



## **APÊNDICE DO ANEXO I - ESTUDO TÉCNICO PRELIMINAR – IN SGD-ME nº 94/2022**

### **1 – Definição**

Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

O Estudo Técnico Preliminar tem por objetivo planejar a contratação de serviço de gerenciamento de segurança cibernética, com suporte técnico especializado e monitoramento (SOCaaS), incluindo o fornecimento das respectivas soluções de software (Kaspersky Next MXDR).

### **1.1 - Diretrizes Gerais para Elaboração dos Estudos Preliminares**

1.1.1 O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Formalização de Demanda - DFD, bem como demonstrar a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, em consonância com o art. 11 da Instrução Normativa SGD-ME nº 94/2022.

### **1.2 - Normativos que disciplinam os serviços a serem contratados**

1.2.1 Lei nº 14.133/2021 - Lei de Licitações e Contratos Administrativos.

Instrução Normativa SGD-ME n.º94, de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo.

1.2.2 Instrução Normativa SGD-ME n.º94, de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo.

### **2 - Das Necessidade de negócio e tecnologia**

Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

2.1 O Conselho Regional de Química IV Região (CRQ-IV/SP) necessita garantir a continuidade, disponibilidade e segurança de seus serviços digitais e dados institucionais.

2.2 O CRQ-IV/SP disponibiliza grande quantidade de serviços e volume de dados com documentos gerados pelos usuários do órgão, e-mails e sistemas internos.

2.3 A crescente sofisticação das ameaças cibernéticas exige mecanismos avançados de detecção e resposta a incidentes de segurança.



### **3.1 – Requisitos da contratação – Identificação das necessidades de negócio**

- 3.1.1 O CRQ-IV/SP necessita elevar seu nível de maturidade em segurança cibernética através do monitoramento contínuo, detecção proativa de ameaças e capacidade de resposta a incidentes. A complexidade crescente das ameaças exige uma operação especializada de um Centro de Operações de Segurança (SOC), capaz de identificar atividades anômalas, suspeitas ou maliciosas em tempo real e fornecer as diretrizes necessárias para contenção e remediação.
- 3.1.2 A adoção do modelo SOCaaS (SOC como Serviço) justifica-se pela necessidade de acesso imediato a tecnologias avançadas de SIEM/SOAR e a analistas de segurança especializados, sem os custos e o tempo associados à implementação de uma infraestrutura e equipe interna equivalentes.
- 3.1.3 Da padronização e compatibilidade com o parque tecnológico atual:
- 3.1.3.1 A indicação expressa da solução Kaspersky Next MXDR Optimum no presente estudo faz-se estritamente necessária e justificada pela pré-existência e plena operação desta plataforma no ambiente tecnológico deste Órgão. A substituição dessas soluções por tecnologias de outros acarretaria a quebra da padronização arquitetônica atual, exigindo complexos, onerosos e arriscados processos de migração de dados (políticas de segurança, histórico de telemetria e configurações de EndPoints).
- 3.1.4 Da Preservação do Conhecimento Técnico e Curva de Aprendizado:
- 3.1.4.1 O corpo funcional do Órgão, abrangendo tanto os usuários finais quanto a equipe técnica de Tecnologia da Informação (TI), já possui proficiência e conhecimento consolidado na operação, administração e sustentação desta ferramenta.
- 3.1.4.2 Impacto Operacional e de Governança (TI): Embora a operacionalização e o gerenciamento contínuo das plataformas sejam objeto da presente contratação (Serviços Gerenciados/SOC), a equipe de infraestrutura de TI do CRQ-IV/SP detém o conhecimento técnico e a proficiência essenciais para a governança, fiscalização e auditoria das soluções Kaspersky. A substituição destas tecnologias por ferramentas de terceiros invalidaria o conhecimento técnico já consolidado pela equipe do Órgão, resultando na perda imediata da capacidade de mensurar adequadamente os Acordos de Nível de Serviço (SLA), auditar as políticas de segurança (tuning) aplicadas pela contratada e avaliar a real eficácia das respostas a incidentes. A introdução de novas plataformas exigiria um longo período de capacitação apenas para que a equipe de TI recuperasse a aptidão técnica de gerir e fiscalizar o contrato com o rigor necessário, gerando uma perigosa lacuna de governança técnica e aumentando a exposição do CRQ-IV/SP a riscos cibernéticos durante esta curva de aprendizado.
- 3.1.5 A manutenção das plataformas atuais protege os investimentos pretéritos realizados pela Administração Pública em treinamentos, parametrizações e integrações de sistemas legados com estas soluções. Uma eventual troca de fabricante não traria apenas os custos diretos de novas licenças, mas também custos indiretos atrelados à migração de dados, perda de



produtividade temporária, riscos de indisponibilidade de serviços essenciais e necessidade de novas capacitações.

- 3.1.6 A especificação da marca Kaspersky atende ao interesse público, não configurando restrição indevida à competitividade, mas sim uma medida de padronização indispensável para garantir a continuidade, a segurança, a estabilidade e a economicidade das operações tecnológicas deste Órgão, encontrando amparo legal no art. 41, inciso I, alíneas "b" e "c", combinado com o art. 43, da Lei nº 14.133/2021.
- 3.1.7 O CRQ-IV/SP pretende contratar empresa para fornecimento da solução com prestação de serviços de gerenciamento, monitoração e suporte na área de infraestrutura de rede lógica e segurança da informação – 3º nível, com atendimento previsto em regime de 24 horas e 07 dias por semana.

### **3.2 – Comprovação da capacidade técnica**

#### **3.2.1 Qualificação Técnica:**

- 3.2.1.1 A licitante deverá comprovar sua qualificação técnica, por meio de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de mínimo 01 (um) atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.
- 3.2.1.2 Os atestados técnicos apresentados pela licitante deverão ser elaborados em papel timbrado, estarem devidamente assinados, com indicação do nome, cargo, e-mail e telefone do responsável pela declaração.
- 3.1.2.3 Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;
- 3.1.2.4 O licitante, quando solicitado pelo pregoeiro, disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MP n. 5/2017.

#### **3.2.2 Qualificação Técnico-Profissional**

- 3.2.2.1 A licitante deverá comprovar que possui credenciamento válido junto ao fabricante Kaspersky, na condição de revenda autorizada, parceira certificada ou canal oficial autorizado para comercialização, fornecimento, renovação de licenças, suporte e demais serviços relacionados às soluções ofertadas, devendo apresentar documentação comprobatória emitida pelo próprio fabricante ou por representante oficialmente autorizado no Brasil.



3.2.2.1.1 O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

3.2.2.2 A licitante vencedora deverá comprovar que possui em seu quadro de funcionários, pelo menos 2 (dois) dois Profissionais Técnicos Certificados pelo fabricante das seguintes soluções Kaspersky conforme descrito abaixo.

3.2.2.2.1 Apresentar 02 (dois) ou mais certificado(s) da equipe técnica dos profissionais certificados como Certified Professional: Kaspersky EDR Optimum (047.12.6);

3.2.2.2.2 Apresentar 02 (dois) ou mais certificado(s) da equipe técnica dos profissionais certificados como Certified Professional: Kaspersky Next XDR Expert (048.1.1);

3.2.2.2.3 Apresentar 02 (dois) ou mais certificado(s) da equipe técnica dos profissionais certificados como Certified Professional: Kaspersky Automated Security Awareness Platform (080.03);

3.2.2.2.4 Apresentar 02 (dois) ou mais certificado(s) da equipe técnica dos profissionais certificados como Certified Professional: Kaspersky Secure Mail Gateway (036.2.1 ou superior);

3.2.2.3 A licitante vencedora, antes da assinatura do contrato, deverá comprovar o vínculo profissional do corpo técnico, por meio de apresentação do vínculo empregatício CLT ou contrato de prestação de serviço.

**Justificativa:** A comprovação de que a licitante é um distribuidor autorizado, tem o objetivo de minimizar riscos para a instituição, como por exemplo, risco de adquirir produtos em desacordo com as regras do fabricante, ou provenientes de descaminhos fiscais ou contrabandos, ou ainda, de licenças não destinadas para uso no território brasileiro.

#### **4 – Definição e justificativa da natureza continuada dos serviços:**

4.1 A contratação encontra-se alinhada com o Plano Anual de Contratações da Gerência de Tecnologia e Informação (GTI) – Item 02 e 05, planejamento estratégico institucional e diretrizes de segurança da informação. O objeto enquadra-se como contratação de solução de TIC conforme a Instrução Normativa SGD/ME nº 94/2022.

4.2 O objeto da contratação tem a natureza de serviço comum de caráter continuado, pois pode ser objetivamente especificado por meio de padrões usuais no mercado e características comuns pré-estabelecidas, além de ser fundamental para a execução das atividades finalísticas do CRQ-IV/SP de forma contínua, devendo ser contratado por meio de processo licitatório na modalidade pregão em sua forma eletrônica.



4.3 Os serviços serão prestados visando garantir a disponibilidade e o armazenamento seguro das informações controladas pelo CRQ-IV/SP.

4.4 O contrato terá vigência de 36 (trinta e seis) meses, podendo ser prorrogado caso a CONTRATANTE tenha interesse. No entanto, poderá ser reiniciado a qualquer momento durante a vigência mediante comunicado prévio de 60 dias à CONTRATADA.

## 5 – Estimativas das quantidades:

5.1 A solução deverá contemplar as quantidades estimadas descritas no quadro abaixo:

Item	Quant.	Unid.	Recorrência	Descrição
1	250	Serviço	Mensal sob demanda	Licenças Next MXDR Optimum (SaaS), podendo chegar a 499 licenças
2	250	Serviço	Mensal sob demanda	Gerenciamento Continuoado (SOCaaS) para solução Kaspersky Next MXDR Optimum, compatível com o número de licenças contratadas.
3	1	Serviço	Única	Instalação e configuração do ambiente Kaspersky Next MXDR Optimum

5.2 A plataforma deve contemplar capacidades avançadas de proteção de EndPoints, detecção estendida de ameaças, resposta automatizada a incidentes e integração de telemetria de múltiplas fontes.

## 6 – Descrição da Solução:

Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

### 6.1 Objeto

Item	Quant.	Unid.	CATSER	DESCRIÇÃO
1	1	Serviço	26972	Prestação de serviço de gerenciamento de segurança cibernética, com suporte técnico especializado, monitoramento (SOCaaS), incluindo o fornecimento das respectivas soluções de software (Kaspersky Next MXDR).

### 6.2 Das quantidades e especificações técnicas dos produtos

Os serviços e seus quantitativos relacionados na tabela abaixo foram estimados considerando a infraestrutura de TIC atualmente no CRQ-IV/SP. Está previsto escalabilidade dos recursos visando garantir que os sistemas e recursos tecnológicos possam crescer ou diminuir conforme a demanda.



Item	Unid.	Descrição	Recorrência	Quant. Mínima	Quant. Máxima
1	Serviços	Licenças Next MXDR Optimum (SaaS)	Mensal sob demanda	150	499
2	Serviços	Gerenciamento Continuoado (SOCaaS) para solução Kaspersky Next MXDR Optimum	Mensal sob demanda	150	499
3	Serviços	Instalação e configuração do ambiente Kaspersky Next MXDR Optimum	Única	1	-

#### 6.2.1 – Quantidade inicial do contrato

Inicialmente o contratado terá as seguintes quantidades:

Item	Quant.	Unid.	Recorrência	Descrição
1	250	Serviço	Mensal sob demanda	Licenças Next MXDR Optimum (SaaS)
2	250	Serviço	Mensal sob demanda	Gerenciamento Continuoado (SOCaaS) para solução Kaspersky Next MXDR Optimum
3	1	Serviço	Única	Instalação e configuração do ambiente Kaspersky Next MXDR Optimum

#### 6.2.2 Do local e horário da prestação dos serviços

6.2.2.1 Os serviços especificados estarão restritos, para atendimento à sede O CRQ-IV/SP (Rua Oscar Freire, 2039, bairro de Pinheiros, São Paulo - SP, CEP 05409-011). Para o atendimento on-site na cidade São Paulo - SP, não deverá haver cobrança sobre gastos com deslocamento, hospedagem e alimentação.

6.2.1.2 Os serviços deverão ser prestados em regime de 24 x 7 x 365, ou seja, poderá ocorrer de segunda a domingo, 24 horas por dia.

#### 6.2.3 Do prazo de instalação das licenças

6.2.3.1 A contratada deverá disponibilizar e entregar todas as licenças Kaspersky MXDR no prazo máximo de até 10 (dez) dias corridos, contados a partir da assinatura do contrato, devidamente ativadas e aptas para utilização pela contratante, incluindo, quando aplicável, os respectivos códigos de ativação, acesso ao portal do fabricante e documentação pertinente.

#### 6.3 Descrição dos Serviços

6.3.1 Disponibilização de licenças Kaspersky Next MXDR Optimum.

6.3.2 Prestação de serviços gerenciados de segurança (SOC 24x7x365).

6.3.3 Monitoramento contínuo, detecção e resposta a incidentes de segurança.

6.3.4. Suporte técnico especializado.



**6.3.5 Faturamento Mensal Baseado em Consumo**

6.3.6 O faturamento dos serviços e licenças será realizado de forma postecipado, refletindo exclusivamente o quantitativo de licenças ativas e provisionadas durante o mês de referência.

**6.4 Hospedagem da Solução**

6.4.1 As licenças da solução deverão, obrigatoriamente, ser hospedadas e gerenciadas na plataforma em nuvem da própria fabricante, Kaspersky Security Center Cloud Console, não sendo admitidas implementações locais ou em infraestruturas de terceiros. Tal exigência visa garantir a gestão centralizada, atualização contínua, alta disponibilidade do serviço, bem como a plena integração com os recursos avançados de detecção e resposta (MXDR), assegurando conformidade com as melhores práticas de segurança da informação e com o modelo operacional da solução contratada.

**6.4.2 Elasticidade (Acréscimos e Supressões):**

6.4.2.1 É garantido ao CRQ-IV/SP o direito de solicitar a inclusão ou a redução de licenças e serviços a qualquer momento durante a vigência contratual.

6.4.2.2 As solicitações de ajuste de quantitativo deverão ser refletidas financeiramente na fatura do ciclo de cobrança subsequente (pró-rata), sem imposição de cotas mínimas de permanência.

**6.4.3 Ausência de Multa e Fidelidade:**

6.4.3.1 Fica expressamente vedada a cobrança de qualquer taxa de cancelamento, multa rescisória, penalidade ou imposição de aviso prévio superior a 30 (trinta) dias para o encerramento parcial ou total dos serviços.

**6.5 Serviço de Gerenciamento Continuado**

Este serviço tem como objetivo garantir a administração contínua, o monitoramento proativo de saúde (Health Check) do ambiente e a resposta a incidentes de segurança, atuando de forma complementar e integrada ao serviço de Managed Extended Detection and Response (MXDR) do Kaspersky NEXT.

**6.6 Gestão Proativa e Manutenção do Ambiente (Health Check)**

6.6.1 Monitoramento de Comunicação: Acompanhamento contínuo no Kaspersky Security Center (KSC) Cloud Console para garantir que os 300 agentes estejam online, atualizados e comunicando perfeitamente com a nuvem e com o SOC da Kaspersky.

6.6.2 Gestão de Atualizações: Homologação e aplicação de patches de segurança do Kaspersky EndPoint Security (KES) e do Network Agent.

6.6.3 Troubleshooting de EndPoints: Atuação remota em equipamentos que apresentem falha no agente de segurança, problemas de performance relacionados aos agentes ou perda de comunicação com a console.





#### 6.7 Triagem e Resposta a Incidentes (Integração com SOC Kaspersky)

6.7.1 Ponto de Contato Focal: Atuação como o principal canal técnico de comunicação entre o cliente e os analistas de segurança da Kaspersky.

6.7.2 Validação de Alertas: Análise contextual dos alertas gerados pelo Kaspersky MXDR. Enquanto a Kaspersky identifica e isola a ameaça (ex: bloqueio de um processo malicioso ou isolamento de rede do EndPoint), nossa equipe valida o impacto operacional daquele bloqueio nas atividades da empresa.

6.7.3 Remediação de Campo: Execução de ações que estão fora do alcance do SOC da Kaspersky, como: reingresso de máquinas na rede após desinfecção, auxílio na contenção de sistemas afetados por credenciais comprometidas, análise de causa raiz após eventos de contaminação.

#### 6.8 Gestão de Políticas e Ajustes Finos (Tuning)

6.8.1 Gestão de Falsos Positivos: Criação de regras de exclusão (whitelisting) para aplicações internas, sistemas legados ou ERPs da empresa que possam ser erroneamente classificados pelo comportamento anômalo.

6.8.2 Controles de Segurança (Device e Web Control): Atualização e manutenção contínua das regras de bloqueio de USBs, controle de navegação web e controle de aplicações, conforme as solicitações de mudança do negócio.

6.8.3 Hardening Contínuo: Revisão periódica das políticas do EPP/EDR para garantir que as configurações acompanhem as melhores práticas da indústria e as recomendações técnicas da própria Kaspersky.

#### 6.9 Estrutura de Atendimento e Suporte Técnico

6.9.1 A operação deste contrato será sustentada pelo centro de operações da Contratada, contando com equipe de analistas especializados.

6.9.2 A estrutura deve permitir escalonamento eficiente das demandas, absorvendo desde requisições simples de desbloqueio até análises complexas de comportamento de malware, respeitando os Acordos de Nível de Serviço (SLA) estabelecidos.

#### 6.10 Entregáveis e Reportes Periódicos

Para garantir total visibilidade do ambiente e comprovar o valor do serviço prestado, deverá ser entregue:

6.10.1 Relatório Executivo Mensal: Documento consolidado com a volumetria de ameaças bloqueadas, incidentes críticos tratados pelo MXDR, taxa de conformidade dos EndPoints (máquinas desatualizadas ou sem proteção) e tempo médio de resposta.





6.10.2 Reunião de Alinhamento (Mensal): Apresentação do relatório para a diretoria/gerência do cliente, discutindo melhorias de postura de segurança, recomendações de infraestrutura e esclarecimento de dúvidas sobre incidentes do período.

6.10.3 Alertas Críticos Imediatos: Comunicação proativa (via telefone e e-mail) para os gestores ou analistas do CRQ-IV/SP sempre que um incidente de severidade "Crítica" for detectado e contido pelo MXDR, informando as ações já tomadas e os próximos passos.

#### 6.11 Dos serviços de monitoração, gerenciamento e suporte

6.11.1 A CONTRATADA deverá fornecer, de forma integrada ao licenciamento, serviços especializados. A prestação de serviços deverá contemplar a administração contínua e a sustentação técnica integral do ecossistema contratado, englobando:

6.11.2. Administração, Monitoração e Sustentação da Solução Kaspersky Next MXDR Optimum:

6.11.2.1 A CONTRATADA deverá prover a gestão integral da plataforma de segurança, bem como a prestação contínua dos serviços gerenciados de detecção e resposta estendida (MXDR), contemplando obrigatoriamente:

6.11.2.2 Administração e Gerenciamento da Plataforma (Sustentação Tecnológica):

6.11.2.2.1 Implantação e Manutenção de Agentes: Instalação, atualização e monitoramento do status de integridade dos agentes de EndPoint (EPP/EDR) em toda a base da CONTRATANTE, garantindo a cobertura total do parque computacional.

6.11.2.2.2 Gestão de Políticas e Tuning: Criação, aplicação e refinamento contínuo de políticas de segurança (tuning de falsos positivos), gestão de exceções, controle de aplicativos (Application Control), controle de dispositivos (Device Control) e controle web.

6.11.2.2.3 Gestão de Vulnerabilidades e Patch Management: Configuração e monitoramento das rotinas de varredura de vulnerabilidades, bem como a aplicação automatizada e gerenciada de atualizações de software (patches) para mitigação de riscos em sistemas operacionais e aplicativos de terceiros suportado pela plataforma.

6.11.2.2.4 Administração da Console Cloud: Gestão de acessos baseada em função (RBAC) na console de administração, provisionamento de novos tenants (se aplicável) e garantia de compliance com as diretrizes de segurança do CRQ-IV/SP.



#### 6.11.2.3 Serviços Gerenciados de Monitoração e MXDR (SOC 24x7x365):

6.11.2.3.1 Monitoramento Contínuo: Operação de Centro de Operações de Segurança (SOC) com cobertura 24 horas por dia, 7 dias por semana, para monitoramento em tempo real da telemetria gerada pelos EndPoints, rede e integrações em nuvem.

6.11.2.3.2 Detecção e Correlação de Eventos: Análise profunda de incidentes apoiada por inteligência de ameaças (Threat Intelligence) do fabricante, utilizando o framework MITRE ATT&CK para mapeamento de táticas, técnicas e procedimentos (TTPs) de adversários.

6.11.2.3.3 Busca Ativa de Ameaças (Threat Hunting): Execução de rotinas proativas (manuais e automatizadas) para identificar ameaças furtivas ou persistentes (APTs) que tenham contornado as barreiras tradicionais de proteção, utilizando indicadores de comprometimento (IoCs) e indicadores de ataque (IoAs).

#### 6.11.2.4 Resposta a Incidentes e Mitigação:

6.11.2.4.1 Triagem e Análise de Causa Raiz (RCA): Investigação detalhada dos alertas críticos para determinar a origem, o vetor de ataque e o escopo do comprometimento (Root Cause Analysis).

6.11.2.4.2 Ações de Contenção e Erradicação: Execução remota de ações de resposta rápida, incluindo, mas não se limitando a: isolamento de hosts comprometidos da rede corporativa, quarentena ou exclusão de arquivos maliciosos, encerramento de processos suspeitos e bloqueio de comunicações de rede (C&C).

6.11.2.4.3 Orientação de Remediação: Fornecimento de diretrizes claras e apoio técnico especializado à equipe de infraestrutura do CRQ-IV/SP para a recuperação e higienização dos ativos afetados.

6.11.2.4.4 Os serviços gerenciados devem prever a entrega de relatórios executivos e técnicos periódicos (mensais), consolidando o cenário de ameaças bloqueadas, incidentes mitigados, tempo médio de resposta (MTTR) e recomendações de melhoria na postura de segurança.

#### 6.12 O serviço de monitoração deverá possuir os seguintes recursos técnicos:

6.12.1 Geração de alertas automatizados por sistema avançado que possua recursos de inteligência através de sensores de gatilho que tomam ações baseadas em informações coletadas no monitoramento com abertura de tickets no sistema de Service Desk da CONTRATADA;



**6.13 Envio dos alertas de forma automatizada através de:**

6.13.1 Mensagens de Whatsapp;

6.13.2 Mensagens de e-mail;

6.13.3 Ligações telefônicas automatizadas por robô e personalizadas ao CRQ-IV/SP;

**6.14 Para o atendimento e abertura de tickets de solicitação de serviços, a CONTRATADA deverá fornecer:**

6.14.1 Acesso ao portal de gerenciamento dos tickets abertos para consulta e interação do time de TI do CRQ-IV/SP com o time de sustentação da CONTRATADA;

6.14.1.1 Atendimento prioritário para os alertas críticos;

6.14.1.2 Dashboard local em telas para o time de TI do CRQ-IV/SP.

6.14.2 VISITAS TÉCNICAS CORRETIVAS: Serão realizadas sob demanda do CRQ-IV/SP sempre que forem verificados problemas que necessitem de atendimento no local. São caracterizadas pelo deslocamento de um técnico da CONTRATADA para as instalações do CRQ-IV/SP para levantamento e aplicação de ações corretivas necessárias à solução de problemas e eventos críticos. Este atendimento deverá ocorrer no prazo máximo de 4 (quatro) horas a contar da abertura do chamado. O atendimento referido será realizado sem qualquer custo ou ônus adicional à CONTRATANTE.

6.14.3 REUNIÕES DE APRESENTAÇÃO DE “STATUS REPORT”: A CONTRATADA deverá apresentar documentação mensal de STATUS REPORT contendo todos os indicadores de atendimento sobre os serviços deste contrato para análise e indicação de plano de melhoria constante contendo:

6.14.3.1 Alertas de erros e alertas críticos;

6.14.3.2 Demandas de atendimento in-loco;

6.14.3.3 Gráfico de acompanhamento de backlog dos tickets;

6.14.3.4 Relatório executivo sobre os serviços de SOCaaS (MXDR).

**6.15 Metodologia de Operação do SOC e Processamento de Alertas.**

6.15.1 A CONTRATADA deverá seguir a seguinte metodologia operacional:

6.15.1.1 Os eventos dos dispositivos do CRQ-IV/SP deverão ser enviados como telemetria para a plataforma MXDR ou gerenciada pela CONTRATADA.



6.15.1.2 A plataforma MXDR deverá utilizar automação para identificar atividades anômalas ou maliciosas, gerando incidentes de segurança para processamento pelos analistas do SOC.

6.15.2.3 Os analistas do SOC deverão, além do monitoramento automatizado, realizar investigações manuais (threat hunting) para prover escrutínio adicional sobre atividades potencialmente maliciosas ou anômalas que não possam ser automatizadas.

6.15.2.4 Descobertas provenientes do "threat hunting" deverão iniciar um incidente de segurança manual.

6.15.2.5 Cada evento de segurança processado pelo SOC deverá ser investigado para identificar sua autenticidade, cronologia (timeline) e severidade.

6.15.2.6 Ao concluir a investigação, o analista deverá classificar o evento e tomar as ações apropriadas conforme a classificação.

#### 6.16 Classificação de Incidentes e Procedimentos de Notificação.

6.16.1 A CONTRATADA deverá classificar os incidentes em três níveis (Menor, Maior, Crítico) e seguir os respectivos procedimentos de notificação:

##### 6.16.1.1 Classificação Menor:

6.16.1.1.1 Definição: Atividades anormais identificadas no EndPoint que não correspondem à expectativa de atividade típica, possuindo alta classificação de 'falso positivo', mas consideradas informativas para o CRQ-IV/SP.

6.16.1.1.2 Notificação: O CRQ-IV/SP deverá ser contatado por e-mail, com o detalhamento da investigação.

6.16.1.1.3 Responsabilidade: A CONTRATADA será responsável por investigar, responder e remediar o alerta.

##### 6.16.1.2 Classificação Maior:

6.16.1.2.1 Definição: Confiança de atividade suspeita ou maliciosa da qual o CRQ-IV/SP deve estar ciente. A atividade não demonstra evidência de um comprometimento, mas notificação e investigação adicional pelo CRQ-IV/SP são recomendadas.

6.16.1.2.2 Notificação: O CRQ-IV/SP deverá ser contatada por e-mail, com o detalhamento da investigação.



6.16.1.2.3 Responsabilidade: A CONTRATADA será responsável por investigar, responder e remediar o alerta.

**6.16.1.3 Classificação Crítica:**

6.16.1.3.1 Definição: Alta confiança de que um comprometimento está ocorrendo dentro do ambiente do CRQ-IV/SP.

6.16.1.3.2 Notificação (Telefone): O CRQ-IV/SP deverá ser notificado por telefone para detalhar a investigação, os passos de resposta tomados e discutir os próximos passos.

6.16.1.3.3 SLA de Notificação (Telefone): O Analista da CONTRATADA deverá realizar quatro (4) tentativas de chamada para o(s) número(s) de contato de emergência na primeira hora. Após a hora inicial, o Analista deverá continuar a ligar uma vez por hora até que o contato seja estabelecido. Todas as tentativas de chamada deverão ser anotadas e retransmitidas no ticket.

6.16.1.3.4 Notificação (E-mail): O CRQ-IV/SP também receberá uma notificação por e-mail detalhando a investigação e os passos de resposta tomados.

6.16.1.3.5 Responsabilidade: A CONTRATADA será responsável por investigar, responder e remediar o alerta.

**6.17 Definição do gerenciamento e proteção MXDR para os endpoints**

6.17.1 Definem-se os termos: ENDPOINT como “dispositivos computacionais (servidores e estações de trabalho, e mobile)”, MXDR como “sistema de detecção e resposta para os dispositivos ENDPOINT com os agentes MXDR instalados” e SOCaaS como “central de operações de segurança gerenciado remotamente pela CONTRATADA em parceria com o fabricante das soluções MXDR”;

6.17.2 A CONTRATADA será responsável pelo fornecimento das licenças e solução de serviços de proteção para EndPoints com MXDR gerenciados como SOCaaS para: 250 dispositivos em formato de serviços completo, podendo chegar a 499 dispositivos (conforme demanda do órgão).

6.17.3 A solução MXDR fornecida deverá possuir as seguintes especificações técnicas:

**a. Do módulo de proteção de EndPoint**

a.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

- a.1.1. Windows 7
- a.1.2. Windows 8
- a.1.3. Windows 8.1
- a.1.4. Windows 10



- a.1.5. Windows 11
- a.2. Servidores
  - a.2.1. Windows Small Business Server 2011
  - a.2.2. Windows MultiPoint Server 2011
  - a.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019, 2022 e 2025
- a.3. Servidores de terminal Microsoft
  - a.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
- a.4. Sistemas operacionais Linux de 32 bits:
  - a.4.1. CentOS 6.7 e posterior
  - a.4.2. Debian GNU/Linux 11.0 e posterior
  - a.4.3. Debian GNU/Linux 12.0 e posterior
  - a.4.4. Red Hat Enterprise Linux 6.7 e posterior
- a.5. Sistemas operacionais Linux de 64 bits:
  - a.5.1. Amazon Linux 2.
  - a.5.2. CentOS 6.7 e mais tarde
  - a.5.3. CentOS 7.2 e posterior.
  - a.5.4. CentOS Stream 8.
  - a.5.5. CentOS Stream 9.
  - a.5.6. Debian GNU/Linux 11.0 e posterior.
  - a.5.7. Debian GNU/Linux 12.0 e posterior.
  - a.5.8. Linux Mint 20.3 e superior.
  - a.5.9. Linux Mint 21.1 e posterior.
  - a.5.10. openSUSE Leap 15.0 e posterior.
  - a.5.11. Oracle Linux 7.3 e posterior.
  - a.5.12. Oracle Linux 8.0 e posterior.
  - a.5.13. Oracle Linux 9.0 e posterior.
  - a.5.14. Red Hat Enterprise Linux 6.7 e posterior
  - a.5.15. Red Hat Enterprise Linux 7.2 e posterior.
  - a.5.16. Red Hat Enterprise Linux 8.0 e posterior.
  - a.5.17. Red Hat Enterprise Linux 9.0 e posterior.
  - a.5.18. Rocky Linux 8.5 e posterior.
  - a.5.19. Rocky Linux 9.1.
  - a.5.20. SUSE Linux Enterprise Server 12.5 ou posterior.
  - a.5.21. SUSE Linux Enterprise Server 15 ou posterior.
  - a.5.22. Ubuntu 20.04 LTS.
  - a.5.23. Ubuntu 22.04 LTS.
  - a.5.24. 9.5 Sistemas operacionais Arm de 64 bits:
  - a.5.25. CentOS Stream 9.
  - a.5.26. SUSE Linux Enterprise Server 15.
  - a.5.27. Ubuntu 22.04 LTS.



- a.6. Sistemas operacionais MAC OS:
  - a.6.1. MacOS 12 – 14
- a.7. Ferramentas de virtualização MAC OS:
  - a.7.1. Parallels Desktop 16 para Mac Business Edition ou superior
  - a.7.2. VMware Fusion 11.5 Professional ou superior
- a.8. A solução proposta deverá suportar as seguintes plataformas virtuais:
  - a.8.1. VMware Workstation
  - a.8.2. VMware ESXi
  - a.8.3. Microsoft Hyper-V Server
  - a.8.4. Citrix Virtual Apps e Desktop
  - a.8.5. Citrix Provisioning
- b. Do módulo de gerenciamento avançado
  - b.1. A solução proposta deve suportar arquitetura cloud-native e on-premise;
  - b.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
    - b.2.1. Amazon Web Services
    - b.2.2. Microsoft Azure
    - b.2.3. Google Cloud
  - b.3. A solução proposta deve incluir as seguintes opções de integração SIEM:
    - b.3.1. HP (Microfoco) ArcSight
    - b.3.2. IBM QRadar
    - b.3.3. Splunk
    - b.3.4. Kaspersky KUMA
  - b.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed EndPoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
  - b.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;
  - b.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
  - b.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
  - b.8. O módulo da solução on-premise deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.





- b.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
- b.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.
- b.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
- b.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.
- b.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
- b.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em único/múltiplos dispositivos com base nas seguintes regras de ativação:
  - b.14.1. Status do dispositivo
  - b.14.2. Tag
  - b.14.3. Diretório ativo
  - b.14.4. Proprietários de dispositivos
  - b.14.5. Hardware
- b.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:
  - b.15.1. E-mail
  - b.15.2. Registro de sistema
  - b.15.3. SMS
- b.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
  - b.16.1. Atributos de rede
  - b.16.2. Nome
  - b.16.3. Domínio e/ou Sufixo de Domínio
  - b.16.4. Endereço de IP
  - b.16.5. Endereço IP para servidor de gerenciamento
  - b.16.6. Localização no Active Directory
  - b.16.7. Unidade organizacional
  - b.16.8. Grupo
  - b.16.9. Sistema operacional
  - b.16.10. Número do pacote de serviço
  - b.16.11. Arquitetura Virtual
  - b.16.12. Registro de aplicativos



- b.16.13. Nome da Aplicação
- b.16.14. Versão do aplicativo
- b.16.15. Fabricante
- b.16.16. Tipo e versão
- b.16.17. Arquitetura
  
- b.17. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.
  
- b.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o EndPoint conectado pela internet/rede pública.
  
- b.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
  - b.19.1. Dispositivos Desktop/Servidores
  - b.19.2. Dispositivos móveis
  - b.19.3. Dispositivos de rede
  - b.19.4. Dispositivos virtuais
  - b.19.5. Componentes OEM
  - b.19.6. Periféricos de computador
  - b.19.7. Dispositivos IoT conectados
  - b.19.8. Telefones VoIP
  - b.19.9. Repositórios de rede
  
- b.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
  - b.20.1. Nome da Aplicação
  - b.20.2. Caminho do aplicativo
  - b.20.3. Metadados do aplicativo
  - b.20.4. Aplicativo Certificado digital
  - b.20.5. Categorias de aplicativos predefinidas pelo fornecedor
  - b.20.6. SHA256 e MD5
  
- b.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
  - b.21.1. Bluetooth
  - b.21.2. Dispositivos móveis
  - b.21.3. Modems externos
  - b.21.4. CD/DVD
  - b.21.5. Câmeras e scanners
  - b.21.6. MTPs
  - b.21.7. E a transferência de dados para dispositivos móveis



**SERVIÇO PÚBLICO FEDERAL**

CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO

**RUA OSCAR FREIRE, 2039 – PINHEIROS – 05409-011 – SÃO PAULO/SP**

[WWW.CRQSP.ORG.BR](http://WWW.CRQSP.ORG.BR)

- b.22.A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
- b.23.A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao EndPoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.
- b.24.A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
  - b.24.1. Estruturas de domínios e grupos de trabalho do Windows
  - b.24.2. Estruturas de grupos do Active Directory
  - b.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador
- b.25.A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.
- b.26.A solução proposta deve permitir realizar as seguintes ações para EndPoints:
  - b.26.1. Verificação manual;
  - b.26.2. Verificação no acesso;
  - b.26.3. Verificação por demanda;
  - b.26.4. Verificação de arquivos compactados
  - b.26.5. Verificação de arquivos individuais, pastas e unidades;
  - b.26.6. Bloqueio e verificação de scripts
  - b.26.7. Proteção contra alteração de registros;
  - b.26.8. Proteção contra estouro de buffer;
  - b.26.9. Verificação em segundo plano/inativa
- b.27.Verificação de unidade removível na conexão com o sistema;
- b.28.A solução proposta deve suportar a instalação do sensor de EndPoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
- b.29.O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
- b.30.A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.



- b.31.A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat etc.
- b.32.A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
- b.33.A solução proposta deve suportar Windows Failover Cluster.
- b.34.A solução proposta deve ter um recurso de clustering integrado.
- b.35.A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
- b.36.A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
- b.37.O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
- b.38.A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
- b.39.A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
- b.40.A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
- b.41.A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
- b.42.A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
- b.43.A solução proposta deverá possuir controles para download de DLL e drivers.
- b.44.A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão.



**SERVIÇO PÚBLICO FEDERAL**

CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO

**RUA OSCAR FREIRE, 2039 – PINHEIROS – 05409-011 – SÃO PAULO/SP**

[WWW.CRQSP.ORG.BR](http://WWW.CRQSP.ORG.BR)

- b.45.A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
- b.46.A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
- b.47.A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
- b.48.A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
- b.49.A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
- b.50.A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
- b.51.A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
- b.52.A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
- b.53.A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
- b.54.A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
- b.55.A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.



**SERVIÇO PÚBLICO FEDERAL**

CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO

**RUA OSCAR FREIRE, 2039 – PINHEIROS – 05409-011 – SÃO PAULO/SP**

[WWW.CRQSP.ORG.BR](http://WWW.CRQSP.ORG.BR)

- b.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
- b.57. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de EndPoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal.
- b.58. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento etc.
- b.59. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
- b.60. A solução proposta deve permitir ao administrador personalizar relatórios.
- b.61. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
- b.62. A solução proposta deve permitir ao administrador definir um período após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
- b.63. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de EndPoint no servidor de gerenciamento.
- b.64. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de EndPoint personalizadas/de terceiros ao servidor de gerenciamento.
- b.65. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos EndPoint, sem exigir acesso físico.
- b.66. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.



- b.67.O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de EndPoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
- b.68.O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
- b.69.A solução proposta deve suportar integração com solução APT.
- b.70.A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
- b.71.A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
- b.71.1. Linux
- b.72. A solução proposta deverá suportar os seguintes servidores de banco de dados:
- b.72.1. Linux:
- |           |            |
|-----------|------------|
| b.72.1.1. | MySQL      |
| b.72.1.2. | MariaDB    |
| b.72.1.3. | PostgreSQL |
- b.73. A solução proposta deverá suportar as seguintes plataformas virtuais:
- b.73.1. Linux:
- |           |   |
|-----------|---|
| b.73.1.1. | VMware vSphere 6.7 e 7.0                      |
| b.73.1.2. | VMware Desktop 16 Pro e 17 Pro                |
| b.73.1.3. | Servidor Microsoft Hyper-V 2012 de 64 bits    |
| b.73.1.4. | Servidor Microsoft Hyper-V 2012 R2 de 64 bits |
| b.73.1.5. | Microsoft Servidor Hyper -V 2016 de 64 bits   |
| b.73.1.6. | Servidor Microsoft Hyper-V 2019 de 64 bits    |
| b.73.1.7. | Servidor Microsoft Hyper-V 2022 de 64 bits    |
| b.73.1.8. | Citrix XenServer 7.1 e 8.x                    |
| b.73.1.9. | Oracle VM VirtualBox 6.x e 7.x                |
- b.74.A solução proposta deve suportar criptografia em vários níveis:
- b.74.1. Criptografia completa do disco – incluindo disco do sistema
- b.74.2. Criptografia de arquivos e pastas
- b.74.3. Criptografia de mídia removível
- b.74.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2
- b.75.A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
- b.75.1. A criptografia de arquivos em unidades de computador locais.





- b.75.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
- b.75.3. A criação de listas criptografadas de pastas em unidades de computador locais.
- b.76. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
  - b.76.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
  - b.76.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
- b.77. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
  - b.77.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
  - b.77.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
- b.78. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia.
- b.79. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.
- b.80. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.
- b.81. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
- b.82. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual



o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

- b.83.A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.
- b.84. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.
- b.85.A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.
- b.86.A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.
- b.87.A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.
- b.88.A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.
- b.89.A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.
- b.90.A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
- b.91.O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.
- b.92.A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
- b.93.A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
- b.94.A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:



- b.94.1. Uso do Trusted Platform Module e configurações de senha.
- b.94.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
- b.95. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
- b.96. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
- b.97. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
  - b.97.1. Instalação remota de software de terceiros
  - b.97.2. Relatórios sobre software e hardware existentes
  - b.97.3. Monitoramento para instalação de software não autorizado
  - b.97.4. Remoção de software não autorizado
- b.98. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
- b.99. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para EndPoints.
- b.100. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os EndPoints, com base em sua criticidade.
- b.101. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
- b.102. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre EndPoints e status de implantação de patches.
- b.103. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
- b.104. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
- b.105. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança.
- b.106. A solução proposta deve permitir ao administrador aprovar atualizações.



- b.107. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em EndPoints individuais e enviar apenas os que são necessários/ausentes.
- b.108. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
- b.109. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
- b.110. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
- b.111. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
- b.112. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
- b.113. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
- b.114. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
- b.115. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'.
- b.116. A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade".
- b.117. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
- b.118. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
- b.119. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
- b.120. A solução proposta deve apoiar a implantação do sistema operacional.
- b.121. A solução proposta deve suportar Wake-on LAN e UEFI.



- b.122. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no EndPoint remoto durante a sessão devem ser registradas no Management Server.
- b.123. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
- b.124. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
- b.125. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
- b.126. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.
- b.127. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
- b.128. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
- b.129. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
- b.130. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
- b.131. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
  - b.131.1. Inicie a instalação ao reiniciar ou desligar o computador.
  - b.131.2. Instale o gerador necessário todos os pré-requisitos do sistema.
  - b.131.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
  - b.131.4. Baixe atualizações para o dispositivo sem instalá-las.
- b.132. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.



- b.133. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
- b.134. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
  - b.134.1. CEF;
  - b.134.2. LEEF;
- b.135. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
- b.136. O relatório da solução proposta deve conter informações CVE.
- b.137. A solução proposta deve suportar instalação de aplicações e software de terceiros;
- c. Requisitos gerais
  - c.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
    - c.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
  - c.2. A solução proposta deve ser de um único fornecedor e suportar todos os módulos descritos neste termo de referência.
  - c.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
  - c.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
  - c.5. A solução proposta deve suportar o subsistema Linux no Windows.
  - c.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
    - c.6.1. Proteção contra ameaças sem arquivos (Fileless);
    - c.6.2. Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
  - c.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;



- c.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
- c.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
- c.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em EndPoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra os ataques remotos de criptografia.
- c.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em EndPoints e na nuvem para servidores e estações de trabalho Windows.
- c.12. A solução proposta deve fornecer análise comportamental baseada em machine learning.
- c.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
- c.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no EndPoint:
  - c.14.1. Controles de aplicativos,
  - c.14.2. Controle web e dispositivos
  - c.14.3. HIPS e Firewall
  - c.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
  - c.14.5. Gerenciamento de criptografia de arquivos e discos;
  - c.14.6. Controle adaptativo para detecção de anomalias;
- c.15. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
- c.16. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
- c.17. A solução proposta deve ter bancos de dados de reputação locais e globais.
- c.18. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.





- c.19. A solução proposta deve incluir um módulo capaz, no mínimo, de:
  - c.19.1. Bloqueio de aplicativos com base em sua categorização.
  - c.19.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
  - c.19.3. A adição de sub-redes e a modificação de permissões de atividade.
- c.20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
- c.21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
- c.22. A solução proposta deve ter armazenamento local nos EndPoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
- c.23. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
  - c.23.1. Modo silencioso;
  - c.23.2. Discos rígidos e dispositivos removíveis;
  - c.23.3. De todos as contas de usuários do dispositivo.
- c.24. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
  - c.24.1. Exclusão imediata de dados;
  - c.24.2. Exclusão de dados adiada.
- c.25. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
  - c.25.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
  - c.25.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
- c.26. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
- c.27. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
- c.28. A solução proposta deve incluir proteção contra os ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.



- c.29. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.
- c.30. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
- c.31. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
- c.32. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
- c.33. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros EndPoint;
- c.34. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
- c.35. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de EndPoint.
- c.36. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
- c.37. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
- c.38. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
- c.39. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
- c.40. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.



- c.41. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer EndPoint.
- c.42. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
- c.43. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
- c.44. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
- c.45. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
- c.46. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
- c.47. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
- c.48. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
- c.49. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
- c.50. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
- c.51. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no EndPoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
- c.52. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
- c.53. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
- c.54. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.



- c.55. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
- c.56. A solução proposta deve suportar o controle de scripts executados em PowerShell.
- c.57. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
- c.58. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
- c.59. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
- c.60. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
- c.61. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
- c.62. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de EndPoint.
- c.63. A solução proposta deve ter proteção contra ameaças de e-mail de EndPoint com:
  - c.63.1. Filtro de anexos.
  - c.63.2. Verificação de mensagens de e-mail ao receber, ler e enviar.
- c.64. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
- c.65. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
- c.66. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (Javascript, Visual Basic Script Scripts WSH (Javascript, Visual Basic Script etc.);
- c.67. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.



- c.68. A solução proposta deve fornecer proteção contra os ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
- c.69. A solução proposta deve incluir suporte ao protocolo IPv6.
- c.70. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
- c.71. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
- c.72. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
- c.73. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
- c.74. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
- c.75. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
- c.76. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
- c.77. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
- c.78. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
- c.79. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
- c.80. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
- c.81. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.



- c.82. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
- c.83. A solução proposta deve suportar a instalação de proteção de EndPoint em servidores sem a necessidade de reinicialização.
- c.84. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
- c.85. A solução proposta deve suportar endereços IPv6.
- c.86. A solução proposta deve suportar verificação em duas etapas (autenticação).
- c.87. A solução proposta deve prever a instalação, atualização e remoção centralizada de software anti-malware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
- c.88. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
- c.89. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de EndPoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do EndPoint de segurança localmente.
- c.90. A solução proposta deve permitir a instalação remota do sensor de EndPoint com os bancos de dados anti-malware mais recentes.
- c.91. A solução proposta deve permitir a atualização automática do sensor de EndPoint e de bases de dados de anti-malware.
- c.92. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
- c.93. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
- c.94. A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos.
- c.95. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.



- c.96. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi, Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hypervisor.
- c.97. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
- c.98. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
- c.99. A Solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de EndPoint está instalado.
- c.100. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
- c.101. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
- c.102. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
- c.103. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
- c.104. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma inglês e português.
- c.105. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de EndPoints.
- c.106. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
- c.107. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
- c.108. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
- c.109. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de EndPoint sem custo adicional.





- c.110. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
- c.111. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
  - c.111.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
  - c.111.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
- c.112. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
- c.113. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de EndPoint instalado.
- d. Do modulo de gerenciamento de dispositivos móveis
  - d.1. O modulo deve ser integrado a console de gerenciamento;
  - d.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
    - d.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)
  - d.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
    - d.3.1. iOS 10–17 ou iPadOS 13–17
  - d.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
  - d.5. A solução proposta deve suportar dispositivos iOS supervisionados.
  - d.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.
  - d.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
  - d.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.



- d.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
- d.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de EndPoint e da proteção web no dispositivo móvel do usuário.
- d.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
- d.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
- d.13. A solução proposta deve ter recursos de containerização para dispositivos Android.
- d.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
  - d.14.1. Dados em contêineres
  - d.14.2. Contas de e-mail corporativo
  - d.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
  - d.14.4. Nome do ponto de acesso (APN)
  - d.14.5. Perfil do Android for Work
  - d.14.6. Recipiente KNOX
  - d.14.7. Chave do gerenciador de licença KNOX
- d.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
  - d.15.1. Todos os perfis de configuração instalados
  - d.15.2. Todos os perfis de provisionamento
  - d.15.3. O perfil iOS MDM
- d.16. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
- d.17. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo.



**SERVIÇO PÚBLICO FEDERAL**

CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO

**RUA OSCAR FREIRE, 2039 – PINHEIROS – 05409-011 – SÃO PAULO/SP**

[WWW.CRQSP.ORG.BR](http://WWW.CRQSP.ORG.BR)

- d.18.A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controle de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
- d.18.1. Critérios de verificação do dispositivo;
  - d.18.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
- d.19.A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak etc.
- d.20.A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
- d.20.1. Cartões de memória e outras unidades removíveis
  - d.20.2. Câmera do dispositivo
  - d.20.3. Conexões Wi-Fi
  - d.20.4. Conexões Bluetooth
  - d.20.5. Porta de conexão infravermelha
  - d.20.6. Ativação do ponto de acesso Wi-Fi
  - d.20.7. Conexão de área de trabalho remota
  - d.20.8. Sincronização de área de trabalho
  - d.20.9. Definir configurações da caixa de correio do Exchange
  - d.20.10. Configurar caixa de e-mail em dispositivos iOS MDM
  - d.20.11. Configure contêineres Samsung KNOX.
  - d.20.12. Definir as configurações do perfil do Android for Work
  - d.20.13. Configurar e-mail/calendário/contatos
  - d.20.14. Defina as configurações de restrição de conteúdo de mídia.
  - d.20.15. Definir configurações de proxy no dispositivo móvel
  - d.20.16. Configurar certificados e SCEP
- d.21. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
- d.21.1. Portal de inscrição móvel KNOX
  - d.21.2. Pacotes de instalação pré-configurados independentes
- d.22. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
- d.23. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
- d.24. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:



- d.24.1. VMware AirWatch 9.3 ou posterior
  - d.24.2. MobileIron 10.0 ou posterior
  - d.24.3. IBM MaaS360 10.68 ou posterior
  - d.24.4. Microsoft Intune 1908 ou posterior
  - d.24.5. SOTI MobiControl 14.1.4 (1693) ou posterior
- d.25.A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
- d.26.A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
- d.27.A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
- d.28.A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
- d.29.A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
- d.30.A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
- d.31.A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
- d.32.A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
- d.33.A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
- d.34.A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
- d.35.A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
- d.36.A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.



- d.37.A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
- d.38.A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
- d.39.A solução proposta deve proteger contra ameaças online em dispositivos iOS.
- e. Do módulo de MXDR
  - e.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
  - e.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
  - e.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
  - e.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
  - e.5. Deve apresentar informações detalhadas contendo:
    - e.5.1. Usuário que executou a ação;
    - e.5.2. Informações acesso privilegiado;
  - e.6. A solução proposta deve ter Sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
  - e.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
  - e.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações etc.)
  - e.9. O agente EDR deve ter integração com o aplicativo de proteção de EndPoint (agente único).
  - e.10.Soluções EDR e proteção de EndPoint devem ter console unificado para administradores e analistas;



- e.11.A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução EndPoint Protection e a tecnologia de Sandbox na nuvem.
- e.12.A solução proposta deve complementar as informações do veredicto da solução EndPoint Protection com artefatos do sistema sobre a detecção.
- e.13.A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
- e.14.A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
- e.15.A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
- e.16.A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
- e.17.A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
- e.18.A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
- e.19.A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
- e.20.A solução proposta deve permitir agregar os alertas com base nas seguintes informações:
  - e.20.1. Nome do dispositivo
  - e.20.2. Conta de usuário
  - e.20.3. Hash do arquivo
- e.21. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
- e.22. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).



- e.23. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
- e.24. Informações gerais sobre a detecção, incluindo modo de detecção.
- e.25. Alterações no registro associadas à detecção.
- e.26. Histórico da presença de arquivos no dispositivo.
- e.27. Ações de resposta executadas pela aplicação.
- e.28. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro etc.
- e.29. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
  - e.29.1. Processo
  - e.29.2. Conexões de rede
  - e.29.3. Alterações no registro
  - e.29.4. Detalhes do download de objeto
- e.30. A solução proposta deve fornecer orientação de resposta (resposta guiada).
- e.31. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente
- e.32. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
  - e.32.1. Impedir a execução de objetos
  - e.32.2. Isolamento de host
  - e.32.3. Excluir objeto do host ou grupo de hosts
  - e.32.4. Encerrar um processo no dispositivo
  - e.32.5. Colocar um objeto em quarentena
  - e.32.6. Execute a verificação do sistema
  - e.32.7. Execução remota de programa/processo/comando
  - e.32.8. Iniciar a varredura IoC para um grupo de hosts.
  - e.32.9. Adicionar o usuário a um grupo de treinamento no módulo de conscientização
  - e.32.10. Bloquear o usuário no Active Directory
  - e.32.11. Resetar a senha do usuário no Active Directory
  - e.32.12. Adicionar o usuário em um grupo de segurança no Active Directory
  - e.32.13. Remover o usuário de um grupo de segurança no Active Directory



- e.33. Deve possuir integração com solução de conscientização, sendo ela da mesma fabricante da solução de XDR
- e.34. Deve possuir integração com o Active Directory para realizar respostas no mesmo
- e.35. Deve possuir integração com o portal de inteligência do fabricante para fazer uma investigação detalhada do arquivo através do módulo de Sandbox em nuvem
- f. Do módulo de proteção para Microsoft 365
  - f.1. Características Gerais
    - f.1.1. A solução deve ser entregue no modelo de “Software as a Service”, onde servidor e console administrativa são hospedados na nuvem.
    - f.1.2. Acesso a console administrativa via HTTPS.
    - f.1.3. A integração com o Office 365 deve ser realizada via API.
    - f.1.4. A autenticação da integração deve ser realizada via protocolo seguro OAuth 2.0.
    - f.1.5. A solução deve prover módulos de proteção para a suíte Microsoft Office 365 (Exchange Online, OneDrive, SharePoint e Teams).
    - f.1.6. A console deve prover painel de informações exibindo as informações principais da operação e do estado dos componentes de proteção.
    - f.1.7. Capacidade de geração de relatórios em no mínimo formato “.pdf”.
    - f.1.8. Capacidade de geração de relatório instantâneo;
    - f.1.9. Capacidade de agendamento automático de relatórios.
    - f.1.10. A solução deve verificar o tráfego de e-mails inbound e outbound.
    - f.1.11. Deve possuir quarentena para armazenar artefatos detectados como maliciosos.
    - f.1.12. A quarentena deve possuir no mínimo as seguintes opções:
    - f.1.13. Exibir detalhes do item;
    - f.1.14. Excluir item;
    - f.1.15. Liberar item;
    - f.1.16. Filtrar itens;
    - f.1.17. Salvar item em disco;
    - f.1.18. A gestão da solução deve ser realizada por usuário com perfil de administrador.
    - f.1.19. Deve ser possível atribuir perfil de administrador para um usuário na console de administração.
    - f.1.20. Deve ser capaz de detectar informação sensível em texto e imagens transmitidos e armazenados através da plataforma e alertar o administrador quanto ao risco de vazamento da informação.
  - f.2. Módulos de Proteção
    - f.2.1. Anti-malware
      - f.2.1.1. Deve proteger as caixas de correio contra vírus, Worms, trojans, entre outras ameaças que podem ser enviadas via e-mail.
      - f.2.1.2. Análise das ameaças deve ser realizada por no mínimo as seguintes tecnologias:





**SERVIÇO PÚBLICO FEDERAL**

CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO

**RUA OSCAR FREIRE, 2039 – PINHEIROS – 05409-011 – SÃO PAULO/SP**

[WWW.CRQSP.ORG.BR](http://WWW.CRQSP.ORG.BR)

- f.2.1.3. Assinaturas;
- f.2.1.4. Heurística;
- f.2.1.5. Comportamento;
- f.2.1.6. Consulta ao repositório de inteligência do fabricante.
- f.2.1.7. Capacidade de detectar ataques conhecidos e desconhecidos.
- f.2.1.8. Ao detectar um malware, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
  - f.2.1.9. Excluir a mensagem e colocá-la em quarentena;
  - f.2.1.10. Excluir anexo infectado e colocá-lo em quarentena;
  - f.2.1.11. Colocar tag no assunto;
  - f.2.1.12. Substituir arquivo por mensagem personalizada;
  - f.2.1.13. Notificar ao administrador sobre novas ameaças encontradas
  - f.2.1.14. Notificar ao proprietário da caixa sobre mensagens excluídas.
  - f.2.1.15. Deve analisar arquivos nas seguintes aplicações:
    - f.2.1.16. Exchange Online
    - f.2.1.17. OneDrive
    - f.2.1.18. SharePoint
    - f.2.1.19. Teams
  - f.2.1.20. Oferecer proteção contra-ataques mailsplit, Ghost spoofing e injeções de código malicioso.

**f.2.2. Antiphishing**

- f.2.2.1. Deve proteger as caixas de correio contra phishing e links maliciosos enviados em mensagens de e-mail, evitando assim infecção por malware, roubo de dados pessoais e acesso a sites fraudulentos.
- f.2.2.2. Deve validar o conteúdo das mensagens para detectar phishing, utilizando as seguintes tecnologias:
  - f.2.2.3. SPF (Sender Policy Framework)
  - f.2.2.4. DKIM (Domain-based Message Authentication)
  - f.2.2.5. DMARC (Domain-based Message Authentication, Reporting and Conformance)
- f.2.2.6. Consulta ao repositório de inteligência do fabricante.
- f.2.2.7. Capacidade de detectar ataques conhecidos e desconhecidos.
- f.2.2.8. Ao detectar um link de phishing, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
  - f.2.2.9. Excluir a mensagem e colocá-la em quarentena;
  - f.2.2.10. Permitir;
  - f.2.2.11. Mover para pasta “Lixo eletrônico”;
  - f.2.2.12. Colocar TAG no assunto;
  - f.2.2.13. Notificar ao administrador sobre novas mensagens encontradas.
  - f.2.2.14. Notificar ao proprietário da caixa sobre mensagens excluídas.
  - f.2.2.15. Permitir a criação de exclusões por e-mail completo ou máscara.



**f.2.3. AntiSpam / Mass Mail**

- f.2.3.1. Deve proteger os caixas de correio contra e-mail não solicitados “SPAM” e e-mails enviados em massa.
- f.2.3.2. A verificação deve ser realizada através dos seguintes métodos:
- f.2.3.3. Verificação de cabeçalho, conteúdo, anexos e elementos de design;
- f.2.3.4. Algoritmos linguísticos e heurísticos;
- f.2.3.5. Consulta ao repositório de inteligência do fabricante;
- f.2.3.6. Ao detectar um SPAM, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
- f.2.3.7. Permitir;
- f.2.3.8. Mover para a pasta “Lixo eletrônico”;
- f.2.3.9. Colocar TAG no assunto;
- f.2.3.10. Notificar ao administrador sobre novas ameaças encontradas
- f.2.3.11. Notificar ao proprietário da caixa sobre mensagens excluídas.
- f.2.3.12. Permitir a criação de exclusões por e-mail completo ou máscara.

**f.2.4. Filtro de conteúdo**

- f.2.4.1. Deve possibilitar a filtragem de anexos em mensagens de e-mail.
- f.2.4.2. Capacidade de detectar anexos pelos seguintes parâmetros:
- f.2.4.3. Formato do arquivo;
- f.2.4.4. Nome completo do arquivo;
- f.2.4.5. Nome do arquivo com máscara;
- f.2.4.6. Arquivos MS Office com macro;
- f.2.4.7. Ao detectar um anexo que se encaixe em uma das regras, a solução deve possibilitar as seguintes ações:
- f.2.4.8. Excluir mensagem e colocá-la em quarentena;
- f.2.4.9. Excluir anexo e colocá-lo em quarentena;
- f.2.4.10. Permitir
- f.2.4.11. Colocar tag no assunto;
- f.2.4.12. Substituir arquivo por mensagem personalizada;
- f.2.4.13. Notificar ao administrador sobre novas ameaças encontradas
- f.2.4.14. Notificar ao proprietário da caixa sobre mensagens excluídas.
- f.2.4.15. Permitir a criação de exclusões por e-mail completo ou máscara.

**g. Do módulo de treinamento de cibersegurança para administradores de TI**

- g.1. A plataforma de treinamento deve equipar os profissionais de TI com habilidades práticas para reconhecer um possível cenário de ataque em um incidente aparentemente benigno, competência para coletar dados de incidentes para a entrega de uma segurança de TI, criar uma paixão por procurar sinais de atividade maliciosa, consolidando o papel de todos os membros da equipe de TI como a primeira linha de defesa de segurança.
- g.2. A plataforma de treinamento deve ser interativa, deve ter simulação de processos reais sem nenhum risco para o computador.



- g.3. A plataforma de treinamento deve criar habilidades e conhecimentos, deve fornecer metodologia "Aprender fazendo".
- g.4. A plataforma de treinamento deve ter um processo de aprendizado intuitivo, navegação conveniente e dicas.
- g.5. A plataforma de treinamento deve abranger todos os principais tópicos e problemas de segurança de TI que a equipe geral de TI enfrenta em seu trabalho.
- g.6. Os módulos da plataforma de treinamento on-line de segurança cibernética para TI devem conter os seguintes tópicos de treinamento:
  - g.6.1. Softwares Maliciosos
  - g.6.2. Programas e arquivos potencialmente indesejados (PuPs).
  - g.6.3. Noções básicas de investigação.
  - g.6.4. Segurança do servidor.
  - g.6.5. Segurança do Active Directory.
  - g.6.6. Phishing e inteligência de código aberto (OSINT).
- g.7. Requisitos para certificados:
  - g.7.1. O usuário deve receber um certificado após a conclusão bem-sucedida do treinamento.
  - g.7.2. Os certificados devem ter o nome do cenário de treinamento, data de conclusão e nome do usuário.
  - g.7.3. O certificado deve ser apresentado em formato eletrônico na interface do usuário e estar disponível para download.
- g.8. Requisitos para idiomas:
  - g.8.1. A interface da plataforma de treinamento, notificações automáticas por e-mail e todos os materiais de treinamento devem estar disponíveis nos seguintes idiomas:
    - g.8.1.1. Inglês.
    - g.8.1.2. Alemão.
    - g.8.1.3. Italiano.
    - g.8.1.4. Frances.
    - g.8.1.5. Espanhol da UE.
    - g.8.1.6. Espanhol LA.
    - g.8.1.7. Português.
- g.9. Especificações técnicas da plataforma de treinamento:
  - g.9.1. A plataforma de treinamento deve suportar:
    - g.9.1.1. Windows - 10, 11.
    - g.9.1.2. Mac - Sierra, High Sierra, Mojave, Catalina.
    - g.9.1.3. Ubuntu 18.04.
    - g.9.1.4. Google Chrome - versão 80 ou superior.
    - g.9.1.5. Firefox - versão 70 e superior.



- h. Do módulo de conscientização automatizada em cibersegurança para usuários finais
  - h.1. Compatibilidade com sistemas operacionais de desktop:
    - h.1.1. Windows 10;
    - h.1.2. Windows 7;
    - h.1.3. MacOS.
  - h.2. Compatibilidade com sistemas operacionais de dispositivos mobiles:
    - h.2.1. iOS 11 ou superiores;
    - h.2.2. Android 5.x e superiores;
  - h.3. Suporte aos browsers:
    - h.3.1. Microsoft Edge;
    - h.3.2. Internet Explorer 11;
    - h.3.3. Firefox;
    - h.3.4. Google Chrome;
    - h.3.5. Safari for MacOS;
    - h.3.6. Safari(iOS);
    - h.3.7. Google Chrome (Android).
  - h.4. Suporte aos leitores de e-mail do usuário final:
    - h.4.1. Apple Mail 10+;
    - h.4.2. MS Outlook 2010+ (Windows, MacOS);
    - h.4.3. Mail.App (iPhone SE ou superior);
    - h.4.4. Outlook (Google Pixel, iPhone 7 ou superior);
    - h.4.5. Gmail;
    - h.4.6. Google Apps;
    - h.4.7. Office 365;
    - h.4.8. Outlook.com;
    - h.4.9. Yahoo!
  - h.5. Características:
    - h.5.1. A plataforma de treinamento deverá conter base de conhecimento com as principais dúvidas, dicas e guias de recomendações para o administrador da plataforma;
    - h.5.2. A plataforma deverá conter vídeos de demonstração de uso da solução;
    - h.5.3. A plataforma deverá conter uma base com possíveis mensagens/banner de alertas e segurança para compartilhamento dentro do programa de conscientização.
    - h.5.4. Durante a validade da licença, as atualizações da plataforma devem ser entregues sem ônus adicional;
    - h.5.5. Atualizações devem ser disponibilizadas para:
      - h.5.5.1. Atualização de conteúdo dos treinamentos;



- h.5.5.2. Adição de novos conteúdos;
- h.5.5.3. Novas funcionalidades para facilitar administração;
- h.5.5.4. Novas funcionalidades para facilitar interação dos usuários;
- h.5.5.5. Melhorias gerais do sistema e correção de bugs;
- h.5.6. As atualizações na plataforma devem ser realizadas sem causar indisponibilidade ou afetar as funcionalidades;
- h.5.7. O usuário deverá informar possíveis Phishing recebido, para isso a plataforma deve disponibilizar de funcionalidade ou plug-in para envio de notificação aos administradores;
- h.5.8. O plano de atualização da plataforma deve:
  - h.5.8.1. Ser apresentado ao administrador da plataforma dias antes da sua execução;
  - h.5.8.2. Possibilitar ao administrador sugerir melhorias e votar estas melhorias durante a fase de discussão destas;
- h.5.9. A interface da plataforma de treinamento, as notificações por e-mail e todo material de treinamento deverá ser disponibilizado minimamente nos idiomas português, inglês, espanhol, alemão e francês;
- h.5.10. A plataforma deverá gerar automaticamente os seguintes relatórios de acompanhamento ao Administrador:
  - h.5.10.1. Relatório resumo com informações sobre o progresso dos usuários:
    - h.5.10.1.1. Deve ser enviado no mínimo semanalmente;
    - h.5.10.1.2. Conter análise dos usuários por categoria de desempenho;
    - h.5.10.1.3. Conter link para relatório completo do treinamento;
    - h.5.10.1.4. Conter links com recomendações para alteração das categorias de treinamento baseado no desempenho do usuário.
  - h.5.10.2. Relatório geral detalhado da empresa:
    - h.5.10.2.1. Deve conter lista de administradores da plataforma;
    - h.5.10.2.2. O número de usuários (número geral e por status de treinamento);
    - h.5.10.2.3. Informações sobre uso de licenças;
    - h.5.10.2.4. Informações sobre categorias de desempenho;
    - h.5.10.2.5. Lista completa de usuários, especificando o grupo de treinamento pertencente;
    - h.5.10.2.6. A data em que o usuário consentiu em participar dos treinamentos;
    - h.5.10.2.7. As datas de conclusão planejadas e calculadas;
    - h.5.10.2.8. O número de unidades de treinamento com datas expiradas;



- h.5.10.2.9. O número de testes não iniciados;
  - h.5.10.2.10. O número de testes a serem repetidos;
  - h.5.10.2.11. O número de certificados recebidos;
  - h.5.10.2.12. Exportar o relatório em formato XLSX.
  - h.5.10.2.13. Conter informações detalhadas sobre todos os alunos que estão em treinamento ou com treinamento suspenso.
- h.5.10.3. Relatório geral sobre grupos de treinamento:
- h.5.10.3.1. Deve incluir os principais dados sobre o progresso do treinamento para todos os grupos:
    - h.5.10.3.1.1. Número de usuários;
    - h.5.10.3.1.2. Usuários em treinamento ou com treinamento concluído;
    - h.5.10.3.1.3. Usuários sem atribuição de grupos;
    - h.5.10.3.1.4. Data de conclusão prevista, baseada na taxa real de treinamento dos usuários;
    - h.5.10.3.1.5. Porcentagem de usuários que concluíram.
- h.5.10.4. Relatório sobre o grupo de treinamento, incluindo:
- h.5.10.4.1. Diagrama da meta e do nível atual de conhecimento do grupo
  - h.5.10.4.2. Dados básicos sobre o progresso do treinamento:
    - h.5.10.4.2.1. Atribuído: número de usuário que foram adicionados ao programa e que receberam treinamento em um nível especificado;
    - h.5.10.4.2.2. Não iniciado: o número de usuários para os quais o treinamento foi atribuído, mas que ainda não iniciaram o treinamento neste nível;
    - h.5.10.4.2.3. Em treinamento: a quantidade de usuários que iniciaram o treinamento no nível indicado;
    - h.5.10.4.2.4. Nível concluído: o número de usuários que concluíram o treinamento no nível indicado.
    - h.5.10.4.2.5. Porcentagem concluído: a porcentagem de usuários (versus o número total de usuários) que alcançaram o nível alvo.
- h.5.10.5. Relatório individual por usuário, incluindo:
- h.5.10.5.1. Deve conter informações sobre o atendimento dos treinamentos por parte dos usuários;
  - h.5.10.5.2. Dinâmica de treinamento para os usuários;
  - h.5.10.5.3. Atividade diária dos usuários;
  - h.5.10.5.4. Histórico de treinamento do usuário em formato de tabela, incluindo as seguintes informações:
    - h.5.10.5.4.1. Data e horas;



- h.5.10.5.4.2. Tipo de atividade (material de treinamento);
  - h.5.10.5.4.3. Unidade;
  - h.5.10.5.4.4. Nome do material de treinamento;
  - h.5.10.5.4.5. Status;
  - h.5.10.5.4.6. Tempo gasto (em minutos);
  - h.5.10.5.5. Tempo total gasto para treinamento;
  - h.5.10.5.6. Recomendações encaminhadas ao usuário;
  - h.5.10.5.7. Sessões agendadas;
  - h.5.10.5.8. Problemas de aprendizagem;
  - h.5.10.5.9. Nível de conhecimento do usuário;
  - h.5.10.5.10. Categoria de desempenho atual;
- h.5.11. O usuário deverá receber e-mails semanais com relatórios de desempenho e de treinamento;
- h.5.12. A plataforma deve definir no mínimo 5 (cinco) categorias de desempenho: “Antes do cronograma”, “Indo bem”, “Atrasado no cronograma”, “Muito atrasado no cronograma”, “Não terminará no prazo”.
- h.5.13. Cada usuário que está participando do treinamento deverá ser atribuído a uma dessas categorias de desempenho:
  - h.5.13.1. Atrasado no cronograma;
  - h.5.13.2. Significativamente atrasado;
  - h.5.13.3. Impossível terminar no prazo;
  - h.5.13.4. Devem conter as subcategorias:
    - h.5.13.4.1. Não realizar os testes;
    - h.5.13.4.2. Falha nos testes;
    - h.5.13.4.3. Nunca entrou na plataforma.
- h.5.14. Requisitos para definir categorias de desempenho do usuário:
  - h.5.14.1. “Não é possível terminar no prazo” caso o usuário não possa concluir o treinamento até a data de conclusão programada conforme especificado no cronograma de treinamento;
  - h.5.14.2. “Significativamente atrasado” se o usuário tiver 4 (quatro) ou mais unidades inacabadas;
  - h.5.14.3. “Atrasado na programação” se o usuário tiver de 1(uma) a 3(três) unidades inacabadas;
  - h.5.14.4. “Antecipado” se o usuário completou mais unidades que o necessário;
  - h.5.14.5. Em todos os outros casos, o usuário é atribuído à categoria “Vai bem”.
- h.5.15. Requisitos para definir subcategorias de performance de usuários:
  - h.5.15.1. “Nunca acessou a plataforma” – Se o usuário não aceitou os termos e condições do treinamento;



- h.5.15.2. “Não realizou os testes” – Se o usuário não iniciou os testes após término das lições;
- h.5.15.3. “Testes falhos” – O usuário falhou em um ou mais testes ou simulações de phishing após término das lições;
- h.5.16. Requisitos para estatísticas de campanhas simuladas de phishing, incluindo no relatório:
  - h.5.16.1. Taxas de cliques;
  - h.5.16.2. Número e data/hora dos e-mails enviados;
  - h.5.16.3. Envio de e-mail;
  - h.5.16.4. Resultado de falha para usuários;
- h.5.17. Requisitos para objetivos e tarefas da plataforma de treinamento:
  - h.5.17.1. A plataforma de treinamento deve auxiliar na realização dos seguintes objetivos em uma organização:
    - h.5.17.1.1. Reduzir o risco de incidentes quando os funcionários usam recursos de TI, trocam dados pela Internet e trocam dados inadequadamente usando dispositivos móveis;
    - h.5.17.1.2. Minimizar os custos trabalhistas de gerenciamento de treinamento para funcionários.
  - h.5.17.2. A plataforma de treinamento deve resolver as seguintes tarefas:
    - h.5.17.2.1. Definir metas de treinamento e atribuir um programa de treinamento aos usuários;
    - h.5.17.2.2. Fornecer aos usuários os materiais de treinamento relevantes para o programa de treinamento;
    - h.5.17.2.3. Fornecer informações sobre o programa de treinamento na forma de relatório e diagramas;
- h.5.18. Requisitos gerais para a plataforma de treinamento:
  - h.5.18.1. A plataforma deve incluir os seguintes elementos:
    - h.5.18.1.1. Interface gráfica de usuário do administrador;
    - h.5.18.1.2. Interface gráfica do usuário;
    - h.5.18.1.3. Materiais de treinamento (conteúdo);
    - h.5.18.1.4. Simulador de ataque de phishing:
      - h.5.18.1.4.1. Comunicando;
      - h.5.18.1.4.2. Configurações;
      - h.5.18.1.4.3. Suporte técnico;
    - h.5.18.1.5. O acesso à plataforma de treinamento deve ser feito via internet, utilizando protocolos HTTPS e HTTP.
- h.5.19. O administrador da plataforma de treinamento deve ser capaz de gerenciar o processo de treinamento de todos os usuários;





- h.5.20. A plataforma de treinamento deve permitir que o administrador crie e remova empresas;
- h.5.21. A plataforma de treinamento deve ser capaz de atribuir uma empresa específica a um administrador e restringir o acesso desse administrador a outras empresas;
- h.5.22. A plataforma de treinamento deve ser capaz de atribuir privilégios diferentes para 4 funções de administrador. Cada administrador pode visualizar e/ou gerenciar apenas nas empresas às quais está atribuído;
- h.5.23. O administrador deve ser capaz de configurar todos os parâmetros da empresa e parâmetros de perfil do usuário, inserir dados do usuário, definir um conjunto de grupos de treinamento em cada empresa, alterar o programa de treinamento no grupo de treinamento, distribuir usuários entre os grupos de treinamento, atribuir e controlar o treinamento do usuário.
- h.5.24. A plataforma deverá enviar notificações automáticas aos usuários, nos requisitos abaixo:
  - h.5.24.1. Os funcionários de um grupo que iniciou o treinamento deverão receber um e-mail com convite para seguir um link exclusivo, gerado pela plataforma usando o nome de domínio especificado pelo Administrador nas configurações da empresa.
  - h.5.24.2. O usuário deve receber automaticamente relatórios semanais de treinamento por e-mail. Tais relatórios deverão incluir a categoria de desempenho atual do usuário e recomendações sobre as unidades de treinamento atribuídas.
  - h.5.24.3. O administrador deve ser capaz de configurar parâmetro de checagem de domínio para não enviar informações de início de campanhas e garantir que soluções de proteção contra phishing não bloqueie as campanhas executadas pela plataforma.
- h.6. Requisitos para definir os parâmetros de uma empresa
  - h.6.1. O administrador deve ser capaz de definir os seguintes parâmetros de uma empresa:
    - h.6.1.1. Nome da empresa;
    - h.6.1.2. Nome de domínio de quarto nível do nome de domínio do site onde os usuários dessa empresa são treinados;
    - h.6.1.3. Idioma padrão (em particular, o idioma usado no primeiro convite enviado ao usuário);
    - h.6.1.4. Nome e endereço de correspondência do funcionário que desempenha as funções de suporte técnico aos usuários;
    - h.6.1.5. Campos (ou atributos) do perfil do usuário nessa empresa. O administrador deve ser capaz de adicionar atributos personalizados ou excluir atributos que foram adicionados anteriormente;



- h.6.1.6. Regras para alocar usuários automaticamente em grupos de treinamento;
- h.6.1.7. Saudações nas mensagens que os usuários recebem da plataforma;
- h.6.1.8. Nome de usuário mostrado e certificados emitidos quando as unidades de treinamento são concluídas.

**h.7. Requisitos para usar licenças de usuário**

- h.7.1. O administrador deve ser capaz de adicionar ou excluir licenças.
- h.7.2. A plataforma não deve estabelecer uma conexão direta entre um usuário específico e uma licença específica.
- h.7.3. A plataforma deve controlar os seguintes parâmetros relacionados à Licença:
  - h.7.3.1. O número de usuários na fase ativa de treinamento;
  - h.7.3.2. O número de licenças disponíveis.
- h.7.4. Quando o administrador atribui treinamento a um usuário, o número de licenças usadas deve aumentar;
- h.7.5. Quando o administrador interromper ou suspender o treinamento de um usuário, o número total de licenças usadas deve diminuir.

**h.8. Requisitos para gerenciamento de treinamento**

- h.8.1. O administrador deve ser capaz de atribuir um programa de treinamento, dependendo da posição do funcionário e do grau de risco de segurança cibernética (conforme definido pela organização).
- h.8.2. A plataforma deve executar automaticamente as seguintes etapas:
  - h.8.2.1. Criar horários de aula para grupos e cada usuário, com base no nível de destino selecionado do grupo;
  - h.8.2.2. Enviar notificações por e-mail automaticamente aos usuários;
  - h.8.2.3. Enviar automaticamente lembretes aos usuários informando que eles podem prosseguir para a próxima tarefa em um determinado estágio;
  - h.8.2.4. Criar e ajustar um cronograma de treinamento individual para cada funcionário;
  - h.8.2.5. Atribuir todos os materiais de treinamento ao usuário;
  - h.8.2.6. Acompanhar o progresso do treinamento de cada usuário;
  - h.8.2.7. Fornecer relatórios de desempenho semanais aos usuários;
  - h.8.2.8. Enviar e-mails aos usuários com recomendações personalizadas, para que possam concluir o curso no prazo e com sucesso;
  - h.8.2.9. Enviar e-mails ao administrador com relatórios semanais, incluindo recomendações sobre como motivar um usuário para a comunicação fora da plataforma de treinamento.

**h.9. Requisitos para gerenciamento de usuários**

- h.9.1. A plataforma deve permitir que o Administrador execute as seguintes tarefas:



- h.9.1.1. Adicionar, editar, arquivar, restaurar, excluir um usuário ou grupo de usuários;
- h.9.1.2. Adicionar usuários à plataforma importando uma lista de usuários de um arquivo XSLX.
  - h.9.1.2.1. O arquivo modelo deve estar disponível no site da plataforma;
- h.9.1.3. Criar grupos e transferir usuários entre estes;
- h.9.2. A plataforma deve ser capaz de se integrar com o Microsoft Active Directory e com outros sistemas via Open API para sincronizar listas de usuários.
- h.10. Requisitos para gerenciamento de grupos
  - h.10.1. O programa de treinamento deve permitir que o Administrador use os grupos de treinamento que existem por padrão ou crie um número ilimitado de novos grupos de treinamento;
  - h.10.2. O programa de treinamento deve permitir que o Administrador altere os parâmetros de treinamento para grupos, como o nome do grupo, o conjunto de tópicos, o nível de destino de cada tópico (definição de quantas sessões o usuário deve realizar neste tópico), a intensidade (define quantos minutos por semana o usuário é recomendado utilizar na plataforma).
    - h.10.2.1. O administrador atribui o nível de treinamento alvo dependendo do risco que cada usuário específico no grupo específico pode representar para a empresa. Quanto maior o risco, maior o nível de destino precisa ser.
    - h.10.2.2. Os níveis (“Iniciante”, “Elementar”, “Intermediário”) são distribuídos respectivamente de acordo com o nível de risco – de baixo a alto.
  - h.10.3. Por padrão, a plataforma deve ter três grupos correspondentes aos três diferentes níveis de treinamento:
    - h.10.3.1. Iniciante: Para funcionários com acesso limitado aos sistemas corporativos de TI;
    - h.10.3.2. Elementar: Para funcionários com acesso total à rede corporativa, mas sem acesso a informações especialmente confidenciais.
    - h.10.3.3. Intermediário: Para funcionários que têm acesso a informações confidenciais e dados pessoais, bem como acesso de administrador em seus computadores.
  - h.10.4. A plataforma de treinamento deve permitir que o administrador crie regras para mover usuários automaticamente para grupos de treinamentos quando são adicionados à plataforma de treinamento.



- h.10.5. Para cada grupo de treinamento, o cronograma de treinamento deve ser calculado automaticamente de acordo com a intensidade do treinamento, a data de início do treinamento e nível alvo para cada um dos tópicos selecionados.
- h.10.6. O cronograma de treinamento deve ser alterado de acordo com a intensidade de treinamento selecionada pelo Administrador da plataforma.
- h.10.7. A plataforma de treinamento deve ser capaz de iniciar e interromper o treinamento de um grupo de usuários ou de um usuário específico.
- h.10.8. A plataforma de treinamento deve ser capaz de iniciar o treinamento para todos os usuários de um grupo específico.
- h.10.9. A plataforma de treinamento deve ser capaz de adicionar um usuário a um grupo de treinamento.
- h.11. Requisitos de metodologia de treinamento
  - h.11.1. O programa de treinamento deve ser elaborado de acordo com os seguintes princípios:
    - h.11.1.1. Os materiais de formação devem constituir um programa de formação, ou seja, os conteúdos e a quantidade de conhecimentos e competências em segurança cibernética necessários à aprendizagem obrigatória, bem como a sua distribuição por tópico, seção e nível de dificuldade;
    - h.11.1.2. Ao passar dos tópicos, o material de aprendizagem aumenta o nível de dificuldade em relação a apresentação de técnicas ciberdelitivas mais avançadas e das contramedidas relacionadas;
    - h.11.1.3. Cada tópico deve ser apresentado pelo mesmo conjunto de materiais de treinamento;
    - h.11.1.4. A estrutura da aula deve ser a mesma para todos os tópicos;
- h.12. Requisitos para o conteúdo dos materiais de treinamento
  - h.12.1. O programa de treinamento da plataforma deve incluir, no mínimo, os seguintes tópicos:
    - h.12.1.1. Senhas e contas;
    - h.12.1.2. Segurança de E-mail;
    - h.12.1.3. Navegação na Web;
    - h.12.1.4. Redes sociais e serviços de mensageria;
    - h.12.1.5. Segurança do PC;
    - h.12.1.6. Dispositivos móveis;
    - h.12.1.7. Informação Confidencial;
    - h.12.1.8. LGPD;
    - h.12.1.9. Segurança de cartões de banco;
    - h.12.1.10. PCI DSS;



- h.12.1.11. Infraestrutura industrial;
- h.12.2. O programa de treinamento deve incluir lições com temas atuais que possam desenvolver as habilidades dos usuários nas seguintes áreas de segurança cibernética:
  - h.12.2.1. Phishing;
  - h.12.2.2. Links maliciosos;
  - h.12.2.3. Ransomware;
  - h.12.2.4. Arquivos perigosos;
  - h.12.2.5. Aplicações maliciosas;
  - h.12.2.6. Engenharia social;

**h.13. Requisitos para o programa de treinamento**

- h.13.1. Cada tópico deve ser dividido em vários níveis dedicados à prática de um grupo específico de habilidades no campo da segurança cibernética.
- h.13.2. Cada nível do programa deve corresponder a ameaças com vários graus de gravidade, desde ataques básicos e em larga escala até proteção contra-ataques complexos e direcionados.
- h.13.3. Cada tópico deve incluir aulas (exercícios), material para reforço (e-mail), teste de conhecimento e simulação de um ataque de phishing.
- h.13.4. Para concluir um tópico com sucesso, o usuário deve fazer o teste de conhecimento relacionado.
- h.13.5. A transição para o próximo nível deve ser possível depois que todos os tópicos anteriores no nível apropriado foram realizados e o teste de conhecimento relacionado aprovado com sucesso.
- h.13.6. O usuário deve ter a opção de passar em um tópico com antecedência, realizando com sucesso o teste de conhecimento antes de aprender os materiais do tópico.

**h.14. Requisitos para materiais de treinamento**

- h.14.1. A estrutura de aulas (incluindo exercícios) para cada tópico deve ser a mesma em todos os tópicos e deve seguir a sequência lógica abaixo:
  - h.14.1.1. Um conjunto de ações a serem realizadas;
  - h.14.1.2. Porque um usuário deve realizar essas ações;
  - h.14.1.3. As consequências potenciais de ações incorretas;
  - h.14.1.4. Os sinais de perigo que um usuário deve identificar;
  - h.14.1.5. As ações que um usuário deve realizar ao detectar sinais de perigo;
  - h.14.1.6. O que fazer se as dúvidas permanecerem.



- h.14.2. Os seguintes tipos de materiais de treinamento devem ser apresentados:
  - h.14.2.1. Aulas, incluindo parte teórica e exercícios práticos com feedback;
  - h.14.2.2. Testes de conhecimento;
  - h.14.2.3. Simulações de ataque de phishing;
  - h.14.2.4. Exercícios de reforço.
- h.14.3. As aulas devem incluir:
  - h.14.3.1. Slides a serem estudados;
    - h.14.3.1.1. Devem conter:
      - h.14.3.1.1.1. Informações textuais e gráficas;
      - h.14.3.1.1.2. Botões para avançar e retornar aos slides;
  - h.14.3.2. Questões para autoavaliação;
- h.14.4. Os exercícios de reforço devem consistir em coleção de conselhos ou recomendações para exercícios anteriores, bem como exemplos reais de consequências do não cumprimento das regras de segurança cibernética.
- h.14.5. O teste deve consistir em questões às quais o usuário deve dar uma resposta ou múltipla escolha de opções.
- h.14.6. Os resultados do teste devem indicar a aprovação ou não.
- h.14.7. Deve ser possível definir um valor mínimo de acertos para êxito no teste.
- h.14.8. Quando o teste for concluído, o usuário poderá dar feedback para cada questão, independentemente de ter respondido corretamente.
- h.14.9. Os ataques simulados de phishing devem permitir que a reação do usuário à ameaça cibernética seja verificada;
- h.14.10. Os materiais de treinamento devem ser adaptados para usuários que suas contas pessoais em um navegador de dispositivo móvel.
- h.15. Requisitos para funcionalidade de simulação de ataques phishing
  - h.15.1. A plataforma de treinamento deve abranger duas opções de atribuição de ataques simulados de phishing:
    - h.15.1.1. Integrado ao caminho de aprendizagem automatizado para dominar especificamente o conjunto de habilidades criadas nas lições anteriores da unidade.
    - h.15.1.2. Possibilidade de criar uma companhia de phishing separada para um grupo específico de usuário não relacionados a nenhuma atividade de treinamento;



- h.15.1.3. Um ataque de phishing simulado deve ser semelhante a uma mensagem real na forma de um texto com layout, imagens (opcional) e um link. Quando clicado, o link deve redirecionar o usuário para uma página simulada especial;
- h.15.1.4. A página simulada para qual o usuário foi redirecionado no ataque simulado de phishing deve conter uma explicação sobre o motivo pelo qual o usuário foi parar naquele site, uma descrição do e-mail que o usuário receber, bem como recomendações sobre o reconhecimento de e-mails de phishing.
- h.15.1.5. A plataforma deve conter pelo menos trinta modelos de phishing diferentes que são enviados aos usuários durante o treinamento;
- h.15.1.6. A campanha deve possibilitar ser agendada ou ser enviada imediatamente;
- h.15.1.7. O usuário deve receber um ataque simulado de phishing em até 4 dias da conclusão com sucesso, dos testes de conhecimento do tópico de treinamento relacionado;
- h.15.1.8. Quando configurada separada do programa de aprendizagem, a campanha de phishing deverá incluir vários modelos para o grupo de pessoas para envio aleatório de um determinado modelo para cada funcionário.
- h.15.1.9. O usuário deverá ser considerado como aprovado no ataque de phishing simulado se ele (a) não clicar no link do e-mail e não for direcionado para a página simulada.
- h.15.1.10. Caso o usuário falhe na simulação, esta deverá acontecer novamente dentro do prazo de 4 (quatro) dias (caso o phishing simulado esteja integrado no caminho de aprendizagem automatizado).

**h.16. Requisitos para o cronograma de treinamento**

- h.16.1. O cronograma de treinamento deve ser baseado nos seguintes intervalos de tempo:
  - h.16.1.1. O material de reforço deve estar disponível em até 4 dias após realização dos exercícios teóricos e práticos;
  - h.16.1.2. O teste de conhecimento deve estar disponível em até 3 dias após o material de reforço;
  - h.16.1.3. A simulação de ataque de phishing deve ser enviada ao usuário em até 4 dias após conclusão bem-sucedida dos testes de conhecimento;
- h.16.2. Os materiais de treinamento deverão ser disponibilizados ao usuário conforme prazo estipulado;
- h.16.3. O cronograma de treinamento deve se readequar de forma automática às velocidades diferentes dos usuários;



- h.16.4. O usuário deverá ser aprovado no teste para um tópico específico antes de passar para o próximo tópico;
  - h.16.5. O usuário deverá ser capaz de refazer o teste reprovado após conclusão do treinamento;
  - h.16.6. No caso de o usuário falhar no ataque de phishing simulado, este deve ser reenviado automaticamente em até 4 dias ao usuário;
  - h.16.7. O cronograma de treinamento do usuário deve ser baseado na intensidade de treinamento, não restringindo o usuário de fazer as aulas teóricas em seu ritmo. Conforme a intensidade aumentar, as quantidades de materiais teóricos atribuídos ao usuário também aumentarão.
  - h.16.8. A plataforma deve calcular automaticamente a programação do usuário com base no programa de treinamento do grupo.
- h.17. Requisitos para a conta pessoal do usuário da plataforma
- h.17.1. Cada usuário deve ter uma conta pessoal única onde tarefas, histórico de treinamento, informações sobre desempenho e progresso estarão disponíveis;
  - h.17.2. A conta pessoal deve ser uma página da web acessível ao usuário através de um link exclusivo que o usuário recebe por meio de notificações por e-mail;
  - h.17.3. O histórico de treinamento deve incluir uma lista de todas as tarefas concluídas e seus respectivos resultados;
  - h.17.4. O usuário deverá ser capaz de retornar ao material preenchido anteriormente para repetir o treinamento;
  - h.17.5. Na conta pessoal do usuário, deverá haver informações sobre andamento e estatísticas sobre os materiais abordados;
  - h.17.6. As estatísticas de treinamento devem ser visíveis para o usuário:
    - h.17.6.1. Informações sobre o nível sobre a habilidade alvo do usuário;
    - h.17.6.2. Porcentagem de habilidade adquiridas até o momento do número total de habilidades para um determinado nível alvo;
    - h.17.6.3. Data planejada de conclusão do treinamento;
    - h.17.6.4. Data prevista de conclusão;
  - h.17.7. A data prevista de conclusão do treinamento do usuário deve ser calculada de acordo com a programação do grupo do qual o usuário faz parte;
  - h.17.8. A data de conclusão da unidade no plano de treinamento do usuário deve ser determinada com base na data planejada do teste e o tempo que o usuário requer para fazer o teste;
  - h.17.9. Na página de treinamento do usuário deverá haver conselhos e recomendações que ajudarão o usuário a concluir o treinamento no prazo;





h.17.10. A conta pessoal do usuário deve ser totalmente adaptada para que possa ser usada em dispositivos móveis.

h.18. Requisitos para certificados

- h.18.1. O usuário deve receber um certificado após a conclusão bem-sucedida de cada tópico realizado;
- h.18.2. O tópico deve ser considerado concluído com êxito quando o usuário tiver concluído com êxito o teste e for aprovado na simulação de ataque de phishing;
- h.18.3. O certificado deve ser apresentado em formato eletrônico na interface do usuário e estar disponível para download;
- h.18.4. O administrador deve ter a possibilidade de escolher como representar o nome do funcionário e outros campos personalizados no certificado.

h.19. Requisitos para customização

- h.19.1. Logo da instituição:
  - h.19.1.1. O Administrador deve ser capaz de adicionar o logotipo da empresa na conta da plataforma;
- h.19.2. Saudações ao aluno:
  - h.19.2.1. O administrador deve ser capaz de personalizar a saudação do funcionário em notificações por e-mail enviadas aos alunos pela plataforma – como convites, lembretes e recomendações.
  - h.19.2.2. A possibilidade deve dar a capacidade de fazer essas saudações mais adequadas às especificidades do país e/ou cultura de diferentes clientes.
  - h.19.2.3. O administrador deve ser capaz de adicionar qualquer texto ou usar marcas para criar o texto necessário.
  - h.19.2.4. As tags devem incluir o nome completo do usuário, saudação curta e todos os campos personalizados criados para esta empresa.
- h.19.3. Certificados dos alunos:
  - h.19.3.1. O administrador deve ser capaz de personalizar a aparência do nome do aluno no certificado;
  - h.19.3.2. O administrador deve ser capaz de adicionar qualquer texto ou usar marcas para criar o texto necessário;
    - h.19.3.2.1. As tags devem incluir o nome completo do usuário, saudação curta e todos os campos personalizados criados para esta empresa.



- h.19.4. Personalização do programa educacional:
  - h.19.4.1. Este recurso deve dar ao administrador a possibilidade de gerenciar o processo de aprendizagem para a empresa:
    - h.19.4.1.1. Desativar/ativar os primeiros testes de teste que permitem ao usuário pular a teoria;
    - h.19.4.1.2. Desativar/ativar a simulação de phishing que é incluída automaticamente no caminho de aprendizagem;
    - h.19.4.1.3. Escolher o nível alvo e os tópicos a serem atribuídos ao grupo de usuários.
- h.19.5. Personalização do caminho de aprendizagem:
  - h.19.5.1. Para cada grupo de treinamento, o administrador deve ser capaz de selecionar:
    - h.19.5.1.1. Tópicos que os alunos neste grupo precisam aprender (e pular aqueles que você não deseja treinar agora).
    - h.19.5.1.2. Nível alvo desejado para que os alunos atinjam em cada tópico específico.
- h.19.6. Personalização de ataques de phishing simulados:
  - h.19.6.1. Possibilidade de personalizar templates de phishing com assunto, textos e fotos e salvar na biblioteca;
  - h.19.6.2. Variedade de domínios de phishing e endereços de e-mail de remetentes para personalização.
  - h.19.6.3. O administrador poderá criar campanhas de Phishing sem a necessidade de consentimentos dos usuários, Campanhas de Phishing “Cegos”
  - h.19.6.4. A plataforma deverá permitir o uso de QR Codes em phishing customizados,
  - h.19.6.5. A plataforma deverá permitir o uso de anexos aos e-mails de phishing customizados com os seguintes formatos: ZIP e PDF.
- i. Do modulo de Sandbox em nuvem
  - i.1. Deve possuir uma solução que permita a execução de arquivos em ambientes isolados
  - i.2. A solução deve possuir os seguintes status para cada análise feita:
    - i.2.1. Limpo
    - i.2.2. Malware
    - i.2.3. Adware ou outros
    - i.2.4. Não confiável
    - i.2.5. Não categorizado



- i.3. A solução deve suportar análise de objetos compactados (arquivos compactados e arquivados)
- i.4. A solução deve manter os resultados do histórico de análise de arquivos por pelo menos 180 dias por padrão
- i.5. A solução deve suportar todos os tipos de arquivos (executáveis, outros formatos, ou seja, PDF, MS office, scripts Java, arquivos de certificado etc.)
- i.6. A solução deve suportar a exportação de resultados de análise de arquivos para vários formatos, tais como:
  - i.6.1. STIX;
  - i.6.2. CSV;
  - i.6.3. JSON;
  - i.6.4. PCAP;
  - i.6.5. DEBUG Report;
- i.7. A solução deverá suportar configurações personalizadas para análise de artefatos, deve conter no mínimo:
  - i.7.1. Ambiente de execução;
  - i.7.2. Tempo de execução do artefato;
  - i.7.3. Tipos de conexão;
  - i.7.4. Senha dos arquivos internos;
  - i.7.5. Comandos e parâmetros;
  - i.7.6. Clique em links;
- i.8. A solução deverá ter Sandbox com informações de sumário executivo, contendo no mínimo:
  - i.8.1. Arquivos detectados dentro da amostra;
  - i.8.2. Atividades maliciosas;
  - i.8.3. Atividades de rede;
- i.9. A solução deverá ter Sandbox com informações técnicas, contendo no mínimo:
  - i.9.1. Mapa de execução do artefato contendo, detalhes técnicos e técnica utilizada mapeada pelo MITRE ATT&CK;
  - i.9.2. Tabela com as Técnicas e táticas mapeadas a partir do MITRE do artefato analisado.
  - i.9.3. Screenshot das telas e comportamentos do artefato.
- j. Do módulo de Serviço de detecção e resposta gerenciado
  - j.1. Do monitoramento, identificação e investigação dos eventos de segurança cibernética
  - j.2. O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados.



**SERVIÇO PÚBLICO FEDERAL**

CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO

**RUA OSCAR FREIRE, 2039 – PINHEIROS – 05409-011 – SÃO PAULO/SP**

[WWW.CRQSP.ORG.BR](http://WWW.CRQSP.ORG.BR)

- j.3. Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços.
- j.4. A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos.
- j.5. É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações.
- j.6. Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança.
- j.7. O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede.
- j.8. O monitoramento deverá ser capaz de identificar as principais ameaças, bem como táticas, técnicas e procedimentos de ataque descritos na base de conhecimento MITRE ATT&CK, sem prejuízo do uso de outras bases de conhecimento ou serviços de inteligência de ameaças, para complementação da capacidade de identificação de atividades maliciosas.
- j.9. Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos anômalos, visando antecipar a identificação de incidentes de segurança.
- j.10. A solução deverá prover inteligência de proteção contra-ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados.
- j.11. O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica da Contratante, para indicar ações de contenção, comunicar à equipe da Contratante sobre o andamento do tratamento dos incidentes.



j.12. Compatibilidade:

j.12.1. É suportada por qualquer um dos seguintes navegadores:

- j.12.1.1. Apple Safari versões mais recentes
- j.12.1.2. Google Chrome versões mais recentes
- j.12.1.3. Microsoft Edge
- j.12.1.4. Mozilla Firefox versões mais recentes

j.13. Requisitos de rede:

- j.13.1. Em condições médias de carga: um canal full-duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo.
- j.13.2. Em condições de carga máxima: um canal full-duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo.

j.14. Compatibilidade de sensor de EndPoint

j.14.1. O agente de EndPoint deve ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados/telemetria ao SOC do fabricante:

- j.14.1.1. Microsoft Windows 7 e superiores;
- j.14.1.2. MacOS 10.14-11;
- j.14.1.3. CentOS 6.7 ou superior;
- j.14.1.4. Debian GNU / Linux 9.4 ou superior;
- j.14.1.5. Linux Mint 19 ou superior;
- j.14.1.6. Oracle Linux 7.3 ou superior;
- j.14.1.7. Red Hat Enterprise Linux 6.7 ou superior;
- j.14.1.8. SUSE Linux Enterprise Server 12 SP5 ou superior;
- j.14.1.9. Ubuntu 18.04 LTS ou superior.

j.15. Capacidades técnicas

- j.15.1. Deve possuir console web própria do serviço, além de integração nativa com a console do “software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets”
- j.15.2. A console deve possuir dashboards com as informações principais, apresentando no mínimo:
- j.15.3. Número de incidentes e status
- j.15.4. Quantidade de dispositivos monitorados
- j.15.5. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:
  - j.15.5.1. E-mail
  - j.15.5.2. Telegram
  - j.15.5.3. WhatsApp<sup>i</sup>
- j.15.6. Deve permitir o envio de relatórios.
- j.15.7. O agente deve enviar a telemetria em tempo real para o SoC do fabricante;
- j.15.8. Os dados coletados devem possuir capacidade de armazenamento do evento original (raw log) junto com o evento normalizado.



- j.15.9. O SIEM/SOAR deve garantir geração de alertas baseada em análise de anomalias e mudanças de comportamento básicos (linha de base).
- j.15.10. O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x265.
- j.15.11. O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD.
- j.15.12. O SIEM/SOAR deve ter a capacidade de:
  - j.15.12.1. Coleta e análise de logs de servidores Microsoft Windows (via Agente ou WMI).
  - j.15.12.2. Coleta e análise de logs de servidores Linux/UNIX (via Syslog ou Agente).
  - j.15.12.3. Coleta e análise de logs de bancos de dados (mínimo MS SQL Server via métodos nativos ou JDBC).
  - j.15.12.4. Capacidade de coletar e analisar logs de aplicações proprietárias (por DSM universal/parser personalizado configurável).
  - j.15.12.5. Integração com ferramentas de controle de acesso (AD, RADIUS/TACACS+).
  - j.15.12.6. Integração com ferramentas IAM e PAM (logs via Syslog/API).
  - j.15.12.7. Coleta e análise de logs de infraestrutura de rede chave (Firewalls, Switches Core).
  - j.15.12.8. Agente para Windows gerenciado centralmente com capacidade de coleta local/RPC e store-and-forward.
  - j.15.12.9. Coleta e análise de fluxos de rede (Netflow v5/v9, IPFIX ou sFlow).
- j.15.13. O SIEM/SOAR deve possuir biblioteca funcional e atualizada de regras de correlação predefinidas (out-of-the-box) para ameaças comuns.
- j.15.14. O SIEM/SOAR deve contar com biblioteca madura de regras de correlação predefinidas alinhadas ao MITRE ATT&CK.
- j.15.15. O SIEM/SOAR do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países.
- j.15.16. O SIEM/SOAR do fabricante deve garantir redundância geográfica e alta disponibilidade (SLA ≥99,9%).
- j.15.17. O SIEM/SOR deve gerar alerta por interrupção de coleta de logs de uma fonte configurada (Log Source Monitoring).
- j.15.18. O SIEM/SOAR do fabricante deve estar hospedado em infraestrutura com certificação SOC 2 Type II, ISO 27001, GDPR.
- j.15.19. O SIEM/SOAR do fabricante deve garantir criptografia em trânsito (TLS) e em repouso (AES-256).
- j.15.20. O SIEM/SOAR do fabricante deve garantir retenção de dados ajustável conforme políticas.
- j.15.21. O SIEM/SOAR do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países) incluindo Brasil.
- j.15.22. O SIEM/SOAR do fabricante deve possuir (relação com XDR):
  - j.15.22.1. Identificação automática de ameaças mediante assinaturas, heurística e machine learning.



- j.15.22.2. Investigação e resposta automatizada a incidentes.
  - j.15.22.3. Integração contextual com múltiplos ambientes.
  - j.15.22.4. Enriquecimento de eventos com inteligência de ameaças global (OTX – Open Threat Exchange).
  - j.15.23. Os dados coletados devem passar por no mínimo:
    - j.15.23.1. Modelos de Machine Learning/Inteligência Artificial;
    - j.15.23.2. Análise humana;
    - j.15.23.3. Correlação com IoA's (indicadores de ataque);
    - j.15.23.4. Emulação em Sandbox (quando necessário);
  - j.15.24. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como "Incidentes"
  - j.15.25. O Incidente deve possuir no mínimo as seguintes informações:
    - j.15.25.1. Resumo
    - j.15.25.2. Prioridade (Baixa, Média e Alta)
    - j.15.25.3. Recomendação
    - j.15.25.4. Data de criação e data de atualização
    - j.15.25.5. Correlacionamento com táticas/técnicas do Framework MITRE ATT&CK
    - j.15.25.6. Dispositivos afetados
    - j.15.25.7. IoC's de host e de rede
    - j.15.25.8. Descrição completa em linha do tempo
  - j.15.26. O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:
    - j.15.26.1. Transferir arquivo para o SoC;
    - j.15.26.2. Isolar um dispositivo;
    - j.15.26.3. Desabilitar isolamento de dispositivo;
    - j.15.26.4. Deletar chave de registro;
    - j.15.26.5. Dump de memória;
  - j.15.27. As ações devem ser aprovadas no portal por profissional da contratante, com a opção de habilitar aprovação automática.
  - j.15.28. Deve possuir console multi-tenant com a possibilidade de separar ativos.
  - j.15.29. Deve possuir Escalabilidade para coleta de dados de dispositivos em sites externos e crescimento futuro.
  - j.15.30. Deve possuir campos para o multi-tenant para melhor visualização:
    - j.15.30.1. Name;
    - j.15.30.2. Status;
    - j.15.30.3. Descrição;
    - j.15.30.4. Criado em;
  - j.15.31. Deve possuir Controle de Acesso Baseado em Perfis (RBAC) granular — por dispositivo, grupo, rede e função específica.
- k. Requisitos para documentação da solução.
- k.1. A documentação da solução de proteção de EndPoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
  - k.2. Ajuda on-line para administradores





- k.3. Ajuda on-line para melhores práticas de implementação
- k.4. Ajuda on-line para proteção de servidores de administração
- k.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
- k.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

#### 6.18 Planejamento das Atividades

##### 6.18.1 A CONTRATADA deverá executar, no mínimo, as seguintes atividades:

- 6.18.1.1 Planejamento e diagnóstico do ambiente atual, incluindo levantamento de ativos, análise das políticas de segurança existentes e definição do plano de migração;
- 6.18.1.2 Adequação e ativação das licenças da solução MXDR, garantindo sua correta vinculação ao ambiente em nuvem já utilizado pelo CRQ-IV/SP;
- 6.18.1.3 Migração assistida da solução EDR para MXDR, assegurando a continuidade da proteção dos ativos e a integridade das configurações existentes, com a devida evolução para o novo modelo de detecção e resposta;
- 6.18.1.4 Integração e consolidação de fontes de eventos e logs, incluindo, quando aplicável, ativos de rede, servidores, serviços de diretório e ambientes em nuvem, de forma a ampliar a visibilidade de segurança;
- 6.18.1.5 Configuração, revisão e otimização das políticas de segurança, regras de detecção, níveis de severidade e fluxos de resposta a incidentes;
- 6.18.1.6 Implantação e operacionalização de serviço de monitoramento contínuo (SOCaaS), com atuação proativa, análise de eventos, detecção de ameaças e apoio à resposta a incidentes de segurança da informação;
- 6.18.1.7 Definição e execução de procedimentos de resposta a incidentes, incluindo ações de contenção, erradicação e recuperação, quando necessário;
- 6.18.1.8 Realização de testes de validação da solução, com simulação de cenários de ataque, ajustes operacionais e garantia de efetividade da detecção e resposta;

#### 6.19 Responsabilidades Gerais

- 6.19.1 Sistema de controle de suporte: Deverá ser utilizado um sistema informatizado, para controle dos serviços de suporte, que funcionará como gerenciador de demandas, devendo possuir registro, acompanhamento e formação de estatísticas sobre a evolução das operações dos atendimentos de suporte. O sistema deve ser disponibilizado através do site da empresa CONTRATADA e deverá ser de responsabilidade da mesma sua manutenção.
- 6.19.2 Abertura de chamados: Os chamados de suporte deverão ser feitos via telefone ou por sistema de Help Desk da CONTRATADA, com interface web e acesso via Internet. O sistema de Help Desk, deverá permitir o controle, por parte do CRQ-IV/SP, de todos os chamados e atendimentos realizados, em aberto ou fechados, além de permitir a emissão de relatórios estatísticos;





6.19.3 Relatório de Atendimento Técnico – RAT: Para cada tarefa concluída e testada, o profissional alocado responsável por sua execução, apresentará relatório conclusivo com documentação e horas gastas em sua execução. Esse relatório será avaliado e aprovado pela equipe de TI.

6.19.4 Procedimento de encerramento do chamado: O encerramento de uma tarefa ou Ordem de Serviço dar-se-á somente após total concordância da equipe de TI com a solução apresentada. O atesto se dará a cada tarefa executada e no Relatório de Atendimento Técnico respectivo.

6.19.5 Chamados abertos de forma automatizada por monitoração: Deverão obedecer aos mesmos critérios.

6.19.6 A CONTRATADA deverá reunir conhecimento técnico e capacidade operacional para lidar com todas tecnologias e ferramentas apresentadas neste termo através dos atestados solicitados na habilitação técnica.

#### 6.20 Tempos e Tipos de Atendimento (SLA)

6.20.1 Tempo de resposta: O tempo de resposta máximo para início dos serviços de suporte às atividades de ambiente de tecnologia da informação da contratante será compatível com o nível de urgência do chamado, conforme descrito a seguir:

<b>Prioridades</b>	<b>Descrição</b>	<b>Tempo para 1º contato com o cliente</b>	<b>Tempo para solução após o registro do chamado</b>
Severidade 1	Impacto crítico impossibilitando o uso do sistema;	20 minutos	Em até 08 (oito) horas
Severidade 2	Impacto significativo prejudicando a operação do sistema;	40 minutos	Em até 16 (dezesseis) horas

6.20.2 Tempo de solução: O tempo de solução de eventos dependerá da extensão, gravidade e disponibilidade das soluções pelos fabricantes. A contratante deverá ser notificada com uma estimativa do tempo de solução do evento dentro das primeiras duas horas do atendimento.

6.20.3 A CONTRATADA deverá prover serviço de monitoramento, detecção e resposta gerenciada (MXDR) com operação **24x7x365** (vinte e quatro horas por dia, sete dias por semana), observando os seguintes Tempos de Reação (Reaction Time):



Severidade do Incidente	Descrição Técnica	SLA de Notificação/Reação
<b>Crítica/Alta</b>	Ameaças com potencial de interrupção imediata ou exfiltração de dados.	<b>Até 03 (três) horas</b>
<b>Média</b>	Anomalias que sugerem atividade suspeita, mas sem impacto imediato.	<b>Até 12 (doze) horas</b>
<b>Baixa</b>	Alertas de conformidade ou detecções de softwares indesejados (adware/riskware).	<b>Até 24 (vinte e quatro) horas</b>

6.20.4 O Tempo de Reação será contabilizado a partir do momento da geração do alerta pela plataforma de telemetria até a disponibilização do incidente validado no console de gestão e envio de notificação à equipe técnica do CRQ-IV/SP.

6.20.5 Da eficácia do SLA:

6.20.5.1 A CONTRATADA deverá manter um índice de conformidade de, no mínimo, **90% (noventa por cento)** dos incidentes atendidos dentro dos prazos estipulados na tabela acima, apurados mensalmente.

6.20.5.2 A comprovação do cumprimento do SLA dar-se-á através de relatórios mensais extraídos diretamente do portal de MxDR (Managed Extension Detection and Response), contendo os timestamps de detecção e notificação.

6.20.5.3 Em caso de descumprimento do acordo de SLA estabelecido, será aplicada multa de 5% do valor total referente ao serviço de suporte técnico e monitoramento (SOCaaS) para cada evento registrado.

6.21 Exclusões

Cabe ressaltar que não pertencem ao escopo desta proposta:

6.21.1 Suporte de serviços de 1º e 2º níveis, ou seja, qualquer tipo de atendimento ao usuário final seja hardware, software, sistemas etc.

6.21.2 Assistência técnica e manutenção de hardware sejam servidores, estações de trabalho, impressoras, switches ou outro ativo de TI;

6.22.3 Execução de instalação e manutenção de cabeamento estruturado (passagem de cabos, troca de patch-panels, obras físicas de engenharia etc.);

6.22.4 Manutenção da rede elétrica e telefônica.

6.22 Obrigações do CRQ-IV/SP

6.22.1 Permitir acesso dos empregados da CONTRATADA às dependências do CRQ-IV/SP para a prestação dos serviços;

6.22.2 Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante da CONTRATADA;

6.22.3 Fornecer em tempo hábil, todos os elementos necessários para a prestação dos serviços;

6.22.4 Notificar imediatamente a CONTRATADA sobre qualquer condição operacional anormal;

6.22.5 Efetuar o pagamento devido, segundo as condições estabelecidas.



#### 6.23 Das obrigações da contratada

##### 6.23.1 Caberá a contratada o cumprimento das seguintes obrigações:

- 6.23.1.1 Responder, em relação aos seus funcionários, por todas as despesas recorrentes do fornecimento dos produtos e por outras correlatas, tais como salários, seguros de acidentes, tributos, indenizações, vales refeição, vales transporte e outras que porventura venham a ser criadas e exigidas pelo Poder Público;
- 6.23.1.2 Respeitar as normas e procedimentos de controle interno, inclusive de acesso às dependências do CRQ-IV/SP;
- 6.23.1.3 Responder pelos danos causados diretamente à Administração ou aos bens do CRQ-IV/SP ou ainda a terceiros, decorrentes de sua culpa ou dolo, durante a execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CRQ-IV/SP;
- 6.23.1.4 A Contratada deverá tratar todas as informações a que tiver acesso no âmbito do CRQ-IV/SP em estrita conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), responsabilizando-se integralmente pela confidencialidade, integridade e segurança dos dados pessoais e sensíveis. Caberá à Contratada adotar medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, vazamentos, perda, alteração ou qualquer forma de tratamento inadequado ou ilícito, bem como assegurar que seus colaboradores e prepostos observem rigorosamente as normas de proteção de dados
- 6.23.1.5 Comunicar à Administração do CRQ-IV/SP qualquer anormalidade constatada e prestar os esclarecimentos solicitados;
- 6.23.1.6 Manter, durante o período de vigência do Contrato, o atendimento das condições de habilitação exigidas neste Pregão.

##### 6.23.2 A contratada caberá assumir a responsabilidade por:

- 6.23.2.1 Todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com o CRQ-IV/SP;
- 6.23.2.2 Todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie forem vítimas os seus empregados durante a execução do contrato, ainda que acontecido em dependência do CRQ-IV/SP;
- 6.23.2.3 Todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução do contrato, originariamente ou vinculada por prevenção, conexão ou continência.

#### 6.24 Sobre inadimplência da contratada

A inadimplência da contratada, com referência aos encargos sociais, comerciais e fiscais não transfere a responsabilidade por seu pagamento ao CRQ-IV/SP, nem poderá onerar o objeto desta contratação, razão pela qual a contratada renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o órgão.



## **7 – Análise comparativa de soluções:**

Inciso II, do artigo II da Instrução Normativa SGD-ME nº 94/2022

Alternativa 1: Manutenção das soluções atuais.

Alternativa 2: Migração para outras plataformas de produtividade e segurança.

Alternativa 3: Implantação de SOC interno ou terceirizado.

A alternativa mais adequada foi a manutenção da solução atual com serviços gerenciados por terceiros.

A continuidade do uso da plataforma Kaspersky justifica-se pela ampla adoção e consolidação dessas soluções no ambiente tecnológico da instituição, garantindo estabilidade operacional, compatibilidade com os sistemas já utilizados e familiaridade dos usuários com as ferramentas. A substituição por outras soluções disponíveis no mercado demandaria processos de migração complexos, reconfiguração de ambientes, capacitação de usuários e possíveis riscos de indisponibilidade ou perda de produtividade. Além disso, ambas as plataformas apresentam elevado nível de maturidade tecnológica, recursos avançados de colaboração e segurança, atualizações contínuas e suporte consolidado, fatores que contribuem para a manutenção da eficiência operacional, da segurança da informação e da continuidade dos serviços institucionais.

A contratação de serviços especializados para monitoramento e gerenciamento da plataforma Kaspersky EndPoint Security/EDR-MXDR justifica-se pela complexidade técnica dessas soluções e pela necessidade de administração contínua, especializada e proativa dos ambientes de colaboração e segurança da informação. Empresas especializadas dispõem de equipes certificadas, ferramentas avançadas de monitoramento e experiência prática na gestão dessas plataformas, garantindo maior eficiência na configuração, resposta a incidentes, aplicação de boas práticas de segurança e atualização tecnológica. Além disso, a terceirização permite otimizar os recursos humanos da própria instituição, evitando a sobrecarga da equipe interna de TI e possibilitando que ela se concentre em atividades estratégicas e no atendimento às demandas institucionais. Dessa forma, a contratação externa contribui para elevar o nível de disponibilidade, segurança e governança dos serviços de tecnologia da informação.

## **7.2 – Necessidades similares em outros órgãos ou entidade da Administração Pública e as soluções adotadas.**

Inciso II, letra “a” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Esta solução é adotada em diversos órgãos da Administração Pública.

## **7.3 – As alternativas de mercado:**

Inciso II, letra “b” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

7.3.1 Foram avaliadas soluções disponíveis no mercado como Microsoft Defender XDR e CrowdStrike para segurança.



7.3.2 A substituição da plataforma atual implicaria migração complexa de dados, perda de padronização, treinamento e impacto operacional.

**7.4 – A existência de softwares disponíveis conforme descrito na Portaria STI/MP Nº 46, de 28/09/2016**

Inciso II, letra “c” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

**7.5 – As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico – ePing, Modelo de Acessibilidade em Governo Eletrônico – eMag, Padrões Web em Governo Eletrônico – ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira – ICP Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil, quando aplicáveis**

Inciso II, letra “d” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

**7.6 – As necessidades de adequação do ambiente do órgão para viabilizar a execução contratual**

Inciso II, letra “e” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Em atendimento ao disposto no inciso II, alínea “e”, do art. 11 da Instrução Normativa SGD/ME nº 94/2022, verifica-se que a presente contratação não demandará adequações na infraestrutura tecnológica, física ou lógica do ambiente da contratante, tendo em vista que a solução pretendida é compatível com o ambiente computacional atualmente existente no órgão, inexistindo necessidade de aquisição adicional de equipamentos, expansão de capacidade, alterações estruturais, adaptações prediais ou modificações significativas nos sistemas e serviços já implantados.

**7.7 – Os diferentes modelos de prestação de serviços;**

Inciso II, letra “f” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

**7.8 – Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;**

Inciso II, letra “g” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.



**7.9 – A possibilidade de aquisição na forma de bens ou contratação como serviço;**

Inciso II, letra “h” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

O objeto desta contratação será como serviço.

**7.10 – A ampliação ou substituição da solução implantada;**

Inciso II, letra “i” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

**7.11 – As diferentes métricas de prestação de serviço e de pagamento;**

Inciso II, letra “j” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Os pagamentos dos serviços contratados serão realizados mensalmente **conforme demanda**.

**8 – Análise comparativa de custos das soluções técnica e funcionalmente viáveis:**

Inciso III, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

**8.1 – Comparação de custos totais de propriedade:**

Inciso III, letra “a” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

**8.2 – Memória de cálculo que referencie os preços e os custos utilizados na análise**

Inciso III, letra “b” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

**9 – Estimativa do custo total da contratação:**

Inciso IV, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

9.1 Para alcançar a melhor contratação, mediante a competitividade em busca da proposta mais vantajosa. O custo estimado desta contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas.



## **10 Identificação dos benefícios a serem alcançados**

Inciso V, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

10.1 Elevação do nível de segurança cibernética, redução de incidentes, melhoria da disponibilidade dos serviços e aumento da produtividade dos usuários.

<b>Economicidade</b>	Espera-se que a presente contratação proporcione economicidade ao órgão por meio da adoção de solução integrada de segurança cibernética, reduzindo custos operacionais relacionados à mitigação de incidentes, indisponibilidade de serviços, perda de dados e contratação fragmentada de ferramentas distintas de proteção digital.
<b>Efetividade</b>	Espera-se que a contratação produza impactos positivos e concretos na segurança da informação institucional, contribuindo para a continuidade dos serviços, aumento da maturidade em cibersegurança, fortalecimento da governança de TIC e redução dos riscos relacionados a ataques cibernéticos e vazamento de informações.
<b>Eficiência</b>	Espera-se a otimização dos processos de segurança da informação mediante atuação especializada, monitoramento contínuo do ambiente, automação de detecção de ameaças e resposta rápida a incidentes, permitindo maior capacidade operacional da equipe interna de TI e melhoria dos níveis de governança e segurança cibernética da contratante.
<b>Eficácia</b>	Espera-se que a solução contratada alcance os resultados pretendidos, garantindo proteção adequada ao ambiente computacional, detecção tempestiva de ameaças, redução de vulnerabilidades e suporte especializado na resposta a incidentes de segurança cibernética.
<b>Objetivo Estratégico</b>	OE11 – Adotar as melhores práticas de Governança e Gestão e OE12 – Promover a inovação de processos e serviços, por meio de melhoria contínua e das ferramentas de Inteligência Artificial.

Elemento Despesa: 33.90.39.006 - Licença de Uso de Sistemas de Informática - Software

## **11 – Declaração de Viabilidade da Contratação:**

Inciso V, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

11.1 Não se recomenda parcelamento da solução devido à necessidade de integração entre licenciamento, monitoramento e serviços de segurança.

11.2 O não parcelamento da contratação justifica-se pela natureza integrada dos serviços e soluções envolvidas, uma vez que o fornecimento das licenças da plataforma Kaspersky EndPoint está diretamente relacionado aos serviços de gerenciamento, monitoramento e suporte especializado dessa ferramenta. A contratação conjunta garante maior eficiência operacional, padronização na administração do ambiente tecnológico e responsabilização clara de um único fornecedor pela disponibilidade, configuração e suporte das soluções. Além disso, a gestão centralizada reduz riscos de incompatibilidades técnicas, falhas de comunicação entre diferentes prestadores e



atrasos na resolução de incidentes, contribuindo para maior segurança da informação, continuidade dos serviços e melhor desempenho do ambiente de TI da instituição.

11.3 A contratação é tecnicamente viável e necessária para garantir continuidade dos serviços institucionais, segurança da informação e eficiência operacional.

Com base nas análises técnicas e econômicas realizadas neste Estudo Técnico Preliminar, conclui-se que a contratação de serviço de gerenciamento de segurança cibernética, com suporte técnico especializado e monitoramento (SOCaaS), incluindo o fornecimento das respectivas soluções de software (Kaspersky Next MXDR), são viáveis e necessárias, atendendo às demandas institucionais e contribuindo para a modernização e segurança da infraestrutura de Tecnologia da Informação.

11.4 Dessa forma, recomenda-se o prosseguimento do processo de contratação com a elaboração do Termo de Referência.

## **12 Classificação quanto ao acesso a informação**

12.1. Nos termos da Lei nº 12.527, de 18 de novembro de 2011, o presente Estudo não se classifica como sigiloso.

São Paulo, 27 maio de 2026.

Equipe Técnica de Planejamento da Contratação

**Alexandre de Paula**  
Integrante Requisitante  
Gerente / Tecnologia da Informação

**Claudio A. Gimenez**  
Integrante Técnico

**Waldemir Menezes da Silva**  
Integrante Administrativo