ENCARTE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

Item	Descrição
6	Solução De Categorização e Inventário De Ativos
	A solução proposta deve permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo: 1.1. Serviços em execução; 1.2. Software instalado; 1.3. Usuários; 1.4. Portas abertas; 1.5. Nome do host; 1.6. FQDN; 1.7. IP v4 / v6; 1.8. Endereço MAC; 1.9. Processador; 1.10. Memória; 1.11. Volumes de disco; 1.12. BIOS. 2. A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante. 3. A solução deve normalizar automaticamente os nomes dos fabricantes de HW e SW com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução. 4. A solução deve possuir a habilidade de etiquetagem (Tags) de ativos para facilitar a identificação, deve permitir a geração de Tags, pelo menos, usando os seguintes parâmetros: 4.1. Palavras-chave; 4.2. Endereço IP e intervalos de IP; 4.3. Segmento de rede;

	4.4. Portas abertas; 4.5. Informações de inventário considerando, no mínimo: 4.5.1. Sistema operacional; 4.5.2. Presença ou ausência de determinado software instalado ou serviço em execução. 4.6. Última localização geográfica detectada incluindo cidade e país; 4.7. Groovy Scriptlet; 4.8. Regex; 4.9. Ativos com softwares autorizados, não autorizados e instalados. 5. A solução deve permitir a aplicação de Tags de forma estática, a critério do administrador da solução. 6. A solução deve permitir identificar o tipo de licenças associadas ao software instalado, classificando-as como comercial, open source e outros tipos de licenciamento. 7. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento. 8. Deve permitir criação de Dashboards personalizados que sejam capazes de trazer as seguintes informações sobre os ativos: 8.1. Categorias de softwares instalados nos ativos; 8.2. Hosts que executam máquinas virtuais; 8.3. Sistemas operacionais utilizados; 8.4. Serviços e portas TCP ou UDP abertas; 8.5. Softwares de segurança instalados; 8.6. Memória total utilizada; 8.7. Quantidade de processadores; 8.8. Quantidade de armazenamento disponível. 9. A solução deve permitir uma interface de busca de ativos que utilize uma sintaxe lógica baseados, no mínimo, nos critérios abaixo: 9.1. Fabricante de hardware; 9.2. Data de lançamento, instalação e fim de suporte do sistema operacional; 9.3. Último usuário logado;

	9.4. Categoria de software instalado; 9.5. Tipo de licenciamento de software instalado (OpenSource ou licenciado). 10. A solução deve permitir a visualização de quantidade de máquinas com um determinado software instalado.
8	Solução De Gerenciamento De Patch – Remediação De Ativos
	A solução deve permitir aplicação de patches de segurança para, no mínimo, as plataformas abaixo, no caso de plataformas que chegaram ao EOL, até o último patch disponibilizado: 1.1. Windows Embedded 7; 1.2. Windows 7; 1.3. Windows 8/8.1; 1.4. Windows 10** (1507 até 21H2); 1.5. Windows 11; 1.6. Windows Server 2022; 1.7. Red Hat Enterprise Linux 6; 1.8. Red Hat Enterprise Linux 7 até 7.9; 1.9. Red Hat Enterprise Linux 8 até 8.5; 1.10. CentOS 6 até 6.7; 1.11. CentOS 7 até 7.8; 1.12. Amazon Linux 2015.09 até 2018.03; 1.13. Amazon Linux 2 2017.03 até 2.0.2021; 1.14. Oracle Enterprise Linux 8 até 8.5; 1.15. Oracle Enterprise Linux (OEL) 6; 1.16. Oracle Enterprise Linux (OEL) 7 até 7.9. 2. A solução deve possuir um catálogo com no mínimo 35.000 patches e permitir aplicação de patches para, no mínimo, os produtos abaixo: 2.1. 7-Zip; 2.2. Acro Software CutePDF Writer;

	2.3. AdoptOpenJDK AdoptOpenJDK JDK; 2.4. AdoptOpenJDK JRE; 2.5. Adobe Acrobat; 2.6. Adobe Flash; 2.7. Adobe Reader; 2.8. Adobe Shockwave; 2.9. AIMP DevTeam AIMP; 2.10. Amazon Corretto; 2.11. Apache Software Foundation Tomcat; 2.12. Apple iCloud; 2.13. Apple iTunes; 2.14. Apple Mobile Device Support; 2.15. Apple Software Update; 2.16. Atlassian HipChat; 2.17. Sourcetree; 2.18. Audacity; 2.19. Azul Zulu JDK; 2.20. Azul Zulu JRE; 2.21. Bandicam Company Bandicut; 2.22. Blue Jeans; 2.23. Blue Jeans Outlook Addin; 2.24. Barco ClickShare; 2.25. Botkind Allway Sync; 2.26. Box Drive; 2.27. Box Edit; 2.28. Box Sync; 2.29. CDBurnerXP; 2.30. Cisco Jabber; 2.31. Cisco WebEx Teams; 2.32. Citrix GoToMeeting; 2.33. Citrix Receiver;

	2.34. Citrix Workspace App; 2.35. Code4ward.net Royal Applications; 2.36. CoreFTP; 2.37. Corel WinDVD Pro; 2.38. CrowdStrike Falcon Sensor; 2.39. dotPDN LLC Paint.NET; 2.40. Dropbox; 2.41. Evernote; 2.42. FileZilla; 2.43. Foxit PhantomPDF; 2.44. Foxit Reader; 2.45. Gimp; 2.46. GIT; 2.47. GlavSoft TightVNC; 2.48. Chrome; 2.49. Google Drive; 2.50. Google Desktop; 2.51. Google Drive File Stream; 2.52. Google Earth Pro; 2.53. Gretech GOM Player; 2.54. Inkscape; 2.55. IrfanView; 2.56. Jabra Direct; 2.57. JAM Software TreeSizeFree; 2.58. Juraj Simlovic TED Notepad; 2.59. KeePass; 2.60. LibreOffice; 2.61. Lightning ImgBurn; 2.62. LogMeIn; 2.63. Malwarebytes Anti-Malware Home; 2.64. Microsoft .Net;

	2.65. Microsoft .Net Core; 2.66. AntiXSS; 2.67. Azure Site Recovery Provider; 2.68. Azure Information Protection Client; 2.69. BizTalk Server; 2.70. Business Contact Manager; 2.71. CAPICOM; 2.72. Microsoft Commerce Server; 2.73. Microsoft Content Management Server; 2.74. Windows Defender; 2.75. Microsoft Digital Image; 2.76. DirectX; 2.77. Microsoft Dynamics; 2.78. Microsoft Edge; 2.79. Microsoft Enhanced Mitigation Experience Toolkit; 2.80. Exchange Server; 2.81. Exchange System Manager; 2.82. Microsoft Expression; 2.83. Forefront Server; 2.84. Front Page Server; 2.85. Host Integration Server; 2.86. Microsoft Identity Manager; 2.87. Internet Explorer; 2.88. Internet Information Server; 2.89. ISA Server; 2.90. Microsoft Journal Viewer; 2.91. Live Meeting; 2.92. Live Messenger; 2.93. Lync; 2.94. Lync Server; 2.95. Skype for Business Server;

	2.96. MDAC; 2.97. Microsoft Mouse and Keyboard Center; 2.98. Microsoft Step By Step Interactive Training; 2.99. Mscomctl; 2.100. MSN Messenger; 2.101. MSXML; 2.102. Office Communicator 2005; 2.103. Office Web Components XP; 2.104. Producer for PowerPoint 1.1; 2.105. Small Business Accounting 2006; 2.106. Works 6-9 Converter; 2.107. Office Communicator 2007; 2.108. Office Communications Server 2007 R2; 2.109. Office Communicator 2007 R2; 2.110. Producer for PowerPoint 2003; 2.111. Suíte Office nas versões 2000, 2002, 2003, 2007, 2010, 2013, 2016; 2.112. System Center Operations Manager; 2.113. Microsoft SQL Server nas versões 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017, 2019; 2.114. SQL Management Studio; 2.115. Microsoft Visual Studio; 2.116. Windows Server 2012, 2016, 2019; 2.117. Windows 7, 8, 8.1, 10, 11; 3. A solução deve permitir a criação de dashboards para acompanhamento de aplicação de patches. 4. Os Dashboards devem permitir inclusão de filtros personalizados para incluir, no mínimo, os requisitos abaixo: 4.1. Ativos que não possuem patches de segurança instalados; 4.2. Ativos pendente de boot para aplicação de patches; 4.3. Patches faltantes por fabricante;

	4.4. Status de aplicação de patches; 4.5. Patches faltantes por severidade. 5. A solução deve permitir mostrar em um mesmo dashboard a quantidade de ativos que possuem um software instalado e quantidade de patches relevantes a esse mesmo software. 6. A solução deve conter uma lista de produtos e softwares priorizados, permitindo visualizar patches relevantes à esses produtos. 7. A solução deve permitir a criação de tarefas de instalação a partir de produtos e softwares priorizados. 8. A solução deve oferecer uma interface que permita buscas com uma sintaxe lógica para visualizar detalhes de um patch específico. 9. As buscas devem considerar, no mínimo, os filtros abaixo: 9.1. Fabricante da aplicação ou software; 9.2. Patches que corrigem falhas de segurança; 9.3. Patches de sistema operacional ou aplicações; 9.4. Severidade do fabricante; 9.5. Número do KB ou boletim; 9.6. CVE associado. 10. A solução deve ser capaz de apresentar informações de patches que já consideram e resolvem correções anteriores. 11. A solução deve apontar fragilidades resolvidas por um determinado patch. 12. A solução deve apontar todas as versões da aplicação que são afetadas e precisam de correção. 13. A solução deve conter referências do fabricante do software ou sistema operacional contendo descrição dos patches disponíveis. 14. Deve ser possível visualizar agentes e último status de comunicação, a quantidade de patches aplicados e faltantes. 15. Deve ser possível definir o intervalo em horas para verificação de patches e reporte à console. 16. A solução deve suportar tarefas de instalação e remoção dos patches.

	17. A solução deve permitir a execução de scripts personalizados durante a tarefa de instalação de patches. 18. Deve ser possível executar scripts Powershell antes e depois da instalação de correções. 19. A solução deve permitir instalação de softwares através de scripts. 20. A tarefa de aplicação de patches deve permitir alteração de chaves de registro. 21. A tarefa de aplicação de correções deve permitir selecionar manualmente os patches a serem aplicados ou através de um filtro de seleção que considere, no mínimo, severidade do patch, fabricante, associação a uma fragilidade, associação a riscos de segurança. 22. Deve ser possível restringir a aplicação de patches à um grupo de máquinas baseados em ranges de IP, software instalado, portas abertas, serviços em execução. 23. Deve ser possível o agendamento de execução de tarefas de patch de forma imediata. 24. Deve ser possível agendar a execução de tarefas de patch em um horário específico com recorrência diária, semanal ou mensal. 25. Deve ser possível agendar a execução de tarefas de patch co agendamento a partir do Patch Tuesday, da Microsoft, de forma automática. 26. Deve ser possível configurar uma janela de tempo máximo para execução de patches em intervalo de horas ou minutos. 27. A solução deve permitir customização de mensagens para o usuário antes, durante e após a aplicação de patches. 28. Deve permitir o download de patches antes do início da tarefa, de forma a otimizar o processo de instalação. 29. A solução deve permitir a supressão do reinício do sistema operacional, forçá-la ou permitir que o usuário reinicie o sistema, caso o patch aplicado exija o reinício.

	30. Deve ser possível restringir o licenciamento a um determinado grupo de máquinas baseado em critérios como sistema operacional, presença de softwares instalados e ranges de IPs. 31. A solução deve conter a inteligência de filtrar automaticamente, sem intervenção, quais ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e a pré-existência de determinada aplicação, evitando assim instalações indesejadas. 32. Deve ser possível gerar relatórios a partir do catálogo de patches a serem aplicados considerando filtros dos patches e dos ativos. 33. O catálogo de patches a serem aplicados deve filtrar de forma simples quais são os patches que precisam ser instalados e exibir somente as últimas versões disponíveis de cada um deles, considerando a obsolescência de versões antigas. 34. Deve ser possível visualizar, pela interface, o status de instalação de cada uma das tarefas de patch criadas. 35. O status individual de cada tarefa de patch deve mostrar quais patches foram instalados com sucesso, os que falharam e quais não foram instalados por não serem necessários. 36. A solução deve exibir, para os patches que não foram instalados com sucesso, qual omotivo do erro. 37. Deve ser possível gerar um relatório CSV para uma tarefa de patch específica, com a finalidade de validar seu progresso e situação final de execução. 38. A solução deve possuir controle de acesso no modelo Role Based Access Control, para que sejam definidos no mínimo dois perfis de usuários caso seja necessário, sendo um deles, necessariamente, incapaz de iniciar uma tarefa de execução de patch. 39. A solução deve possuir uma interface de API para permitir automatização de ativadas com no mínimo as seguintes funções: 39.1. Criação de tarefa de patch; 39.2. Listagem de ativos;

	39.3. Listagem de patches; 39.4. Listagem de tarefas de patch.
9	Solução De Gerenciamento De Vulnerabilidades
	A solução deve permitir varreduras com base em: a. Sistemas Operacionais b. Serviços WEB c. Portas TCP e UDP d. Serviços e. Aplicações f. Bancos de dados g. Dispositivos de rede como switches, roteadores e balanceadores de carga 2. No mínimo, a ferramenta deve abranger os seguintes sistemas operacionais, bancos de dados e aplicativos. a. Microsoft Windows b. UNIX c. LINUX d. MacOS e. Mac OS X f. Cisco g. Vmware h. FortiOS 3. Detectar e analisar fragilidades nas principais versões de Bancos de Dados, pelo menos: a. Microsoft SQL Server b. MySQL c. Oracle

	d. Sybase 4. Detectar e analisar fragilidades em plataformas WEB, pelo menos: a. IIS b. Apache Tomcat 5. Detectar e analisar fragilidades em portas e serviços TCP e UDP. 6. Detectar fragilidades em pelo menos os seguintes aplicativos ou plataformas: a. Adobe b. Apple c. HP d. McAfee e. Microsoft (Office, IIS, Exchange) f. Oracle g. Oracle Java h. VMware 7. Permitir a descoberta de fragilidades na rede, oferecendo as seguintes alternativas de varredura: a. Varredura ativa de rede não autenticada b. Varredura ativa de rede autenticada c. Agente d. Varreduras externas 8. A base de conhecimento de fragilidade deve ser atualizada semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve ter pelo menos uma base de conhecimento de 35.000 CVEs relacionados incluindo tecnologias legadas e atuais. 9. A solução deve oferecer suporte ao padrão da indústria para pontuação de fragilidade do Common Vulnerability Scoring System (CVSS). 10. A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL).

	11. A solução deve permitir vincular as fragilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware. 12. A solução deve ser capaz de indicar explorações disponíveis e códigos disponíveis para uma fragilidade, quando aplicável. 13. O banco de dados deve relacionar a maioria das fragilidades ao CVE e Bugtraq. 14. A solução deve oferecer suporte à integração para autenticação por ferramentas de cofres de senha com ao menos duas dos seguintes fabricantes, Thycotic/Centrify, CyberArk, BeyondTrust. 15. A solução deve permitir buscas interativas de fragilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS, CVE ou KB. 16. A solução deve permitir a utilização de operadores lógicos na busca de fragilidades para que seja possível encontrar, no mínimo, as seguintes informações: 17. Fragilidades associadas a ransomware e que possuem patches disponíveis a. Fragilidades detectadas em um segmento de rede b. Fragilidades detectadas em serviços específicos c. Fragilidades detectadas por um usuário específico d. Fragilidades detectadas por tag AWS ou Azure específicas e. Vulnerabildiades detectadas em hardware específico 18. Na busca de fragilidades deve permitir agrupamento para mostrar, no mínimo, as seguintes visualizações: f. Quantidade de ocorrências de uma mesma fragilidade g. Quantidade de fragilidades por sistema operacional h. Quantidade de fragilidades por host i. Quantidade de fragilidades por Exploit disponível j. Quantidade de fragilidades por produto/software vulnerável

	19. A solução deve permitir exportar buscas e filtros criados para um dashboard. 20. A solução deve permitir salvar filtros criados em buscas para reutilização. 21. Deve mostrar dashboards que consigam mostrar variação histórica de fragilidades novas, corrigidas, reabertas. 22. Deve permitir mostrar dashboards que contenham quantidades de fragilidades associadas a ramsonware, que contém exploits públicos e que permitem exploração sem autenticação. 23. Deve mostrar dashboards que mostrem o racional de fragilidades que podem ser corrigidas através de patches. 24. Deve mostrar patches faltantes em sistemas operacionais independente da relação com uma fragilidade existente. 25. A solução deve oferecer a possibilidade de monitorar dispositivos móveis Android, IOS, IpadOS.
7	Solução De Detecção E Resposta E Proteção Contra Malware
	32. A solução deve permitir detecções e bloqueio de ataques incluindo malwares, ataques sem arquivo (Fileless), phishing, roubo de credenciais, entre outros. 33. Deverá permitir varreduras em tempo real e agendadas. 34. Para varreduras em tempo real, deverá permitir pelo menos as ações abaixo: e. Negar acesso ao arquivo infectado; f. Limpar o arquivo infectado; g. Deletar o arquivo infectado. 35. Deverá permitir a inspeção de arquivos comprimidos para varredura em tempo real. 36. Deve manter uma cópia de quarenta de arquivos detectados. 37. Deverá permitir agendamento de varreduras em disco, com agendamento pré-definido.

	38. Deverá permitir exclusões com base em informações de detecção para pelo menos,arquivos e pastas, processos detectados, endereços IP e domínios envolvidos em um evento de detecção. 39. Deverá conter mecanismos específicos para proteção de ataques de rede, sendo capaz de detectar, pelo menos os seguintes comportamentos: h. Acesso inicial; i. Roubo de credenciais; j. Movimentação lateral; k. Ações de descoberta com finalidade maliciosa. 40. Deverá analisar o tráfego de rede dos equipamentos incluindo inspeção SSL. 41. Deverá permitir aplicação de políticas diferentes para equipamentos que estejam fora da rede interna. 42. Deve ser possível configurar alertas locais para detecção de malwares ou atividades suspeitas. 43. Deve ser possível proteger contra alteração de configurações locais através de definição de senha. 44. Os eventos gerados devem ser enviados a console centralizada da solução. 45. Deve ser possível limitar o consumo de CPU. 46. Deve ser possível pesquisar os incidentes gerados a partir da console de gerenciamento. 47. Cada incidente deve conter, no mínimo as seguintes informações: l. Nome da ameaça; m. Nome do arquivo; n. Caminho do arquivo; o. Ação realizada; p. Hash SHA 256; q. Fragilidades associadas; r. Permitir pesquisar pela presença de fragilidades associadas. 48. A solução deve agrupar eventos relacionados a uma mesma ameaça, permitindo uma investigação assertiva.

	49. Deverá mostrar o processo responsável pela execução de uma ameaça. 50. A console deverá prover uma interface para pesquisa rápida de incidentes. 51. Deve suportar ao menos as pesquisas abaixo para incidentes encontrados: s. Táticas e técnicas do MITRE ATT&CK e ativo específico; t. Incidente de detecção de arquivos no último mês; u. Agrupar incidentes por nível de risco e categoria de malware específica; v. Detecções de um sistema operacional específico. 52. RELATÓRIOS E DASHBOARDS: 53. A solução deve conter painéis que exibam, no mínimo, as seguintes informações: a. Ativos com anti-malware habilitado; b. Ativos sem proteção instalada; c. Agrupar em tabela quantidade de incidentes por ativo; d. Agrupar em gráfico incidentes separados por tipo de malware; e. Detecções separadas por tática e técnica do MITRE ATT&CK; f. Gráfico em linha mostrando detecções por dia nos últimos 30 dias; g. Quantidade de conexões de rede de endpoints para uma determinada porta. 54. A solução deve permitir a customização dos painéis fazendo uso de qualquer um dos dados disponíveis associados aos ativos protegidos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre incidentes. 55. A solução deve fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução. 56. Deve ser possível criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo. 57. Deve permitir a criação de um painel que mostre quantidade de softwares instalados nos ativos protegidos. 58. A solução deve conter painéis previamente criados que possam ser importados pelos administradores.
10	Solução De Verificação E Scan De Aplicações Web

	1. A solução proposta deve habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem. 2. A solução deve permitir varreduras autenticadas, complexas e progressivas. 3. A solução deve suportar varreduras programadas de serviços SOAP e REST API. 4. A solução deve deve contar com uma API e integração com Jenkins para automação em um ambiente de CI / CD. 5. A solução deve detectar, identificar, avaliar, rastrear os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e configurações incorretas, também ameaças de WASC, fragilidades CWE e CVEs associados em aplicações da web. 6. A solução deve suportar a capacidade de re-testar uma fragilidade específica que foi detectada anteriormente na aplicação web. 7. A solução deve ter capacidade de encontrar aplicações web aprovadas e não aprovados em sua rede, gerando um processo contínuo de catalogação e descoberta de aplicações web. 8. A solução deve gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados. 9. A solução deve permitir que se faça a varredura de grandes aplicações da web usandoum mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez. 10. A solução deve definir a hora exata de início e duração das verificações. 11. A solução deve permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente. 12. A solução deve permitir integração nativa com uma das seguintes ferramentas de WAF: F5, Fortinet, Imperva, Citrix NetScaler.

	13. A solução deve consolidar os dados de varredura automatizada da solução com dados de ferramentas que permitem a avaliação manual de fragilidades por meio do Burp Suite e Bugcrowd, para uma visão unificada de fragilidades de aplicações web detectadas automática e manualmente. 14. A solução deve fornecer relatórios resumidos e de varredura do site que podem ser exportados para os formatos HTML e PDF. 15. A solução deve oferecer suporte à criação de escopos e funções definidos pelo usuário e permitir que as permissões apropriadas sejam atribuídas a cada função. 16. São listados na tabela abaixo as modalidades de licenciamento previstas para este item. A inclusão dos variados quantitativos de licenciamento, foi realizada prevendo diferentes quantidades de dispositivos controlados para atender os diversos cenários institucionais, permitindo assim o atendimento de todos esses cenários.
1	Serviço De Implementação Categorização E Inventário De Ativos
	A CONTRATADA será responsável pela implementação das ferramentas descritas nos Item 6. 2. O serviço de implementação para o item 6 segue variadas versões de pacotes de implementação, prevendo diferentes quantidades de dispositivos controlados e visa atender os diversos cenários institucionais permitindo assim o atendimento de todos esses cenários. Sendo o serviço de implementação atrelado ao seguinte quantitativo: Item Quantidade 1 Pacote de implementação para 500 ativos 3. FASES: a. Avaliação de Pré-implementação: i. A CONTRATADA deve prover um especialista com certificação nas ferramentas ofertadas a CONTRATANTE, sendo necessária comprovação técnica delas. ii. O especialista da CONTRATADA analisará os requisitos da

	CONTRATANTE e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. b. Cronograma do plano de implementação: i. Reunião de alinhamento inicial, em conjunto com o Consultor Técnico de Cibersegurança da CONTRATADA, com as áreas internas da CONTRATANTE para estabelecimento de metas, cronogramas e prazos médios; ii. Após a avaliação, o especialista da CONTRATADA designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. iii. Não faz parte do escopo: 1. Avaliação referente a processos e adequações internas de utilização da ferramenta; c. Execução: i. A implementação deverá ser realizada de acordo com o plano aceito pela CONTRATANTE anteriormente, este baseado nas melhores práticas recomendadas pelo FABRICANTE. ii. A implementação será realizada de maneira Remota, sendo de responsabilidade da CONTRATANTE disponibilizar os acessos necessários a equipe técnica da CONTRATADA. iii. Será de responsabilidade da CONTRATADA definir o meio de implementação da ferramenta mais eficaz para o ambiente de acordo com a necessidade da CONTRATANTE, podendo esta ser realizada por agente ou por scanners. Devendo a CONTRATANTE designar equipe técnica que possa auxiliar em qualquer demanda referente ao processo de deploy.

	iv. Para fins de eficiência o planejamento inicial deve ser executado considerando uma margem máxima de 5% de atraso, seja da CONTRATANTE ou da CONTRATADA. Caso ocorram atrasos de maior proporção, este contrato poderá ser renegociado entre as partes. d. Relatório de Implementação: i. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à CONTRATANTE uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h e 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. A CONTRATADA, depois de concluído o serviço de configuração da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE, período este não excedente a 48 horas. 6. Após a reunião final de Go-live, o suporte, bem como abertura de chamados e sustentação relacionados a ferramenta é de responsabilidade da CONTRATANTE e do FABRICANTE.
2	Serviço De Implementação De Gerenciamento De Patch – Remediaçao De Ativos

	A CONTRATADA será responsável pela implementação das ferramentas descritas nos Item 8. 2. O serviço de implementação para o item 8 segue variadas versões de pacotes de implementação, prevendo diferentes quantidades de dispositivos controlados e visa atender os diversos cenários institucionais permitindo assim o atendimento de todos esses cenários. Sendo o serviço de implementação atrelado ao seguinte quantitativo: Item Quantidade 1 Pacote de implementação para 500 ativos 3. FASES: a. Avaliação de Pré-implementação: i. A CONTRATADA deve prover um especialista com certificação nas ferramentas ofertadas a CONTRATANTE, sendo necessária comprovação técnica delas. ii. O especialista da CONTRATADA analisará os requisitos da CONTRATANTE e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. b. Cronograma do plano de implementação: i. Reunião de alinhamento inicial, em conjunto com o Consultor Técnico de Cibersegurança da CONTRATADA, com as áreas internas da CONTRATANTE para estabelecimento de metas, cronogramas e prazos médios; ii. Após a avaliação, o especialista da CONTRATADA designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.

	iii. Não faz parte do escopo: 1. Avaliação referente a processos e adequações internas de utilização da ferramenta; c. Execução: i. A implementação deverá ser realizada de acordo com o plano aceito pela CONTRATANTE anteriormente, este baseado nas melhores práticas recomendadas pelo FABRICANTE. ii. A implementação será realizada de maneira Remota, sendo de responsabilidade da CONTRATANTE disponibilizar os acessos necessários a equipe técnica da CONTRATADA. iii. Será de responsabilidade da CONTRATADA definir o meio de implementação da ferramenta mais eficaz para o ambiente de acordo com a necessidade da CONTRATANTE, sendo esta realizada através de implementação de agentes. Devendo a CONTRATANTE designar equipe técnica que possa auxiliar em qualquer demanda referente ao processo de deploy. iv. Para fins de eficiência o planejamento inicial deve ser executado considerando uma margem máxima de 5% de atraso, seja da CONTRATANTE ou da CONTRATADA. Caso ocorram atrasos de maior proporção, este contrato poderá ser renegociado entre as partes. d. Relatório de Implementação: i. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à CONTRATANTE uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados.

	4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h e 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas. nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. A CONTRATADA, depois de concluído o serviço de configuração da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE, período este não excedente a 48 horas. 6. Após a reunião final de Go-live, o suporte, bem como abertura de chamados e sustentação relacionados a ferramenta é de responsabilidade da CONTRATANTE e do FABRICANTE.
4	Serviço De Implementação De Solução De Gerenciamento De Vulnerabilidades
	A CONTRATADA será responsável pela Implementação das ferramentas descritas no Item 9. 2. O serviço de implementação para o item 9 segue variadas versões de pacotes de implementação, prevendo diferentes quantidades de dispositivos controlados e visa atender os diversos cenários institucionais permitindo assim o atendimento de todos esses cenários. Sendo o serviço de implementação atrelado ao seguinte quantitativo: Item Quantidade 1 Pacote de implementação para 500 ativos FASES: a. Avaliação de Pré-implementação:

	i. A CONTRATADA deve prover um especialista com certificação nas ferramentas ofertadas a CONTRATANTE, sendo necessária comprovação técnica delas. ii. O especialista da CONTRATADA analisará os requisitos da CONTRATANTE e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. b. Cronograma do plano de implementação: i. Reunião de alinhamento inicial, em conjunto com o Consultor Técnico de Cibersegurança da CONTRATADA, com as áreas internas da CONTRATANTE para estabelecimento de metas, cronogramas e prazos médios; ii. Após a avaliação, o especialista da CONTRATADA designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. iii. Não faz parte do escopo: 1. Avaliação referente a processos e adequações internas de utilização da ferramenta; c. Execução: i. A implementação deverá ser realizada de acordo com o plano aceito pela CONTRATANTE anteriormente, este baseado nas melhores práticas recomendadas pelo FABRICANTE. ii. A implementação será realizada de maneira Remota, sendo de responsabilidade da CONTRATANTE disponibilizar os acessos necessários a equipe técnica da CONTRATADA. iii. Será de responsabilidade da CONTRATADA definir o meio de implementação da ferramenta mais eficaz para o ambiente de acordo

	com a necessidade da CONTRATANTE, podendo esta ser realizada por agente ou por scanners. Devendo a CONTRATANTE designar equipe técnica que possa auxiliar em qualquer demanda referente ao processo de deploy. iv. Para fins de eficiência o planejamento inicial deve ser executado considerando uma margem máxima de 5% de atraso, seja da CONTRATANTE ou da CONTRATADA. Caso ocorram atrasos de maior proporção, este contrato poderá ser renegociado entre as partes. d. Relatório de Implementação: i. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à CONTRATANTE uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h e 17h, de segunda à sexta-feira, devendo eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. A CONTRATADA, depois de concluído o serviço de configuração da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE, período este não excedente a 48 horas. 6. Após a reunião final de Go-live, o suporte, bem como abertura de chamados e sustentação relacionados a ferramenta é de responsabilidade da CONTRATANTE e do FABRICANTE.

3	Serviço De Implementação De Solução De Detecção E Resposta E Proteção Contra Malware
	A CONTRATADA será responsável pela Implementação das ferramentas descritas nos Item 7. 2. O serviço de implementação para o item 7 segue variadas versões de pacotes de implementação, prevendo diferentes quantidades de dispositivos controlados e visa atender os diversos cenários institucionais permitindo assim o atendimento de todos esses cenários. Sendo o serviço de implementação atrelado ao seguinte quantitativo: 3. Item Quantidade 1 Pacote de implementação para 500 ativos FASES: a. Avaliação de Pré-implementação: i. A CONTRATADA deve prover um especialista com certificação nas ferramentas ofertadas a CONTRATANTE, sendo necessária comprovação técnica delas. ii. O especialista da CONTRATADA analisará os requisitos da CONTRATANTE e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. b. Cronograma do plano de implementação: i. Reunião de alinhamento inicial, em conjunto com o Consultor Técnico de Cibersegurança da CONTRATADA, com as áreas internas da CONTRATANTE para estabelecimento de metas, cronogramas e prazos médios; ii. Após a avaliação, o especialista da CONTRATADA designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos

	requisitos. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. iii. Não faz parte do escopo: 1. Avaliação referente a processos e adequações internas de utilização da ferramenta; c. Execução: i. A implementação deverá ser realizada de acordo com o plano aceito pela CONTRATANTE anteriormente, este baseado nas melhores práticas recomendadas pelo FABRICANTE. ii. A implementação será realizada de maneira Remota, sendo de responsabilidade da CONTRATANTE disponibilizar os acessos necessários a equipe técnica da CONTRATADA. iii. Será de responsabilidade da CONTRATADA definir o meio de implementação da ferramenta mais eficaz para o ambiente de acordo com a necessidade da CONTRATANTE, sendo esta implementada através da instalação de agentes. Devendo a CONTRATANTE designar equipe técnica que possa auxiliar em qualquer demanda referente ao processo de deploy. iv. Para fins de eficiência o planejamento inicial deve ser executado considerando uma margem máxima de 5% de atraso, seja da CONTRATANTE ou da CONTRATADA. Caso ocorram atrasos de maior proporção, este contrato poderá ser renegociado entre as partes. d. Relatório de Implementação: i. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à CONTRATANTE uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados.

	5. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h e 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 6. A CONTRATADA, depois de concluído o serviço de configuração da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE, período este não excedente a 48 horas. 7. Após a reunião final de Go-live, o suporte, bem como abertura de chamados e sustentação relacionados a ferramenta é de responsabilidade da CONTRATANTE e do FABRICANTE.
5	Serviço De Implementação De Solução De Verificação E Scan De Aplicações Web
	A CONTRATADA será responsável pela Implementação das ferramentas descritas nos Item 10. 2. O serviço de implementação para o item 10 segue variadas versões de pacotes de implementação, prevendo diferentes quantidades de dispositivos controlados e visa atender os diversos cenários institucionais permitindo assim o atendimento de todos esses cenários. Sendo o serviço de implementação atrelado ao seguinte quantitativo: Item Quantidade 1 Pacote de Implementação de 10 Url’s

FASES:

a. Avaliação de Pré-implementação:

i. A CONTRATADA deve prover um especialista com certificação nas ferramentas ofertadas a CONTRATANTE, sendo necessária comprovação técnica delas.

ii. O especialista da CONTRATADA analisará os requisitos da CONTRATANTE e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas.

b. Cronograma do plano de implementação:

i. Reunião de alinhamento inicial, em conjunto com o Consultor Técnico de Cibersegurança da CONTRATADA, com as áreas internas da CONTRATANTE para estabelecimento de metas, cronogramas e prazos médios;

ii. Após a avaliação, o especialista da CONTRATADA designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.

iii. A CONTRATANTE será a responsável por definir no escopo inicial as URL's a serem monitoradas pela ferramenta.

iv. Não faz parte do escopo:

1. Avaliação referente a processos e adequações internas de utilização da ferramenta;

c. Execução:

i. A implementação deverá ser realizada de acordo com o plano aceito pela CONTRATANTE anteriormente, este baseado nas melhores práticas recomendadas pelo FABRICANTE.

	ii. A implementação será realizada de maneira Remota, sendo de responsabilidade da CONTRATANTE disponibilizar os acessos necessários a equipe técnica da CONTRATADA. iii. Será de responsabilidade da CONTRATADA definir o meio de implementação da ferramenta mais eficaz para o ambiente de acordo com a necessidade da CONTRATANTE, operando esta ferramenta por scanners. Devendo a CONTRATANTE designar equipe técnica que possa auxiliar em qualquer demanda referente ao processo de deploy. iv. Para fins de eficiência o planejamento inicial deve ser executado considerando uma margem máxima de 5% de atraso, seja da CONTRATANTE ou da CONTRATADA. Caso ocorram atrasos de maior proporção, este contrato poderá ser renegociado entre as partes. d. Relatório de Implementação: i. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à CONTRATANTE uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 4. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h e 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas estes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 5. A CONTRATADA, depois de concluído o serviço de configuração da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela

	CONTRATANTE, período este não excedente a 48 horas. 6. Após a reunião final de Go-live, o suporte, bem como abertura de chamados e sustentação relacionados a ferramenta é de responsabilidade da CONTRATANTE e do FABRICANTE

F0054 - ENCARTE DO TERMO DE REFERÊNCIA Nº 14/2023 - SETI (10.53)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 28/11/2023 09:35)
CASSIANO CARLOS ZANUZZO
SECRETARIO
SETI (10.53)
Matrícula: ###096#1

(Assinado digitalmente em 28/11/2023 11:20)
EDIVANDRO LUIZ TECCHIO
PRO-REITOR
PROAD (10.46)
Matrícula: ###223#8

(Assinado digitalmente em 28/11/2023 09:07)
FLAVIO HUMBERTO TESTA
ANALISTA DE TEC DA INFORMACAO
DITI (10.53.05)
Matrícula: ###882#4

(Assinado digitalmente em 28/11/2023 11:04)
JONES JEFERSON MUNERON
DIRETOR
DITI (10.53.05)
Matrícula: ###162#7

(Assinado digitalmente em 28/11/2023 09:09)
MARCOS EUGENIO DIETRICH
TEC DE TECNOLOGIA DA INFORMACAO
DRT (10.53.05.02)
Matrícula: ###269#8