02070.005297/2021-34
Número Sei:9568956

INTEGRA+
Programa de Integridade do ICMBio

ICMBio
INSTITUTO CHICO MENDES
MMA

MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

EQSW 103/104, Bloco C, Complexo Administrativo, - Bairro Sudoeste - Brasília - CEP 70670350
Telefone: (61) 2028-9666

ESPECIFICAÇÕES TÉCNICAS

ANEXO - I

(Termo de Referência COTEC - 9538814)

1. IDENTIFICAÇÃO DO PROCESSO

1.1. O presente processo tem como objeto o detalhamento das especificações técnicas dos itens constantes do registro de preços para a contratação de expansão da solução integradora de Firewall NEXT GENERATION composta de hardware e software de segurança da informação do tipo UTM (Unified Threat Management), para interligar de forma segura, a rede central do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio) a suas Unidades Descentralizadas.

1.2. Desta forma, estas especificações técnicas são parte integrante do Termo de Referência COTEC (9538814), devendo, portanto, que todas as exigências constantes deste documento sejam consideradas como requisitos mínimos para cada item a ser fornecido.

1.3. Uma vez que trata-se de requisitos mínimos, resta verificado que poderão ser aceitos equipamentos com configurações superiores, desde que atendam todos os requisitos mínimos exigidos para cada item.

2. COMPOSIÇÃO DOS ITENS DO PREGÃO

COMPOSIÇÃO DA SOLUÇÃO				
LOTE	**ITEM**	**DESCRIÇÃO**	**UNIDADE**	**QUANT.**
01	**01**	Módulo de segurança tipo 01 (compatibilidade do Appliance - redes com até 30 usuários)	UN.	40
	02	Módulo de segurança tipo 02 (compatibilidade do Appliance - redes de 30 até 70 usuários)	UN.	100
	03	Módulo de segurança tipo 03 (compatibilidade do Appliance - redes de 70 até 150 usuários)	UN.	50
	04	Módulo de segurança tipo 04 (compatibilidade do Appliance - redes acima de 150 usuários)	UN.	10
	05	Upgrade de Licenciamento Security Management R80 - Módulo de gerenciamento de até 200 firewalls	UN.	1
	06	Log Server Dedicado R80 - Licenciamento para implementação de serviço de armazenamento de logs dedicado	UN.	1
02	**07**	Nobreak Senoidal 1,5kva	UN.	200

3. ESPECIFICAÇÕES TÉCNICAS DO LOTE 01

3.1. ESPECIFICAÇÕES TÉCNICAS GERAIS PARA O LOTE 01

3.1.1. A solução deverá ser composta de hardware e software licenciado do mesmo fabricante;

3.1.2. Tendo em vista o fato de que o projeto trata-se de expansão de solução de segurança, onde os equipamentos e softwares fornecidos serão gerenciados de forma centralizada, todos os itens deverão ser totalmente compatíveis com o módulo de gerenciamento do ICMBio (Security Management R80) devendo:

3.1.2.1. possuir recurso automatizado de atualização de políticas por meio de consulta ao módulo de gerência centralizado;

3.1.2.2. possuir recurso para disponibilização de logs em Log Server Dedicado;

3.1.2.3. ser compatível com serviço SNMP;

3.1.2.4. garantir comunicação entre os appliances de segurança e o módulo de gerência através de meio criptografado.

3.1.3. Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

3.2. **ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 01 - MÓDULO DE SEGURANÇA TIPO 01**

3.2.1. Desempenho requerido de Next Generation Firewall: 600 Mbps.

3.2.2. Desempenho requerido de Threat Prevention: 340 Mbps.

3.2.3. Desempenho requerido de VPN: 950 Mbps.

3.2.4. Desempenho requerido de IPS: 650 Mbps.

3.2.5. Deverá suportar 10.000 novas conexões por segundo.

3.2.6. Deverá suportar 500.000 conexões simultâneas.

3.2.7. Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

3.2.8. Deverá suportar Policy-based routing.

3.2.9. Deverá possuir pelo menos 5 (cinco) interfaces 10/100/1000Base-T RJ-45.

3.2.10. Deverá possuir 1 (uma) interface USB.

3.2.11. Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

3.2.12. Deverá suportar modem 3G/4G.

3.2.13. Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

3.3. **ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 02 - MÓDULO DE SEGURANÇA TIPO 02**

3.3.1. Desempenho requerido de Next Generation Firewall: 800 Mbps.

3.3.2. Desempenho requerido de Threat Prevention: 450 Mbps.

3.3.3. Desempenho requerido de VPN: 1.2 Gbps.

3.3.4. Desempenho requerido de IPS: 850 Mbps.

3.3.5. Deverá suportar 14.000 novas conexões por segundo.

3.3.6. Deverá suportar 500.000 conexões simultâneas.

3.3.7. Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

3.3.8. Deverá suportar Policy-based routing.

3.3.9. Deverá possuir pelo menos 5 (cinco) interfaces 10/100/1000Base-T RJ-45.

3.3.10. Deverá possuir 1 (uma) interface USB.

3.3.11. Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

3.3.12. Deverá suportar modem 3G/4G.

3.3.13. Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

3.4. **ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 03 - MÓDULO DE SEGURANÇA TIPO 03**

3.4.1. Desempenho requerido de Next Generation Firewall: 950 Mbps.

3.4.2. Desempenho requerido de Threat Prevention: 500 Mbps.

3.4.3. Desempenho requerido de VPN: 1.8 Gbps.

3.4.4. Desempenho requerido de IPS: 1 Gbps.

3.4.5. Deverá suportar 15.000 novas conexões por segundo.

3.4.6. Deverá suportar 500.000 conexões simultâneas.

3.4.7. Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

3.4.8. Deverá suportar Policy-based routing.

3.4.9. Deverá possuir pelo menos 8 (oito) interfaces 10/100/1000Base-T RJ-45.

3.4.10. Deverá possuir 1 (uma) interface USB.

3.4.11. Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

3.4.12. Deverá possuir 1 (uma) interface dedicada para DMZ sendo do tipo RJ45 ou Fibra.

3.4.13. Deverá suportar modem 3G/4G.

3.4.14. Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

3.5. **ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 04 - MÓDULO DE SEGURANÇA TIPO 04**

3.5.1. Desempenho requerido de Next Generation Firewall: 3.0 Gbps.

3.5.2. Desempenho requerido de Threat Prevention: 1.5 Gbps.

3.5.3. Desempenho requerido de VPN: 3 Gbps.

3.5.4. Desempenho requerido de IPS: 3.2 Gbps.

3.5.5. Deverá suportar 50.000 novas conexões por segundo.

3.5.6. Deverá suportar 2.200.000 conexões simultâneas.

3.5.7. Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

3.5.8. Deverá suportar Policy-based routing.

3.5.9. Deverá possuir pelo menos 16 (dezesseis) interfaces 10/100/1000Base-T RJ-45.

3.5.10. Deverá possuir 1 (uma) interface dedicada para DMZ sendo do tipo RJ45 ou Fibra.

3.5.11. Deverá possuir 1 (uma) interface dedicada para WAN sendo do tipo RJ45 ou Fibra.

3.5.12. Deverá possuir 1 (uma) interface USB.

3.5.13. Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

3.5.14. Deverá possuir 1 (uma) interface DSL.

3.5.15. Deverá suportar modem 3G/4G.

3.5.16. Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

3.6. **ESPECIFICAÇÕES TÉCNICAS MÍNIMAS EXIGIDAS PARA OS ITENS 01, 02, 03 E 04 - (MÓDULOS DE SEGURANÇA)**

3.6.1. **Funcionalidade de Firewall**

3.6.1.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

3.6.1.2. O hardware e o software que executam as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

3.6.1.3. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

3.6.1.4. Realizar upgrade via interface WEB;

3.6.1.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: suporte a, no mínimo, VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, DHCP Relay, DHCP Server;

3.6.1.6. Deve suportar os seguintes tipos de NAT: Nat dinâmico (Many-to-1), NAT estático (1-to-1), NAT de Origem, NAT de Destino;

3.6.1.7. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

3.6.1.8. A solução deve possuir aplicativo para Smartphones da própria solução para integrar ao dispositivo remoto e criar visibilidade e monitoramento das principais ameaças, conectividade e também receber notificações de ameaças ou qualquer outra falha no gateway de segurança;

3.6.1.9. Enviar logs para sistemas de monitoramento externos, simultaneamente;

3.6.1.10. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

3.6.1.11. A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos:

a) transparente;

b) mode sniffer (monitoramento e análise o tráfego de rede);

c) camada 2 (L2); e

d) camada 3 (L3).

3.6.1.12. A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

3.6.2. **Funcionalidade de IPS**

3.6.2.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

3.6.2.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance.

3.6.2.3. Para os appliances em plantas sem conexão a Internet deve ser possível realizar a atualização manual importando o pacote de atualização.

3.6.2.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta a scanning de portas CIFS, Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS-SQLServer, IKE aggressive Exchange;

3.6.2.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

3.6.2.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

3.6.2.7. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

3.6.2.8. A solução deverá possuir dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

3.6.2.9. Em cada proteção de segurança, deve estar incluso informações como: categoria, tipo de impacto na ferramenta, severidade e tipo de ação que a mesma irá executar;

3.6.2.10. A solução de IPS deve incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas;

3.6.2.11. Deve ser possível criar regras de exceção no IPS para que a engine não faça a inspeção de um tráfego específico por proteção, origem, destino, serviço ou porta;

3.6.2.12. Deve ser possível visualizar a lista de proteções disponíveis no appliance com os detalhes.

3.6.3. **Funcionalidade de controle de aplicação Web e URL**

3.6.3.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

3.6.3.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

3.6.3.3. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking;

3.6.3.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool;

3.6.3.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por:

a) Usuário do Active Directory;

b) IP;

c) Rede.

3.6.3.6. Deve ser possível configurar com apenas um clique o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

3.6.3.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

3.6.3.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

3.6.3.9. Deve ser possível limitar o consumo de banda de aplicações.

3.6.3.10. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp e etc;

3.6.3.11. Na própria interface de gerência web deve ser possível realizar a recategorização de uma URL.

3.6.3.12. A base de aplicações deve ser superior a 4500 aplicações já categorizada na base de administração da solução.

3.6.3.13. Deve ser possível customizar e também definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

a) Aceitar e informar;

b) Bloquear e informar;

c) Perguntar.

3.6.4. **Identificação de Usuários**

3.6.4.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

3.6.4.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

3.6.4.3. A solução deve identificar usuários das seguintes fontes:

a) Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

b) Autenticação via navegador - para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

c) Identificação do usuário registrado no Microsoft Active Directory - deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

d) Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando.

3.6.5. **Funcionalidades de Anti-Vírus e Anti-Malware**

3.6.5.1. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar / bloquear a comunicação entre os hosts infectados com bot e operador remoto.

3.6.5.2. A solução deve bloquear arquivos potencialmente maliciosos infectados com vírus.

3.6.5.3. A solução de proteção contra vírus e bot devem compartilhar a mesma política para facilitar o gerenciamento.

3.6.5.4. A solução de proteção contra vírus e bot devem incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas.

3.6.5.5. As proteções devem ser ativadas baseadas em critério de nível de confiança, ações da proteção e impacto de performance.

3.6.5.6. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta.

3.6.5.7. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

3.6.5.8. Deve ser possível criar regras de exceção para que a engine não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

3.6.5.9. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

a) Inspecionar tipos de arquivos conhecidos que contém malware;

b) Inspecionar todos os tipos de arquivos;

c) Inspecionar tipos de arquivos de famílias específicas.

d) Deve bloquear acesso a URLs com malware.

e) Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado.

3.6.6. **Funcionalidades de VPN Site to Site**

3.6.6.1. A solução deve prover acesso seguro criptografado entre dois sites através da Internet.

3.6.6.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros.

3.6.6.3. A solução deve suportar autenticação com senha ou certificado.

3.6.6.4. Deve suportar criptografia AES 128 e 256;

3.6.6.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto.

3.6.6.6. Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

3.6.6.7. A solução deve suportar DPD (Dead Peer Detection) para minimizar a quantidade de mensagens trocadas para verificar a disponibilidade do Peer.

3.6.6.8. A solução deve suportar CA para configuração das VPNs.

3.7. **MÓDULO DE GERENCIAMENTO CENTRALIZADO – ITEM 05**

3.7.1. A solução de gerenciamento e administração centralizada, Security Management R80, em produção no ambiente gerenciado pela equipe COTEC instalado no Datacenter do Ministério do Meio ambiente, localizado em Brasília, deve sofrer um upgrade para suportar até 200 dispositivos conectados (**a quantidade de dispositivo é referente aos módulos de segurança conforme previsto nos itens 01, 02, 03 e 04 do lote 01**);

3.7.2. As funcionalidades do módulo de gerencia, assim como funcionam atualmente, devem ser capazes de gerenciar e administrar todas as soluções descritas neste termo:

a) Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

b) Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

c) Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

d) O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

e) O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

f) Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

g) Suportar backup das configurações e rollback de configuração para a última configuração salva;

h) Suportar validação de regras antes da aplicação;

i) Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;

j) Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

k) Permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

3.7.3. A solução de gerenciamento deverá ser entregue como upgrade do appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

3.7.4. Todos os custos para a instalação e atualização deverão ser de responsabilidade da CONTRATADA.

3.7.5. Para a realização do upgrade da solução deverão ser providenciados todos os testes antes da migração da gerência para o novo ambiente de gerencia com o upgrade.

3.8. **SERVIÇO DE GERÊNCIA E ARMAZENAMENTO DE LOGS DEDICADO - ITEM 06**

3.8.1. Deve ser contemplado nesse projeto solução dedicada para armazenamento de logs de todos os dispositivos conectados na gerência centralizada;

3.8.2. A solução de log server pode ser entregue através de appliance físico do próprio fabricante ou solução virtual desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 1TB de dados;

3.8.3. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a sua maior capacidade suportada ou ilimitada;

3.8.4. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

3.8.5. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

3.8.6. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

3.8.7. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

3.8.8. Deve possibilitar a integração com outras soluções de SIEM de mercado;

3.8.9. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

3.8.10. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;

3.8.11. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware) e URLs que passaram pela solução;

3.8.12. Deve ser possível exportar os logs em CSV;

3.8.13. Deve possibilitar a geração de relatórios de eventos no formato PDF;

3.8.14. Possibilitar rotação do log;

3.8.15. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

3.8.15.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

3.8.16. Deve permitir a criação de relatórios personalizados;

3.8.17. Suportar enviar os relatórios de forma automática via PDF;

3.8.18. A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

3.8.19. Deve consolidar logs e relatórios de todos os dispositivos administrados;

3.8.20. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

3.8.21. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

3.8.22. Permitir que os relatórios possam ser salvos, enviados e impressos;

3.8.23. Deve incluir uma ferramenta do próprio fabricante ou de outro, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;

3.8.24. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

3.8.25. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

a) Visualizar a quantidade de tráfego utilizado de aplicações e navegação;

b) Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

3.8.26. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

3.8.27. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

3.8.28. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

3.8.29. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

3.8.30. Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;

3.8.31. Permitir a visualização de gráficos e mapa de ameaças;

3.8.32. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

3.8.33. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

3.8.34. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

3.8.35. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

3.8.36. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

3.8.37. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

4. **ESPECIFICAÇÕES TÉCNICAS DO ITEM DO LOTE 02**

4.1. **Estabilizador/Nobreak 1,5KVA**

4.1.1. Topologia: Nobreak (UPS) interativo com regulação on-line;

4.1.2. Potência: 1500 VA/975W;

4.1.3. Tensão entrada: Bivolt automático 115/127/220V~ ;

4.1.4. Tensão saída: 115V~;

4.1.5. Forma de Onda: Senoidal por aproximação - retangular PWM;

4.1.6. Fator de potência de saída: 0.65;

4.1.7. Conexão de entrada: Plugue NBR 14136;

4.1.8. Conexão de saída: 8 tomadas NBR 14136 (no mínimo 5 no painel traseiro + extensão elétrica complementar);

4.1.9. Tempo de autonomia: 65 minutos para computador on board + 01 monitor LED 15,6" ;

4.1.10. Estabilizador: Interno Com 4 Estágios De Regulação;

4.1.11. Proteções do nobreak: Sobreaquecimento no transformador e inversor, Potência excedida, Descarga total da bateria, Curto-circuito no inversor.;

4.1.12. Proteções para a carga: Queda de rede (Blackout), Ruído de rede elétrica, Sobretensão de rede elétrica, Subtensão de rede elétrica;

4.1.13. Surtos de tensão na rede, Correção de variação da rede elétrica por degrau;

4.1.14. Battery Saver: Prolonga a vida útil da bateria evitando gastos desnecessários com sua substituição prematura.;

4.1.15. Função TRUE RMS: Analisa corretamente os disturbios da rede elétrica proporcionando uma proteção precisa.;

4.1.16. Recarregador Strong Charger: Permite a recarga das baterias mesmo com níveis muito baixos de carga, inclusive com o nobreak desligado;

4.1.17. Circuito desmagnetizador: Garante o valor de tensão adequado na saída do nobreak para equipamentos de informática e similares (cargas não lineares);

4.1.18. Alarme Audiovisual: Sinaliza com alarme sonoro as condições críticas de operação do nobreak, como: queda de rede, subtensão, sobretensão, fim do tempo de autonomia, final de vida útil da bateria, potência excedida e sobretemperatura;

4.1.19. Função Mute: Permite inibir o alarme sonoro durante alguma anormalidade;

4.1.20. Expansão de autonomia: Através da conexão de módulos externos é possível aumentar o tempo de autonomia do nobreak (UPS);

4.1.21. Filtro de Linha: Atenua os ruídos provenientes da rede elétrica;

4.1.22. Fusível: Porta fusível externo com unidade reserva ;

4.1.23. Autodiagnóstico de bateria: Informa o momento certo de trocar a bateria;

4.1.24. Autoteste: Ao ser ligado testa todos os circuitos internos;

4.1.25. DC Start: Permite ser ligado na ausência de rede elétrica;

4.1.26. Sinalizações: Led bicolor que indica as principais condições de operação do nobreak;

4.1.27. Botão liga/desliga: Temporizado para evitar desligamentos acidentais e/ou involuntários;

4.1.28. Inversor sincronizado com a rede elétrica (sistema PLL): Evita oscilações bruscas na saída durante a transição de rede para bateria e vice-versa;

4.1.29. Tempo de garantia: No mínimo 12 meses, onsite;

4.1.30. Equipamento novo de primeiro uso e em linha de fabricação.

4.1.31. compatível com redes instáveis ou com geradores de energia elétrica;

4.1.32. Gabinete em plástico anti-chama ou metal;

4.1.33. Para este item os equipamentos deverão ser entregues nas localidades cujos endereços deverão constar da Ordem de Fornecimento.

4.1.34. O hall de endereços que serão indicados para entrega constam da **Planilha de endereços de entregas para o LOTE 02.**

5. PLANEJAMENTO DE EXECUÇÃO

5.1. De forma a disponibilizar aos licitantes as informações quanto às expectativas em relação ao fluxo de preparação e execução do fornecimento dos itens constantes do objeto deste processo licitatório, apresenta-se a seguir o cronograma estimado:

ESTIMATIVA DE EXECUÇÃO DO PROJETO																									
ESTIMATIVA DE EXECUÇÃO DO PROJETO		FASES DO PROJETO																							
Ação	Descrição	Fase 1 - Implantação						Fase 2 - serviço catalogado (os módulos de segurança devem ser entregues configurados prontos para instalação simplificada). Nesta fase o prazo de entrega de equipamentos na sede do ICMBio é de 30 dias da data da solicitação.																	
		PERÍODO EM SEMANAS						PERÍODO EM SEMANAS																	
		1ª	2ª	3ª	4ª	5ª	6ª	7ª	8ª	9ª	10ª	11ª	12ª	13ª	14ª	15ª	16ª	17ª	18ª	19ª	20ª				
1	**Assinatura do contrato**	x																							
2	Reunião de Inicialização	x																							
3	Planejamento das ações	x	x																						
4	Solcitação de fornecimento de módulos		x	x																					
5	Upgrade do Módulo de Gestão			x	x																				
6	Instalação do serviço de armazenamento de log			x	x																				
7	Configuração de Módulo padrão de firewall				x																				
8	Transferência de conhecimento (da ação anterior)				x	x																			
9	**Fornecimento e instalação dos módulos de firewall**						x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
10	Avaliação/reavaliação das Unidades de Conservação ápitas	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
11	Envio de módulos para as Unidades de Conservação						x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
12	instalação e testes dos módulos nas Unidades de Conservação						x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				

5.2. Desta forma, serão consideradas duas fases conforme elencado a seguir:

5.2.1. **Fase 01 - Implantação.**

5.2.1.1. Nesta fase, a CONTRATADA, por meio do estudo da solução de segurança em produção no ICMBio, deverá agendar as atividades de implantação dos itens 5 e 6 preparando a Rede-ICMBio para o gerenciamento das redes filiais a serem implantadas.

5.2.1.2. A CONTRATADA deverá apresentar para aprovação da equipe de fiscalização, em até 10 dias úteis da assinatura do CONTRATO, um projeto com o cronograma de atividades que contemple todas as etapas desde o planejamento da migração até a implantação de do *Módulo de Gerenciamento de Segurança Centralizado (item 05), do Serviço Dedicado de Armazenamento de Logs (item 06) integrados ao firewall principal do ICMBio instalado na sede, e de pelo menos mais 02 (dois) módulos de segurança implantados em unidades descentralizadas para que sejam efetuados os testes de integração total da solução de segurança.*

5.2.1.3. O aceite definitivo os itens 5 e 6 somente será emitido após a conclusão do projeto de implementação restando comprovado pela CONTRATADA aos fiscais o efetivo funcionamento integrado da solução de segurança entre todos os itens contemplados no projeto.

5.2.1.4. Desta forma, serão providenciados todos o serviços relacionados ao upgrade do módulo de gestão, a implantação do módulo de armazenamento centralizado de logs e configuração e testes de pelo menos 02 (dois) equipamentos previstos nos itens de 01 a 04 para que sejam homologados os padrões de configurações a serem fornecidos na fase 02.

5.2.1.5. Durante esta fase, a CONTRATADA deverá montar no laboratório da COTEC na sede do ICMBio, um ambiente que possibilite a realização de teste de bancada para os módulos de segurança, onde serão realizados os testes e a transferência de conhecimento para que a equipe de servidores e colaboradores da COTEC seja capaz de efetuar a instalação de um módulo de segurança pré-configurado integrado com o módulo de gerenciamento centralizado e com o serviço de armazenamento de logs.

5.2.1.6. A fase de implantação será finalizada após a criação e homologação de um **modelo de teste padrão** que será utilizado para o recebimento dos módulos de segurança a partir da fase 02.

5.2.2. **Fase 02 - Serviço catalogado (fornecimento de módulos de segurança sob demanda)**

5.2.2.1. Com a conclusão da fase 01 - a CONTRATADA passará a fornecer os itens 01, 02, 03 e 04 sob demanda, devendo entregá-los na Sede do ICMBio, pré-configurados e prontos para serem instalados nas Unidades de Conservação.

5.2.2.2. Nesta fase, a CONTRATADA poderá efetuar as atividades de configuração e testes de integração nas dependências do CONTRATANTE.

5.2.2.3. O prazo de entrega dos ***Módulos de Segurança (tens 01, 02, 03 e 04), será de 30 dias contados a partir do início da fase 02, ou da data de assinatura da Ordem de fornecimento, caso a fase 02 já tenha sido concluída.***

5.2.2.4. O recebimento definitivo dos equipamentos constantes de cada Ordem de Fornecimento somente será efetuado após a realização do **teste padrão** definido na fase 01.

5.2.2.5. A instalação dos Módulos de segurança nas Unidades de Conservação, a partir da fase 2, será agendado pela COTEC junto aos pontos focais da Unidade, devendo a CONTRATADA manter os canais de contato para que seja prestado o suporte técnico remoto para auxiliar as equipes locais das Unidades com as atividades de instalação dos equipamentos sempre que for solicitado.

Documento assinado eletronicamente por **Felipe Finger Santiago**, **Analista em Tecnologia da Informação**, em 27/09/2021, às 19:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Jaime Heleno Correa de Lisboa**, **Coordenador**, em 27/09/2021, às 19:25, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Jose Luiz Roma**, **Coordenador**, em 27/09/2021, às 20:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Guilherme Palma de Sousa**, **Técnico Administrativo**, em 27/09/2021, às 20:59, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.icmbio.gov.br/autenticidade informando o código verificador **9568956** e o código CRC **48D186B0**.

Criado por 80255914172, versão 64 por 80255914172 em 23/09/2021 09:32:13.