DIÁRIO OFICIAL
MUNICÍPIO DE SALTINHO

Conforme Lei Municipal nº 677, de 17 de abril de 2019

www.saltinho.sp.gov.br | www.imprensaoficialmunicipal.com.br/saltinho

SUMÁRIO

PODER EXECUTIVO DE SALTINHO	2
Atos Oficiais	2
Decretos	2
Licitações e Contratos	43
Dispensas - Aviso de Abertura	43
Comunicados	43
Concursos Públicos/Processos Seletivos	43
Convocação	43

EXPEDIENTE

O Diário Oficial do Município de Saltinho, veiculado exclusivamente na forma eletrônica, é uma publicação das entidades da Administração Direta e Indireta deste Município, sendo referidas entidades inteiramente responsáveis pelo conteúdo aqui publicado.

ACERVO

As edições do Diário Oficial Eletrônico de Saltinho poderão ser consultadas através da internet, por meio do seguinte endereço eletrônico: www.saltinho.sp.gov.br
Para pesquisa por qualquer termo e utilização de filtros, acesse www.imprensaoficialmunicipal.com.br/saltinho
As consultas e pesquisas são de acesso gratuito e independente de qualquer cadastro.

ENTIDADES

Prefeitura Municipal de Saltinho
CNPJ 66.831.959/0001-87
Avenida Sete de Setembro, 1733
Telefone: (19) 3439-7800
Site: www.saltinho.sp.gov.br
Diário: www.imprensaoficialmunicipal.com.br/saltinho

Câmara Municipal de Saltinho
CNPJ 01.637.738/0001-27
Avenida Sete de Setembro, 1711
Telefone: (19) 3439-1707 | (19) 3439-1178
Site: www.camarasaltinho.sp.gov.br

Diário Oficial Assinado Eletronicamente com Certificado Padrão ICPBrasil, em conformidade com a MP nº 2.200-2, de 2001

O Município de Saltinho garante a autenticidade deste documento, desde que visualizado através do site www.saltinho.sp.gov.br

Compilado e também disponível em www.imprensaoficialmunicipal.com.br/saltinho

Prefeitura do Município de Saltinho
Estado de São Paulo
CNPJ 66.831.959/0001-87

DECRETO Nº 2050, DE 27 DE OUTUBRO DE 2021.
"Institui o Plano Diretor de Tecnologia da Informação - PDTI, e a Política de Segurança de Informação – PSI e dá outras providências".

HÉLIO FRANZOL BERNARDINO, Prefeito do Município de Saltinho, Estado de São Paulo, no uso das atribuições que lhe são consideradas por Lei,

CONSIDERANDO, que a tecnologia da informação – TI, é atualmente reconhecida pelos gestores públicos como uma ferramenta fundamental para atender as necessidades estratégicas e operacionais, sendo um dos principais alicerces para a modernização da Gestão Municipal;

CONSIDERANDO, que o planejamento de TI deve estar alinhado e integrado com o planejamento estratégico da Administração Pública de Saltinho;

CONSIDERANDO a necessidade de elaboração do Plano Diretor de Tecnologia da Informação - PDTI, bem como, a elaboração da Política de Segurança da Informação – PSI.

D E C R E T A:

Art. 1º – Fica instituído o Plano Diretor de Tecnologia da Informação - PDTI, instrumento de diagnóstico, planejamento e gestão de recursos e processos de Tecnologia da Informação – TI, implantando no âmbito da Administração Pública Municipal, consistente no Anexo I deste ato.

Parágrafo único – O Plano Diretor de Tecnologia da Informação - PDTI, tem como objetivo determinar as prioridades nos diversos desafios e ações de TI na Administração Pública Municipal, alinhando as atividades com às metas da Administração.

Art. 2° – Fica instituído ainda, a Política de Segurança da Informação – PSI, instrumento que orienta e estabelece as diretrizes corporativas da Prefeitura Municipal de Saltinho para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários, consistente no Anexo II deste ato.

Parágrafo único – A Política de Segurança da Informação – PSI, tem como objetivo estabelecer diretrizes que permitam aos colaboradores da Prefeitura Municipal de

Saltinho seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Art. 3º – Este Decreto entra em vigor na data de sua publicação.

Saltinho/SP, 27 de outubro de 2021.

HÉLIO FRANZOL BERNARDINO
- Prefeito Municipal –

Publicado no mural de avisos do Paço Municipal e no Diário Oficial Eletrônico do Município de Saltinho/SP (https://imprensaoficialmunicipal.com.br/saltinho).

MARCELO MONTEBELLO
- Diretor do Departamento Administrativo -

Prefeitura do Município de Saltinho
Estado de São Paulo
CNPJ 66.831.959/0001-87

ANEXO I
(DECRETO Nº 2050/2021)

PREFEITURA MUNICIPAL DE SALTINHO

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO – PDTI (2021-2024)

SALTINHO/SP – OUTUBRO/2021

Av. Sete de Setembro, 1733 • Centro • Saltinho/SP • CEP 13.440-013
Fone: 3439-7800 • e-mail: gabinetedoprefeito@saltinho.sp.gov.br

1. INTRODUÇÃO

Atualmente vivemos em um mundo altamente globalizado, caracterizado por constantes transformações, inundando-se regularmente por novos produtos, serviços e descobertas.

Isto tem feito com que as organizações também da gestão pública se preocupassem cada vez mais em identificar a melhor forma de empregar seus recursos buscando a melhoria na qualidade dos serviços prestados ao cidadão. Isso significa melhorias no ambiente da gestão pública pelo aumento da eficácia organizacional: agilidade nos processos, na estrutura, na comunicação e na eliminação da burocracia.

Na atual "Era da Atualização e Informação", o uso estratégico da tecnologia da informação e a administração dos recursos de informática podem e devem melhorar o atendimento da população e o desenvolvimento sustentável deste município.

Em razão disso, a Tecnologia da Informação (TI), que durante muito tempo foi considerada apenas um item de suporte aos processos internos, uma fonte de despesas, sem influência direta nos objetivos e metas da gestão pública, deve ser repensada como um fator crítico para a prestação de serviços públicos, resultando em crescimento da atuação do poder público exercendo assim um forte domínio sobre os interesses da população.

Nesse contexto, a Prefeitura Municipal de Saltinho, sempre busca aprimorar, expandir e melhorar os processos de atendimento aos munícipes, necessitando de recursos tecnológicos para tal, bem como, de novas ferramentas para aperfeiçoar esse grande fluxo de dados.

Dessa forma, a elaboração deste plano torna-se de extrema importância para o planejamento e serve de norte para esta importante transição permeada de grandes desafios a serem implantados, fornecendo ferramentas para medir, controlar e expandir as prioridades do TI no município.

Isto posto, salienta-se que o Plano Diretor de Tecnologia da Informação foi desenvolvido a partir de levantamentos e análises das situações organizacionais e tecnológicas do Município e poderá ser reavaliado a cada quadriênio, ajustado para melhor atendimento dos serviços prestados. Podendo ainda, possíveis aspectos táticos e operacionais decorrentes do PDTI, serem definidos em etapa posterior, em conjunto com representantes dos Departamentos Municipais.

2. OBJETIVO

Apresentar propostas que auxiliem na instauração de um processo de melhoria continua nos itens de software, hardware, administração da rede, infraestrutura, banco de dados e proteção da informação, apontando soluções para os problemas identificados que estejam limitando o alcance das metas da Prefeitura de Saltinho.

O PDTI será o documento norteador para elaboração do planejamento e execução de todas as ações da tecnologia da informação. A fase do planejamento consiste em definir as ações que serão tomadas para atendimento às necessidades levantadas a partir do diagnóstico da situação atual.

Com vista aos objetivos estratégicos do município, este Plano Diretor de Tecnologia da Informação pretende estabelecer linhas coerentes e concisas capazes de nortear a questão de Tecnologia da Informação para com seus investimentos em infraestrutura, sistemas corporativos e de apoio ao cidadão. Bem como, visa dar apoio tecnológico aos projetos municipais, prestação de serviço de suporte técnico, manutenção reativa e proativa, integração e administração de sistemas de gestão e infraestrutura de tecnologia da informação nas unidades da gestão do Município de Saltinho.

Os objetivos estratégicos deste plano, poderão ser desenvolvidos pela gestão municipal, dentro de um prazo de 04 (quatro) anos, de 2021 à 2024. Porém, a volatilidade do segmento de tecnologia da informação poderão ser feitas mudanças e atualizações no plano haja vista a possibilidade de mudanças de tendências.

Item	Objetivo
1.	Atualizar as condições de trabalho das equipes municipais através do fornecimento de cursos de especialização para os funcionários atuais.
2.	Atualização dos Departamentos Municipais, com modernização de equipamentos de tecnologia da informação.
3.	Consolidar a infraestrutura dos demais setores com novas aquisições, readequações e upgrades estruturais.
4.	Dar preferência para locação dos equipamentos de informática, de forma a permitir ao contratante renovação da estrutura física.

5.	Promover segurança por meio de políticas, planos, documentações e reorganização formal das rotinas de trabalho dos Departamentos Municipais.
6.	Aprimorar processos e sistemas de atendimento a usuários de tecnologia da informação por meio de sistemas e acesso físico.
7.	Implantar novos sistemas corporativos para automatizar rotinas de trabalho e reduzir custos operacionais
8.	Promover a inclusão digital e social por meio de programas municipais.
9.	Garantir a observância da Lei Geral de Proteção de Dados Pessoais – LGPD, dentro da sua competência.

3. PARTES INTERESSADAS

Nome	Cargo	Área
Hélio Franzol Bernardino	Prefeito Municipal	Gabinete
Diretorias Municipais	Diretores Municipais	Diretorias Municipais
Controle Interno	Controle Interno	Controle Interno

4. RECURSOS E ESTRUTURA ORGANIZACIONAL DE TI

Esta seção demonstra o ambiente de tecnologia da informação da gestão municipal, apresentando dessa forma os recursos de TI existentes na Prefeitura Municipal de Saltinho.

4.1. SISTEMAS PRÓPRIOS E TERCEIRIZADOS UTILIZADOS PARA MANUTENÇÃO DOS HARDWARES PELA PREFEITURA DO MUNICÍPIO DE SALTINHO.

Os sistemas utilizados pela Prefeitura do Município de Saltinho são terceirizados através de licitação e a empresas prestadoras dos serviços são Fiorilli Sociedade Civil Ltda; System Brasil Soluções Tecnológicas EIRELI EPP; Carolina Mariele Bovi Bruzza ME e Portal Quéops Telecomunicações e Serviços de Internet EIRELI ME.

4.1.1. A empresa Fiorilli Sociedade Civil Ltda, presta serviços referentes a cessão onerosa de licença de uso temporário diversos softwares/módulos de sistemas informatizados integrados de gestão financeira, com implantação, customização, migração de dados, treinamento e manutenção, cuja plataforma possui os seguintes módulos implantados no servidor local:

I - Contabilidade Pública/Sistema AUDESP;

II - Planejamento e Orçamento;

III – Tesouraria;

IV - Administração de Estoque;

V - Gestão de Compras e Licitação/Transparência;

VI - Gestão do Patrimônio;

VII - Administração de Frota;

VIII - Folha de Pagamentos/Gestão de Pessoal;

IX - Controle Interno;

X – Arrecadação/Tributação/ISSQN Eletrônico/Nota Fiscal Eletrônica Responsabilidade Fiscal (RF).

4.1.2. A empresa System Brasil Soluções Tecnológicas EIRELI EPP, presta serviços referentes a implantação em fase única e cessão onerosa mensal de licença de uso temporário de plataforma tecnológica de gerenciamento integrado da unidade de saúde, unidades escolares e cadastro social do cidadão, com vistas a buscar informações e produzir subsídios que agilizem e maximizem as ações públicas, conforme quantidades estimadas e especificações técnicas, cuja plataforma possui os seguintes módulos implantados no servidor local:

I - Módulo da Educação;

II - Módulo da Saúde;

III - Módulo do Cadastro Social, da Mobilidade Urbana e da Inclusão Social das Pessoas Portadoras de Necessidades Especiais;

IV - Administrar o servidor onde estão alocados todos os módulos da empresa Fiorilli Sociedade Civil Ltda.

4.1.3. O Município de Saltinho, possui outro contrato em vigor com a empresa System Brasil Soluções Tecnológicas EIRELI EPP, contrato este voltado para a área administrativa, e visa a cessão onerosa de licença de uso temporário de sistema informatizado de captura de imagens e gestão eletrônica de fluxo de documentos, com implantação, customização, migração de dados, treinamento, manutenção e migração de ambiente físico para virtual.

Salienta-se que com relação ao atendimento de suporte reativo, se o problema for lógico em nível de software, é realizado o acesso remoto para sua resolução. Em relação ao atendimento de suporte preventivo, há política definida para atualização dos softwares e sistemas operacionais das estações de trabalho e servidores.

4.1.4. A empresa Carolina Mariele Bovi Bruzza ME, presta serviços de manutenção preventiva e corretiva nos equipamentos de informática, serviços de instalação e configuração de software, suporte de rede, desenvolvimento e suporte de Web Design e suporte técnico conforme as necessidades desta Administração Pública, com fornecimento de mão de obra, conforme condições estabelecidas e descritas abaixo:

I - Formatação e instalação de sistema operacional e aplicativos;

II - Ampliação de cabo de rede e colocação de novos pontos de rede;

III - Revisão e reinstalação de sistema operacional e dos softwares;

IV - Limpeza interna e externa dos equipamentos;

V - Instalação, configuração e compartilhamentos de impressoras, além de substituição de peças que sejam necessárias;

VI - Quando constatado a necessidade de substituição de peças nos equipamentos, deverá ser informado o Diretor do Departamento Administrativo, para autorização da mesma, posteriormente aquisição por parte da Prefeitura para concluir a manutenção;

VII - Quando solicitado pela Prefeitura, a contratada deverá dispor de um profissional técnico especializado para solucionar o problema ora apresentado, indicando o local o qual deverá comparecer fisicamente;

VIII - A empresa contratada deverá apresentar relatório mensal dos serviços realizados no respectivo período, demonstrando efetivamente as atividades realizadas, com o atesto da unidade requisitante.

4.1.5. A empresa Portal Quéops Telecomunicações e Serviços de Internet EIRELI ME, presta serviços de telecomunicações, com o intuito de obter acesso a internet, dedicado, bidirecional e simétrico na velocidade mínima de 200 Mpbs por ponto instalado, estimando-se até 20 (vinte) pontos de acesso, sendo que em todos os pontos deverão ter roteador Wi-fi devidamente instalado, conforme descritivo abaixo:

I - O acesso deverá ser fornecido obrigatoriamente através de fibra óptica, não sendo aceito, em nenhuma hipótese, outro meio de transporte de dados para internet dedicado bidirecional e simétrico na velocidade mínima de 200 Mbps por ponto instalado;

II - Acesso bidirecional (trafegar nos dois sentidos);

III - Acesso simétrico (mesma velocidade nominal nos dois sentidos);

IV - Velocidade mínima de 96,8% da velocidade nominal;

V - Disponibilidade média mensal de 99,2% (SLA);

VI - O uso da fibra óptica como meio de transporte dos dados deverá ser utilizado em todos os enlaces (trajeto) desde o Backbone da operadora de Telecomunicações, até os Modems instalados nos locais de funcionamento;

VII - É vedada a sublocação do objeto deste termo de referência, em partes ou em seu todo;

VIII - A contratante não terá qualquer tipo de limitação quanto a quantidade (em bytes) e conteúdo da informação trafegada no acesso;

IX - Possuir taxa de perda de pacotes menor ou igual que 2%;

X - Latência média de 220 ms (dos locais de funcionamento até a central da contratada);

XI - Vedada à utilização de rádios em qualquer frequência;

XII - Fornecimento de no mínimo de 20 (vinte) endereços IP (V4) por acesso;

XIII - A contratada deverá possuir Termo de Autorização para a prestação de Serviço Comunicação Multimídia (SCM) outorgado pela ANATEL;

XIV - A contratada deverá possui uma Central de Atendimento 24 (vinte e quatro) horas por dia, 365 (trezentos e sessenta e cinco) dias por ano através de um número 0800;

XV - A contratada deverá garantir a resolução de problemas em até 04 (quatro) horas após abertura de chamado no 0800;

XVI - A contratada deverá fornecer rack especifico para abrigar os ativos de rede, a ser instalado dentro do Datacenter da contratante;

XVII - O roteador será fornecido pela contratada com instalação, configuração e gerência compartilhada com os responsáveis pela área de tecnologia designados pela contratante;

XVIII - Deverá estar disponível no Datacenter da contratante um roteador em redundância, em caso de falha ou defeito;

XIX - A configuração será executada para que a rede de computadores da contratante possua acesso à internet;

XX - Possuir a quantidade mínima necessária de memória que atenda a velocidade e funcionalidades deste item, em conformidade com as recomendações do fabricante;

XXI - Possuir quatro portas de LAN a 10/100/1000 Mbps que seja compatível com o padrão IEEE 802.3;

XXII - As portas deverão ser fornecidas no padrão RJ-45;

XXIII - Possuir protocolo de gerenciamento SNMP e MIB-II implementados em conformidade com a RFC 1157 e RFC 1213, respectivamente;

XXIV - Todos os roteadores deverão ter capacidade para suportar o tráfego com banda completamente ocupada, sem exceder a 80% de utilização de CPU e memória;

XXV - Responder por todas as normas definidas pela Agência Nacional de Telecomunicações – ANATEL;

XXVI - Os equipamentos para o funcionamento do link serão fornecidos pela contratada com instalação, configuração e gerência compartilhada com os responsáveis pela área de tecnologia designados pela contratante;

XXVII - Deverão estar disponíveis no Datacenter da contratante equipamentos em redundância, em caso de falha ou defeito;

XXVIII - A configuração será executada para que a rede de computadores da contratante possua acesso à internet;

XXIX - Possuir a capacidade mínima que atenda a velocidade e funcionalidades deste item, em conformidade com as recomendações do fabricante;

XXX - Possuir mínimo de uma porta WAN e quatro portas de LAN a 10/100/1000 Mbps que sejam compatíveis com o padrão IEEE 802.3;

XXXI - As portas deverão ser fornecidas no padrão RJ-45;

XXXII - Possuir protocolo de gerenciamento SNMP e MIB-II implementados em conformidade com a RFC 1157 e RFC 1213, respectivamente;

XXXIII - Todos os equipamentos deverão ter capacidade para suportar o tráfego com banda completamente ocupada, sem exceder a 80% de utilização de CPU e memória;

XXXIV - Responder por todas as normas definidas pela Agência Nacional de Telecomunicações - ANATEL;

XXXV - A contratante disponibilizará espaço em rack contendo o tamanho máximo de até 08 (oito) us;

XXXVI - A contratante disponibilizará os seguintes recursos para instalação dos equipamentos a infraestrutura: tomada elétrica tri polar com tensão estabilizada 110 ou 220V; tubulação (dutos) desobstruída com fio guia; cabeamento necessário do PT (ponto de terminação da rede da contratada) até o local onde serão instalados os equipamentos da solução;

XXXVII - Toda a infraestrutura externa para a instalação, ativação e equipamentos (cabos, equipamentos, conectores) do acesso à Internet dedicado não deverá possuir qualquer ônus para a contratante;

XXXVIII - Toda manutenção dos equipamentos deverá ser agendada com o gestor do contrato;

XXXIX - A contratada deverá fornecer a contratante acesso a portal WEB com no mínimo as seguintes informações: Identificação do ponto de acesso e

respectivo número do acesso; velocidade do acesso; informações do tráfego de entrada e saída; taxa média de ocupação do link (throughput); visualização de gráfico detalhando a utilização da banda;

XL - A solução de gerência da rede da contratada deverá atuar de forma proativa, de acordo com o Nível de Serviço (SLA), realizando o acompanhamento dos defeitos e desempenho do serviço;

XLI - Manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados;

XLII - Quando solicitada, a contratada deverá demonstrar para análise as configurações dos roteadores instalados no ambiente da contratante;

XLIII - A contratante terá diretos em também administrar a rede lógica, e em conjunto com a contratada comunicar e interagir em demandas e necessidades específicas de acesso e diretos junto à rede;

XLIV - Caso a empresa declarada vencedora possua contrato vigente de link dedicado de internet com esta Prefeitura, deverá efetuar a instalação da solução com uma abordagem diferente.

4.2. SEGURANÇA

Atualmente a Prefeitura Municipal de Saltinho utiliza como segurança de firewall, Proxy e monitoramento nos acessos os softwares pfSense e EndianCE. Quanto à utilização de antivírus, os servidores principais utilizam antivírus ESET File Security, as estações que utilizam o software Microsoft Essentials Security ou Windows Defender contido na versão do Windows 10.

4.3. BACKUP

Os Backups são realizados manualmente, e com alguns processos automáticos.

São armazenadas em ferramentas disponíveis, através do servidor.

5. INFRAESTRUTURA FÍSICA E LÓGICA DA REDE

Uma infraestrutura física de tecnologia da informação adequada é fundamental para garantir a eficácia e eficiência dos serviços providos por sistemas

automatizados, oferecendo condições ideais de segurança e disponibilidade para acomodação de equipamentos de tecnologia da informação.

5.1. REDE FÍSICA E CABEAMENTO

A estrutura de comunicação de uma organização é fundamental para a melhoria de processos administrativos e redução de custos operacionais.

Caso haja o crescimento das plataformas de transmissão de dados, do quadro de agentes públicos e aumento da demanda por serviços eletrônicos, poderá ser necessário um constante aumento, tanto na abrangência, quanto na capacidade da rede atual, mostrando assim, uma deficiência do sistema existente e expondo a necessidade de uma nova infraestrutura planejada. Este possível projeto deverá satisfazer, no mínimo, os seguintes objetivos:

I - Garantir segurança física dos equipamentos de tecnologia da informação e consequentemente a proteção física contra acesso indevido;

II - Garantir o condicionamento adequado dos equipamentos de tecnologia da informação para o provimento de suas funções;

III - Prevenir desastres no ambiente de tecnologia da informação causados por fenômenos naturais ou falhas humanas;

IV - Reformular toda a estrutura de cabeamento de dados.

5.2 REDE LÓGICA CABEADA

A infraestrutura lógica da rede é parte essencial para a manutenção da disponibilidade, integridade e confidencialidade dos dados. A rede de dados da Prefeitura Municipal de Saltinho poderá ser readequada, por meio de um projeto técnico.

5.3. SEGURANÇA FÍSICA E LÓGICA

Vivemos em um mundo globalizado, com o espaço geográfico fragmentado, porém fortemente articulado pelas redes, onde a informação, independente do seu formato, é um dos maiores patrimônios de uma organização moderna, sendo vital

para quaisquer níveis hierárquicos e dentro de qualquer instituição que deseja manter-se competitiva no mercado.

Considerada um ativo importantíssimo para a realização do negócio a informação deve ser protegida e gerenciada. Nos últimos anos as tecnologias de informação e comunicação têm evoluído de forma rápida, fazendo com que as organizações tenham maior eficiência e rapidez nas tomadas de decisão, devido a este fato as chances de uma empresa não usar sistemas de informação tornou-se praticamente nula.

Neste contexto a importância de se utilizar mecanismos de segurança é vital para a sobrevivência. Mecanismos estes, que conseguem:

I - Prevenir ataques à rede corporativa com proteção para o acesso de sistemas corporativos publicados para a Internet;

II - Controlar o fluxo de entrada e saída de tráfego de dados entre as redes remotas (secretarias), a Internet, e a rede interna da Prefeitura do Município de Saltinho;

III - Promover maior desempenho no acesso à Internet, com segurança apropriada e capaz de detectar ataques modernos;

IV - Aperfeiçoar o uso de conectividade Internet entre as secretarias apenas para tráfego útil ao desempenho das rotinas de trabalho;

5.3.1 FIREWALL DE PERÍMETRO INTERNET (UTM)

Quando a rede corporativa é conectada à Internet, garantir a segurança contra intrusos passa a ser de importância vital. O método mais efetivo é utilizar um sistema de firewall entre a rede local e a Internet. O firewall certifica que toda comunicação entre a rede corporativa e a Internet esteja em conformidade com a política de segurança definida pela Prefeitura Municipal de Saltinho.

Para efetivamente prover uma segurança real, o firewall necessita identificar e controlar o fluxo de informações que passa através dele, para que a partir de uma tomada de decisão possa permitir, rejeitar, incitar ou logar. as tentativas de comunicação.

Um sistema de firewall necessita obter, armazenar, recuperar e manipular informações derivadas de todas as camadas de comunicação e de outras aplicações.

Os Firewalls são responsáveis pela tarefa de cuidar para que o tráfego não desejado ou não autorizado com origem em uma rede "promíscua", como é o caso da Internet, não atinja o segmento de rede privado da Prefeitura Municipal, sem validação e inspeção.

A solução de segurança de perímetro Internet baseada em firewall considera-se as seguintes premissas:

I - Controlar e segmentar fisicamente o tráfego entre as redes internas, rede DMZ, Internet, Prefeitura Municipal de Saltinho e redes locais remotas (Departamentos); - Implantar uma rede desmilitarizada (DMZ) onde serão acomodados servidores com serviços publicados para a Internet;

II - Integrar funcionalidades de UTM (UnifiedTheat Management) como IPS/IDS, Anti-spam, Antivírus, Anti-spyware e Controle de Conteúdo Web;

III - Estabelecer tunelamento VPN com outras soluções através do protocolo IPS ou SSL; - Atuar preferencialmente em modo Ativo/Passivo para assegurar persistência e manutenção da conectividade em situações de falhas;

IV - Permitir o gerenciamento centralizado de todas as camadas, com funcionalidades de UTM aplicada as regiões de segurança monitoradas.

5.3.2. ACESSO REMOTO SEGURO

No atual ambiente, onde funcionários estão sempre em movimento, a capacidade de acessar informações essenciais a partir de qualquer lugar não é um luxo, mas uma necessidade.

Os criminosos on-line estão sempre em busca de novas maneiras de roubar informações confidenciais, como senhas. Atualmente existem soluções simples de implantar e gerenciar, que oferecem acesso remoto seguro aos recursos da rede para funcionários e prestadores de serviço de forma fácil.

Facilitando a implementação do acesso remoto seguro esse tipo de solução ajuda a maximizar o ROI, diminuir os custos de TI e aumentar a segurança da rede. A solução de segurança de acesso remoto seguro deverá ser implantada por meio de um projeto técnico considerando-se as seguintes premissas:

I - Acesso remoto seguro com criptografia SSL;

II - Acesso remoto assistido para suporte via web;

III - Acesso a aplicações, correio eletrônico e arquivos;

IV - Acesso granular baseado no perfil do usuário/grupo;

V - Integração com solução de autenticação forte;

VI - Sem a necessidade de um cliente de VPN (Clientes);

VII - Integração com serviço de Diretório e RADIUS;

VIII - Controle de acesso integrado ao End-Point;

IX - Independentemente da plataforma utilizado pelo computador.

5.3.3. CONTROLE DE ACESSO A REDE

Uma solução de Controle de Acesso a Rede atua na pré e pós-conexão dos ativos na rede corporativa permitindo aos administradores de TI implementar uma condição que garanta que somente os usuários autorizados tenham acesso à devida informação, no local certo e na hora certa.

Os dados ficam protegidos contra acesso indevido, visto que somente pessoas e/ou computadores expressamente autorizados possuem acesso. A solução pode ainda realizar avaliação de vulnerabilidades e retificação assistida, além de isolar computadores e usuários suspeitos. Com isso, para a solução de controle de acesso a rede lógica considerando-se as seguintes premissas:

I - Prover autenticação, autorização, conformidade e remediação para usuários de dispositivos em rede;

II - Analisar continuamente as ameaças à rede corporativa oriundas de pessoas e máquinas conectadas;

III - Manter a capacidade de rastreabilidade e auditorias de todas as conexões na rede; - Provisionar as aplicações e servidores de forma segura e baseada no perfil de fluxos gerados;

IV - Isolar dispositivos suspeitos e bloquear dispositivos indesejados, garantindo conformidade dos dispositivos conectados à rede;

V - Reduzir a superfície de ameaças geradas por dispositivos conectados internet à rede interna;

5.4. INVENTÁRIO

Uma solução de inventário é projetada para atender a demanda de diversos ambientes de rede. Ela deve reunir dados abrangentes de software e hardware de qualquer computador executando qualquer sistema operacional e também de ativos de rede. Uma variedade de opções de distribuição e coleção de dados garante que a solução trabalhe em qualquer ambiente.

Para ajudar a maximizar o investimento, a solução deve ir além de uma simples obtenção de dados. Ao fornecer um console de gerenciamento, diretivas para alertá-lo sobre informações críticas, e relatórios com qualidade profissional, a solução também devem incluir as ferramentas necessárias para transformar dados de inventário em informações úteis.

A solução deve fornecer inventário abrangente para computadores e ativos de rede, incluindo número de série, inventário de hardware, inventário de auditoria de software, máquina virtual, e informações de usuário/contato quando aplicável.

A solução de inventário deverá considerar as seguintes premissas para desenvolvimento do projeto:

I - Deve apresentar precisão em relatórios para apoio na tomada de decisões a partir de dados concretos, com um inventário abrangente de sistemas em servidores e estações de trabalho;

II - A solução deverá incluir inventário tanto para servidores e estações de trabalho quanto ativos de rede como switches, Access Points, roteadores e appliances de segurança;

III - O projeto de inventário deve identificar e coletar informações de hardware e configurações específicas em servidores através da normalização, consolidação e segurança dos dados em um repositório central e da geração de relatórios com informações detalhadas sobre os ativos.

5.4.1. MONITORAMENTO

Monitorar um ambiente de rede é uma das preocupações mais constantes entre empresas e organizações. Dispor de ferramentas que façam esse controle é fundamental para facilitar o trabalho e identificar imediatamente algum tipo de erro providenciando assim uma ação efetiva.

Um dos aspectos destacados nesse tipo de solução é opção por controle através de gráficos e relatórios, além de alertas pelos quais o administrador pode ter a opção de ser avisado se acontecer qualquer instabilidade na rede, proporcionando um acompanhamento em tempo real dos eventos.

A solução de monitoramento deverá considerar as seguintes premissas para desenvolvimento do projeto:

I - Solução preferencialmente corporativa para provimento de monitoramento básico de ativos de rede via SNMP;

II - Permitir monitoramento básico para switches, roteadores e servidores, verificando estado do equipamento (ligado/desligado), taxa de transferência das interfaces, throughput do equipamento e processamento;

III - Capacidade de envio de alertas sonoros, SMS e e-mails quanto anomalias forem detectadas;

IV - Capacidade de geração de gráficos sumarizados e relatórios detalhados com histórico das ocorrências relacionadas a um ativo

5.4.2. POLÍTICA DE SEGURANÇA

O principal propósito de uma política de segurança é informar aos usuários e equipes as suas obrigações para a proteção da tecnologia e do acesso à informação.

A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados. Outro propósito é oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos.

Portanto, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma política de segurança implícita não faz sentido. Uma política de uso apropriado (Appropriate - ou Acceptable - Use Policy - AUP) pode também ser parte de uma política de segurança.

Ela deveria expressar o que os usuários devem e não devem fazer em relação aos diversos componentes do sistema, incluindo o tipo de tráfego permitido nas redes. A AUP deve ser tão explícita quanto possível para evitar ambiguidades ou maus entendimentos.

Para que uma política de segurança se torne apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de empregados dentro da organização.

É especialmente importante que a gerência corporativa suporte de forma completa o processo da política de segurança, caso contrário haverá pouca chance que ela tenha o impacto desejado.

As características de uma boa política de segurança são:

I. Ela deve ser implementável através de procedimentos de administração, publicação das regras de uso aceitáveis, ou outros métodos apropriados;

II. Ela deve ser exigida com ferramentas de segurança, onde apropriado, e com sanções onde a prevenção efetiva não seja tecnicamente possível;

III. Ela deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes.

5.4.3. PLANO DE CONTINUIDADE DE NEGÓCIO

A elaboração deste plano envolve todas as atividades necessárias para garantir que todos os processos de negócios críticos da Prefeitura Municipal de Saltinho sejam contemplados numa solução de continuidade, que busca o menor custo operacional possível.

Para tanto, é levantada toda a infraestrutura de tecnologia da informação e são mapeadas todas as ameaças que podem determinar uma interrupção de atividades. A adoção de metodologia de continuidade de negócios padrão internacional por consultores de comprovada experiência no assunto, garantem a implantação de um plano eficaz e economicamente viável.

Os benefícios de um plano de continuidade se resumem a:

I - Identificação proativa dos impactos de uma interrupção operacional;

II - Resposta eficiente às interrupções, minimizando o impacto à organização;

III - Capacidade de gerenciar os riscos que não podem ser segurados;

IV - Demonstra uma resposta possível por meio de um processo de testes;

V - Proteger a marca, a reputação e a imagem da organização; - Manter conformidade com suas obrigações legais e regulamentações.

Um plano de continuidade deve oferecer:

I - Garantia de continuidade operacional de todos os processos críticos de negócios;

II - Mitigação dos riscos de todas as ameaças de interrupção;

III - Previsão dos custos e investimentos para implementação do plano;

IV - Dimensionamento dos postos de trabalho de contingência;

V - Documentação e treinamento de todos os procedimentos de contingência e continuidade; - Recomendação do plano de testes de contingência.

6. CONSIDERAÇÕES FINAIS

A falta de investimentos em hardwares, softwares, equipamentos, sistemas operacionais, gerenciadores de banco de dados, além da ausência de procedimentos formais, conduz a um ambiente desprovido de padrões e vulnerável.

Não há sistemas e equipamentos redundantes para provimento de serviços de missão crítica, além de uma equipe técnica enxuta e responsável por uma enorme quantidade de atividades associadas à unidade de tecnologia da informação.

Por outro lado, observa-se que a despeito das deficiências acima descritas, apesar das limitações orçamentárias, há uma preocupação aparente na reversão do quadro atual, que se inicia com a conclusão deste PDTI.

Após a leitura e análise deste documento, consideramos o mesmo **HOMOLOGADO** e apto para orientar nossas possíveis metas quanto ao uso de nossos recursos de tecnologia e informação de nossa instituição.

Saltinho/SP, 27 de outubro de 2021.

HÉLIO FRANZOL BERNARDINO
Prefeito Municipal

Prefeitura do Município de Saltinho
Estado de São Paulo
CNPJ 66.831.959/0001-87

ANEXO II
(DECRETO Nº 2050/2021)

PREFEITURA MUNICIPAL DE SALTINHO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

SALTINHO/SP – OUTUBRO/2021

Av. Sete de Setembro, 1733 • Centro • Saltinho/SP • CEP 13.440-013
Fone: 3439-7800 • e-mail: gabinetedoprefeito@saltinho.sp.gov.br

1. INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Prefeitura Municipal de Saltinho para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da administração.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores da Prefeitura Municipal de Saltinho seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da Prefeitura Municipal de Saltinho quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte. Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu diretor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4. PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Prefeitura Municipal de Saltinho pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A Prefeitura Municipal de Saltinho, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5. REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da Prefeitura Municipal de Saltinho a fim de que a política seja cumprida dentro e fora da empresa.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas quando forem necessárias, sempre que algum fato relevante ou evento motive sua revisão.

Nos contratos celebrados pela Prefeitura Municipal de Saltinho constarão, preferencialmente, anexo de Acordo de Confidencialidade e/ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela administração, nos termos da Lei Geral de Proteção de Dados Pessoais - LGPD.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Os colaboradores deverão assinar um Termo de que foram corretamente orientados sobre as suas responsabilidades nos procedimento de segurança. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao superior competente para conhecimento e análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas gerenciais desenvolvidos pela Prefeitura Municipal de Saltinho ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação. A Prefeitura Municipal de Saltinho exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada na Prefeitura Municipal de Saltinho por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

6. DAS RESPONSABILIDADES ESPECÍFICAS

6.1 - Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada por regime da CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a Prefeitura Municipal de Saltinho e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

6.2 - Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto neste. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

6.3 - Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Prefeitura Municipal de Saltinho.

Os colaboradores deverão assinar um Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Prefeitura Municipal de Saltinho.

Antes de conceder acesso às informações da instituição, os colaboradores casuais e prestadores de serviços deverão assinar um Acordo de Confidencialidade, de forma a atender as regras Lei Geral de Proteção de Dados Pessoais - LGPD.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

7. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI, a Prefeitura Municipal de Saltinho poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede - a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior);

- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

8. USO DO CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores da Prefeitura Municipal de Saltinho quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da Prefeitura Municipal de Saltinho é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a instituição e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico, para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Prefeitura Municipal de Saltinho ou suas unidades vulneráveis a ações civis ou criminais;

- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- Apagar mensagens pertinentes de correio eletrônico quando a Prefeitura Municipal de Saltinho estiver sujeita a algum tipo de investigação.

- Produzir, transmitir ou divulgar mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do município;

- Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

- Vise obter acesso não autorizado a outro computador, servidor ou rede;

- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- Vise burlar qualquer sistema de segurança; vise vigiar secretamente ou assediar outro usuário;

- Vise acessar informações confidenciais sem explícita autorização do proprietário;

- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

- Inclua imagens criptografadas ou de qualquer forma mascaradas;

- Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet);

- Tenha conteúdo considerado impróprio, obsceno ou ilegal;

- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas; tenha fins políticos locais ou do país (propaganda política);

- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- Gerência ou departamento;
- Nome da empresa;
- Telefone(s);
- Correio eletrônico.

9. USO DA INTERNET

Todas as regras atuais da Prefeitura Municipal de Saltinho visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o município, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear

qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Prefeitura Municipal de Saltinho, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos na instituição.

Como é do interesse da Prefeitura Municipal de Saltinho que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome da Prefeitura Municipal de Saltinho para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na instituição e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Direção.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

Qualquer software não autorizado baixado será excluído. Os colaboradores não poderão em hipótese alguma utilizar os recursos da Prefeitura Municipal de Saltinho para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca a alguma atividade específica.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.
Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a Prefeitura Municipal de Saltinho ou de dados de sua

propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da Prefeitura Municipal de Saltinho para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos após análise do superior. Não é permitido acesso a sites de proxy.

10. IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Prefeitura Municipal de Saltinho e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade).
Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na Prefeitura Municipal de Saltinho, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Prefeitura Municipal de Saltinho e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de Recursos Humanos da Prefeitura Municipal de Saltinho é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

Poderão ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá troca imediatamente a sua senha conforme as orientações apresentadas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente providencia o bloqueio do usuário. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou solicitar pessoalmente à área técnica responsável para cadastrar uma nova.

11. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da Prefeitura Municipal de Saltinho, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento do superior responsável. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de

suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no servicedesk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da Prefeitura Municipal de Saltinho (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da Prefeitura Municipal de Saltinho e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do diretor responsável.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados.
- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Prefeitura Municipal de Saltinho ou por terceiros devidamente contratados para o serviço.

- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

- O colaborador deverá manter a configuração do equipamento disponibilizado pela Prefeitura, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

- Todos os recursos tecnológicos adquiridos pela Prefeitura Municipal de Saltinho devem ter imediatamente suas senhas padrões (default) alteradas.

- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

- Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Prefeitura Municipal de Saltinho.

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

- Burlar quaisquer sistemas de segurança.

- Acessar informações confidenciais sem explícita autorização do proprietário.

- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do
titular;

- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

12. DISPOSITIVOS MÓVEIS

A Prefeitura Municipal de Saltinho deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Sistemas, como: notebooks, smartphones e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A Prefeitura Municipal de Saltinho, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a

ter conhecimento em razão de suas funções na Prefeitura Municipal de Saltinho, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade da Prefeitura Municipal de Saltinho e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico autorizado pelo município.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela Prefeitura Municipal de Saltinho.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Prefeitura Municipal de Saltinho, notificar imediatamente seu superior. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a Prefeitura Municipal de Saltinho e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Prefeitura Municipal de Saltinho deverá pedir autorização de seu superior.

Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

13. BACKUP

Todos os backups poderão ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" - períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da Prefeitura Municipal de Saltinho, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

14. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Prefeitura Municipal de Saltinho. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

Saltinho/SP, 27 de outubro de 2021.

HÉLIO FRANZOL BERNARDINO
Prefeito Municipal

DIÁRIO OFICIAL
MUNICÍPIO DE SALTINHO

Conforme Lei Municipal nº 677, de 17 de abril de 2019

www.saltinho.sp.gov.br | www.imprensaoficialmunicipal.com.br/saltinho

Licitações e Contratos

Dispensas - Aviso de Abertura

Dispensa de Licitação 29/2021 – Processo Administrativo 4966/2021.

O Departamento Administrativo torna público para o conhecimento de interessados que está sendo processada uma dispensa de licitação, após competente parecer jurídico elaborado pelo Dr. Jorge Eduardo Vasconcellos Zangarini, OAB/SP 252.707, (juridico@saltinho.sp.gov.br), Diretor do Departamento de Assuntos Jurídico, objetivando a contratação de empresa especializada visando a confecção personalizada e locação de elementos decorativos, iluminação, manutenção, montagem, desmontagem, logística de transporte de todo o material (inclusive descartáveis) para o evento do "Natal de Luz e Fantasia" em que será palco cenográfico a Praça Central "Nossa Senhora de Fátima", no período compreendido entre 06/12/2021 a 06/01/2022. Contratante: Município de Saltinho/SP. Contratada: Fabrício Campos de Oliveira Produções EIRELI ME, CNPJ 18.051.427/0001-84. Valor Global: R$ 47.962,00. Base legal: inciso II, artigo 75, da Lei Federal 14.133/2021. Marcelo Montebello (marcelo@saltinho.sp.gov.br), Diretor Administrativo. Fica autorizada a contratação constante deste processo de dispensa de licitação, nos moldes do inciso VIII, artigo 72, da Lei Federal 14.133/2021, Hélio Franzol Bernardino (gabinetedoprefeito@saltinho.sp.gov.br), Prefeito Municipal (autoridade competente/ordenador das despesas). Este extrato deverá ser publicado em sítio eletrônico oficial (www.saltinho.sp.gov.br) para que produza os efeitos legais, nos termos do parágrafo único, do artigo 72, da aludida legislação. Saltinho/SP, 27/10/2021.

Marcelo Montebello Diretor Administrativo - Portaria 1.599/2021	Hélio Franzol Bernardino Prefeito Municipal

Comunicados

COMUNICADO DE HABILITAÇÃO – TOMADA DE PREÇOS 06/2021

A Comissão de Abertura e Julgamento de Licitações da Prefeitura do Município de Saltinho/SP, com Paço Municipal à Avenida 07 de setembro, 1733, Centro, Saltinho/SP, torna público, para conhecimento de interessados, que deliberou sobre a habilitação referente a documentação apresentados à Tomada de Preços 06/2021, que objetiva a contratação de empresa de engenharia com personalidade jurídica devidamente constituída, para executar obras e serviços de construção de um prédio para abrigar o CRAS – Centro de Referência de Assistência Social, a Rua José Torrezan, Jardim Torrezan, Saltinho/SP, por empreitada e preço global, com fornecimento de materiais, mão de obra e equipamentos necessários. Após a abertura do envelope com os documentos de habilitação e com base no parecer da engenharia, deliberamos por habilitar a empresa: Projecon e Construção Civil Piracicaba Ltda, por ter cumprido com todas as exigências do Edital. Fica aberto o prazo de 05 (cinco) dias úteis, contados da data da publicação oficial, para a eventual apresentação de recursos administrativos. Não havendo recursos, será aberto o envelope com a proposta financeira da empresa habilitada as 09:00 horas do dia 10/11/2021, no Paço Municipal. Saltinho/SP, 27/10/2021.

FERNANDO RENATO HYPPOLITO

Presidente da Comissão de Licitações (Decreto 1982/2021)

Concursos Públicos/Processos Seletivos

Convocação

CONVOCAÇÃO

Convocamos para que se apresente com os documentos abaixo relacionados na Prefeitura de Saltinho sito a Avenida Sete de Setembro n. 1733 Centro na Divisão de Recursos Humanos até dia 29/10/2021 (03 dias úteis da data da convocação) no horário das 08:00 às 10:30 e das 13:00 às 16:00 horas ref. ao Processo

Seletivo 002/2020 de estágio que foi aprovado(a) nessa Prefeitura.

- Tem que estar estudando .

- caso for desistir da vaga mandar email para rh@ saltinho.sp.gov.br

Deverá se apresentar com os seguintes documentos, caso não entre em contato até a data prevista será considerado por essa administração como desistência.

-2 cópias do RG

-2 cópias do CPF

-2 cópias do comprovante de endereço

-cópia da certidão de nascimento/casamento

-Declaração original e legível da Instituição de Ensino constando que está matriculado e frequentando as aulas habitualmente .

-Carteira de Trabalho e 1 foto 3x4 recente

Se for de menor :

2 cópias RG e CPF dos pais

Saltinho, 26/10/2021

Elisângela Aparecida Tenca Camilli

Chefe de Divisão de Recursos Humanos

2º Patricia Aparecida de Macedo Silva Estágio Administração