Intersec Solutions
Segurança da Informação

+ 55 54 98133 5657
jeison@itsl.com.br
www.itsl.com.br

PREFEITURA DE VERANÓPOLIS | Veranópolis / RS

PROJETO: Gestão de Serviços Gerenciados de Tecnologia e Segurança da Informação

Data: 19/08/2025

Aos cuidados de: Bernardo Boff

Proposta Comercial

Instalação, configuração e manutenção dos Servidores

Instalação, configuração, atualização, manutenção preventiva e suporte de até 30 servidores, físicos ou virtualizados, nas plataformas Windows, Linux ou VMWare, inclusive servidores que executam serviços de terceiros. A contratada deverá ser responsável pela implementação e suporte de todos os serviços ativos nos servidores (active directory, dhcp, dns, IIS, web server, servidor de e-mail, etc), exceto serviços específicos de terceiros.

Monitoramento online dos Servidores

A contratada deverá fornecer e manter uma solução de monitoramento de servidores com as seguintes características:

- Monitoramento de todos os servidores em tempo real, fornecendo indicadores de performance (CPU, Memória, Rede, espaço em disco, processos e serviços) através de relatórios ou gráficos.

- Suporte para Autenticação de dois fatores

- Gerenciamento automático de patches de segurança, com agendamento parametrizado para instalação e correção

- Monitoramento de antivírus, com possiblidade de ativar e desativar o antivírus remotamente

- Monitoramento de serviços (com possibilidade iniciar e parar qualquer serviço)

- Monitoramento de interface de rede

- A solução deve permitir acesso remoto, com dupla camada de proteção e conexão criptografada

- Suporte de notificações por push

- Execução remota de comandos através de prompt de comando e powershell (para Windows) e comandos de terminal (para Linux)

- Suporte a descoberta de ativos de rede automática

- Suporte a workflow automatizado para resolução de problemas de forma automática

- Suporte a execução e scripts automatizados (Windows e Linux)

- Fornecimento de Interface web para acompanhar o monitoramento dos servidores. A interface deve possuir acesso seguro através de conexão protegida por SSL.

- Fornecimento de aplicativo para acompanhar o monitoramento dos servidores. O Aplicativo deve ter a suporte para realizar todas as operações descritas acima. O Aplicativo deve suportar no mínimo as plataformas IOS e Android.

- Criação de usuários com níveis de acesso customizados.

- Possibilidade de envio de alertas em tempo real via e-mail e push para os usuários cadastrados.

Proteção de Dados Pessoais e LGPD

Auxílio no mapeamento de dados pessoais coletados pelo Município e suas secretarias

Auxílio na elaboração de Diagnóstico situacional do Município, mapeando o nível de maturidade de Segurança da Informação e Proteção de Dados

Auxílio na gestão e gerenciamento de projeto para LGPD

Auxílio na elaboração de Relatórios de Análise de Impacto mapeados como necessários

Auxílio no gerenciamento de requisição de titulares de Dados

Auxílio na elaboração de documentos específicos, como o SOA, ROPA e RIPD

Elaboração e manutenção da documentação de TI

Criação de documentação que contemple todas as configurações de infraestrutura física e lógica do ambiente de TI existente. Essa documentação deve ser atualizada a cada alteração física ou lógica no ambiente de TI.

Gerenciamento, projetos e controle da rede lógica de dados

Gerenciar e controlar a rede lógica, através de documentação, serviços e ferramentas de controle, assim como elaborar projetos que envolvem o ambiente de TI quando necessário. A contratada deve prestar suporte em todas as ferramentas utilizadas para o controle lógico da rede. A contratada deve ser responsável pela implementação lógica de interligação de pontos de rede (VLANs, roteamento, QOS, etc) caso necessário.

Gerenciamento, projetos e controle da rede wireless

Gerenciar e controlar a rede wireless, através de documentação, serviços e ferramentas de controle, assim como elaborar projetos que envolvem o ambiente de WIFI quando necessário. A contratada deve prestar suporte em todas as ferramentas utilizadas para o controle lógico da rede wireless. A contratada deve ser responsável pela implementação lógica da rede wireless (VLANs, roteamento, QOS, etc) caso necessário.

Controle de aquisição e instalação de hardware

Auxiliar a contratante na homologação e aquisição de equipamentos e periféricos necessários para o funcionamento da rede.

Controle de aquisição de instalação de software

Auxiliar a contratante na homologação e aquisição de softwares.

Controle e gerenciamento da padronização da rede de computadores

Garantir que os objetos da rede de computadores sejam padronizados, através de nomenclatura homologada e de endereçamento categorizado homologado pela contratante.

Elaboração e controle de projeto de manutenção preventiva dos servidores, rede e equipamentos de segurança

Elaboração e gerenciamento de política de licenciamento de software

Elaboração de Políticas de Segurança da Informação

Desenvolvimento de Política de Segurança da Informação, Normas de Acesso, Procedimentos e Termos de Uso. Documentação baseada na ISO/IEC 27001.

Entregáveis:

- Política Geral de Segurança: contém o propósito, escopo, diretrizes, papéis e responsabilidades, sanções e punições, referentes a política a ser implantada.

- Termo de Uso: termo de conhecimento a ser assinado pelos colaboradores e prestadores de serviço da organização.

- Norma de Acesso Remoto: define as diretrizes para o acesso remoto a ativos/serviços de informação e recursos computacionais.

- Norma de Uso de Equipamentos Pessoais: define as diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo.

- Norma de Classificação e Manuseio da Informação: define as diretrizes para a classificação, rotulagem, manuseio, guarda e descarte seguro de informações em formato digital ou em suporte físico.

- Norma de Proteção contra Códigos Maliciosos: define as diretrizes para proteção dos ativos/serviços de informação contra ameaças e códigos maliciosos de qualquer natureza.

- Norma de Uso de Serviços de E-Mail e Comunicadores Instantâneos: define as diretrizes para utilização dos serviços de e-mail e comunicadores instantâneos da organização.

- Norma de Gestão de Identidade e Controle de Acesso: define as diretrizes para garantir que o acesso aos ativos de informação ou sistemas de informação tenham níveis adequados de proteção.

- Norma de Acesso a Internet e Comportamento em Mídias Sociais: define as diretrizes para utilização segura do acesso à internet e do comportamento de colaboradores em mídias e redes sociais.

- Norma para Monitoramento de Ativos e Serviços da Informação: define as diretrizes para o monitoramento de ativos/serviços de informação e recursos computacionais.

- Norma de Resposta a Incidentes de Segurança da Informação: define as diretrizes para responder eventos ou incidentes de segurança que estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos computacionais.

- Norma de Uso Aceitável de Ativos de Informação: define as diretrizes para o uso aceitável de ativos de informação por seus usuários autorizados.

Controle do projeto de prevenção e combate a malwares

A contratada é responsável por definir, implementar e gerenciar projeto de prevenção e combate a malwares.

Elaboração, execução e controle das políticas de backup de dados

A contratada é responsável por definir, implementar e gerenciar plano de backup automático das informações e dados com necessidade de contingência. Essas informações de dados serão homologadas pela contratante. A contratada deverá prestar suporte nas ferramentas utilizadas para a execução do plano de backup.

Elaboração, execução e controle de políticas de contingência da rede de computadores

A contratada é responsável por definir, implementar e gerenciar política de contingência de rede, a fim de evitar que sinistros afetem diretamente a disponibilidade de serviços críticos.

Controle da estrutura de rede para o ambiente de telecomunicações

A contratada deverá ser responsável por gerenciar e realizar as implementações de configurações de rede necessárias para o funcionamento do ambiente de telecomunicações.

Manutenção e gerenciamento do firewall

A contratada deverá ser responsável pela manutenção, gerenciamento e suporte do firewall e firewall HA existente na contratante (Sonicwall NSA 4700).

Execução de auditoria de segurança mensal através de software homologado

A contratada deverá ser responsável por executar mensalmente auditoria de segurança interna e externa nos ativos da contratante (ativos que estejam localizados nas dependências da contratante e ativos que estejam localizados na nuvem, caso existam). A auditoria deverá ser realizada por software que seja homologado para atender os seguintes requisitos:

- Relatórios customizados, sendo possível exportá-los para PDF, HTML ou CSV

- Escaneamento:

- Escaneamento de vulnerabilidades baseado em banco de dados de CVEs
- Escaneamento de sistemas baseado em credenciais

- Cobertura para os seguintes ativos:

- Dispositivos de rede
- Domínios
- URL
- Servidores
- Aplicações Web
- Banco de Dados

- Gerenciamento:

- Suporte a escaneamento remoto, escaneamento local via conexão VPN, com suporte aos seguintes sensores: Detecção de Malware, Scan de DNS, Descoberta de Vulnerabilidades (básica, avançada e agressiva), Scan de Portas, Scan de SO Windows, Verificação de Certificados SSL, Verificação de Blacklists
- Scores de Risco: Ranking de vulnerabilidades baseado em CVSS, com níveis de severidade (Crítico, Alto, Médio, Baixo e Info)

- Relatórios que o software deve gerar:

- Relatório detalhado de Ativos
- Relatório de Riscos de Segurança
- Relatório de escaneamento detalhado
- Relatório de Riscos por Grupos Definidos
- Relatório de Ocorrências

- Conformidade:

O software deve estar em conformidade com as seguintes normas:

LGPD:

- Art. 6 – Princípios de Segurança e Prevenção

- Seção I – da Segurança e do Sigilo de Dados – Art. 46. Os agentes de tratamento devem adotar medidas de segurança técnicas aptas a proteger os dados pessoais de acessos não autorizados

e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

- 2° II – demonstrar a efetividade de seu programa de governança em privacidade, quando apropriado

- Art. 50 1° - Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular.

ISO 27001: 2013

- A.12.6.1 – Gestão de vulnerabilidades técnicas

- A.14.2.3 – Análise crítica técnica das aplicações

- A.16.1.3 – Notificação de fragilidades de segurança da informação

- A.18.2.2 – Conformidade com as políticas e procedimentos de segurança da informação

- A.18.2.3 – Análise crítica da conformidade técnica

NIST

- PROTECT – PR.IP-12: Um plano de gerenciamento de vulnerabilidades deve ser desenvolvido e implementado

- DETECT-DE.CM-8: Verificação de vulnerabilidades são executadas

RESOLUÇÃO 4.658 (Bacen):

- 2° Os procedimentos e os controles de que trata o inciso II do caput devem abranger... a detecção de intrusão, a prevenção de vazamento das informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos.

- Art. 3° - A política de segurança cibernética deve contemplar, no mínimo: II – os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética.

PCI DSS:

- Requisito 5: Manter um programa de gerenciamento de vulnerabilidades

- Requisito 6: Desenvolver e manter sistemas e aplicativos seguros – 6.1

Acordo de Confidencialidade

Todas as informações contidas neste documento são estritamente confidenciais.

Todo o material, ideias, conceitos e demais detalhes técnicos e comerciais aqui contidos, devem ser utilizados exclusivamente para avaliar a capacidade da INTERSEC SOLUTIONS em oferecer uma solução tecnológica de acordo com as premissas, necessidades e objetivos do projeto aqui descrito.

O conteúdo deste documento não deverá ser utilizado para nenhuma outra finalidade e não deve ser publicado ou revelado nenhum conteúdo deste documento, por qualquer meio, nem no todo ou em parte, sem permissão prévia e por escrito da INTERSEC SOLUTIONS.

O uso deste documento, em seu processo interno de avaliação e escolha de soluções, projetos, produtos, serviços e/ou fornecedores, implica no aceite incondicional dos termos deste Acordo de Confidencialidade.

Investimento

Valor Mensal: R$ 4.352,00 / mês (Revisão contínua dos controles definidos ou implementados)

Condições Comerciais e Entrega

Entrega imediata.

Pagamento mensal.

Estamos à disposição para esclarecer quaisquer dúvidas referente ao projeto acima.

gov.br
Documento assinado digitalmente
JEISON NONDILLO
Data: 19/08/2025 17:22:41-0300
Verifique em https://validar.iti.gov.br

Atenciosamente,

Jeison Nondillo