TERMO DE JUSTIFICATIVA DE CONTRATAÇÃO EMERGENCIAL DE PRESTAÇÃO DE SERVIÇOS DE SUPORTE DE TECNOLOGIA DA INFORMAÇÃO (TI) PARA A POLICLINICA ESTADUAL DA REGIÃO NORDESTE - UNIDADE POSSE

CONSIDERANDO QUE:

A – Em 09 de julho de 2024 o IMED foi convidado pelo Estado de Goiás, por meio de sua Secretaria de Estado da Saúde para celebrar Termo de Colaboração por meio de Dispensa de Chamamento Público fundamentada no inc. I, art. 30 da Lei nº 13.019, de 31 de julho de 2014;

B – Foi firmado em 25 de julho de 2024 e publicado em 26 de julho de 2024, o **Termo de Colaboração n° 94/2024 – SES** (Processo n° 202400010044191), entre o IMED – INSTITUTO DE MEDICINA, ESTUDOS E DESENVOLVIMENTO, associação civil sem fins lucrativos de apoio à gestão de saúde, qualificado como Organização Social de Saúde no Estado de Goiás, e o Estado de Goiás, por meio de sua Secretaria de Estado da Saúde, por um período de 180 (cento e oitenta) dias, com vistas ao fomento, gerenciamento, operacionalização e execução das ações e serviços de saúde na Policlínica Estadual da Região Nordeste - Unidade Posse ("Policlínica de Posse"), localizada na Avenida Juscelino K de Oliveira, Setor Buenos Aires, CEP.: 73.900-000, Posse/GO;

C – Dada a exiguidade do lapso temporal entre os eventos retro indicados, não é possível nem razoável ao IMED iniciar e concluir o processo ordinário de seleção para fins de contratação de serviços e fornecimento de bens relacionados à referida unidade; e

D – Mesmo diante da exiguidade temporal já mencionada, não pode haver risco de interrupção ou mesmo suspensão, ainda que parcial, dos serviços diretos ou indiretos disponibilizados e utilizados pela população usuária da Policlínica de Posse,

justifica-se o seguinte:

1. DO PREÂMBULO:

1.1. O **IMED – INSTITUTO DE MEDICINA, ESTUDOS E DESENVOLVIMENTO**, associação civil sem fins lucrativos de apoio à gestão de saúde, qualificado como Organização Social de Saúde no Município de São Paulo, celebrou, em 25.07.2024, o **Termo de Colaboração n° 94/2024 – SES** com o Estado de Goiás, e o Estado de Goiás, por meio de sua Secretaria de Estado da Saúde, por um período de 180 (cento e oitenta) dias, com vistas ao fomento, gerenciamento, operacionalização e execução das ações e serviços de saúde na Policlínica Estadual da Região Nordeste - Unidade Posse ("Policlínica de Posse"), localizada na Avenida Juscelino K de Oliveira, Setor Buenos Aires, CEP.: 73.900-000, Posse/GO.

1.2. A contratação visa dar início, em caráter emergencial, às atividades de Prestação de serviços de suporte de tecnologia da informação (TI) junto à referida Unidade de Saúde, por força do qual lavra o presente Termo de Justificativa de Contratação Emergencial, diante das condições e dos fundamentos nele expressos.

1.3. Integram o presente Termo de Justificativa, como se nele estivessem transcritos, os seguintes anexos:

a) Anexo I – Publicação realizada no dia 26.07.2024 junto ao Diário Oficial do Estado de Goiás; e

b) Anexo II – Proposta da Empresa Contratada, de forma emergencial.

2. DO FUNDAMENTO:

2.1. O presente Termo de Justificativa encontra fundamento no artigo 15, inciso VIII, do REGULAMENTO PARA OS PROCEDIMENTOS DE COMPRA, CONTRATAÇÃO DE OBRAS, CONTRATAÇÃO DE SERVIÇOS E ALIENAÇÕES DO IMED – INSTITUTO DE MEDICINA, ESTUDOS E DESENVOLVIMENTO do Imed para a Policlínica Estadual da Região Nordeste - Unidade Posse ("Regulamento"), o qual **AUTORIZA A TOMADA DE PROVIDÊNCIAS EXCEPCIONAIS EM CASOS DE URGÊNCIA - EM ESPECIAL, COMO É O CASO PRESENTE, EM FACE DA GRITANTE INEXISTÊNCIA DE TEMPO HÁBIL ÀS PROVIDÊNCIAS DE ROTINA PARA A CONTRATAÇÃO DE TERCEIROS,** abrindo exceção às regras de contratação ordinária nas seguintes hipóteses:

"CAPÍTULO V

DAS EXCEÇÕES

Art. 15 Ficam excepcionalizados da publicidade prévia disposta no artigo 6° os seguintes casos::

"*(...)*

VIII. Aquisição/ contratação realizada em caráter de urgência ou emergência, caracterizada pela ocorrência de fatos inesperados e imprevisíveis, cujo não atendimento imediato seja mais gravoso importando em prejuízos ou comprometendo a segurança de pessoas ou equipamentos, reconhecidos pela administração..

(...)".

3. DAS JUSTIFICATIVAS:

3.1. **JUSTIFICATIVA DA CONTRATAÇÃO:** Após a celebração, em 25.07.2024, **Termo de Colaboração n° 94/2024 – SES** com o Estado de Goiás, e o Estado de Goiás, por meio de sua Secretaria de Estado da Saúde, com vistas ao fomento, gerenciamento, operacionalização e execução das ações e serviços de saúde na Policlínica de Posse, o IMED iniciou suas operações junto à respectiva Unidade de Saúde.

Contudo, considerando que, consoante anteriormente informado e destacado, não há tempo suficiente para a realização de contratações pelo procedimento ordinário previsto no Regulamento, sem que disso resulte indiscutível prejuízo ao regular funcionamento da Unidade de Saúde, inclusive com risco de interromper os atendimentos à uma população que deles necessitam, é imprescindível a contratação, em caráter emergencial, dos serviços/fornecimento objeto deste Termo de Justificativa.

3.2. **RAZÃO DA ESCOLHA DO PRESTADOR DE SERVIÇOS:** A empresa contratada, de forma emergencial, foi escolhida por se dispor a atender, **de forma imediata e em caráter de urgência**, a solicitação da demanda das atividades pertinentes.

A empresa contratada deverá executar as atividades e cumprir com todas as obrigações dispostas no contrato emergencial de prestação/fornecimento de bens e serviços firmado até que o processo seletivo correspondente seja finalizado ou até quando os serviços ou fornecimento de bens se mostrem necessários.

3.3. **JUSTIFICATIVA DE PREÇO**: O preço contratado foi negociado adotando-se como premissas: (i) o escopo necessário; (ii) a melhor relação custo x benefício; (iii) a necessidade de início imediato dos serviços contratados, bem como (iv) os valores praticados no mercado.

4. DO OBJETO:

4.1. Constitui-se como objeto do presente Termo de Justificativa a CONTRATAÇÃO EMERGENCIAL DE PRESTAÇÃO DE SERVIÇOS DE SUPORTE DE TECNOLOGIA DA INFORMAÇÃO (TI), NECESSÁRIOS AO PLENO E EFETIVO FUNCIONAMENTO DA POLICLÍNICA DE POSSE

5. PRAZO DE EXECUÇÃO E REAJUSTE:

5.1. Referida contratação de prestação de serviços terá vigência inicial de até 90 (noventa) dias, podendo ser prorrogada até a conclusão do processo seletivo de contratação ordinária, caso necessário.

5.2. Fica estabelecido que os valores contratados não sofrerão reajustes durante o período de vigência contratual e que o contrato firmado será considerado automaticamente rescindido quando da conclusão do processo de contratação ordinária ou do seu encerramento sem a renovação correspondente.

6. DA DOTAÇÃO ORÇAMENTÁRIA:

6.1. As despesas decorrentes da contratação correrão por conta da dotação orçamentária prevista no Termo de Colaboração n° 94/2024 – SES.

7. DO FORO:

7.1. O foro competente para dirimir possíveis dúvidas, após se esgotarem todas as tentativas de composição amigável, e/ou litígios pertinentes ao objeto do presente Termo de Justificativa, independente de outro que por mais privilegiado seja, será o da Comarca de Goiânia - GO.

8. DA DELIBERAÇÃO:

8.1. Nada mais havendo a tratar, e tendo em vista todas as condições apresentadas retro, encerra-se o presente Termo de Justificativa, sendo ratificado e assinado, na forma de aceite, pelo representante legal do IMED, para que sejam produzidos os efeitos jurídicos e legais desejados.

Posse/GO, 28 de agosto de 2024.

IMED – Instituto de Medicina, Estudos e Desenvolvimento
André Silva Sader – Representante Legal

ANEXO I – PUBLICAÇÃO REALIZADA NO DIA 26.07.2024 JUNTO AO DIÁRIO OFICIAL DO ESTADO DE GOIÁS

EXTRATO DO TERMO DE COLABORAÇÃO Nº 94/2024-SES/GO. Processo nº 202400010044191. Parceiro Público: Estado de Goiás - Secretaria de Estado da Saúde. Parceiro Privado: Instituto de Medicina, Estudos e Desenvolvimento - IMED. Objeto: Gerenciamento, operacionalização e execução das ações e serviços de saúde em regime de no mínimo 12 horas/dia, na Policlínica Estadual da Região Nordeste - Posse, localizada na Avenida Juscelino K. de Oliveira, Setor Buenos Aires, Posse - Goiás. Valor: R$ 18.292.179,00. Vigência: 180 (cento e oitenta) dias ou até a conclusão do chamamento público, contados a partir da publicação deste extrato no Diário Oficial do Estado de Goiás. Dotação Orçamentária: 2850.10.302.1043. 2516.03. 25000100. 50. Signatários: Rasível dos Reis Santos Júnior - Secretário de Estado da Saúde. André Fonseca Leme - IMED.

Protocolo 476159

ANEXO II – PROPOSTA DA EMPRESA CONTRATADA, DE FORMA EMERGENCIAL.

Soares Soluções Tecnológicas LTDA
Rua HM8 Qd. 11 Lt. 38 Casa 02 – Goiânia GO – CEP: 74.573-394 Resd. Hugo de Morais

Empresa: Soares Soluções Tecnológicas LTDA

FONE: (62) 3284-0738

CNPJ: 42.804.612/0001-87

Para: IMED – INSTITUTO DE MEDICINA, ESTUDOS E DESENVOLVIMENTO

Assunto: Prestação de Serviços de Suporte de TI

A/C: Departamento de Compras / Diretoria

SOARES SOLUÇÕES

A Soares Soluções, fornece os mais variados serviços em TI, desde terceirização de mão de obra (outsourcing), infraestrutura de TI e apoio em soluções de software.

"nós preocupamos com a TI, para que você tenha mais tempo para seu negócio"

PROPOSTA TÉCNICA

Prezados Senhores,

Vimos pela presente apresentar nossa Proposta Técnica para atender à Requisição de **Prestação de Serviços de Suporte de TI** para fins de suporte às atividades de gestão desenvolvidas pelo IMED junto à Policlínica de Posse.

1 - OBJETO

Prestação de Serviços de Suporte de TI para fins de suporte às atividades de gestão desenvolvidas pelo IMED junto à **Policlínica de Posse**.

2 - DESCRIÇÃO DETALHADA

DESCRIÇÃO DOS SERVIÇOS

- Disponibilização de 01 colaborador com o cargo de **TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO**, carga horária de 44 horas semanais, no regime CLT, presencialmente na Policlínica de Posse;

- Fornecimento de Serviços de SUPORTE N2 e COORDENAÇÃO DE TI REMOTO com equipe mínima de 2 profissionais disponíveis por telefone e ou Whatsapp 24 horas por dia 7 dias por semana com comprovação de vínculo com a contratada;

- Fornecimento de SUPORTE N2 PRESENCIAL quando solicitado antecipadamente;

- Fornecimento de ferramenta de monitoramento e gerenciamento remoto, com portal unificado que incluem: painéis com informação de todo parque de máquinas, gerenciamento de inventário incluindo relatórios, monitoramento remoto de hardware e software, geração de scripts para manutenção remota de desktops e servidores, acesso remoto seguro com logs se segurança e gravação de tela e antivírus para 3 servidores;

- Fornecimento de ferramenta de backup e recuperação de desastres remoto, com rotinas diárias de backup para todos os servidores localizados na clínica, em formato bare metal e incremental com a possibilidade de restauração via internet de forma integral ou arquivos e pastas, sem limitação de armazenamento e retenção mínima de 15 dias;

- As atividades devem ser executadas exclusivamente em equipamentos ou serviços dentro das dependências da Policlínica de Posse.

DESCRIÇÃO DAS ATIVIDADES

ATIVIDADES DE COORDENADOR EM TECNOLOGIA DA INFORMAÇÃO

- Supervisão direta de uma equipe de profissionais de TI, incluindo técnicos, administradores de sistemas, engenheiros de rede e outros especialistas. Isso envolve atribuir tarefas, monitorar o progresso do trabalho, fornecer orientação e feedback, e promover um ambiente de trabalho colaborativo e produtivo;

- Desenvolvimento e implementação de uma estratégia de TI alinhada com os objetivos organizacionais de longo prazo. Isso inclui a identificação de necessidades de TI, avaliação de tecnologias emergentes, definição de metas e prioridades, e alocação de recursos;

- Supervisão e coordenação de projetos de TI desde o planejamento até a implementação e manutenção. Isso envolve a definição de escopo, cronograma e orçamento do projeto, alocação de recursos, acompanhamento do progresso e resolução de problemas;

- Estabelecimento de políticas, procedimentos e padrões de segurança de TI para proteger os ativos de informação da organização e garantir conformidade com regulamentações relevantes;

- Supervisão da infraestrutura de TI da organização, incluindo servidores, redes, sistemas de armazenamento, dispositivos de segurança e outros recursos de hardware e software. Isso envolve garantir que os sistemas estejam operacionais, atualizados e seguros;

- Avaliação de soluções de tecnologia da informação para atender às necessidades da organização. Isso inclui a análise de custo-benefício, revisão de propostas de fornecedores, negociação de contratos e coordenação de implementações;

- Identificação e mitigação de riscos de segurança de TI, como ataques cibernéticos, vazamento de dados e interrupções de serviço. Isso envolve a implementação de controles de segurança, treinamento de funcionários e resposta a incidentes de segurança;

- Colaboração com líderes de negócios e outras partes interessadas para entender suas necessidades de TI e garantir que os sistemas de informação suporte efetivamente as operações organizacionais;

- Identificação das necessidades de treinamento da equipe de TI e fornecimento de oportunidades de desenvolvimento profissional para melhorar as habilidades e conhecimentos da equipe;

- Avaliação do desempenho da equipe de TI e dos sistemas de informação para identificar áreas de melhoria e implementar medidas corretivas conforme necessário.

ATIVIDADES DE TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO

- Prestar suporte técnico aos funcionários do hospital para resolver problemas de hardware, software e rede, tanto presencialmente quanto remotamente. Isso inclui diagnóstico e resolução de problemas em computadores, impressoras, scanners, sistemas de comunicação etc.;

- Realizar manutenção preventiva em equipamentos de TI, como atualização de sistemas operacionais, aplicação de patches de segurança, limpeza física de computadores e substituição de componentes defeituosos;

- Auxiliar na implantação e configuração de novos sistemas de informação e aplicativos clínicos, como sistemas de registros eletrônicos de saúde (EHR), sistemas de imagem médica (PACS), sistemas de laboratório, etc;

- Implementar e manter medidas de segurança de TI para proteger os dados do paciente e garantir conformidade com regulamentações de privacidade. Isso inclui configuração de firewalls, antivírus, controle de acesso e monitoramento de logs de segurança;

- Configurar e gerenciar soluções de backup para garantir a integridade dos dados do paciente e a disponibilidade contínua dos sistemas críticos em caso de falha ou desastre;

- Manter um inventário atualizado de todos os ativos de TI do hospital, incluindo computadores, servidores, dispositivos móveis, software e licenças, e garantir que os registros estejam em conformidade com as políticas de gerenciamento de ativos;

- Fornecer treinamento e orientação aos funcionários do hospital sobre o uso adequado de sistemas de TI, práticas de segurança cibernética e conformidade com as políticas e procedimentos de TI;

- Responder prontamente a emergências de TI, como falhas de sistema, ataques cibernéticos, interrupções de rede ou qualquer outro incidente que possa afetar a prestação de cuidados aos pacientes;

- Trabalhar em estreita colaboração com equipes clínicas, administrativas e de segurança para entender suas necessidades de TI e garantir que os sistemas de informação atendam aos requisitos operacionais e regulamentares;

- Pesquisar, avaliar e recomendar novas tecnologias e soluções de TI que possam melhorar a eficiência, segurança e qualidade dos cuidados prestados pelo hospital.

ATIVIDADES DE GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

- Gerência de projetos da equipe de tecnologia da informação;

- Alinhamento estratégico entre as tecnologias disponíveis e os objetivos da direção do hospital;

- Utilização de ferramentas de monitoramento remoto para acompanhar o desempenho de sistemas, redes e aplicativos, identificando problemas potenciais antes que impactem os usuários finais;

- Manutenção de um inventário de ativos de TI remotos, incluindo computadores, dispositivos móveis, software e licenças, utilizando ferramentas de gerenciamento de ativos baseadas na nuvem;

- Gerencia de projetos de TI à distância, incluindo o planejamento, execução e acompanhamento de projetos de desenvolvimento de software, implantação de infraestrutura, migrações de dados, entre outros;

- Utilização de ferramentas de comunicação remota, como e-mail, videoconferência, mensagens instantâneas e plataformas de colaboração online, para manter a comunicação eficaz com a equipe de TI e outros stakeholders;

- Fornecimento de treinamento presencial para usuários sobre o uso adequado de sistemas e ferramentas de TI, boas práticas de segurança cibernética e outras habilidades relacionadas à tecnologia;

- Realização de auditorias de segurança presenciais para identificar vulnerabilidades físicas e medidas de segurança inadequadas nas instalações de TI da organização;

- Gerenciar atividades com fornecedores de serviços de TI presencialmente, como provedores de internet, empresas de manutenção de hardware, e outros fornecedores de tecnologia.

ATIVIDADES DE SUPORTE N2

- Disponibilidade 24 horas por dia 7 dias por semana;

- Identificação e solução de problemas complexos em sistemas de TI, redes e aplicativos;

- Resposta imediata a incidentes críticos de segurança, interrupções de serviço ou falhas de sistemas;

- Configuração, otimização e manutenção de infraestrutura de rede complexa, incluindo roteadores, switches, firewalls e balanceadores de carga;

- Planejamento e execução de implementações e atualizações de sistemas operacionais, aplicativos e software de segurança, garantindo mínima interrupção para os usuários finais;

- Implementação de sistemas de monitoramento proativo para detectar e resolver problemas antes que afetem os usuários finais;

- Coordenação e implementação de mudanças complexas em ambientes de TI, garantindo que os impactos sejam avaliados e gerenciados adequadamente;

- Assistência especializada para aplicativos de software específicos utilizados no contexto do hospital, como sistemas de gestão hospitalar, PACS (Picture Archiving and Communication System), e sistemas de informações laboratoriais;

- Implementação e manutenção de políticas de segurança da informação rigorosas, incluindo proteção contra ameaças cibernéticas, gerenciamento de acesso e conformidade com regulamentações relevantes;

- Recuperação de Desastres e Continuidade de Negócios: Desenvolvimento e teste de planos de recuperação de desastres para garantir a disponibilidade contínua de sistemas críticos em caso de falhas ou desastres;

- Fornecimento de treinamento especializado para usuários finais e equipe de suporte interno, juntamente com a documentação completa de processos e procedimentos de suporte;

- Definição e implementação de regras de firewall para controlar o tráfego de entrada e saída com base em endereços IP, portas e protocolos;

- Acompanhamento contínuo do tráfego de rede para identificar padrões, anomalias ou atividades suspeitas que possam indicar uma violação de segurança;

- Administração de listas de permissões e negações para controlar o acesso a recursos específicos da rede;

- Aplicação regular de patches e atualizações de segurança para garantir que o firewall esteja protegido contra vulnerabilidades conhecidas;

- Estabelecimento e configuração de conexões VPN para permitir comunicações seguras entre redes remotas ou usuários remotos;

- Realização de auditorias periódicas de segurança para avaliar a eficácia das políticas de firewall e identificar áreas de melhoria;

- Diagnóstico e resolução de problemas relacionados ao firewall, incluindo bloqueios de tráfego indevidos, falhas de conexão e outras questões de segurança;

- Desenvolvimento e implementação de políticas de segurança abrangentes, alinhadas com os requisitos de conformidade e as melhores práticas do setor;

- Coleta e análise de logs de firewall para monitorar atividades de rede, detectar possíveis ameaças e facilitar investigações de segurança;

- Oferecimento de treinamento e conscientização em segurança cibernética para funcionários, ajudando a garantir o uso adequado do firewall e a proteção dos recursos de rede;

- Criação e configuração de novas máquinas virtuais para suportar diferentes cargas de trabalho e aplicativos;

- Implantação e gerenciamento de contêineres utilizando tecnologias como LXC (Linux Containers) ou Docker, para fornecer ambientes isolados e eficientes para aplicativos;

- Acompanhamento do uso de CPU, memória, armazenamento e largura de banda das VMs e contêineres para garantir um desempenho adequado e detectar possíveis gargalos;

- Implementação de políticas de backup automatizadas para proteger os dados das VMs e contêineres, juntamente com procedimentos de restauração em caso de falha ou perda de dados;

- Configuração e gerenciamento de armazenamento de dados, incluindo armazenamento local, armazenamento em rede (NFS, CIFS) e armazenamento em bloco (iSCSI, FC);

- Configuração de clusters Proxmox para alta disponibilidade, garantindo que as VMs e contêineres continuem funcionando mesmo em caso de falha de hardware ou software;

- Aplicação de patches de segurança e atualizações de software para manter o Proxmox e seus componentes atualizados e protegidos contra vulnerabilidades conhecidas;

- Integração do Proxmox com sistemas de monitoramento de terceiros para obter insights detalhados sobre o desempenho e a integridade do ambiente virtualizado;

- Implementação de scripts e ferramentas de automação para simplificar tarefas repetitivas, como provisionamento de VMs, configuração de redes e gerenciamento de backups;

- Realização de auditorias periódicas de segurança e conformidade para garantir que o ambiente Proxmox atenda aos padrões e regulamentações de segurança relevantes;

- Instalação inicial do Windows Server em hardware físico ou virtual, incluindo configuração de parâmetros básicos como nome do servidor, configurações de rede e ativação de licenças;

- Criação, modificação e exclusão de contas de usuário e grupos locais ou integrados ao domínio, juntamente com a atribuição de permissões e políticas de segurança;

- Configuração de políticas de grupo para padronizar configurações de segurança, permissões, configurações de desktop e outras configurações para usuários e computadores em um ambiente de domínio;

- Implantação e configuração de serviços de rede como DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), Active Directory, File Services, Print Services, entre outros;

- Monitoramento do desempenho do servidor, diagnóstico de problemas de hardware ou software, e aplicação de correções e atualizações de segurança;

- Configuração e manutenção de volumes de armazenamento, discos rígidos, RAID (Redundant Array of Independent Disks) e sistemas de arquivos para garantir a disponibilidade e integridade dos dados;

- Implementação de políticas de backup automatizadas para proteger dados importantes e garantir a capacidade de recuperação em caso de falha de hardware, corrupção de dados ou desastres;

- Implementação e manutenção de medidas de segurança, incluindo configuração de firewalls, políticas de senha, controle de acesso, criptografia e auditorias de segurança;

- Configuração e gerenciamento de serviços de terminal para fornecer acesso remoto a aplicativos e desktops, garantindo segurança e desempenho adequados;

- Realização de auditorias periódicas para garantir a conformidade com políticas internas, regulamentações governamentais e padrões de segurança da indústria;

- Desenvolvimento de plano de implantação de rede que leve em consideração a cobertura necessária, capacidade, segurança e compatibilidade com dispositivos existentes;

- Instalação física dos pontos de acesso Wi-Fi em locais estratégicos para garantir uma cobertura eficaz em toda a área desejada;

- Definição e configuração de múltiplos SSIDs para segregação de tráfego, oferecendo diferentes níveis de acesso e segurança para diferentes grupos de usuários;

- Implementação de protocolos de segurança Wi-Fi, como WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) ou WPA3, para proteger a rede contra acesso não autorizado;

- Configuração de métodos de autenticação, como WPA2-Enterprise ou WPA3-Enterprise, para autenticar usuários através de um servidor de autenticação centralizado, como RADIUS (Remote Authentication Dial-In User Service);

- Configuração de servidores DHCP (Dynamic Host Configuration Protocol) para atribuir endereços IP de forma dinâmica aos dispositivos conectados à rede sem fio;

- Monitoramento contínuo do desempenho da rede sem fio, incluindo latência, largura de banda, interferência e níveis de sinal, para garantir uma experiência de usuário otimizada;

- Implementação de políticas de QoS (Quality of Service) para priorizar determinados tipos de tráfego de rede, como voz sobre IP (VoIP) ou streaming de vídeo, garantindo uma qualidade de serviço consistente;

- Aplicação regular de atualizações de firmware e patches de segurança nos pontos de acesso e controladores de rede sem fio para garantir a estabilidade e segurança da infraestrutura;

- Realização de auditorias periódicas de segurança para identificar e corrigir potenciais vulnerabilidades na configuração da rede sem fio;

- Desenvolvimento de uma arquitetura de rede que atenda às necessidades da organização, considerando fatores como tamanho, localização geográfica, requisitos de largura de banda e segurança;

- Instalação física e configuração de dispositivos de rede, como switches, roteadores, firewalls, pontos de acesso sem fio (APs) e servidores de rede;

- Atribuição de endereços IP estáticos ou dinâmicos aos dispositivos de rede, configuração de servidores DHCP (Dynamic Host Configuration Protocol) e implementação de políticas de gerenciamento de endereços IP;

- Divisão da rede em sub-redes lógicas ou VLANs (Virtual LANs) para melhorar o desempenho, segurança e eficiência do tráfego de rede;

- Implementação e configuração de serviços de rede essenciais, como DNS (Domain Name System), DHCP, NAT (Network Address Translation), VPN (Virtual Private Network) e servidor de arquivos;

- Configuração de políticas de acesso para controlar quem pode acessar recursos de rede, implementação de firewalls para proteger contra ameaças externas e internas, e configuração de sistemas de detecção e prevenção de intrusões (IDS/IPS);

- Monitoramento contínuo do tráfego de rede, uso de largura de banda, latência e outros indicadores de desempenho para identificar problemas e otimizar a rede;

- Inventário e monitoramento de dispositivos de rede, incluindo switches, roteadores, firewalls, APs, servidores e dispositivos de rede de terceiros;

- Implementação de políticas de backup regulares para configurar os dispositivos de rede e os arquivos de configuração dos dispositivos, garantindo a rápida recuperação em caso de falha ou erro de configuração;

- Realização de auditorias regulares de segurança e conformidade para garantir que a rede esteja em conformidade com políticas internas, regulamentações governamentais e padrões do setor;

- Avaliação das necessidades da organização e identificação dos serviços e cargas de trabalho adequados para migrar para a nuvem;

- Pesquisa e seleção de um provedor de serviços em nuvem que atenda aos requisitos de negócios da organização, levando em consideração fatores como custo, desempenho, segurança e conformidade;

- Configuração e provisionamento de recursos de computação, armazenamento, rede e outros serviços necessários na plataforma de nuvem escolhida;

- Migração ou implantação de aplicativos na infraestrutura de nuvem, garantindo compatibilidade, desempenho e segurança adequados;

- Implementação de políticas de segurança para proteger os dados e aplicativos na nuvem, incluindo configuração de firewalls, controles de acesso, criptografia e monitoramento de ameaças;

- Integração dos serviços em nuvem com sistemas e aplicativos existentes na infraestrutura local, garantindo interoperabilidade e continuidade operacional;

- Configuração de serviços de gerenciamento de identidade e acesso (IAM) para controlar e monitorar o acesso aos recursos na nuvem, incluindo autenticação multifatorial e controle de acesso baseado em função;

- Implementação de ferramentas de monitoramento para acompanhar o desempenho dos serviços em nuvem, identificar gargalos e otimizar a utilização de recursos;

- Configuração de políticas de backup e recuperação de dados para proteger contra perda de dados e garantir a disponibilidade contínua dos serviços em nuvem;

- Treinamento de funcionários para garantir que eles estejam familiarizados com os serviços em nuvem, suas funcionalidades e melhores práticas de uso.

FUNÇÕES DA FERRAMENTA DE GERENCIAMENTO / MONITORAMENTO DE RECURSOS DE TI

- Gerenciamento centralizado via portal com todas as ferramentas disponíveis centralizadas (gerenciamento remoto, antivírus, gerador de scripts, acesso remoto, monitoramento de hardware);

- Monitoramento contínuo do desempenho do sistema, incluindo CPU, memória, disco, rede e outros recursos, permitindo a detecção precoce de problemas de desempenho;

- Geração de alertas e notificações em tempo real para eventos críticos, como falhas de sistema, problemas de segurança, indisponibilidade de serviço e outros eventos importantes;

- Automatização do processo de aplicação de patches de segurança e atualizações de software em dispositivos monitorados, ajudando a garantir que os sistemas estejam sempre atualizados e protegidos;

- Capacidade de acessar dispositivos remotamente para solução de problemas, configuração de sistemas, instalação de software e outras tarefas de manutenção sem a necessidade de intervenção física no dispositivo;

- Manutenção de um inventário completo de ativos de TI, incluindo detalhes como hardware, software instalado, configurações do sistema e histórico de manutenção;

- Implementação de recursos de segurança, como criptografia de dados, autenticação de dois fatores, controle de acesso baseado em função e auditorias de segurança para proteger os dados do cliente e garantir a conformidade com regulamentações;

- Geração de relatórios detalhados sobre o desempenho do sistema, utilização de recursos, histórico de alertas, conformidade de segurança e outros aspectos importantes da infraestrutura de TI;

- Integração com outras ferramentas e sistemas de gerenciamento de TI, como sistemas de ticketing, ferramentas de monitoramento de rede e sistemas de gerenciamento de serviços de TI (ITSM), para facilitar processos e fluxos de trabalho;

- Automatização de rotinas de manutenção e administração de TI, permitindo que tarefas repetitivas sejam executadas de forma programada e eficiente, reduzindo a carga de trabalho manual;

- Oferecer visão geral das métricas de desempenho e saúde do sistema;

- Apresentar gráficos e widgets personalizáveis para monitoramento em tempo real;

- Listar e categorizar alertas e notificações críticas;

- Permitir a rápida identificação e resolução de problemas de infraestrutura;

- Exibir o status das atualizações de software e patches aplicados nos dispositivos monitorados;
- Facilitar o gerenciamento proativo das atualizações de segurança e correções de bugs;

- Apresentar lista detalhada de todos os ativos de TI monitorados;

- Permitir a organização e filtragem por tipo de dispositivo, status e outras métricas relevantes;

- Fornecer uma visão geral das medidas de segurança implementadas e do status de conformidade;

- Destacar possíveis vulnerabilidades e áreas de melhoria na segurança da infraestrutura de TI;

- Incluir detalhes como fabricante, modelo, especificações técnicas e número de série;

- Listar todos os programas de software instalados nos dispositivos monitorados;

- Manter registro completo de todos os dispositivos de hardware monitorados;

- Fornecer informações sobre versões, licenças, datas de instalação e atualizações disponíveis;

- Bloqueio de acesso a sites maliciosos, phishing, conteúdo inapropriado ou não relacionado ao trabalho para proteger os usuários contra ameaças e garantir a conformidade com as políticas da empresa;

- Verificação de arquivos baixados e sites visitados em busca de malware, vírus, ransomware e outras ameaças cibernéticas, prevenindo infecções e ataques de malware;

- Detecção e bloqueio de ameaças avançadas, incluindo ataques de dia zero, botnets, ataques de phishing sofisticados e outros tipos de ameaças cibernéticas;

- Monitoramento e controle do uso de aplicativos e protocolos de rede, evitando atividades maliciosas e vazamento de dados;

- Bloqueio de acesso a URLs maliciosos ou suspeitos com base em listas de URLs conhecidas de fontes confiáveis ou comportamento suspeito;

- Inspeção de tráfego criptografado para identificar e bloquear ameaças ocultas em conexões HTTPS, protegendo contra-ataques de malware que usam criptografia para evadir a detecção.

FUNCIONALIDADE DA FERRAMENTA DE BACKUP REMOTO

- Permite fazer backup de dados de dispositivos locais, como computadores Windows, servidores Windows, servidores Linux e VMs Vmware/Hyper-V diretamente para um NAS Synology;

- Oferece suporte para fazer backup de dados de aplicativos específicos, como Microsoft Exchange, Microsoft SQL Server, Microsoft Office 365, G Suite e SharePoint;

- Fornece suporte para fazer backup de máquinas virtuais VMware e Hyper- V, permitindo a proteção de VMs hospedadas em ambientes virtuais;

- Permite restaurar arquivos individuais, pastas, e-mails, bancos de dados e outros itens de backup sem a necessidade de restaurar todo o backup;

- Realiza verificações regulares de integridade nos backups para garantir que os dados estejam protegidos e não tenham sido corrompidos;

- Permite configurar agendamentos flexíveis para executar backups automáticos em horários específicos, garantindo que os dados estejam sempre protegidos e atualizados;

- Permite configurar políticas de retenção de dados para controlar por quanto tempo os backups são mantidos, ajudando a cumprir requisitos de conformidade e economizar espaço de armazenamento;

- Oferece recursos de monitoramento em tempo real e geração de relatórios para acompanhar o status dos backups, identificar problemas e garantir que os backups estejam sendo executados conforme o esperado.

PROPOSTA COMERCIAL

Conforme cenário exposto, oferecemos a proposta para melhorar os serviços na área de tecnologia da informação, entregando suporte N1 presencial, suporte N2 remoto e também Serviços de Gerencia e Coordenação de T.I;

Além desses itens de serviço, é importante manter a segurança e a qualidade de atendimento com uma ferramenta que forneça: **acesso remoto, antivírus para servidores, monitoramento de hardware e segurança.**

Segue abaixo valores propostos para atender as demandas citadas:

Valor Mensal: 10.900,00 **(Dez Mil e Novecentos Reais)**

DADOS DE PAGAMENTO:

BANCO: Caixa Econômica Federal
AGENCIA: 1340
CONTA: 3691-5
PIX CNPJ: 42804612000187

Goiânia, 10 de julho de 2024.

Leonardo Soares da Silva
Soares Soluções Tecnológicas LTDA
42.804.612/0001-87