nos critérios abaixo:

4.3.27.1. Família de Sistemas Operacionais;

4.3.27.2. Build específicas de Sistemas Operacionais;

4.3.27.3. Softwares instalados;

4.3.27.4. Versões Específicas de Softwares;

4.3.27.5. Último usuário logado.

4.3.28. A solução deve permitir a visualização de quantidade de máquinas com um determinado software instalado inclusive suas versões.

4.3.29. Possibilitar o filtro negativo de forma a excluir, no mínimo, nos critérios abaixo:

4.3.29.1. Família de Sistemas Operacionais;

4.3.29.2. Build específicas de Sistemas Operacionais;

4.3.29.3. Softwares instalados;

4.3.29.4. Versões Específicas de Softwares.

Gestão de Vulnerabilidades

4.3.30. A solução deve permitir descobrir, avaliar, priorizar e auxiliar na correção de vulnerabilidades / configurações, incluindo estações de trabalho, servidores, máquinas virtuais, proporcionando através de única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto.

4.3.31. Detectar e analisar vulnerabilidades nas principais versões de Bancos de Dados, suportando pelo menos:

4.3.31.1. Microsoft SQL Server.

4.3.31.2. MySQL.

4.3.31.3. Oracle.

4.3.31.4. PostgreSQL.

4.3.31.5. MariaDB

4.3.32. Detectar vulnerabilidades em pelo menos 500 aplicações de terceiros, incluindo:

4.3.32.1. Adobe;

4.3.32.2. Microsoft (Office, IIS, Exchange);

4.3.32.3. Oracle Java;

4.3.32.4. VMware.

4.3.33. A solução deve oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade do Common Vulnerability Scoring System (CVSS).

4.3.34. A solução deve permitir buscas interativas de vulnerabilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS ou CVE.

4.3.35. A solução deve permitir a utilização de operadores lógicos na busca de vulnerabilidades para que seja possível encontrar, no mínimo, as seguintes informações:

4.3.36. Vulnerabilidades associadas a exploit e que possuem patches disponíveis.

4.3.37. Na busca de vulnerabilidades deve permitir agrupamento para mostrar, no mínimo, as seguintes visualizações:

4.3.37.1. Quantidade de ocorrências de uma vulnerabilidade.

4.3.37.2. Quantidade de vulnerabilidades por sistema operacional.

4.3.37.3. Quantidade de vulnerabilidades por host.

4.3.37.4. Quantidade de vulnerabilidades por produto/software vulnerável.

4.3.38. Deve mostrar dashboards que consigam mostrar variação histórica de vulnerabilidades novas, corrigidas.

4.3.39. Deve permitir mostrar quantidades de vulnerabilidades que contém exploits e que permitem exploração sem autenticação.

4.3.40. Deve mostrar o número de vulnerabilidades que podem ser corrigidas através de patches.

Gestão de Conformidade

4.3.41. A solução deve oferecer avaliação de configuração com base no benchmark CIS padrão da indústria, cobrindo esta funcionalidade nas seguintes categorias:

4.3.41.1. Sistemas operacionais.

4.3.41.2. Software de servidor.

4.3.41.3. Software de desktop.

4.3.42. A solução deve suportar detecção de falhas de conformidades através de agente instalado diretamente no ativo monitorado.

4.3.43. A solução deve permitir que os administradores recebam informação de conformidade de sistemas operacionais Windows e Linux, mesmo que não estejam conectados na rede corporativa.

Gerenciamento de Patches

4.3.44. A solução proposta deve correlacionar vulnerabilidades e patches automaticamente para os hosts da organização.

4.3.45. A solução deve mapear automaticamente os patches com CVEs associados às vulnerabilidades detectadas.

4.3.46. Deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente.

4.3.47. Deve mostrar patches faltantes para no mínimo as seguintes categorias:

4.3.47.1. Apps;

4.3.47.2. Sistemas Operacionais.

4.3.48. A solução deve permitir filtros no dashboard para acompanhamento da aplicação dos patches.

4.3.49. Deve-se permitir inclusão de filtros personalizados para incluir, no mínimo, os requisitos abaixo:

4.3.49.1. Ativos que não possuem patches instalados.

4.3.49.2. Ativos pendentes de “boot” para aplicação de patches.

4.3.49.3. Patches faltantes.

4.3.49.4. Status de aplicação de patches.

4.3.49.5. Patches faltantes classificados por severidade.

4.3.50. A solução deve permitir mostrar em um mesmo dashboard a quantidade de ativos que possuem um software instalado e quantidade de patches relevantes a esse mesmo software.

4.3.51. A solução deve conter uma lista de produtos e softwares priorizados, permitindo visualizar patches relevantes a esses produtos.

4.3.52. A solução deve permitir a criação de tarefas de instalação a partir de produtos e softwares priorizados.

4.3.53. A solução deve apontar vulnerabilidades resolvidas por um determinado patch.

4.3.54. A solução deve conter referências do fabricante do software ou sistema operacional contendo descrição dos patches disponíveis.

4.3.55. Deve ser possível visualizar agentes instalados, seu último status de comunicação com o servidor, a quantidade de patches aplicados e faltantes.

4.3.56. A solução deve suportar tarefas de instalação e remoção dos patches.

4.3.57. A solução deve permitir a execução de scripts personalizados durante a tarefa de instalação de patches ou correções customizadas.

4.3.58. A solução deve permitir fazer upload de arquivos para a console de forma a ser utilizada por scripts posteriormente.

4.3.59. Deve ser possível executar scripts Python, CMD/Powershell(Windows), Shell (Linux), Shell MacOs antes e depois da instalação de correções.

4.3.60. A solução deve permitir a instalação de softwares através de scripts.

4.3.61. A solução deve permitir a remoção de softwares através de scripts.

4.3.62. A solução deve possuir scripts de templates, para detecção, remediação e operação de forma a ser possível selecionar e executar tais scripts.

4.3.63. A tarefa de aplicação de patches/scripts deve permitir alteração de chaves de registro na plataforma Windows.

4.3.64. A tarefa de aplicação de correções deve permitir selecionar manualmente os patches a serem aplicados ou através de um filtro de seleção que considere, no mínimo, severidade do patch, associação a uma vulnerabilidade e a associação a riscos de segurança.

4.3.65. Deve ser possível restringir a aplicação de patches a um grupo de máquinas baseados em grupo dinâmico de máquinas configurado pelo administrador da solução.

4.3.66. Deve ser possível o agendamento de execução de tarefas de patches de forma imediata.

4.3.67. Deve ser possível agendar a execução de tarefas de patches em um horário específico com recorrência diária, semanal ou mensal.

4.3.68. Deve ser possível agendar a execução de tarefas de patches com agendamento a partir do Patch Tuesday, da Microsoft, de forma automática.

4.3.69. Deve ser possível configurar uma janela de tempo máximo para execução de patches em intervalo de horas ou minutos.

4.3.70. A solução de ter a opção de selecionar uma quantidade de máquinas por hora que devem sair ao mesmo tempo para fazer o download dos patches, de forma a evitar que todas as máquinas saiam para a internet e saturem o link de internet.

4.3.71. A solução deve permitir customização de mensagens para o usuário antes, durante e após a aplicação de patches.

4.3.72. A solução deve permitir a configuração pelo administrador da supressão do reinício do sistema operacional, forçá-la ou permitir que o usuário reinicie o sistema, caso o patch aplicado exija o reinício.

4.3.73. A solução deve conter a inteligência de filtrar automaticamente, sem intervenção, quais ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e a pré-existência de determinada aplicação, evitando assim instalações indesejadas.

4.3.74. Deve ser possível gerar relatórios a partir do catálogo de patches a serem aplicados considerando filtros dos patches e dos ativos.

4.3.75. O catálogo de patches a serem aplicados deve filtrar de forma simples quais são os patches que precisam ser instalados e exibir somente a última versão disponível de cada um deles.

4.3.76. Deve ser possível visualizar, pela interface, o status de instalação de cada uma das tarefas de patch criadas.

4.3.77. O status individual de cada tarefa de patch deve mostrar quais patches foram instalados com sucesso, que falharam e quais não foram instalados por não serem necessários.

4.3.78. A solução deve exibir, para os patches que não foram instalados com sucesso, qual o motivo do erro.

4.3.79. Deve ser possível gerar um relatório CSV para uma tarefa de patch específica, com a finalidade de criar validar seu progresso e situação final de execução.

4.3.80. A solução deve possuir controle de acesso no modelo Role Based Access Control, para que sejam definidos no mínimo três perfis de usuários caso seja necessário, sendo um deles, necessariamente, incapaz de iniciar uma tarefa de execução de patch.

4.3.81. A solução deve possuir uma interface de API para permitir automatização de ações com no mínimo as seguintes funções:

4.3.81.1. Criação de tarefas de patches.

4.3.81.2. Listagem de ativos.

4.3.81.3. Listagem de patches.

4.3.81.4. Listagem de tarefas de patches.

4.3.81.5. Criação e geração de relatórios.

Console de Gerenciamento

4.3.82. A solução deve permitir administração centralizada via interface gráfica WEB usando HTTPS.

4.3.83. A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto.

4.3.84. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração.

4.3.85. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional da CONTRATANTE.

4.3.86. A solução deve permitir o acesso de um usuário autorizado a partir de qualquer local, desde que atendido os requisitos de autenticação e segurança definidos pelo administrador da solução.

4.3.87. A solução deve suportar integração com uma biblioteca API REST.

4.3.88. A solução deve suportar autenticação de dois fatores para usuários e logins administrativos.

4.3.89. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação.

4.3.90. A solução deve suportar a capacidade de distribuir relatórios em PDF.

4.3.91. A solução deve suportar acesso por SSO (Single Sign-on) usando o padrão SAML 2.0.

4.3.92. A solução deve suportar o segundo fator de autenticação (MFA) para o login na solução, sendo que ao menos deve suportar MFA do próprio fabricante, MFA Google ou MFA Microsoft.
4.3.93. A solução deve permitir o controle de alterações com trilhas de auditoria à prova de violação.
4.3.94. A solução proposta deve gerar relatórios por Grupos, que por sua vez devem ser baseados em, no mínimo, IPs, Tags, Aplicações, tipos de SO, nível de Risco, status (online-offline).
4.3.95. A solução deve permitir a geração de relatórios de qualquer Host previamente verificado.
4.3.96. A solução deve permitir agendar relatórios diários, semanais, mensais e sob demanda.
4.3.97. A solução deve permitir o envio de notificações por e-mail sempre que um relatório estiver disponível para o administrador da solução, usuários específicos e perfis diferentes criados na ferramenta.
4.3.98. A solução deve permitir pelo menos os seguintes tipos de relatórios:
4.3.98.1. Relatório de patches pendentes;
4.3.98.2. Relatório de vulnerabilidades ativas;
4.3.98.3. Relatório de eventos de vulnerabilidades;
4.3.98.4. Relatório de Atividades realizadas (sumário e detalhado);
4.3.98.5. Relatório de Ativos (sumário e detalhado);
4.3.98.6. Relatório de Sistema Operacional (sumário e detalhado);
4.3.98.7. Relatório de linha do tempo de eventos segurança;
4.3.98.8. Relatório de proteção proativa (virtual patch);
4.3.98.9. Relatório Executivo de Risco.
4.3.99. A solução deve fornecer relatórios de correção por grupo de ativos e vulnerabilidade.
4.3.100. A solução deve permitir relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório.
4.3.101. A solução deve permitir relatar as descobertas com base no status das vulnerabilidades detectadas e seu status, conforme lista abaixo:
4.3.101.1. Detectado;
4.3.101.2. Mitigado;
4.3.101.3. Ativo;

Relatórios

4.3.102. A solução deve permitir relatórios que incluam vulnerabilidades com base na data de publicação.
4.3.103. A solução deve fornecer relatórios automatizados de tendências e diferenciais.
4.3.104. A solução deve fornecer várias opções de distribuição de relatórios, incluindo PDF.
4.3.105. A solução deve permitir a exportação de relatórios para os formatos XLSX, PDF e CSV.
4.3.106. A solução deve permitir que relatórios sejam apresentados em tabelas e gráficos com as ocorrências ocorridas.
4.3.107. A solução deve permitir em seus relatórios comparar o nível de conformidade entre políticas, tecnologias e ativos.
4.3.108. A solução deve possuir um painel (dashboard) que, por padrão, permite que o administrador da solução visualize tendências de vulnerabilidades, período e status de remediação.

Sistemas Operacionais e Aplicativos Suportados

4.3.109. A solução deve permitir aplicação de patches de segurança para, no mínimo, as seguintes plataformas e aplicações:
4.3.109.1. Windows: 7, 8, 10, 11 e superior; Windows Server 2008, 2012, 2012R2, 2016, 2019, 2022 e superior;

4.3.109.2. Linux: Red Hat Enterprise Linux 6, 7, 8 e 9; CentOS 6, 7 e 8; Ubuntu Server 16, 18, 20 e 22; Debian 10, 11, 12; Amazon Linux; Oracle Linux; SUSE; Rock Linux; Linux Mint, Alma Linux;
4.3.109.3. Mac: macOS, macOS X. (Intel/Arm);
4.3.109.4. Microsoft Office (todas as versões, incluindo 365);
4.3.109.5. Microsoft SQL Server (todas as versões);
4.3.109.6. Navegadores: Google Chrome, Firefox, Microsoft Edge, Safari;
4.3.109.7. LibreOffice;
4.3.109.8. Filezilla;
4.3.109.9. Exchange Server;
4.3.109.10. Adobe Acrobat, Flash, Reader;
4.3.109.11. 7-Zip;
4.3.109.12. Zoom;
4.3.109.13. 1password;
4.3.109.14. MongoDB;
4.3.109.15. Signal;
4.3.109.16. WhatsApp;
4.3.109.17. Microsoft OneDrive.
4.3.110. A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do item sem necessidade de prévia consulta e/ou qualquer liberação por parte da empresa licitante.
4.3.111. A abertura de chamados poderá ser realizada através de Telefone ou através de endereço de e-mail do Fabricante.

4.4. Solução de Gestão de Vulnerabilidades de Aplicações WEB

4.4.1. A CONTRATADA deve prover uma plataforma no modelo (SaaS) para a gestão de vulnerabilidades de aplicações WEB e API da CONTRATANTE que utilize o conceito de testes dinâmicos (DAST);
4.4.2. A solução deve ser entregue no modelo SaaS no ambiente da fabricante da solução ofertada e com acesso através da internet em ambiente entregue pela contratada;
4.4.3. A plataforma deve suportar e estar licenciada conforme volumetria prevista na seção ESCOPO DE FORNECIMENTO desta especificação técnica.
4.4.4. A solução deve ser compatível com os Browsers: Google Chrome, Mozilla Firefox, Mozilla Firefox ESR e Microsoft Edge;
4.4.5. Para administração a plataforma deve implementar RBAC (Role-Based Access Control);
4.4.6. No conceito de RBAC a plataforma deve possuir minimamente os niveis de acesso:
4.4.6.1. Administrador;
4.4.6.2. Visualização e Alteração;
4.4.6.3. Visualização;
4.4.7. A plataforma deve possuir minimamente as seguintes roles:
4.4.7.1. Dono da Aplicação;
4.4.7.2. Gerenciador de Varreduras ou Scans;
4.4.7.3. Remediação;
4.4.8. A plataforma de permitir a criação e administração baseado em grupos;

4.4.9. No contexto de autenticação local na plataforma SaaS, a solução deve possuir mecanismos para customizar e permitir que as credenciais sigam um padrão elevado de criação, rotação e modificação;
4.4.10. Suportar Single Sign-On para autenticação ao portal de administração da solução;
4.4.11. A solução deve suportar autenticação via Single Sign-On minimamente para as plataformas:
4.4.11.1. Azure;
4.4.11.2. Active Directory Federation Services (AD FS);
4.4.11.3. Okta;
4.4.11.4. Duo;
4.4.11.5. Google;
4.4.12. Suportar nativamente Multiplo Fator de Autenticação para login na plataforma;
4.4.13. Possuir disponível para utilização minimamente as opções de MFA:
4.4.13.1. OKTA;
4.4.13.2. Google Authenticator;
4.4.13.3. SMS Authentication;
4.4.14. Possuir auditoria de todos logins realizados na plataforma;
4.4.15. Disponibilizar configuração nativa para expiração de sessões autenticadas para cada usuário;

Requisitos Técnicos

4.4.16. Suportar nativamente varredura em aplicações desenvolvidas nas mais variadas e recentes linguagens;
4.4.17. Possuir biblioteca com no mínimo 70 tipos de ataques Web e melhores práticas;
4.4.18. Disponibilizar pelo menos um scanner em Cloud SaaS do fabricante da solução para realização dos testes de vulnerabilidades WEB;
4.4.19. Disponibilizar scanners locais sem custos adicionais;
4.4.20. Possuir funcionalidade que permita que o desenvolvedor valide as vulnerabilidades diretamente de relatórios gerados pela solução, sem a necessidade de ele possuir um usuário na plataforma;
4.4.21. A solução deve possuir configuração para notificações de e-mails nos seguintes casos:
4.4.21.1. Falha de Scan;
4.4.21.2. Scan aguardando autenticação;
4.4.21.3. Scanner local está offline;
4.4.22. Para apoio no processo de SDLC (Software Development Life Cycle) da contratante a solução deve possuir nativamente integrações com as plataformas:
4.4.22.1. Jenkins;
4.4.22.2. Azure DevOps;
4.4.22.3. Bamboo;
4.4.22.4. Github;
4.4.22.5. GitLab;
4.4.23. A solução proposta deve habilitar varreduras dinâmicas profundas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem;
4.4.24. A solução deverá ser capaz de executar varreduras em sistemas web através de seus endereços FQDN / URL;
4.4.25. Capacidade de identificação de links em aplicações WEB e de navegação pelos links identificados;
4.4.26. A solução deve permitir varreduras autenticadas, complexas e progressivas;
4.4.27. Detectar uma alta gama de ataques e dentro desta gama atender integralmente a lista abaixo:

4.4.27.1. Blind SQL Injection;
4.4.27.2. Browser Cache Directive (Leaking sensitive information);
4.4.27.3. Brute Force;
4.4.27.4. Command Injection;
4.4.27.5. Credentials Stored in Clear Text in a Cookie (Password exposure);
4.4.27.6. Cross-Site Request Forgery (CSRF);
4.4.27.7. Cross-Site Scripting (XSS, DOM-Based Reflected via AJAX Request);
4.4.27.8. Cross-Site Scripting (XSS, DOM-Based);
4.4.27.9. File Inclusion;
4.4.27.10. LDAP Injection;
4.4.27.11. Out of Band Cross-Site Scripting (XSS);
4.4.27.12. Parameter Fuzzing;
4.4.27.13. PHP Code Execution;
4.4.27.14. Reflection;
4.4.27.15. Reverse Clickjacking;
4.4.27.16. SQL Injection;
4.4.27.17. URL Rewriting;
4.4.27.18. XPath Injection;
4.4.27.19. XML External Entity Attack;
4.4.27.20. Server Side Include (SSI) Injection.
4.4.28. A solução deve suportar a capacidade de retestar uma vulnerabilidade específica que foi detectada anteriormente na aplicação web;
4.4.29. A solução deve gerar tags para facilitar a localização;
4.4.30. A solução deve permitir definir a hora exata de início e duração das verificações.
4.4.31. Deve suportar varreduras simultâneas de aplicações web.
4.4.32. Deve possuir modelos (templates) prontos de varreduras e ser possível a criação de modelos customizados;
4.4.33. Deverá também permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
4.4.34. Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;
4.4.35. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
4.4.36. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
4.4.37. Deve ser capaz de instituir no mínimo os seguintes limites:
4.4.38. Número máximo de URLs para crawl e navegação;
4.4.39. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal;
4.4.40. Deve ser capaz de enviar notificações sobre a varredura através de e-mail;
4.4.41. Deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;
4.4.42. Deverá avaliar sistemas web utilizando frameworks modernos, como AJAX, HTML5 e SPA;
4.4.43. Deverá ser compatível com avaliação de RESTful APIs, utilizando o padrão OpenAPI (Swagger);
4.4.44. Deverá suportar no mínimo os seguintes esquemas de autenticação:
4.4.44.1. Autenticação básica (digest);
4.4.44.2. Form de login;
4.4.44.3. Autenticação de Cookies;

4.4.44.4. Autenticação através de Selenium;

4.4.45. Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário;

4.4.46. Deve ser capaz de exibir os resultados das varreduras em dashboard dedicados para este tipo de análise;

4.4.47. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

4.4.48. Para cada vulnerabilidade encontrada, deve ser exibido evidências dela em seus detalhes;

4.4.49. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:

4.4.49.1. Payload injetado;

4.4.49.2. Evidência em forma de resposta da aplicação;

4.4.49.3. Detalhes da requisição HTTP;

4.4.49.4. Detalhes da resposta HTTP;

4.4.50. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

4.4.51. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

4.4.52. A solução deverá possuir nativamente scanners pré-configurados em nuvem, para realização de scans externos. Estes scanners deverão obrigatoriamente possuir IP dedicado, com divulgação pública, para configuração de listas de permissões em Firewalls, WAFs, ou outros sistemas de proteção.

4.4.53. Possuir a funcionalidade de status para todas as vulnerabilidades identificadas através da plataforma nas aplicações WEB com no mínimo os seguintes status:

4.4.53.1. Sem Visualização;

4.4.53.2. Novo;

4.4.53.3. Ignorada;

4.4.53.4. Falso-Positivo;

4.4.53.5. Verificada;

4.4.53.6. Corrigida;

4.4.53.7. Duplicada;

4.4.54. A solução deve possuir ao menos duas formas de medir a severidade de uma vulnerabilidade e neste caso uma das formas deve ser o CVSS 3.1 e a outra forma deve ser gerada pelo fabricante da solução através do seu conhecimento para uma possível exploração da vulnerabilidade em questão;

4.4.55. Possuir nativamente integração com ferramentas de ticket para exportação das vulnerabilidades descobertas, neste caso as integrações necessárias são:

4.4.55.1. Jira;

4.4.55.2. ServiceNow;

Dashboards, Relatórios e API

4.4.56. A solução deve possibilitar o monitoramento dos dados através de Dashboards interativos;

4.4.57. Deve ser entregue junto com a solução dashboards nativos para que a contratante desde o início obtenha visibilidade das vulnerabilidades detectadas;

4.4.58. Os dashboards devem ser customizáveis e permitir a adição de outras informações geradas pela plataforma;

4.4.59. Deve-se possibilitar realizar filtros dentro dos dashboards com o intuito de separar as informações visualizadas;

4.4.60. A solução deve fornecer relatórios resumidos e de varredura do site que podem ser exportados, no mínimo, para os formatos HTML e PDF.

4.4.61. A solução deve possuir ao menos os seguintes tipos de relatórios:

4.4.61.1. Relatório Executivo para uma aplicação;

4.4.61.2. Relatório Executivo para todas as aplicações;

4.4.61.3. Relatório de vulnerabilidades sumarizado;

4.4.61.4. Relatório de vulnerabilidades com suas mitigações;

4.4.61.5. Relatório OWASP TOP 10 API Security Risks - 2023;

4.4.61.6. Relatório OWASP 2021;

4.4.61.7. Relatório Payment Card Industry (PCI);

4.4.61.8. Relatório GDPR;

4.4.61.9. Relatório SOX;

4.4.62. A solução deve possuir API aberta para automação mínima das seguintes funcionalidades:

4.4.62.1. Visualização de aplicações individuais e seus respectivos scans;

4.4.62.2. Visualização das vulnerabilidades descobertas em um scan específico;

4.4.62.3. Acionar e gerenciar um scan;

4.4.62.4. Criar novas aplicações dentro da plataforma;

4.4.62.5. Criar novas configurações de scan;

4.4.62.6. Cancelar um scan;

4.4.62.7. Apagar um scan cancelado.

4.4.63. A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do item sem necessidade de prévia consulta e/ou qualquer liberação por parte da empresa licitante.

4.4.64. A abertura de chamados poderá ser realizada através de Telefone ou através de endereço de e-mail do Fabricante.

4.5. Solução de Monitoramento de Deep & Dark Web

4.5.1. A solução deve suportar e estar licenciada conforme volumetria prevista na seção ESCOPO DE FORNECIMENTO desta especificação técnica, e pode ser composta por soluções de fabricantes distintos.

4.5.2. A solução deve ser capaz de realizar buscas, no mínimo, nos seguintes ambientes:

4.5.2.1. Na Darknet;

4.5.2.2. Em plataformas de compartilhamento de documentos;

4.5.2.3. Pelas seguintes categorias: Paste sites, incluindo histórico, Darknet: Tor and I2P, Wikileaks & Cryptome, Government sites of North Korea and Russia, Data Leaks, Whois Data, Dumpster, Public Web;

4.5.2.4. Por Site Público: .com, .org, .net, .info, .eu;

4.5.2.5. Por Geolocalização Regiões: China, Rússia, Américas, África, Coreia do Norte e Europa.

4.5.3. A solução deve permitir a busca de termos considerando, no mínimo, as seguintes categorias:

4.5.3.1. Email address;

4.5.3.2. Domínios, como *.example.com;

4.5.3.3. Marcas;

4.5.3.4. URL;

4.5.3.5. IP, CIDR. Both IPv4 and IPv6 are fully supported;

4.5.3.6. Phone Number;
4.5.3.7. Bitcoin address;
4.5.3.8. Ethereum address;
4.5.3.9. MAC address;
4.5.3.10. IPFS Hash;
4.5.3.11. Credit Card Number;
4.5.3.12. Social Security Number;
4.5.3.13. IBAN (International Bank Account Number);
4.5.3.14. Simhash;

4.5.4. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados de pelo período mínimo de 1 ano.

4.5.5. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:

4.5.5.1. Com base nos seguintes tipos de documentos: PDF, imagem, Word e Excel;
4.5.5.2. Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);
4.5.5.3. Com base nos domínios, e-mails e URLs encontrados;
4.5.5.4. Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;
4.5.5.5. Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.

4.5.6. A solução de monitoramento de Deep/Dark Web deve implementar amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web, incluindo:

4.5.6.1. Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;
4.5.6.2. Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;
4.5.6.3. Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;
4.5.6.4. Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC's;
4.5.6.5. Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.

4.5.7. As investigações deverão ser realizadas por uma equipe especializada à medida que informações monitoradas forem identificadas na Deep/Dark Web.

4.5.8. A solução deve gerar alertas, acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.

4.5.9. A solução deve ter recursos para visualização gráfica das descobertas, permitindo a sua filtragem por, no mínimo, data source e data type.

4.5.10. A solução deve permitir visualizar com segurança o conteúdo das descobertas de darknet para, no mínimo, arquivos PDF e imagens.

5. REQUISITOS TÉCNICOS GERAIS DOS SERVIÇOS

5.1. Fornecimento e Ativação das Soluções Ofertadas

5.1.1. Todos os componentes das soluções ofertadas, softwares, subscrições e eventuais equipamentos necessários ao seu funcionamento, devem ser fornecidos e estar operacionais para a CONTRATANTE em, no máximo, 30 (TRINTA) dias contados a partir da data de ASSINATURA DO CONTRATO.

5.1.2. A implantação, configuração, ativação e atualização das soluções e seus componentes será de responsabilidade da CONTRATADA, bem como as despesas diretas ou indiretas para a execução das atividades pela sua equipe técnica.

5.1.3. Os processos de implantação, configuração e ativação das soluções deverão ser realizados por técnicos capacitados da CONTRATADA, supervisionados por servidores do CONTRATANTE, conforme requisitos desta especificação técnica.

5.1.4. Os processos de sustentação das soluções deverão ser realizados durante toda a vigência do contrato por técnicos capacitados da CONTRATADA, supervisionados por servidores do CONTRATANTE, conforme requisitos desta especificação técnica.

5.2. Implantação, Ativação e Transição dos Serviços

5.2.1. A CONTRATADA deverá realizar o planejamento, implantação e ativação dos serviços ofertados em, no máximo, 30 (TRINTA) dias contados a partir da data de ASSINATURA DO CONTRATO.

5.2.2. A CONTRATADA deverá apresentar o PLANO DE PROJETO abrangendo, no mínimo, as seguintes atividades:

Planejamento

5.2.2.1. *Kick-off do Projeto:*

5.2.2.1.1. Reunião inicial com stakeholders.

5.2.2.1.2. Definição de objetivos, escopo e entregáveis.

5.2.2.2. *Levantamento de Requisitos e Diagnóstico:*

5.2.2.2.1. Avaliação do ambiente atual de TI e de segurança.

5.2.2.2.2. Identificação de gaps e priorização de serviços.

5.2.2.3. *Plano de Gerenciamento do Projeto:*

5.2.2.3.1. Definição de apresentação de cronograma detalhado de implantação, ativação e transição.

5.2.2.3.2. Alocação de recursos e soluções ofertadas.

5.2.2.3.3. Análise de riscos e estratégias de mitigação.

5.2.2.3.4. Estratégias de implantação e transição.

5.2.2.4. *Plano de Comunicação e Governança:*

5.2.2.4.1. Estabelecimento de canais de comunicação.

5.2.2.4.2. Definição de papéis e responsabilidades.

Implantação

5.2.2.5. *Configuração de Infraestrutura e Ferramentas:*

5.2.2.5.1. Preparação de infraestrutura e requisitos.

5.2.2.5.2. *Ativação e Configuração de Soluções Ofertadas:*

5.2.2.5.2.1. Monitoramento, Detecção, Investigação, Notificação e Resposta a Ataques Cibernéticos (SIEM/SOAR).

5.2.2.5.2.2. Gestão de Vulnerabilidades de Segurança da Informação.

5.2.2.5.2.3. Monitoramento de Deep/Dark Web.

5.2.2.5.2.4. Soluções complementares, se aplicável.

5.2.2.6. Integração com Ambiente da CONTRATANTE:

5.2.2.6.1. Integração das soluções de segurança ao ambiente existente.

5.2.2.6.2. Configuração de APIs, soluções e dashboards de monitoramento.

5.2.2.7. Testes de Integração:

5.2.2.7.1. Testes de integração e desempenho.

5.2.2.7.2. Ajustes iniciais e validação técnica.

5.2.2.7.3. Homologação pela CONTRATANTE.

5.2.2.8. Implantação e Ativação do SOC/MDR e Monitoramento:

5.2.2.8.1. Instalação e configuração de coletores.

5.2.2.8.2. Configuração de regras de detecção de ameaças, correlação e notificação.

5.2.2.8.3. Ativação de dashboards de monitoramento.

5.2.2.9. Implantação e Ativação dos Serviços de Gestão de Vulnerabilidades:

5.2.2.9.1. Instalação e configuração de agentes.

5.2.2.9.2. Configuração de regras e políticas de gestão de vulnerabilidades e conformidade.

5.2.2.9.3. Execução de varredura inicial.

5.2.2.9.4. Priorização e planejamento de correções.

5.2.2.10. Implantação e Ativação dos Serviços de Resposta a Incidentes:

5.2.2.10.1. Planejamento dos processos de resposta a incidentes.

5.2.2.10.2. Integração dos processos de resposta a incidentes aos processos da CONTRATANTE.

5.2.2.10.3. Homologação dos processos de resposta a incidentes.

5.2.2.11. Implantação e Ativação dos Serviços de Segurança Ofensiva:

5.2.2.11.1. Execução dos testes e elaboração de relatórios, conforme cronograma estabelecido.

5.2.2.12. Monitoramento de Deep e Dark Web:

5.2.2.12.1. Ativação e configuração do monitoramento de Deep e Dark Web.

5.2.2.12.2. Relatórios iniciais com ameaças identificadas.

5.2.2.13. Validação Final e Aceite:

5.2.2.13.1. Reunião de validação com a CONTRATANTE.

5.2.2.13.2. Testes finais e aceitação formal das soluções pela CONTRATANTE.

5.2.2.14. Documentação:

5.2.2.14.1. Manuais operacionais e técnicos.

5.2.2.14.2. Relatórios de configuração, testes e segurança ofensiva.

Transição e Sustentação

5.2.2.15. Handoff da sustentação das soluções de segurança da CONTRATANTE para a equipe da CONTRATADA:

5.2.2.16. Prestação dos serviços e sustentação das soluções ofertadas pela CONTRATADA:

5.2.2.16.1. Serviços de SOC/MDR.

5.2.2.16.2. Serviços de Resposta a Incidentes de Segurança da Informação.

5.2.2.16.3. Serviços de Gestão de Vulnerabilidades de Segurança da Informação.

5.2.2.16.4. Serviços de Monitoramento de Deep e Dark Web.

5.2.2.17. Apuração de SLAs e demais atividades de suporte e apoio necessárias ao pleno atendimento dos requisitos desta especificação técnica.

5.2.3. A CONTRATADA deverá realizar, após o término das fases de planejamento, implantação e ativação dos serviços e soluções ofertados, o treinamento e a transferência de conhecimento para equipe técnica da CONTRATANTE, com carga horária mínima de 16 horas sobre cada solução ofertada.

5.3. Acordo de Nível de Serviços (SLA)

5.3.1. Denomina-se acordo de nível de serviço ou SLA (Service Level Agreement), para efeito do presente contrato, o nível de desempenho técnico do serviço prestado proposto pela CONTRATADA, sendo certo que tal acordo não representa diminuição de responsabilidade da CONTRATADA, mas sim indicador de excelência técnica.

5.3.2. Os serviços deverão ser prestados em estrita observância das condições de Acordo do Nível de Serviços (SLA) descrito nas tabelas a seguir, arcando a CONTRATADA, em caso de descumprimento, com as penalidades dispostas:

Indicador	Cálculo	Indicador	Medição	Multa
Soluções				
Disponibilidade da Solução de Monitoramento, Detecção, Investigação, Notificação e Resposta a Ataques Cibernéticos	Tempo médio de disponibilidade das soluções	99,9% de disponibilidade	Mensal	5% valor da parcela mensal
Disponibilidade da Solução de Gestão de Vulnerabilidades de Servidores e Estações de Trabalho	Tempo médio de disponibilidade das soluções	99,9% de disponibilidade	Mensal	5% valor da parcela mensal
Disponibilidade da Solução de Monitoramento de Deep & Dark Web	Tempo médio de disponibilidade das soluções	99,9% de disponibilidade	Mensal	5% valor da parcela mensal
Serviços de SOC/MDR, Resposta a Incidentes de Segurança da Informação e Serviços de Monitoramento de Deep & Dark Web				
Tempo de Resposta a Incidentes (TTR)	TTR (Time to Respond): Tempo para iniciar a resposta após a detecção de um incidente	98% das respostas realizados em até 1 hora	Mensal	2,5% do valor da parcela mensal

Tempo de Atendimento – Severidade Baixa	Tempo médio de atendimento aos chamados de severidade baixa	90% dos atendimentos realizados em até 24 horas	Mensal	1% valor da parcela mensal
Tempo de Atendimento – Severidade Média	Tempo médio de atendimento aos chamados de severidade média	90% dos atendimentos realizados em até 8 horas	Mensal	1% valor da parcela mensal
Tempo de Atendimento – Severidade Alta	Tempo médio de atendimento aos chamados de severidade alta	90% dos atendimentos realizados em até 1 hora	Mensal	2,5% valor da parcela mensal
Serviços de Gestão de Vulnerabilidades de Segurança da Informação				
Gestão de Vulnerabilidades	Percentual de agentes que se reportam on-line na console da solução e no período de medição e que possuem patches aplicados	90% dos patches críticos aplicados ou mitigados	Mensal	1% valor da parcela mensal
Atualização de Patches	Percentual de agentes que se reportam on-line na console da solução e no período de medição e que possuem patches aplicados	90% dos patches críticos aplicados ou mitigados	Mensal	1% valor da parcela mensal
Relatórios de Medição de SLA				
Relatório Mensal de Medição de SLA	Envio de relatório evidenciando os indicadores de performance, com detalhamento da composição, até o 5º (quinto) dia útil do mês subsequente, para análise da CONTRATANTE	Relatório Mensal Enviado até o 5º (quinto) dia útil do mês	Mensal	2,5% valor da parcela mensal

5.3.3. Para os cálculos de disponibilidade das soluções, serão descontadas manutenções programadas, períodos de indisponibilidade causados por fatores externos a solução e não decorrentes de falhas de operação da contratada.

5.3.4. As seguintes definições serão adotadas para medição dos níveis de serviço especificados:

5.3.4.1. Tempos de Resposta e Tempo de Atendimento: tem o objetivo de medir os prazos de atendimento referente a solicitação de chamados, seja requisição ou incidente, com base no tipo de severidade do atendimento, conforme a tabela seguinte:

SEVERIDADE	TEMPO DE RESPOSTA	TEMPO DE ATENDIMENTO
ALTA	15 minutos	1 hora
MÉDIA	2 horas	8 horas
BAIXA	4 horas	24 horas

5.3.4.2. Os prazos serão contabilizados a partir do registro das requisições. Esses prazos podem ser suspensos em situações que dependam de algum fator externo de responsabilidade da CONTRATANTE ou outro fornecedor.

5.3.5. O cálculo de severidade baseia-se na relação entre Impacto e Urgência.

5.3.5.1. Impacto refere-se à abrangência do ocorrido, ou quantas pessoas estão sendo afetadas.

5.3.5.2. Urgência relaciona-se a velocidade em que o serviço precisa ser restaurado.

5.3.6. O IMPACTO classifica-se em:

5.3.6.1. Alto: Impacta um site inteiro ou todos os usuários;

5.3.6.2. Médio: Impacta uma equipe inteira ou um pequeno grupo de usuários;

5.3.6.3. Baixo: afeta um único usuário ou um número desconhecido de usuários.

5.3.7. A URGÊNCIA classifica-se em:

5.3.7.1. Alto: Precisa ser restaurado imediatamente, pois impede que uma função ou serviço principal do negócio seja executado;

5.3.7.2. Médio: Pode ser restaurado em uma janela de tempo maior que a de urgência alta, pois restringe a eficácia de uma função ou serviço;

5.3.7.3. Baixo: Pode ser restaurado de maneira planejada pois possui impacto menor nas tarefas do dia a dia.

5.3.8. O cruzamento dessas duas variáveis provê a severidade conforme a tabela a seguir:

MATRIZ DE SEVERIDADES		**URGÊNCIA**		
		ALTO	**MÉDIO**	**BAIXO**
IMPACTO	**ALTO**	ALTA	ALTA	MÉDIA
	MÉDIO	ALTA	MÉDIA	BAIXA
	BAIXO	MÉDIA	BAIXA	BAIXA

5.3.9. Caso o SLA não seja atingido, mensalmente, a CONTRATANTE aplicará as multas descritas na tabela de SLA desta especificação, considerando o percentual cumulativo máximo de 20% sobre valor fixo mensal.

5.3.10. A CONTRATADA deverá enviar relatório evidenciando os indicadores de performance, com detalhamento da composição, até o 5º (quinto) dia útil do mês subsequente, para análise da CONTRATANTE, e respectivo pagamento da fatura mensal.

5.3.11. Para efeito de ajustes e adaptações da CONTRATADA aos níveis de serviço exigidos, as penalidades previstas quando do não cumprimento dos prazos de atendimento não serão aplicadas nos primeiros 30 (trinta) dias de contrato.

5.3.12. A incidência recorrente de violação deste acordo de nível de serviços, por 6 (seis) meses consecutivos ou alternados em um intervalo de 12 (doze) meses de contrato, e onde haja a incidência de multa superior a 5% da parcela mensal nos referidos meses, poderá ensejar o cancelamento unilateral do contrato por parte da CONTRATANTE.

6. IMPEDIMENTO DE CONTRATAÇÃO DA MESMA EMPRESA PARA DATACENTER E SOC

Com o objetivo de preservar a integridade das operações, assegurar a transparência na prestação dos serviços e garantir a conformidade com as melhores práticas de

governança e compliance, a empresa proponente poderá participar de ambos os lotes. Contudo, será permitida a celebração de contrato com apenas um dos lotes, ficando vedada a contratação da mesma empresa para os Lotes 1 e 2 desta licitação, sendo eles:

Lote 1: Serviços de Datacenter (**DATACENTER, NOC (NETWORK OPERATIONS CENTER), SUPORTE ESPECIALIZADO E BACKUP**)
Lote 2: Serviços de Segurança da Informação (**SOC/MDR, GESTÃO DE VULNERABILIDADES E RESPOSTA A INCIDENTES**).

Apesar de haver, em tese, vantagens operacionais na concentração dos serviços em uma única empresa, a sobreposição de responsabilidades entre os dois lotes representa um risco relevante de conflito de interesses, especialmente sob a ótica da segurança da informação. A empresa contratada para o serviço de Datacenter será responsável por hospedar os dados e os sistemas críticos da instituição, enquanto a empresa contratada para o serviço de SOC terá a função de monitorar, identificar e alertar sobre incidentes de segurança que possam ocorrer nesses ambientes.

Permitir que a mesma empresa atue como provedora da infraestrutura e como fiscalizadora e respondente de incidentes dessa mesma infraestrutura compromete a imparcialidade e a independência do serviço de monitoramento e resposta. Em cenários de incidentes cibernéticos, como vazamentos de dados, falhas de configuração, acessos não autorizados ou outras não conformidades operacionais, pode haver omissão, retardo na comunicação ou mascaramento de eventos críticos, afetando a capacidade da instituição de reagir adequadamente.

Portanto, com base no princípio da segregação de funções, visando a redução de riscos operacionais e legais, a empresa vencedora do Lote 1 (Datacenter NOC (NETWORK OPERATIONS CENTER), SUPORTE ESPECIALIZADO E BACKUP) não poderá ser contratada para o Lote 2 (SOC /MDR, GESTÃO DE VULNERABILIDADES E RESPOSTA A INCIDENTES), ou vice-versa, ainda que atenda aos requisitos técnicos de ambos os lotes.

7. QUALIFICAÇÃO TÉCNICA

7.1. Da Contratada

7.1.1. A CONTRATADA deve apresentar, no momento da sua habilitação no processo licitatório, Atestado(s) de Capacidade Técnica (ACT) em seu favor e emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado ou estar prestando:

7.1.1.1. Fornecimento de serviços continuados de SOC, pelo prazo mínimo de 12 meses, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 700 (setecentos) ativos;

7.1.1.2. Fornecimento de serviços continuados de Gestão de Vulnerabilidades de Segurança da Informação, pelo prazo mínimo de 12 meses, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 700 (setecentos) ativos;

7.1.1.3. Fornecimento de serviços continuados de Deep e Dark Web, pelo prazo mínimo de 12 meses, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 700 (setecentos) ativos;

7.1.1.4. Fornecimento e instalação de solução de solução de monitoramento, detecção, investigação, notificação e resposta a ataques cibernéticos, similar a proposta para atendimento a esta especificação técnica, para ambiente compatível ao da CONTRATANTE, contendo no mínimo 700 (setecentos) ativos;

7.1.1.5. Fornecimento e instalação de solução de gestão de vulnerabilidades de servidores e estações de trabalho, similar a proposta para atendimento a esta especificação técnica, para ambiente compatível ao da CONTRATANTE, contendo no mínimo 700 (setecentos) ativos;

7.1.1.6. Fornecimento e instalação de gestão de vulnerabilidades de Aplicações WEB, similar a proposta para atendimento a esta especificação técnica, para ambiente compatível ao da CONTRATANTE, contendo no mínimo 01 (um) FQDN;

7.1.1.7. Fornecimento de serviços continuados de Resposta a Incidentes Cibernéticos, pelo prazo mínimo de 12 meses, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 700 (setecentos) ativos;

7.1.2. O proponente deve apresentar, no momento da sua habilitação no processo licitatório, planilha de comprovação de atendimento aos itens da especificação técnica devidamente preenchida, conforme Anexo II – Comprovação de atendimento aos itens da Especificação Técnica, onde deverá constar a forma de atendimento a cada um dos itens mencionados no documento.

7.1.3. O proponente deve INDICAR através de GRIFOS, CANETA MARCA TEXTO etc. em sua DOCUMENTAÇÃO TÉCNICA das soluções ofertadas (folhetos técnicos, datasheet, manuais, documentos do fabricante, DATASHEETS) a comprovação dos principais requisitos técnicos exigidos no edital. DEVERÁ ser entregue JUNTAMENTE com a PROPOSTA COMERCIAL.

7.2. Do Quadro Profissional da Contratada

7.2.1. A CONTRATADA deve apresentar, no ato da assinatura do contrato, a certificação da sua equipe técnica, comprovando a sua qualificação para implantação, sustentação e operação dos serviços e soluções propostas:

7.2.2. 01 (um) profissional certificado PMP – Project Management Professional, Prince2 Practitioner Certificate in Project Management ou Professional SCRUM Master;

7.2.3. 01 (um) profissional certificado pelo fabricante da solução de monitoramento, detecção, investigação, notificação e resposta a ataques cibernéticos;

7.2.4. 01 (um) profissional certificado pelo fabricante da solução de gestão de vulnerabilidades de servidores e estações de trabalho;

7.2.5. 01 (um) ou mais profissionais que detenham individualmente ou em conjunto, pelo menos, 04 das seguintes certificações de segurança:

7.2.5.1. GCIH – GIAC Certified Incident Handler

7.2.5.2. GCIA – GIAC Certified Intrusion Analyst

7.2.5.3. GCFA – GIAC Certified Forensic Analyst
7.2.5.4. GMON – GIAC Continuous Monitoring Certification
7.2.5.5. GCDA – GIAC Certified Detection Analyst
7.2.5.6. CompTIA CySA+ (Cybersecurity Analyst)
7.2.5.7. CompTIA Security+
7.2.5.8. Cisco CyberOps Associate
7.2.5.9. Microsoft SC-200 (Security Operations Analyst)
7.2.5.10. Offensive Security Web Expert (OSWE);
7.2.5.11. Certified Red Team Expert (CRTE);
7.2.5.12. ISO/IEC 27035 Lead Incident Manager (PECB)
7.2.5.13. Offensive Security Certified Expert (OSCE);
7.2.5.14. Certified Ethical Hacker (CEH).
7.2.5.15. CISM (Certified Information Security Manager)

7.2.6. Deverá ser comprovado vínculo entre os profissionais detentores dos certificados e a CONTRATADA, através de cópia do livro de registro de funcionários ou cópia da carteira de trabalho contendo as respectivas anotações de contrato de trabalho; ou como contratado, por meio de contrato de prestação de serviços.

7.2.7. A CONTRATADA deverá promover, no prazo máximo de 3 (três) meses, a atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido a modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

7.2.8. Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas.

7.2.9. A CONTRATANTE se reserva ao direito de realizar auditorias a qualquer tempo para verificar se as competências mínimas solicitadas são atendidas pela CONTRATADA durante toda a vigência do contrato. Desta forma, quando solicitado, a CONTRATADA deverá apresentar os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas.

7.3. Do Fabricante

7.3.1. Licenças e subscrições

Todas as licenças e subscrições necessárias para o pleno funcionamento da solução deverão ser fornecidas pela CONTRATADA, conforme as quantidades e faixas discriminadas nesta especificação.

8. PAGAMENTO SOB MEDIÇÃO

8.1. Relatórios de Medição e documentação de atividades realizadas

8.1.1. O pagamento à CONTRATADA será efetuado sob o **regime de medição**, com base nos quantitativos efetivamente **demandados pela CONTRATANTE e executados pela CONTRATADA** e nos critérios previamente estabelecidos na planilha de preços contratual. A liberação dos valores estará condicionada à apresentação e validação do Relatório de Medição e documentação de atividades realizadas, elaborado pela contratada e atestado pela fiscalização designada pela contratante. Somente após a verificação da conformidade dos serviços prestados, com base nos parâmetros técnicos, quantitativos e qualitativos descritos no Termo de Referência e demais documentos contratuais, será autorizado o pagamento correspondente.

8.1.2. Para fins de validação e liberação do pagamento, a CONTRATADA deverá encaminhar no mínimo os seguintes documentos:

- Relatório de medição contendo a discriminação dos itens executados no período, acompanhada do respectivo cálculo monetário com base nos preços unitários dos quantitativos contratados.
- As atividades realizadas no período;
- Indicadores de desempenho (SLAs e métricas acordadas);
- Eventos e incidentes identificados e tratados;
- Evidências das ações de resposta e mitigação;
- Status do ambiente monitorado;
- Evolução da gestão de vulnerabilidades, riscos e segurança;
- Detalhamento das análises de logs e investigações conduzidas;
- Casos relevantes identificados em fontes de risco externas, como Deep & Dark Web.

8.1.3. A não apresentação do relatório mensal, ou a apresentação incompleta, poderá acarretar a suspensão do pagamento até a devida regularização.

9. PRAZOS

9.1. Prazo de Vigência do Contrato

12 (Doze) meses.

9.2. Prazo de Implantação, Ativação e Transição

A transição das operações dos serviços executados pelo CONTRATANTE para a CONTRATADA deverá estar concluída em no máximo 30 (TRINTA) dias, contados a partir da data de assinatura de contrato.

10. ANEXO I – SOLUÇÕES DE SEGURANÇA DA INFORMAÇÃO DA CONTRATANTE

ANEXO I – PARQUE COMPUTACIONAL DAS CONTRATANTES

CENÁRIO SENAC:

Servidores:

Ativo	Quantitativo
Servidores	14

Workstation:

Ativo	Quantitativo
Workstation	600

Switches:

Ativo	Quantitativo
Switches	66

Firewall:

Ativo	Modelo	Quantitativo
Firewall	Check Point	12
Firewall	Fortigate	2

Domínios de E-mails:

Domínios
es.senac.br
aluno.es.senac.br
edu.es.senac.br
Hotelilhadoboi.com.br

Marcas a serem monitoradas:

Marcas
Senac
Senac ES
Serviço Nacional de Aprendizagem Comercial
Inspira + ES

Considerar como fontes de eventos:

Fontes de Eventos	Quantitativo
Firewalls Check Point	12
Firewalls Fortinet	2
Clear Pass (NAC)	1
Active Directory	1
End point – Trend Micro	1
Syslog (Servidores)	1
Banco de Dados	2
Microsoft 365	1
Azure	1

CENÁRIO SESC:

Servidores:

Ativo	Quantitativo
Servidores	38

Workstation:

Ativo	Quantitativo
Workstation	800

Switches:

Ativo	Quantitativo

Switches	30

Firewall:

Ativo	Modelo	Quantitativo
Firewall	Fortigate	19

Domínios de E-mails:

Domínios
sesc-es.com.br

Marcas a serem monitoradas:

Marcas
Sesc
Sesc ES

Considerar como fontes de eventos:

Fontes de Eventos	Quantitativo
Firewall Fortigate	1
Active Directory	1
Endpoint - Kaspersky	1
Microsoft 365	1
Azure	1
(Switches)	1
Banco de Dados	2

11.ANEXO II - PROVA DE CONCEITO

A Prova de Conceito (PoC) **será realizada presencialmente,** com o objetivo de validar a eficácia da solução de monitoramento e resposta a incidentes proposta pelo fornecedor. A PoC deverá demonstrar a abrangência sobre todos os ativos críticos definidos pela CONTRATANTE, comprovando a capacidade da plataforma de detectar vulnerabilidades, correlacionar eventos e responder de forma ágil a ameaças cibernéticas.
Durante a PoC, deverão ser realizados testes controlados, incluindo a simulação de eventos de segurança como acessos não autorizados e tráfego malicioso, para validar a coleta e correlação de logs em tempo real, cobertura dos ativos e detalhamento dos alertas gerados. Será exigida a apresentação de relatórios técnicos ao final de cada etapa, contendo:

- Gaps técnicos identificados e recomendações de melhoria;
- Precisão na detecção de vulnerabilidades e análise comparativa entre métodos;
- Eficácia e tempo médio de resposta a incidentes (MTTD/MTTR);
- Avaliação da integração com ferramentas e processos já existentes;
- Confiabilidade na correlação de eventos oriundos de múltiplas fontes.

A PoC também deverá demonstrar a capacidade de resposta automatizada ou assistida, o funcionamento da gestão de vulnerabilidades com detecção de falhas reais, e a precisão das correlações de eventos. A solução

deve ser capaz de priorizar riscos, emitir alertas eficazes e sustentar o monitoramento contínuo com visibilidade completa.
Ao término da PoC, será apresentado um relatório conclusivo contendo as métricas de desempenho, cobertura e recomendação técnica quanto à viabilidade da solução para o ambiente SENAC/SESC. Em caso de identificação de falhas, as recomendações para ajuste deverão estar devidamente documentadas para análise antes da decisão final de contratação.

12. ANEXO III – COMPROVAÇÃO DE ATENDIMENTO AOS ITENS DA ESPECIFICAÇÃO TÉCNICA

12.1 INDICAR através de GRIFOS, CANETA MARCA TEXTO etc. em sua DOCUMENTAÇÃO TÉCNICA do equipamento ofertado (folhetos técnicos, datasheet, manuais, documentos do fabricante, DATASHEETS) a comprovação dos principais requisitos técnicos exigidos no edital. DEVERÁ ser entregue JUNTAMENTE com a PROPOSTA COMERCIAL.

Acordo de confindencialidade

A *<Nome da Empresa>,* sediada em *<Endereço Completo>,* inscrita no CNPJ sob o n°*<Numero do CNPJ>,* doravante denominada **CONTRATADA**.

Declara por meio de tal ato que as atividades objeto da presente contratação encontram-se em conformidade com a legislação de proteção de dados pessoais, incluída, mas não limitada à Lei Geral de Proteção de Dados Pessoais (LGPD), e que em seu escopo compromete-se a:

Garantir as medidas de segurança técnicas e administrativas, inclusive referentes à confidencialidade, aptas à proteção dos dados pessoais objeto da presente contratação em suas atividades e nas de seus eventuais subcontratados;

- Fornecer à SESC e SENAC, sempre que solicitado, informações ou documentos necessários ao atendimento de direitos de titulares de dados, no prazo de 3 (três) dias úteis, bem como efetuar alterações ou exclusões de dados sempre que orientado pelo SESC e/ou SENAC, em função de solicitação dos titulares de dados;
- Comunicar à SESC e SENAC eventual ocorrência de incidente de segurança e/ou de privacidade que envolva os dados objeto na presente contratação, no prazo de 24 (vinte e quatro) horas de sua ciência e cooperar de forma coordenada com o SESC e SENAC, previamente a quaisquer comunicações oficiais;

- Indenizar O SESC e SENAC em caso de dano decorrente do descumprimento da legislação de proteção de dados, por quaisquer perdas, danos, obrigações, responsabilidades, custos e despesas, incluindo honorários advocatícios, custas judiciais, juros e multas em que O SESC e SENAC tenham incorrido.

O Fornecedor ainda, declara estar ciente que:

(i) Dados pessoais são considerados qualquer informação que possa levar à individualização de uma pessoa, seja de maneira direta ou indireta. Inclui: dados cadastrais, hábitos, preferências, histórico de consumo, dados bancários e financeiros, logs e registros eletrônicos, geolocalização, IP etc. (ii) Titular é a pessoa física a qual se referem os dados pessoais.

- Tratamento é considerado qualquer atividade praticada com dados pessoais. Inclui: acesso, coleta, visualização, compartilhamento, exclusão, armazenamento etc.
- Controlador dos dados é a pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais (parte que decide "como" e "por que" tratar os dados em uma relação contratual).
- Co-Controlador dos dados é a pessoa natural ou jurídica terceira a quem também competem (ainda que parcialmente) parte das decisões referentes ao tratamento de dados pessoais (parte que decide "como" e "por que" tratar os dados em uma relação contratual).
- Operador dos dados é a pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (parte que apenas executa uma atividade de tratamento de dados requisitada pela outra).

Esta Declaração LGPD deverá ser aprovada exclusivamente pelo(s) representante(s) legal(is) do Fornecedor de acordo com os poderes estabelecidos em seu Contrato Social, Estatuto Social, atas de assembleia/eleição e procurações outorgadas.

Vitória, XX de XXXXXXX de 20XX.

_____

<Representante Legal>

<Cargo><Contrata>

13. ANEXO IV - TERMO DE COMPROMISSO DE MANUTENÇÃO, SIGILO E SEGURANÇA

O Serviço Social do Comércio, localizado na Av./Rua XXXXXXXXXXXXXXXXXXXXXX, 99999 - Centro – Vitória - 29999999999, doravante denominado SESC/SENAC; resolve deixar o presente TERMO DE COMPROMISSO, DE MANUTENÇÃO DE SIGILO E SEGURANÇA, doravante **DECLARAÇÃO,** com as seguintes cláusulas e condições:

Considerando:

- Que em razão do presente **Termo de Referência**, doravante denominado **TERMO,** a CONTRATADA poderá ter acesso a informações sensíveis ou sigilosas da **SESC/SENAC**;

- A necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;
- E cumprir todas as Normas de Segurança da Informação vigentes na **SESC/SENAC**;

DO OBJETO:

Constitui objeto desta **DECLARAÇÃO** o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela **CONTRATADA**, no que diz respeito ao trato de informações sensíveis, documentos e materiais sigilosos, disponibilizadas pela SESC/SENAC, por força dos procedimentos necessários para a execução do objeto do presente **TERMO.**

DAS RESPONSABILIDADES:

A *<Nome da Empresa>,* sediada em *<Endereço Completo>,* inscrita no CNPJ sob o n°*<Numero do CNPJ>,* doravante denominada **CONTRATADA**.

clara para os devidos fins, que por ter acesso e utilizar as informações cedidas pela **SESC/SENAC,** estas serão restritas à execução do **TERMO**, não revelando, copiando, transmitindo, reproduzindo, transportando, alterando ou dando conhecimento a terceiros, bem como não permitindo que qualquer empregado envolvido direta ou indiretamente na execução do **TERMO**, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso indevido de informações sensíveis ou sigilosas ou efetue qualquer procedimento que não se enquadre nas Políticas, Normas ou Procedimentos de Segurança da Informação, vigentes na **SESC/SENAC**;

As restrições impostas por esta **DECLARAÇÃO** não se aplicam a INFORMAÇÕES que sejam comprovadamente de domínio público e/ou tenham sido comprovada e legitimamente recebidas de terceiros e/ou sejam reveladas em razão de requisição judicial ou outra determinação válida do Município ou Estado, somente até a extensão de tais ordens.

DAS PUNIÇÕES:

A **INTERESSADA** poderá responder civil e criminalmente pela quebra do Sigilo das informações sensíveis ou sigilosas da **SESC/SENAC**, ainda que por omissão, sem prejuízo das sanções administrativas previstas no Resolução SESC nº 1.593/2024 e SENAC Nº 1.270/2024, apuradas em regular processo administrativo ou judicial.

Vitória, XX de XXXXXXX de 20XX.

_____

<Representante Legal>

<Cargo><Contrata>

14. ANEXO V - TERMO DE ACORDO DE SIGILO, CONFIDENCIALIDADE E PRIVACIDADE DE DADOS - LGPD

Este acordo de confidencialidade complementa o contrato, XXXX, realizado entre SESC/SENAC e XXXX., e regula a manutenção da confidencialidade das informações internas e dos dados pessoais obtidos no âmbito do contrato acordo com as condições que se seguem:

1. O presente Contrato tem por objeto a Contratação de XXXX.

2. As presentes determinações se aplicam a todos os procedimentos em que há compartilhamento de documentos pessoais do SESC/SENAC, assumindo-se o conhecimento e o compromisso de manter a segurança das informações e dos dados disponibilizados pela entidade.

3. Nesse sentido, este Acordo de Sigilo, Confidencialidade e Privacidade de Dados discorre, de maneira clara e acessível, como as informações e dados devem ser coletados; utilizados; compartilhados; armazenados e descartados.

4. A aceitação do mencionado Acordo ocorre, automaticamente, a partir do momento em que a Parte/Terceiros acessam e/ou utilizam os documentos e informações disponibilizados pelo SESC/SENAC. Esse mecanismo assegura que os usuários estão cientes e em total concordância com a forma de utilização e de compartilhamento das nossas informações e dados.

5. Assim, no Acordo de Sigilo, Confidencialidade e Privacidade de Dados do SESC/SENAC, destacam-se os seguintes compromissos a serem respeitados pelas Partes e/ou terceiros:

(i) Finalidade: este Acordo tem o condão de especificar que a utilização dos dados pessoais enviados deverá se limitar à finalidade precípua para a qual foi solicitado, bem como evitar a utilização não autorizada de informações pessoais e confidenciais compartilhadas durante as fases de (a) Tratativas Contratuais Preliminares, (b) Propostas, (c) Pré-Contratos e Contratos, conforme o art. 7º, inciso V, da Lei 13.709/2018.

(ii) Uso Restrito: as informações confidenciais enviadas pelo SESC/SENAC deverão ser utilizadas apenas para analisar o desenvolvimento do objeto deste Acordo.

(ii.a) Definição de Informações Confidenciais: são consideradas informações confidenciais todos os dados pessoais dos representantes legais do SESC/SENAC e de outros agentes envolvidos no processo contratual.

(iii) Titularidade das Informações: os documentos contendo informações confidenciais são de propriedade da Parte Fornecedora. A Parte Receptora não adquire direitos sobre esses documentos, salvo acordo expresso e por escrito.

(iv) Proteção de Dados: as Partes se comprometem a respeitar a privacidade e proteção dos dados pessoais conforme a Lei 13.709/2018, de forma resguardar e manter em sigilo todos os dados fornecidos, exceto quando obrigadas a revelá-los às autoridades públicas pelos seguintes motivos: (a) questões legais, (b) administrativas ou judiciais.

(v) Medidas de Segurança: as Partes adotarão medidas técnicas e administrativas de segurança apropriadas para proteger os dados pessoais compartilhados, no intuito de evitar o extravio, alteração, exclusão, acesso não autorizado ou qualquer outro uso indevido por indivíduos não autorizados.

(vi) Notificação de Violações: cada Parte notificará prontamente a outra sobre qualquer Violação de Dados Pessoais e fornecerá informações sobre o incidente. Além disso, também notificará quanto a ocorrência de ordens judiciais ou administrativas que exijam a revelação de informações confidenciais.

(vii) Prazo de Conservação dos Dados: os dados deverão ser conservados pelo tempo necessário para cumprir sua finalidade ou por até 2 (dois) anos, salvo exigências legais. Após o referido prazo, os dados deverão ser excluídos, deletados, destruídos ou devolvidos.

(viii) Consequências da Divulgação Indevida: a divulgação indevida de informações confidenciais causará danos irreparáveis, ensejando o direito de a Parte prejudicada pleitear, judicialmente, a execução de medidas cautelares e/ou a indenização por perdas e danos.

(ix) Direitos de Propriedade Intelectual: este Acordo não concede direitos de exploração de marcas, invenções, patentes, direitos autorais ou outros direitos de propriedade intelectual.

(x) Cumprimento das Leis Anticorrupção: as Partes declaram estar cientes e cumprir as Leis Anticorrupção Brasileiras ou outras leis anticorrupção aplicáveis, comprometendo-se a não violar essas disposições.

6. O respeito a este Acordo de Sigilo, Confidencialidade e Privacidade de Dados é imprescindível para a manutenção da segurança dos dados pessoais compartilhados durante as tratativas entre as Partes, assegurando o devido sigilo e a privacidade, em conformidade com a legislação vigente.

Esta obrigação se estende a todos Dados pessoais, dados sensíveis e demais informações da empresa, independentemente da forma em que existam e se são ou não expressamente designados como confidenciais.

Confirmo que estou ciente dos regulamentos de proteção de Dados pessoais relevantes e me comprometo a manter a confidencialidade das informações e dados e que esta obrigação de confidencialidade continuará a existir após o término da relação contratual.

_____

Responsável Legal pela empresa XXXX

Empresa XXXX