



**SERVIÇO PÚBLICO FEDERAL**

**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

## **ANEXO I.3**

**CADERNO TÉCNICO - PRODUTOS E SERVIÇOS**



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

**CADERNO TÉCNICO - PRODUTOS E SERVIÇOS**

**1. SOLUÇÃO DE ANTI-VIRUS EDR e GESTÃO**

**Tabela 1 - fornecimento**

Item	Descrição	Apuração	Qtde	Unidade
1	Licenças Kaspersky Next Optimum – Brazilian Edition (3years)	Única	1400	Licenças
2	Serviço de Sustentação, Suporte, Monitoramento	Mensal	36 meses	Serviço
3	Serviço de Capacitação. Fornecimento de 5 Vouchers para o treinamento KL002.12.1 - Kaspersky Endpoint Security and Management. Conforme especificado no Caderno Técnico.	Única	1	Serviço

**1.1. A contratação compreende**

- 1.1.1. A renovação das licenças do sistema de Antivírus do CREA-SP para todos os Desktops, Notebooks e aparelhos móveis pelo período da vigência do contrato.
- 1.1.2. A adequação do Console de Gerenciamento
- 1.1.3. O serviço de operação do sistema de Antivírus e sua console pelo período da vigência do contrato
- 1.1.4. O serviço de capacitação da equipe interna do CREA-SP

**2. CARACTERÍSTICAS GERAIS**

**3. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS**

**3.1. REQUISITOS E FUNCIONALIDADES MÍNIMOS DAS LICENÇAS FORNECIDAS**

- 3.1.1. Do módulo de proteção de endpoint
  - 3.1.1.1. A solução proposta deverá proteger os sistemas operacionais abaixo:
    - 3.1.1.1.1. Windows 7
    - 3.1.1.1.2. Windows 8
    - 3.1.1.1.3. Windows 8.1
    - 3.1.1.1.4. Windows 10
    - 3.1.1.1.5. Windows 11
  - 3.1.1.2. Servidores
    - 3.1.1.2.1. Windows Small Business Server 2011
    - 3.1.1.2.2. Windows MultiPoint Server 2011
    - 3.1.1.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
  - 3.1.1.3. Servidores de terminal Microsoft
    - 3.1.1.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server
      - 3.1.1.3.2. 2008 R2, 2012 R2, 2016, 2019 e 2022
  - 3.1.1.4. Sistemas operacionais Linux de 32 bits:



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.1.4.1. CentOS 6.7 e posterior
- 3.1.1.4.2. Debian GNU/Linux 11.0 e posterior
- 3.1.1.4.3. Debian GNU/Linux 12.0 e posterior
- 3.1.1.4.4. Red Hat Enterprise Linux 6.7 e posterior
- 3.1.1.5. Sistemas operacionais Linux de 64 bits:
  - 3.1.1.5.1. Amazon Linux 2.
  - 3.1.1.5.2. CentOS 6.7 e mais tarde
  - 3.1.1.5.3. CentOS 7.2 e posterior.
  - 3.1.1.5.4. CentOS Stream 8.
  - 3.1.1.5.5. CentOS Stream 9.
  - 3.1.1.5.6. Debian GNU/Linux 11.0 e posterior.
  - 3.1.1.5.7. Debian GNU/Linux 12.0 e posterior.
  - 3.1.1.5.8. Linux Mint 20.3 e superior.
  - 3.1.1.5.9. Linux Mint 21.1 e posterior.
  - 3.1.1.5.10. openSUSE Leap 15.0 e posterior.
  - 3.1.1.5.11. Oracle Linux 7.3 e posterior.
  - 3.1.1.5.12. Oracle Linux 8.0 e posterior.
  - 3.1.1.5.13. Oracle Linux 9.0 e posterior.
  - 3.1.1.5.14. Red Hat Enterprise Linux 6.7 e posterior
  - 3.1.1.5.15. Red Hat Enterprise Linux 7.2 e posterior.
  - 3.1.1.5.16. Red Hat Enterprise Linux 8.0 e posterior.
  - 3.1.1.5.17. Red Hat Enterprise Linux 9.0 e posterior.
  - 3.1.1.5.18. Rocky Linux 8.5 e posterior.
  - 3.1.1.5.19. Rocky Linux 9.1.
  - 3.1.1.5.20. SUSE Linux Enterprise Server 12.5 ou posterior.
  - 3.1.1.5.21. SUSE Linux Enterprise Server 15 ou posterior.
  - 3.1.1.5.22. Ubuntu 20.04 LTS.
  - 3.1.1.5.23. Ubuntu 22.04 LTS.
  - 3.1.1.5.24. Sistemas operacionais Arm de 64 bits:
  - 3.1.1.5.25. CentOS Stream 9.
  - 3.1.1.5.26. SUSE Linux Enterprise Server 15.
  - 3.1.1.5.27. Ubuntu 22.04 LTS
- 3.1.1.6. Sistemas operacionais MAC OS:
  - 3.1.1.6.1. macOS 12 – 15
- 3.1.1.7. Ferramentas de virtualização MAC OS:
  - 3.1.1.7.1. Parallels Desktop 16 para Mac Business Edition
  - 3.1.1.7.2. VMware Fusion 11.5 Profissional
  - 3.1.1.7.3. VMware Fusion 12 Profissional
- 3.1.1.8. A solução proposta deverá suportar as seguintes plataformas virtuais:
  - 3.1.1.9. VMware Workstation 17.0.2 Pro
  - 3.1.1.10. VMware ESXi 8.0 Update 2
  - 3.1.1.11. Microsoft Hyper-V Server 2019
  - 3.1.1.12. Citrix Virtual Apps e Desktop 7 2308
  - 3.1.1.13. Citrix Provisioning 2308
  - 3.1.1.14. Citrix Hypervisor 8.2 Update 1
- 3.1.2. Do módulo de gerenciamento avançado



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.1. A solução proposta deve suportar arquitetura cloud-native e on-premise;
- 3.1.2.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
  - 3.1.2.2.1. Amazon Web Services
  - 3.1.2.2.2. Microsoft Azure
  - 3.1.2.2.3. Google Cloud
- 3.1.2.3. A solução proposta deve incluir as seguintes opções de integração SIEM:
  - 3.1.2.3.1. HP (Microfoco) ArcSight
  - 3.1.2.3.2. IBM QRadar
  - 3.1.2.3.3. Splunk
  - 3.1.2.3.4. Kaspersky KUMA
- 3.1.2.4. 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.
- 3.1.2.5. 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;
- 3.1.2.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
- 3.1.2.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
- 3.1.2.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.
- 3.1.2.9. 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.
- 3.1.2.10. 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.
- 3.1.2.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
- 3.1.2.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.
- 3.1.2.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
- 3.1.2.14. 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 um único/múltiplos dispositivos com base nas seguintes regras de ativação:
  - 3.1.2.14.1. Status do dispositivo





**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.14.2. Tag
- 3.1.2.14.3. Diretório ativo
- 3.1.2.14.4. Proprietários de dispositivos
- 3.1.2.14.5. Hardware
- 3.1.2.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:
  - 3.1.2.15.1. E-mail
  - 3.1.2.15.2. Registro de sistema
  - 3.1.2.15.3. SMS
- 3.1.2.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
  - 3.1.2.16.1. Atributos de rede
  - 3.1.2.16.2. Nome
  - 3.1.2.16.3. Domínio e/ou Sufixo de Domínio
  - 3.1.2.16.4. Endereço de IP
  - 3.1.2.16.5. Endereço IP para servidor de gerenciamento
  - 3.1.2.16.6. Localização no Active Directory
  - 3.1.2.16.7. Unidade organizacional
  - 3.1.2.16.8. Grupo
  - 3.1.2.16.9. Sistema operacional
  - 3.1.2.16.10. Número do pacote de serviço
  - 3.1.2.16.11. Arquitetura Virtual
  - 3.1.2.16.12. Registro de aplicativos
  - 3.1.2.16.13. Nome da Aplicação
  - 3.1.2.16.14. Versão do aplicativo
  - 3.1.2.16.15. Fabricante
  - 3.1.2.16.16. Tipo e versão
  - 3.1.2.16.17. Arquitetura
- 3.1.2.17. 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.
- 3.1.2.18. 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.
- 3.1.2.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
  - 3.1.2.19.1. Dispositivos Desktop/Servidores
  - 3.1.2.19.2. Dispositivos móveis
  - 3.1.2.19.3. Dispositivos de rede
  - 3.1.2.19.4. Dispositivos virtuais
  - 3.1.2.19.5. Componentes OEM
  - 3.1.2.19.6. Periféricos de computador
  - 3.1.2.19.7. Dispositivos IoT conectados
  - 3.1.2.19.8. Telefones VoIP
  - 3.1.2.19.9. Repositórios de rede
- 3.1.2.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.20.1. Nome da Aplicação
- 3.1.2.20.2. Caminho do aplicativo
- 3.1.2.20.3. Metadados do aplicativo
- 3.1.2.20.4. Aplicativo Certificado digital
- 3.1.2.20.5. Categorias de aplicativos predefinidas pelo fornecedor
- 3.1.2.20.6. SHA256 e MD5
- 3.1.2.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
  - 3.1.2.21.1. Bluetooth
  - 3.1.2.21.2. Dispositivos móveis
  - 3.1.2.21.3. Modems externos
  - 3.1.2.21.4. CD/DVD
  - 3.1.2.21.5. Câmeras e scanners
  - 3.1.2.21.6. MTPs
  - 3.1.2.21.7. E a transferência de dados para dispositivos móveis
- 3.1.2.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
- 3.1.2.23. 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.
- 3.1.2.24. 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:
  - 3.1.2.24.1. Estruturas de domínios e grupos de trabalho do Windows
  - 3.1.2.24.2. Estruturas de grupos do Active Directory
  - 3.1.2.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador
- 3.1.2.25. 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.
- 3.1.2.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:
  - 3.1.2.26.1. Verificação manual;
  - 3.1.2.26.2. Verificação no acesso;
  - 3.1.2.26.3. Verificação por demanda;
  - 3.1.2.26.4. Verificação de arquivos compactados
  - 3.1.2.26.5. Verificação de arquivos individuais, pastas e unidades;
  - 3.1.2.26.6. Bloqueio e verificação de scripts
  - 3.1.2.26.7. Proteção contra alteração de registros;
  - 3.1.2.26.8. Proteção contra estouro de buffer;
  - 3.1.2.26.9. Verificação em segundo plano/inativa
- 3.1.2.27. Verificação de unidade removível na conexão com o sistema;
- 3.1.2.28. 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.



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.29. 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.
- 3.1.2.30. 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.
- 3.1.2.31. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
- 3.1.2.32. 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.
- 3.1.2.33. A solução proposta deve suportar Windows Failover Cluster.
- 3.1.2.34. A solução proposta deve ter um recurso de clustering integrado.
- 3.1.2.35. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
- 3.1.2.36. 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.
- 3.1.2.37. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
- 3.1.2.38. 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.
- 3.1.2.39. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
- 3.1.2.40. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
- 3.1.2.41. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
- 3.1.2.42. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
- 3.1.2.43. A solução proposta deverá possuir controles para download de DLL e drivers.
- 3.1.2.44. 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.
- 3.1.2.45. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

- 3.1.2.46. 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).
- 3.1.2.47. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
- 3.1.2.48. 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.
- 3.1.2.49. 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.
- 3.1.2.50. 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.
- 3.1.2.51. 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.
- 3.1.2.52. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
- 3.1.2.53. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
- 3.1.2.54. 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.
- 3.1.2.55. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
- 3.1.2.56. 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.
- 3.1.2.57. 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. .
- 3.1.2.58. 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.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.59. 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 de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
- 3.1.2.60. A solução proposta deve permitir ao administrador personalizar relatórios.
- 3.1.2.61. 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.
- 3.1.2.62. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
- 3.1.2.63. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
- 3.1.2.64. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
- 3.1.2.65. 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.
- 3.1.2.66. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
- 3.1.2.67. 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;
- 3.1.2.68. 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.
- 3.1.2.69. A solução proposta deve suportar integração com solução APT.
- 3.1.2.70. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
- 3.1.2.71. A solução proposta deve permitir instalar o módulo de gerenciamento on-premise nos seguintes sistemas operacionais:
  - 3.1.2.71.1. Windows
  - 3.1.2.71.2. Linux
- 3.1.2.72. A solução proposta deverá suportar os seguintes servidores de banco de dados:
  - 3.1.2.72.1. Windows:
    - 3.1.2.72.1.1. Microsoft SQL Server
    - 3.1.2.72.1.2. Microsoft Banco de dados SQL do Azure



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.72.1.3. MySQL Standard e Enterprise
- 3.1.2.72.1.4. MariaDB
- 3.1.2.72.1.5. PostgreSQL
- 3.1.2.72.2. Linux:
  - 3.1.2.72.2.1. MySQL
  - 3.1.2.72.2.2. MariaDB
  - 3.1.2.72.2.3. PostgreSQL
- 3.1.2.73. A solução proposta deverá suportar as seguintes plataformas virtuais:
  - 3.1.2.73.1. Windows:
    - 3.1.2.73.1.1. VMware vSphere 6.7 e 7.0
    - 3.1.2.73.1.2. Estação de trabalho VMware 16 Pro
    - 3.1.2.73.1.3. Servidor Microsoft Hyper-V 2012 de 64 bits
    - 3.1.2.73.1.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
    - 3.1.2.73.1.5. Microsoft Servidor Hyper -V 2016 de 64 bits
    - 3.1.2.73.1.6. Servidor Microsoft Hyper-V 2019 de 64 bits
    - 3.1.2.73.1.7. Servidor Microsoft Hyper-V 2022 de 64 bits
    - 3.1.2.73.1.8. Citrix XenServer 7.1 LTSR
    - 3.1.2.73.1.9. Citrix XenServer 8.x
    - 3.1.2.73.1.10. Oracle VM VirtualBox 6.x
  - 3.1.2.73.2. Linux:
    - 3.1.2.73.2.1. VMware vSphere 6.7, 7.0 e 8.0
    - 3.1.2.73.2.2. VMware Desktop 16 Pro e 17 Pro
    - 3.1.2.73.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
    - 3.1.2.73.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
    - 3.1.2.73.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
    - 3.1.2.73.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
    - 3.1.2.73.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
    - 3.1.2.73.2.8. Citrix XenServer 7.1 e 8.x
    - 3.1.2.73.2.9. Oracle VM VirtualBox 6.x e 7.x
- 3.1.2.74. A solução proposta deve suportar criptografia em vários níveis:
  - 3.1.2.74.1. Criptografia completa do disco – incluindo disco do sistema
  - 3.1.2.74.2. Criptografia de arquivos e pastas
  - 3.1.2.74.3. Criptografia de mídia removível
  - 3.1.2.74.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2
- 3.1.2.75. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
  - 3.1.2.75.1. A criptografia de arquivos em unidades de computador locais.
  - 3.1.2.75.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
  - 3.1.2.75.3. A criação de listas criptografadas de pastas em unidades de computador locais.
- 3.1.2.76. 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:



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.76.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
- 3.1.2.76.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
- 3.1.2.77. 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:
  - 3.1.2.77.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
  - 3.1.2.77.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
- 3.1.2.78. 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
- 3.1.2.79. 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.
- 3.1.2.80. 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.
- 3.1.2.81. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
- 3.1.2.82. 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.
- 3.1.2.83. 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.
- 3.1.2.84. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.
- 3.1.2.85. 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.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.86. 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.
- 3.1.2.87. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.
- 3.1.2.88. 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.
- 3.1.2.89. 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.
- 3.1.2.90. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
- 3.1.2.91. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados independentemente da localização e/ou usuário.
- 3.1.2.92. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
- 3.1.2.93. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
- 3.1.2.94. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
  - 3.1.2.94.1. Uso do Trusted Platform Module e configurações de senha.
  - 3.1.2.94.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
- 3.1.2.95. 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).
- 3.1.2.96. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
- 3.1.2.97. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
  - 3.1.2.97.1. Instalação remota de software de terceiros
  - 3.1.2.97.2. Relatórios sobre software e hardware existentes
  - 3.1.2.97.3. Monitoramento para instalação de software não autorizado
  - 3.1.2.97.4. Remoção de software não autorizado
- 3.1.2.98. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.





**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.99. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
- 3.1.2.100. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
- 3.1.2.101. 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.
- 3.1.2.102. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.
- 3.1.2.103. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
- 3.1.2.104. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
- 3.1.2.105. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança.
- 3.1.2.106. A solução proposta deve permitir ao administrador aprovar atualizações.
- 3.1.2.107. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
- 3.1.2.108. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
- 3.1.2.109. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
- 3.1.2.110. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
- 3.1.2.111. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
- 3.1.2.112. 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).
- 3.1.2.113. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
- 3.1.2.114. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
- 3.1.2.115. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'.



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.116. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
- 3.1.2.117. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
- 3.1.2.118. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
- 3.1.2.119. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
- 3.1.2.120. A solução proposta deve apoiar a implantação do sistema operacional.
- 3.1.2.121. A solução proposta deve suportar Wake-on LAN e UEFI.
- 3.1.2.122. 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.
- 3.1.2.123. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
- 3.1.2.124. 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.
- 3.1.2.125. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
- 3.1.2.126. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.
- 3.1.2.127. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
- 3.1.2.128. 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.
- 3.1.2.129. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
- 3.1.2.130. 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.
- 3.1.2.131. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
  - 3.1.2.131.1. Inicie a instalação ao reiniciar ou desligar o computador.
  - 3.1.2.131.2. Instale o gerador necessário todos os pré-requisitos do sistema.



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.2.131.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
- 3.1.2.131.4. Baixe atualizações para o dispositivo sem instalá-las.
- 3.1.2.132. 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.
- 3.1.2.133. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
- 3.1.2.134. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
  - 3.1.2.134.1. CEF;
  - 3.1.2.134.2. LEEF;
- 3.1.2.135. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
- 3.1.2.136. O relatório da solução proposta deve conter informações CVE.
- 3.1.2.137. A solução proposta deve suportar instalação de aplicações e software de terceiros;
- 3.1.3. Do módulo de gerenciamento simplificado
  - 3.1.3.1. A solução proposta deve suportar arquitetura cloud;
  - 3.1.3.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
  - 3.1.3.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
  - 3.1.3.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
  - 3.1.3.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
  - 3.1.3.6. A solução proposta deve atender as condições apontadas no item e subitens 6.
  - 3.1.3.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
  - 3.1.3.8. 3.8. A solução proposta deve incluir informações do endpoint:
    - 3.1.3.8.1. IP público de internet;
    - 3.1.3.8.2. IP interno do dispositivo;
    - 3.1.3.8.3. Versão do agente de proteção;
    - 3.1.3.8.4. Última comunicação com a console, contendo data e hora;
    - 3.1.3.8.5. Informações do sistema operacional;



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.3.9. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
- 3.1.3.10. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
- 3.1.3.11. A solução proposta deve incluir treinamento em segurança cibernética.
- 3.1.4. Requisitos gerais da Ferramenta
  - 3.1.4.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
    - 3.1.4.1.1. 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.
    - 3.1.4.1.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
    - 3.1.4.1.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
    - 3.1.4.1.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
    - 3.1.4.1.5. A solução proposta deve suportar o subsistema Linux no Windows.
    - 3.1.4.1.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
      - 3.1.4.1.6.1. Proteção contra ameaças sem arquivos (Fileless);
      - 3.1.4.1.6.2. Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
    - 3.1.4.1.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
    - 3.1.4.1.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
    - 3.1.4.1.9. 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.
    - 3.1.4.1.10. 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 ataques remotos de criptografia.
    - 3.1.4.1.11. 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.



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.4.1.12. A solução proposta deve fornecer análise comportamental baseada em machine learning.
- 3.1.4.1.13. 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.
- 3.1.4.1.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
  - 3.1.4.1.14.1. Controles de aplicativos,
  - 3.1.4.1.14.2. Controle web e dispositivos
  - 3.1.4.1.14.3. HIPS e Firewall
  - 3.1.4.1.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
  - 3.1.4.1.14.5. Gerenciamento de criptografia de arquivos e discos;
  - 3.1.4.1.14.6. Controle adaptativo para detecção de anomalias;
- 3.1.4.1.15. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
- 3.1.4.1.16. 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.
- 3.1.4.1.17. A solução proposta deve ter bancos de dados de reputação locais e globais.
- 3.1.4.1.18. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
- 3.1.4.1.19. A solução proposta deve incluir um módulo capaz, no mínimo, de:
  - 3.1.4.1.19.1. Bloqueio de aplicativos com base em sua categorização.
  - 3.1.4.1.19.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
  - 3.1.4.1.19.3. A adição de sub-redes e a modificação de permissões de atividade.
- 3.1.4.1.20. 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.
- 3.1.4.1.21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
- 3.1.4.1.22. A solução proposta deve ter armazenamento local no 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.
- 3.1.4.1.23. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
  - 3.1.4.1.23.1. Modo silencioso;
  - 3.1.4.1.23.2. Discos rígidos e dispositivos removíveis;



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.4.1.23.3. De todos as contas de usuários do dispositivo.
- 3.1.4.1.24. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
  - 3.1.4.1.24.1. Exclusão imediata de dados;
  - 3.1.4.1.24.2. Exclusão de dados adiada.
- 3.1.4.1.25. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
  - 3.1.4.1.25.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
  - 3.1.4.1.25.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
- 3.1.4.1.26. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
- 3.1.4.1.27. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
- 3.1.4.1.28. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
- 3.1.4.1.29. 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.
- 3.1.4.1.30. 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.
- 3.1.4.1.31. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
- 3.1.4.1.32. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
- 3.1.4.1.33. 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;
- 3.1.4.1.34. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.4.1.35. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
- 3.1.4.1.36. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
- 3.1.4.1.37. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
- 3.1.4.1.38. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
- 3.1.4.1.39. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
- 3.1.4.1.40. 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.
- 3.1.4.1.41. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
- 3.1.4.1.42. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
- 3.1.4.1.43. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
- 3.1.4.1.44. 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.
- 3.1.4.1.45. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
- 3.1.4.1.46. 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;
- 3.1.4.1.47. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
- 3.1.4.1.48. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
- 3.1.4.1.49. 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.
- 3.1.4.1.50. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.4.1.51. 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.
- 3.1.4.1.52. 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.
- 3.1.4.1.53. 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.
- 3.1.4.1.54. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
- 3.1.4.1.55. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
- 3.1.4.1.56. A solução proposta deve suportar o controle de scripts executados em PowerShell.
- 3.1.4.1.57. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
- 3.1.4.1.58. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
- 3.1.4.1.59. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
- 3.1.4.1.60. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
- 3.1.4.1.61. 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.
- 3.1.4.1.62. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
- 3.1.4.1.63. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
  - 3.1.4.1.63.1. Filtro de anexos.
  - 3.1.4.1.63.2. Verificação de mensagens de email ao receber, ler e enviar.
- 3.1.4.1.64. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
- 3.1.4.1.65. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;





**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.4.1.66. 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.);
- 3.1.4.1.67. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
- 3.1.4.1.68. A solução proposta deve fornecer proteção contra 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.
- 3.1.4.1.69. A solução proposta deve incluir suporte ao protocolo IPv6.
- 3.1.4.1.70. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
- 3.1.4.1.71. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
- 3.1.4.1.72. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
- 3.1.4.1.73. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
- 3.1.4.1.74. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
- 3.1.4.1.75. 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.
- 3.1.4.1.76. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
- 3.1.4.1.77. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
- 3.1.4.1.78. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
- 3.1.4.1.79. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
- 3.1.4.1.80. 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.
- 3.1.4.1.81. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

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.

- 3.1.4.1.82. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
- 3.1.4.1.83. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
- 3.1.4.1.84. 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.
- 3.1.4.1.85. A solução proposta deve suportar endereços IPv6.
- 3.1.4.1.86. A solução proposta deve suportar verificação em duas etapas (autenticação).
- 3.1.4.1.87. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
- 3.1.4.1.88. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
- 3.1.4.1.89. 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.
- 3.1.4.1.90. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
- 3.1.4.1.91. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
- 3.1.4.1.92. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
- 3.1.4.1.93. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
- 3.1.4.1.94. A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos.
- 3.1.4.1.95. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
- 3.1.4.1.96. 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.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.4.1.97. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
- 3.1.4.1.98. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
- 3.1.4.1.99. 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.
- 3.1.4.1.100. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
- 3.1.4.1.101. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
- 3.1.4.1.102. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
- 3.1.4.1.103. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
- 3.1.4.1.104. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
- 3.1.4.1.105. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
- 3.1.4.1.106. 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.
- 3.1.4.1.107. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
- 3.1.4.1.108. 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.
- 3.1.4.1.109. 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.
- 3.1.4.1.110. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
- 3.1.4.1.111. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
  - 3.1.4.1.111.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
  - 3.1.4.1.111.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
- 3.1.4.1.112. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.4.1.113. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.
- 3.1.5. Do módulo de gerenciamento de dispositivos móveis
  - 3.1.5.1. O módulo deve ser integrado a console de gerenciamento;
  - 3.1.5.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
    - 3.1.5.2.1. 5.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)
  - 3.1.5.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
    - 3.1.5.3.1. iOS 10–17 ou iPadOS 13–17
  - 3.1.5.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
  - 3.1.5.5. A solução proposta deve suportar dispositivos iOS supervisionados.
  - 3.1.5.6. 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.
  - 3.1.5.7. 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.
  - 3.1.5.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
  - 3.1.5.9. 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).
  - 3.1.5.10. 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.
  - 3.1.5.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
  - 3.1.5.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
  - 3.1.5.13. A solução proposta deve ter recursos de containerização para dispositivos Android.
  - 3.1.5.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
    - 3.1.5.14.1. Dados em contêineres
    - 3.1.5.14.2. Contas de e-mail corporativo
    - 3.1.5.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.5.14.4. Nome do ponto de acesso (APN)
- 3.1.5.14.5. Perfil do Android for Work
- 3.1.5.14.6. Recipiente KNOX
- 3.1.5.14.7. Chave do gerenciador de licença KNOX
- 3.1.5.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
  - 3.1.5.15.1. Todos os perfis de configuração instalados
  - 3.1.5.15.2. Todos os perfis de provisionamento
  - 3.1.5.15.3. O perfil iOS MDM
- 3.1.5.16. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
- 3.1.5.17. 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 .
- 3.1.5.18. 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:
  - 3.1.5.18.1. Critérios de verificação do dispositivo;
  - 3.1.5.18.2. 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;
- 3.1.5.19. 5.19. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
- 3.1.5.20. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
  - 3.1.5.20.1. Cartões de memória e outras unidades removíveis
  - 3.1.5.20.2. Câmera do dispositivo
  - 3.1.5.20.3. Conexões Wi-Fi
  - 3.1.5.20.4. Conexões Bluetooth
  - 3.1.5.20.5. Porta de conexão infravermelha
  - 3.1.5.20.6. Ativação do ponto de acesso Wi-Fi
  - 3.1.5.20.7. Conexão de área de trabalho remota
  - 3.1.5.20.8. Sincronização de área de trabalho
  - 3.1.5.20.9. Definir configurações da caixa de correio do Exchange
  - 3.1.5.20.10. Configurar caixa de e-mail em dispositivos iOS MDM
  - 3.1.5.20.11. Configure contêineres Samsung KNOX.
  - 3.1.5.20.12. Definir as configurações do perfil do Android for Work
  - 3.1.5.20.13. Configurar e-mail/calendário/contatos
  - 3.1.5.20.14. Defina as configurações de restrição de conteúdo de mídia.
  - 3.1.5.20.15. Definir configurações de proxy no dispositivo móvel



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.5.20.16. Configurar certificados e SCEP
- 3.1.5.21. 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 .
- 3.1.5.22. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
  - 3.1.5.22.1. Portal de inscrição móvel KNOX
  - 3.1.5.22.2. Pacotes de instalação pré-configurados independentes
- 3.1.5.23. 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.
- 3.1.5.24. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
- 3.1.5.25. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
  - 3.1.5.25.1. VMware AirWatch 9.3 ou posterior
  - 3.1.5.25.2. MobileIron 10.0 ou posterior
  - 3.1.5.25.3. IBM MaaS360 10.68 ou posterior
  - 3.1.5.25.4. Microsoft Intune 1908 ou posterior
  - 3.1.5.25.5. SOTI MobiControl 14.1.4 (1693) ou posterior
- 3.1.5.26. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
- 3.1.5.27. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
- 3.1.5.28. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
- 3.1.5.29. 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.
- 3.1.5.30. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
- 3.1.5.31. 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.
- 3.1.5.32. 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.
- 3.1.5.33. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
- 3.1.5.34. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
- 3.1.5.35. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.5.36. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
- 3.1.5.37. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
- 3.1.5.38. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
- 3.1.5.39. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
- 3.1.5.40. A solução proposta deve proteger contra ameaças online em dispositivos iOS.
- 3.1.6. 6. Do módulo de EDR
  - 3.1.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
  - 3.1.6.2. 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.
  - 3.1.6.3. 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;
  - 3.1.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
  - 3.1.6.5. Deve apresentar informações detalhadas contendo:
    - 3.1.6.5.1. Usuário que executou a ação;
    - 3.1.6.5.2. Informações acesso privilegiado;
  - 3.1.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
  - 3.1.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
  - 3.1.6.8. 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.)
  - 3.1.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).
  - 3.1.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas.
  - 3.1.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
  - 3.1.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
- 3.1.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
- 3.1.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
- 3.1.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
- 3.1.6.17. 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.
- 3.1.6.18. 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.
- 3.1.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
- 3.1.6.20. 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:
- 3.1.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
- 3.1.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
- 3.1.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.
- 3.1.6.24. Alterações no registro associadas à detecção.
- 3.1.6.25. Histórico da presença de arquivos no dispositivo.
- 3.1.6.26. Ações de resposta executadas pela aplicação.
- 3.1.6.27. 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.
- 3.1.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
- 3.1.6.29. Processo
- 3.1.6.30. Conexões de rede
- 3.1.6.31. Alterações no registro
- 3.1.6.32. Detalhes do download de objeto
- 3.1.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).
- 3.1.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente





**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.1.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
- 3.1.6.36. Impedir a execução de objetos
- 3.1.6.37. Isolamento de host
- 3.1.6.38. Excluir objeto do host ou grupo de hosts
- 3.1.6.39. Encerrar um processo no dispositivo
- 3.1.6.40. Colocar um objeto em quarentena
- 3.1.6.41. Execute a verificação do sistema
- 3.1.6.42. Execução remota de programa/processo/comando
- 3.1.6.43. Iniciar a varredura IoC para um grupo de hosts.
- 3.1.7. Requisitos para documentação da solução.
  - 3.1.7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
  - 3.1.7.2. Ajuda on-line para administradores
  - 3.1.7.3. Ajuda on-line para melhores práticas de implementação
  - 3.1.7.4. Ajuda on-line para proteção de servidores de administração
  - 3.1.7.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti- malware.
  - 3.1.7.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;
- 3.2. REQUISITOS DO SERVIÇO DE SUSTENTAÇÃO, SUPORTE, MONITORAMENTO
  - 3.2.1. REQUISITOS DO SERVIÇO DE SUSTENTAÇÃO
    - 3.2.1.1. Os serviços de sustentação do ambiente de TI envolvem atividades contínuas destinadas a manter a infraestrutura de tecnologia da informação de uma organização funcionando de forma eficiente, segura e confiável. Esses serviços abrangem uma ampla gama de áreas, incluindo suporte técnico, monitoramento, manutenção preventiva, resolução de problemas e implementação de melhorias. Além disso, eles garantem a disponibilidade e a integridade dos sistemas e aplicativos essenciais para as operações da empresa.
    - 3.2.1.2. A CONTRATADA deverá desenvolver o Serviço de Sustentação através das seguintes atividades:
    - 3.2.1.3. Atividades mensais recorrentes:
      - 3.2.1.3.1. Atendimento de chamados de Nível 1;
      - 3.2.1.3.2. Atendimento de chamados de Nível 2;
      - 3.2.1.3.3. Atendimento de chamados de Nível 3 junto ao fornecedor;
      - 3.2.1.3.4. Criação do Relatório Mensal da saúde do ambiente e sugestões de melhorias;
      - 3.2.1.3.5. Envio de Book Mensal do CREA/SP através do CONTRATADA Help.
    - 3.2.1.4. Atividades Anuais
      - 3.2.1.4.1. Documentação de Health Check do ambiente (6 meses após a sustentação ou a atividade de atualização da console);
      - 3.2.1.4.2. Atualização da console do cliente;
      - 3.2.1.4.3. Análise de tendências e áreas que precisam de melhorias;
      - 3.2.1.4.4. Criação da documentação "As is - To be" e melhorias a serem feitas;
      - 3.2.1.4.5. Revisar e Atualizar políticas após aprovação;



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

3.2.1.4.6. Enviar apresentação por e-mail (mediante atualização do Book Mensal).

3.2.1.5. Atividades Comuns de Sustentação:

3.2.1.5.1. Suporte para Desenvolvimento/Correção de políticas de segurança;

3.2.1.5.1.1. Criar White/ Black list

3.2.1.5.2. Controle de acesso à web e dispositivos para evitar roubo de informações;

3.2.1.5.3. Preparação de perfis de segurança permitidos/restritos;

3.2.1.5.4. Configuração de relatórios para análise;

3.2.1.5.5. Análise e criação de regras de firewall para endpoints;

3.2.1.5.6. Análise e distribuição de vacinas e atualizações;

3.2.1.5.7. Análise comportamental do servidor KSC;

3.2.1.5.8. Criação de imagem padrão para deploy de Sistema Operacional e Aplicativos;

3.2.1.5.9. Gestão de licenças e de inventário de hardware;

3.2.1.5.10. Criação de controle de vulnerabilidade e gestão de patches Microsoft ou terceiros;

3.2.1.5.11. Criação de política de criptografia de Disco, arquivos e pastas e USB.

3.2.1.5.12. Acompanhamento dos alertas, tarefas do EDR e relatórios do que ocorre no ambiente com Notificações para a Equipe de TI do CREA-SP;

3.2.1.5.13. Instalação do Endpoint Agent em máquinas adicionadas no ambiente;

3.2.1.5.14. Envio semanalmente dos relatórios sobre as ameaças detectadas;

3.2.1.5.15. Recriação da política do EDR se houver necessidade

**3.2.2. REQUISITOS DO SERVIÇO DE SUPORTE**

3.2.2.1. O Atendimento e resolução dos chamados do suporte técnico deverá estar disponível, no mínimo, 8 (horas) horas por dia, 05 (cinco) dias por semana, durante o horário comercial, das 9:00 as 17:00, em português ou por meio de um tradutor.

3.2.2.2. A CONTRATADA deverá prestar assistência técnica durante todo o período contratual.

3.2.2.3. Deve haver Abertura ilimitada de chamados de suporte.

3.2.2.4. Não haverá limitante algum, inclusive de quantidade de horas, para o atendimento dos chamados abertos durante a vigência do contrato.

3.2.2.5. O atendimento será preferencialmente remoto. Caso haja necessidade de intervenção presencial "onsite", por qualquer motivo que impeça o atendimento remoto, independente de culpa ou responsabilidade do CREA, ou da CONTRATADA, este deverá ser executada pela CONTRATANTE.

3.2.2.6. Toda e qualquer despesa relacionadas a prestação do serviço de suporte presencial "onsite", inclusive, mas não se limitando a locomoção, estadia, alimentação e despesas trabalhistas são de responsabilidade inteira e exclusiva da CONTRATADA.

3.2.2.7. Qualquer atendimento presencial "onsite" deverá ser executado em uma das sedes do CREA na Capital de São Paulo.

3.2.2.8. Todos os atendimentos, (remotos ou locais), deverão ser executados sempre com acompanhamento e supervisão da equipe técnica da CONTRATANTE.



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.2.2.9. A CONTRATADA deverá oferecer manutenção e suporte técnico conforme o nível de severidade de cada chamado e dentro dos tempos de resposta definidos abaixo:
- 3.2.2.10. Quando um chamado for aberto pela CONTRATADA, a CONTRATANTE deverá atribuir ao chamado o nível de severidade de acordo com a avaliação do tipo do problema e do impacto/dano.
- 3.2.2.11. O CREA-SP poderá a qualquer momento, a seu próprio critério solicitar a mudança da severidade do chamado.
- 3.2.2.12. No qual deve ser prontamente atendido pela CONTRATADA, que deve passar a atendê-lo de acordo com a nova severidade.
- 3.2.2.13. A CONTRATADA deverá prestar o suporte necessário para solucionar problemas, resolver questões e dirimir quaisquer dúvidas relativas ao sistema de Anti-virus instalado, desempenhando no mínimo as seguintes atividades de Suporte:
- 3.2.2.13.1. Processamento de solicitações relacionadas ao mau funcionamento do software e atualizações regulares de banco de dados;
- 3.2.2.13.2. Processamento de solicitações relacionadas às descrições e recursos apontados no tópico Descritivo de Solicitações;
- 3.2.2.13.3. Assistência com informações de recuperação de licenças perdidas ou danificada;
- 3.2.2.13.4. Consultas sobre as dúvidas a seguir e relacionadas também aos recursos apontados no tópico
- 3.2.2.13.5. Descritivo de Solicitações:
- 3.2.2.13.6. Como e onde baixar o Software
- 3.2.2.13.7. Onde encontrar informações sobre o Software.
- 3.2.2.13.8. Relatório Mensal enviado através do CONTRATADA Help quanto a saúde do ambiente.
- 3.2.2.13.9. Envio de Book Mensal informando o total de tickets atendidos, solicitantes, fluxos, SLA, Capacity e Recomendações com base nos relatórios anteriores;
- 3.2.2.13.10. Atualização Anual da Console Kaspersky, bem como a criação da documentação "As is - To be".
- 3.2.2.13.11. Acesso Remoto em estações de trabalho (Notebook, computadores, servidores) quando necessário
- 3.2.2.13.12. Desinfecção de computadores infectados por um malware/ ransomware (incluindo a mitigação dos efeitos de tais infecções) pelos especialistas do Suporte Técnico;
- 3.2.2.13.13. Auxílio ao Usuário pelo telefone ou via bate-papo ao coletar dados para análise e/ou aplicação de recomendações;
- 3.2.2.13.14. Rol Mínimo de requisições que a CONTRATADA deverá atender

Item	Descrição	Recurso
------	-----------	---------



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

1	Configuração de Escaneamento de Arquivos: Ajustar as configurações de escaneamento para detectar e neutralizar ameaças em arquivos armazenados.	Proteção contra Ameaças ao Arquivo
2	Atualização de Assinaturas de Vírus: Garantir que as assinaturas de vírus estejam sempre atualizadas para detectar novas ameaças.	Proteção contra Ameaças ao Arquivo
3	Análise de Logs de Segurança: Revisar regularmente os logs de segurança para identificar e responder a possíveis ameaças.	Proteção contra Ameaças ao Arquivo
4	Filtragem de Spam e Phishing: Configurar filtros para bloquear e-mails de spam e phishing.	Proteção Contra Ameaças ao Correio
5	Escaneamento de Anexos de E-mail: Implementar escaneamento automático de anexos de e-mail para detectar malware.	Proteção Contra Ameaças ao Correio
6	Configuração de Filtros de URL: Bloquear acesso a sites maliciosos conhecidos.	Proteção Contra Ameaças da Web
7	Análise de Tráfego Web: Analisar o tráfego web em busca de atividades suspeitas.	Proteção Contra Ameaças da Web
8	Implementação de Políticas de Navegação Segura: Definir e aplicar políticas de navegação segura para os usuários.	Proteção Contra Ameaças da Web
9	Análise de Tráfego de Rede: Análise sobre o tráfego de Rede.	Proteção Contra Ameaças à Rede
10	Configuração de IDS/IPS: Implementar sistemas de detecção e prevenção de intrusões.	Proteção Contra Ameaças à Rede
11	Análise de Vulnerabilidades de Rede: Realizar análise para identificar e corrigir vulnerabilidades na rede.	Proteção Contra Ameaças à Rede
12	Configuração de Regras de Firewall: Definir e ajustar regras de firewall para controlar o tráfego de rede.	Firewall
13	Análise de Logs de Firewall: Revisar logs de firewall para identificar tentativas de intrusão.	Firewall
14	Atualização de Firmware do Firewall: Atualização do firmware do firewall atualizado para garantir a proteção contra novas ameaças.	Firewall
15	Configuração de Políticas de Detecção de Comportamento: Ajustar políticas para detectar comportamentos anômalos.	Detecção de Comportamento, Prevenção de Exploit e



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

		Mecanismo de Remediação
16	Implementação de Prevenção de Exploits: Configuração de mecanismos para prevenir exploits conhecidos.	Detecção de Comportamento, Prevenção de Exploit e Mecanismo de Remediação
17	Automatização de Respostas de Remediação: Configurar respostas automáticas para remediar ameaças detectadas.	Detecção de Comportamento, Prevenção de Exploit e Mecanismo de Remediação
18	Execução de Ferramentas de Limpeza: Utilização da ferramenta de limpeza para remover dados desnecessários e maliciosos.	Limpeza de Dados de um Dispositivo Windows
19	Revisão de Programas Instalados: Verificar e remover programas não autorizados ou suspeitos.	Limpeza de Dados de um Dispositivo Windows
20	Atualização do Sistema Operacional: Garantir que o sistema operacional esteja atualizado com os últimos patches de segurança.	Limpeza de Dados de um Dispositivo Windows
21	Configuração de Escaneamento Automático: Configurar o escaneamento automático de unidades removíveis ao serem conectadas.	Verificação de Unidades Removíveis na Conexão
22	Análise de Logs e Eventos: Analisar logs e eventos para identificar a causa raiz de incidentes.	Root-Cause Analysis
23	Implementação de Medidas Corretivas: Desenvolver e implementar medidas para prevenir a recorrência de incidentes.	Root-Cause Analysis
24	Análise de Tráfego de Nuvem: Analisar o tráfego de serviços em nuvem para identificar atividades suspeitas.	Cloud Discovery: Monitoramento de Serviços em Nuvem
25	Relatórios de Uso de Nuvem: Geração de relatórios sobre o uso de serviços em nuvem e possíveis riscos.	Cloud Discovery: Monitoramento de Serviços em Nuvem
26	Configuração de HIPS: Implementar e configurar sistemas de prevenção de intrusão no host.	Prevenção de Intrusão do Host
27	Monitoramento de Atividades do Host: Analisar atividades do host em busca de comportamentos suspeitos.	Prevenção de Intrusão do Host
28	Atualização de Assinaturas de Intrusão: Manter assinaturas de intrusão atualizadas para detectar novas ameaças.	Prevenção de Intrusão do Host



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

29	Definição de Políticas de Controle de Dispositivos: Estabelecer políticas para controlar o uso de dispositivos externos.	Controle de Dispositivos
30	Monitoramento de Conexões de Dispositivos: Revisar logs de conexão de dispositivos para identificar atividades não autorizadas.	Controle de Dispositivos
31	Configuração de Filtros de Conteúdo: Implementar filtros para bloquear conteúdo web inadequado ou malicioso.	Controle da Web
32	Monitoramento de Atividades Web: Analisar atividades web dos usuários para identificar comportamentos de risco.	Controle da Web
33	Relatórios de Uso da Web: Gerar relatórios sobre o uso da web e possíveis violações de políticas.	Controle da Web
34	Definição de Políticas de Controle de Aplicativos: Estabelecer políticas para controlar a instalação e uso de aplicativos.	Controle de Aplicativos
35	Monitoramento de Execução de Aplicativos: Análise de logs de execução de aplicativos para identificar atividades suspeitas.	Controle de Aplicativos
36	Avaliação de Aplicativos: Avaliar aplicativos instalados para garantir que sejam seguros e necessários.	Controle de Aplicativos

3.2.2.13.15. Atividades Não incluídas no Serviço de Suporte:

- 3.2.2.13.15.1. Desenvolvimento de novas funcionalidades do Software a pedido de um Usuário;
- 3.2.2.13.15.2. Aprimoramento do desempenho e configuração do dispositivo do Usuário;
- 3.2.2.13.15.3. Perguntas sobre aplicativos e/ou sistemas operacionais de terceiros;
- 3.2.2.13.15.4. Uso de patches de terceiros para sistemas operacionais e aplicativos para correção de vulnerabilidades;
- 3.2.2.13.15.5. Integração do Software Kaspersky com software de terceiros;
- 3.2.2.13.15.6. Configuração e verificação do desempenho do Software por especialistas do Suporte Técnico;
- 3.2.2.13.15.7. Treinamento no Software focado em usuários finais ou viés técnico;

3.2.2.13.16. Demonstração e/ou implantação do Software

3.2.3. REQUISITOS DO SERVIÇO DE MONITORAMENTO

- 3.2.3.1. A equipe da contratada deverá monitorar os casos de infecção por agentes maliciosos, realizando todas as atividades necessárias para manter aos dispositivos gerenciados e a Console do sistema livre de ameaças.

3.2.4. REQUISITOS GERAIS DO SERVIÇO DE SUSTENTAÇÃO, SUPORTE E MONITORAMENTO

- 3.2.4.1. A Empresa CONTRATADA deverá fornecer os serviços em Regime de horário comercial, das 9:00 as 18:00, de segunda a sexta-feira.



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.2.4.2. Pelo menos um membro da equipe deve fornecer o atendimento presencial na sede do CREA-SP, na avenida Brigadeiro Faria Lima, 1059, Pinheiros, São Paulo, no mínimo dois dias da semana, podendo os demais três dias serem oferecidos apenas por atendimento remoto.
- 3.2.4.3. O Serviço de sustentação está restrito ao sistema de antivírus contratado, sua console e aos dispositivos a ele conectados via agente.
- 3.2.4.4. O Ambiente tecnológico do CREA-SP que será relacionado aos serviços de sustentação do AntiVirus é composto de:
  - 3.2.4.4.1. Até 200 Servidores Windows Server.
  - 3.2.4.4.2. Até 1000 estações de trabalho Desktops com Windows 10 ou acima.
  - 3.2.4.4.3. Até 300 aparelhos celulares com sistema operacional Android.
  - 3.2.4.4.4. Até 50 aparelhos celulares com sistema operacional IOS.
  - 3.2.4.4.5. Todos os equipamentos Desktops, Servidores são interligados pela rede MPLS do CREA-SP.
  - 3.2.4.4.6. Os Celulares e Notebooks poderão estar conectados à Internet ou à rede Interna do CREA-SP.
- 3.2.4.5. **ATIVIDADES**
  - 3.2.4.5.1. A equipe da CONTRATADA deve executar todos os serviços, sob supervisão da Equipe de Infra estrutura de T.I. do CREA-SP:
  - 3.2.4.5.2. Gerenciamento de Dispositivos:
    - 3.2.4.5.2.1. Instalação/Remoção do Agente: Instalação e remoção do agente do Anti-Vírus nos dispositivos.
    - 3.2.4.5.2.2. Registro de Dispositivos: Configuração para permitir que os dispositivos se registrem no Console do AntiVirus para gerenciamento.
    - 3.2.4.5.2.3. Configuração de Perfil de Dispositivo: Definir políticas para controlar as regras de segurança pertinentes a cada dispositivo
  - 3.2.4.5.3. Monitoramento e Resolução de Problemas:
    - 3.2.4.5.3.1. Monitoramento de Dispositivos: Acompanhamento do estado de conformidade e saúde dos dispositivos gerenciados pelo Kaspersky.
    - 3.2.4.5.3.2. Resolução de Problemas Remotamente: Diagnóstico e solução de problemas relacionados ao AntiVirus em dispositivos, como reinicialização remota, atualizações de versão dos agentes e remoção de aplicativos maliciosos.
  - 3.2.4.5.4. Relatórios e Auditoria:
    - 3.2.4.5.4.1. Geração de Relatórios de Conformidade: Criação de relatórios para monitorar a conformidade dos dispositivos com as políticas de segurança e conformidade.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.2.4.5.4.2. Auditoria de Dispositivos: Revisão periódica dos registros de atividades para identificar e responder a quaisquer violações de segurança ou anomalias.
- 3.2.4.5.5. Comunicação com Usuários:
- 3.2.4.5.5.1. Gerenciamento de Endpoints por Solicitação: Entrar em contato com os usuários para adicionar, retirar ou verificar o status dos endpoints. Isso pode incluir a instalação do agente do Kaspersky em novos dispositivos, remoção de dispositivos desativados ou perdidos e verificação do status de conformidade dos dispositivos com as políticas de segurança.
- 3.2.4.5.5.2. Suporte ao Usuário: Fornecer orientação e suporte aos usuários sobre o uso correto AntiVirus, varreduras de segurança., remoção de itens maliciosos, etc;
- 3.2.4.5.5.3. Comunicação de Políticas e Procedimentos: Informar os usuários sobre as políticas de segurança e procedimentos relacionados ao uso d AntiVirus nos dispositivos corporativos, garantindo a conformidade e a conscientização dos funcionários sobre as práticas recomendadas de segurança da informação.
- 3.2.4.6. REGISTRO DAS ATIVIDADES
- 3.2.4.6.1. Todas as atividades da equipe de sustentação deverão ser registradas no sistema de ITSM do CREA-SP. Tanto as solicitações quanto as tratativas até a solução final dos problemas.
- 3.2.4.6.1.1. O CREA-SP utiliza a ferramenta de ITSM GLPI;
- 3.2.5. REQUISITOS DE ACESSO REMOTO
- 3.2.5.1. VPN – Virtual Private Network
- 3.2.5.2. O acesso remoto da equipe da CONTRATADA na infraestrutura interna do CREA-SP deverá ser feito **exclusivamente** por VPN entre o CREA-SP e a CONTRATADA e seus analistas/técnicos, e/ou presencialmente na sede Faria Lima do CREA-SP.
- 3.2.5.3. Os acessos devem ser individuais, por analista, não sendo permitidos acessos genéricos.
- 3.2.6. REQUISITOS DE NÍVEL DE SERVIÇO
- 3.2.6.1. A CONTRATADA deverá atender solicitações do tipo incidentes e do tipo requisições.
- 3.2.6.2. Os incidentes deverão ser classificados em 3 níveis de severidade:
- 3.2.6.3. A tabela abaixo traz exemplos de tipos de problemas e níveis de severidade.

Nível de Severidade	Descrição de suporte e operações
Severidade A (Crítica)	1 - Ambiente sem condições de funcionamento. 2 - Um ou mais serviços não estão acessíveis ou não podem ser usados. A produção, as operações ou as datas limite para implantação são gravemente afetadas, ou há um grave impactos obre a produção ou as atividades da instituição, ou de algum (qualquer) usuário da mesma.





**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

	3 - Um único, ou mais usuários, clientes ou serviços é afetado parcial ou totalmente. 4 - Situação que, mesmo não representando problema técnico grave, possa estar impactando na prestação do serviço do CREA-SP. Ex. Máquina do pregoeiro com problema de vírus, impedindo que seja realizado um pregão na data e hora marcados.
Severidade B (Médio)	Problema que gera restrições ao pleno funcionamento do ambiente. O serviço pode ser usado, mas com limitações. A situação tem impacto operacional moderado e é possível lidar com ela durante o horário comercial. Um único usuário, cliente ou serviço é afetado parcial ou totalmente.
Severidade C (Baixo)	Problema que não afeta o funcionamento do ambiente. A situação tem impacto operacional mínimo. O problema é importante, mas não tem impacto expressivo na produtividade e no serviço atual do cliente. Um único usuário experimenta interrupção parcial, mas existe uma solução alternativa aceitável

3.2.6.4. As requisições (solicitações que não necessariamente representam problema no ambiente) serão classificadas em 3 níveis de severidade:

3.2.6.4.1. Nível VIP - Solicitações de usuários de alta prioridade: Presidência, Superintendência, etc.

3.2.6.4.2. Nível Alto – Solicitações de um usuário ou um pequeno grupo que tenha prioridade no atendimento de sua demanda.

3.2.6.4.3. Nível Médio – Solicitações planejadas, que podem ser priorizadas pelos gestores responsáveis

3.2.6.4.4. Nível Baixo – Solicitações de baixa prioridade, que podem ser executadas durante o horário administrativo e não impactam nas atividades do cliente.

3.2.6.5. O prazo para atendimento de requisições definido para esta sustentação está descrito abaixo:

Nível	Prioridade	Tipo	Tempo de Proatividade	Tempo de Reação	Tempo Total de Atendimento (Solução)	Tempo Total	Assertividade %
VIP	0	Remoto ou Presencial	30 min	30 minutos	2 horas	3 horas	99
Alto	1		1 hora	3 horas úteis	11 horas úteis	15 horas úteis	97
Médio	2		1 hora	10 horas úteis	40 horas úteis	51 horas úteis	95



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

Baixo	3		1 hora	14 horas úteis	60 horas úteis	75 horas úteis	95
-------	---	--	--------	-------------------	-------------------	-------------------	----

**3.2.6.6. REQUISITOS DE NÍVEL DE SERVIÇO MÍNIMO (NMS)**

**3.2.6.7.** Quanto ao tempo de resposta inicial do suporte técnico, deverá ser baseado nos níveis de assertividade descritos nas tabelas de prazo de atendimento acima.

**3.2.6.8.** Assertividade é a porcentagem de chamados atendidos dentro do prazo estipulado. Mede-se fazendo o calculo: (Chamados atendidos dentro do prazo no período/ Total de chamados no período) \* 100.

**3.2.6.9.** Tempo de Proatividade refere-se ao tempo decorrente entre a solicitação e a efetivação da abertura do chamado.

**3.2.6.10.** Tempo de reação refere-se ao tempo decorrente entre a abertura do chamado e o contato entre a contratada e o analista do CREA-SP.

**3.2.6.11.** Tempo de solução é o tempo decorrido da abertura do chamado até a solução de contorno ou definitiva;

**3.2.6.12.** Solução de contorno entende-se por uma solução temporária que restaure a funcionalidade perdida de forma que os efeitos do problema não sejam mais percebidos pelos usuários.

**3.2.6.13.** Solução definitiva entende-se pela solução que sanará a causa do problema.

**3.2.6.14.** Nas situações em que for detectado e/ou comprovado um problema de software (bug) na solução ofertada, o prazo de atendimento será fornecido diretamente pela engenharia do fabricante da solução ofertada.

**3.2.6.15.** Não será aceito fechamento unilateral de qualquer chamado, por qualquer motivo, ou seja, para que algum chamado seja encerrado deverá haver a anuência do CREA-SP.

**3.2.6.16.** Chamados que dependam de ação do CREA poderão ficar em estado de pausa, em que o tempo para solução não é contado, até que o CREA execute a ação que retire de sua responsabilidade a referida dependência. Nesses Casos, todos os tempos de atendimento e pausa devem ser registrados pela CONTRATADA.

**3.2.6.17.** Os chamados abertos não poderão, em hipótese alguma, ser fechados e/ou pausados unilateralmente pela CONTRATADA sem anuência por escrito do CREA-SP.

**3.2.6.18.** Qualquer chamado que seja fechado e/ou pausado sem anuência por escrito do CREA-SP deverá ser imediatamente reaberto pela CONTRATADA, permanecendo assim até que seja dada solução, ou justificativa para o fechamento/pausa. E em quaisquer dos casos devem ser aceitos formalmente, por escrito, pelo CREA-SP.

**3.2.6.19.** A empresa contratada deverá apresentar mensalmente relatório contendo todos os chamados abertos pelo CREA-SP, os tempos de reação, tempos de atendimento, assertividade, e plano de ação para solucionar problemas recorrentes ou sem solução os quais estejam impactando no funcionamento do ambiente, resguardando o direito do CREA-SP em elaborar seus próprios relatórios de auditoria para confrontá-los ao relatório da contratada.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

**3.2.6.20. MATRIZ DE RESPONSABILIDADES**

**3.2.6.21.** A tabela a seguir apresenta os recursos diretos ligados a sustentação.

Grupo de Responsabilidade	Descrição da Responsabilidade	Empresa
<b>Gestor do CONTRATO</b>	<ul style="list-style-type: none"><li>• Ser contato com a área comercial da CONTRATADA e coordenador do <b>CREA/SP</b></li><li>• Aprovar prazos em baseline e alterações de conclusão do projeto.</li></ul>	<b>CREA/SP</b>
<b>Fiscal Técnico</b>	<ul style="list-style-type: none"><li>• Ser o contato entre o Coordenador CONTRATADA e os usuários do <b>CREA/SP</b>;</li><li>• Fornecer os documentos e listas necessárias para a continuidade dos serviços;</li><li>• Fornecer métodos de acesso a empresa para a execução dos serviços.</li></ul>	<b>CREA/SP</b>
<b>Gerente de Projetos</b>	<ul style="list-style-type: none"><li>• Estabelecer contato com o cliente e com os especialistas da CONTRATADA para demandar as atividades;</li><li>• Acordar planos e alterações do plano diretamente com o cliente;</li><li>• Fornecer documentações do ambiente.</li></ul>	<b>CONTRATADA</b>
<b>Analistas e Especialistas</b>	<ul style="list-style-type: none"><li>• Ser o contato com o coordenador do <b>CREA/SP</b> e com o coordenador CONTRATADA;</li><li>• Executar diretamente as atividades dentro do escopo;</li><li>• Executar as atividades fora do escopo, somente se autorizada pelo Cliente e pelo Gestor do Contrato;</li><li>• Fornecer relatórios de execução das atividades;</li><li>• Apresentar status de atividades não concluídas para a acompanhamento do cliente.</li></ul>	<b>CONTRATADA</b>



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

<b>Gerente de Serviços</b>	<ul style="list-style-type: none"><li>• Single Point of Contact responsável por todo o desempenho e performance operacional do serviço;</li><li>• Gerenciar o contrato de forma unificada com foco em prover os serviços contratados com excelência;</li><li>• Escalonar e comunicar ocorrências que causem perda de performance ou indisponibilidade nos serviços contratados;</li><li>• Gerir o processo de melhoria contínua de produtividade.</li></ul>	<b>CONTRATADA</b>
----------------------------	---	-------------------

**3.2.7. REQUISITOS DO SERVIÇO DE ADEQUAÇÃO DA CONSOLE DE GERENCIAMENTO**

**3.2.7.1. PASSAGEM DE CONHECIMENTO**

**3.2.7.1.1.** A CONTRATADA deverá fornecer a passagem do conhecimento relativo ao console da solução a quatro membros da equipe de Sustentação de TI do CREA. Através de workshops de instalação e operação do ambiente e do sistema de Antivírus atrelado às licenças de software atualizadas, nas versões fornecidas pela CONTRATADA.

**3.2.7.1.2.** A Contratada deverá fornecer dois workshops, em datas diferentes, sendo o primeiro para 2 pessoas, e o segundo para outras duas pessoas.

**3.2.7.1.3.** A CONTRATADA deverá fornecer essa transferência de conhecimento sobre o ambiente atualizado do CREA-SP em até 10 dias depois da finalização dos serviços de atualização do Servidor e dos Clientes.

**3.2.7.1.4.** Os serviços de transferência de conhecimento podem ser executados presencial, ou remotamente e não devem gerar nenhum ônus financeiro ao CREA-SP.

**3.2.8. REQUISITOS DO SERVIÇO DE CAPACITAÇÃO**

**3.2.8.1.** A Contratada deverá fornecer vouchers par a realização do seguinte treinamento Kaspersky.

**3.2.8.1.1.** KL002.12.1 - Kaspersky Endpoint Security and Management

**3.2.8.2.** O treinamento deverá ser fornecido por centro de treinamento autorizado da Kaspersky. Não serão aceitos cursos e/ou workshops (mesmo com o conteúdo programático idêntico) fornecidos por funcionários da empresa contratada nem que utilizem laboratórios ou recursos da mesma, ou qualquer outra forma de não utilizar os centros autorizados pela Kaspersky.



**SERVIÇO PÚBLICO FEDERAL  
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA  
DO ESTADO DE SÃO PAULO – CREA-SP**

- 3.2.8.3. O treinamento deverá ser fornecido na língua portuguesa;
- 3.2.8.4. A CONTRATADA (centro de treinamento oficial) deverá fornecer certificado de participação válido por um ano e reconhecido pela Kaspersky;
- 3.2.8.5. A Contratada deverá fornecer 5 vouchers para o treinamento individual de cinco analistas do CREA-SP;
- 3.2.8.6. Os treinamentos poderão ser realizados durante a vigência do contrato, sem data de validade pré determinada, ou prazo de expiração anterior ao da vigência contratual;
- 3.2.8.7. O conteúdo programático mínimo a ser coberto pelo treinamento está no anexo I deste Caderno Técnico: ANEXO I- Conteúdo programático Mínimo de Capacitação Kaspersky

**3.2.9. REQUISITOS GERAIS PARA A EXECUÇÃO DOS SERVIÇOS**

- 3.2.9.1. Os serviços devem:
- 3.2.9.2. Ser executados dentro dos parâmetros estabelecidos neste processo de contratação, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios, observando sempre os critérios de qualidade;
- 3.2.9.3. Adequar-se aos padrões normativos orientados pela Política de Segurança do CREA-SP;
- 3.2.9.4. Realizar os serviços de modo que não prejudiquem o andamento normal das atividades do Órgão em horário de seu expediente;
- 3.2.9.5. Implantar o planejamento, a execução e a supervisão permanente dos serviços demandados;
- 3.2.9.6. Responsabilizar-se pela definição da forma, metodologia, processos, local e modelo e execução dos serviços.

**3.2.10. REQUISITOS DE QUALIFICAÇÕES DOS PROFISSIONAIS**

- 3.2.10.1. Todos os serviços realizados pela CONTRATADA no âmbito desta CONTRATAÇÃO devem ser executados por profissionais qualificados treinados e certificados pelas fabricantes das Soluções.

**3.2.11. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE**

- 3.2.11.1. Quanto à LGPD, a CONTRATADA deverá cumprir o determinado no ANEXO C - CLÁUSULAS DE PROTEÇÃO DE DADOS PESSOAIS, NOS TERMOS DA LEI Nº 13.709/2018, anexo do Termo de Referência.



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

## **1. ANEXO I - Conteúdo programático Mínimo de Capacitação Kaspersky**

- 1.1. O treinamento deve estar atualizado no mínimo para as versões versão 14.1 do Kaspersky Security Center e versão 12.1 do Kaspersky Endpoint Security.
- 1.2. O principal objetivo deste treinamento deve ser fornecer aos participantes todo o conhecimento necessário para implementar, configurar e gerenciar a solução.
- 1.3. O curso deve ensinar como projetar, implementar e manter sistemas de proteção baseados no Kaspersky Endpoint Security e gerenciá-lo centralmente por meio do Kaspersky Security Center. Ele deve descrever produtos projetados para proteger uma rede de até 1000 terminais em um único local. Os endpoints abordados neste treinamento devem ser servidores e workstations que executam o Windows.
- 1.4. A parte teórica do curso e os laboratórios devem proporcionar aos participantes os conhecimentos e competências necessários para:
- 1.5. Descrever os recursos do Kaspersky Endpoint Security for Windows e do Kaspersky Security Center.
- 1.6. Projetar e implementar uma solução de proteção ideal baseada no Kaspersky Endpoint Security em uma rede Windows e gerenciá-la por meio do Kaspersky Security Center.
- 1.7. Manter o sistema implantado.
- 1.8. **Produtos abordados**
  - 1.8.1. Kaspersky Security Center
  - 1.8.2. Kaspersky Endpoint Security for Windows
- 1.9. **Conteúdo Programático**
  - 1.9.1. Módulo 1 – Implementação
    - 1.9.1.1. Aspectos gerais
    - 1.9.1.2. Instalação do Kaspersky Security Center
      - 1.9.1.2.1. Lab 1. Instalando o Kaspersky Security Center
    - 1.9.1.3. Implementação do Kaspersky Endpoint Security
      - 1.9.1.3.1. Lab 2. Implementando o Kaspersky Endpoint Security
    - 1.9.1.4. Trabalhando com grupos de dispositivos gerenciados
      - 1.9.1.4.1. Lab 3. Criando uma estrutura de dispositivos gerenciados
    - 1.9.1.5. Kaspersky Security Center Cloud Console
  - 1.9.2. Módulo 2 - Gerenciamento de Proteção
    - 1.9.2.1. Como o Kaspersky Endpoint Security protege os computadores
    - 1.9.2.2. Como configurar a proteção de arquivos
    - 1.9.2.3. Como configurar a proteção contra ameaças de rede
      - 1.9.2.3.1. Lab 4. Configurando a proteção de arquivos
      - 1.9.2.3.2. Lab 5. Configurando o Mail Threat Protection
      - 1.9.2.3.3. Lab 6. Testando a Web Threat Protection
    - 1.9.2.4. Como configurar a proteção contra ameaças sofisticadas
      - 1.9.2.4.1. Lab 7. Protegendo diretórios de rede contra ransomware
      - 1.9.2.4.2. Lab 8. Testando a proteção contra ameaças fileless
      - 1.9.2.4.3. Lab 9. Testando a proteção contra exploits



**SERVIÇO PÚBLICO FEDERAL**  
**CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA**  
**DO ESTADO DE SÃO PAULO – CREA-SP**

- 1.9.2.4.4. Lab 10. Configurando o Host Intrusion Prevention para proteger contra ransomware
- 1.9.2.5. Como controlar as conexões de rede
  - 1.9.2.5.1. Lab 11. Testando o Network Threat Protection
- 1.9.3. Módulo 3 – Controle
  - 1.9.3.1. Aspectos gerais
  - 1.9.3.2. Controle de aplicativos
    - 1.9.3.2.1. Lab 12. Configurando o controle de aplicativos
    - 1.9.3.2.2. Lab 13. Bloqueando inicialização de aplicativos desconhecidos na rede
  - 1.9.3.3. Controle de dispositivos
  - 1.9.3.4. Controle Web
    - 1.9.3.4.1. Lab 14. Configurando o controle de acesso web
  - 1.9.3.5. Controle adaptativo de anomalias
    - 1.9.3.5.1. Lab 15. Configurando o controle adaptativo de anomalias
- 1.9.4. Módulo 4 - Kaspersky EDR Optimum
  - 1.9.4.1. Aspectos gerais
  - 1.9.4.2. Implementação do Kaspersky EDR Optimum
  - 1.9.4.3. Resposta a incidentes:
    - 1.9.4.3.1. Lab 16. Simulando um ataque na rede corporativa
    - 1.9.4.3.2. Lab 17. Implementando o Kaspersky EDR Optimum
    - 1.9.4.3.3. Lab 18. Preparando o EDR Optimum
    - 1.9.4.3.4. Lab 19. Respondendo a um incidente
- 1.9.5. Módulo 5 – Administração
  - 1.9.5.1. Proteção do servidor de administração
  - 1.9.5.2. Backup, restauração e manutenção
  - 1.9.5.3. Configuração de políticas e tarefas Lab 20. Configurando proteção de senha
  - 1.9.5.4. Armazenamento de eventos e integração com SIEM
  - 1.9.5.5. Gestão de vulnerabilidades
  - 1.9.5.6. Monitoramento e relatórios
    - 1.9.5.6.1. Lab 21. Customizando o dashboard
    - 1.9.5.6.2. Lab 22. Configurando relatórios
  - 1.9.5.7. Checklists
  - 1.9.5.8. Contatando o suporte técnico
    - 1.9.5.8.1. Lab 23. Coletando informações de diagnóstico