Prefeitura Municipal da Estância Turística de Holambra

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 1.0

SUMÁRIO

1. ABREVIAÇÕES E TERMOS

ABNT – Associação Brasileira de Normas Técnicas

BO – Boletim de Ocorrência

DTI – Divisão de Tecnologia da Informação

ICP – Infraestrutura de Chaves Públicas

ISO – *International Organization for Standardization*

LGPD – Lei Geral de Proteção dos Dados

NBR – Norma Brasileira

PAD – Processo Administrativo Disciplinar

PMETH – Prefeitura Municipal da Estância Turística de Holambra

PSI – Política de Segurança da Informação

TI – Tecnologia da Informação

Correio eletrônico/E-mail – Serviço utilizado para a troca de mensagens, podendo ou não fazer uso dos recursos da Internet. Também conhecido como e-mail.

Download – Consiste na obtenção de uma cópia, no computador local, de um arquivo originalmente armazenado em um computador remoto ou em uma rede.

Gestor – Refere-se a qualquer pessoa responsável por departamentos ou secretarias municipais. Na PMETH, incluem-se diretores, secretários e chefias de gabinete.

Hardware – Compreende o microcomputador e seus componentes internos, como processador, memórias, unidades de disco fixo, leitores/gravadores de CD/DVD, assim como periféricos como monitores, teclado, mouse, impressoras e outros. Inclui ainda dispositivos portáteis como notebooks, tablets, equipamentos de rede e servidores.

Internet – É o conjunto global de computadores interligados em uma rede de abrangência mundial, comunicando-se por meio de um protocolo único.

Log – São registros que têm o propósito de descrever eventos relacionados ao funcionamento e à utilização dos sistemas pelos colaboradores, assim como interações com outros softwares.

Site – Um sítio, conhecido como site, website ou web site, refere-se a uma coleção de páginas web, ou seja, documentos acessíveis pela Internet.

Software – Refere-se às instruções, programas e dados associados utilizados durante a operação do sistema.

Upload – Consiste na transmissão de dados de um sistema de computador para outro através de uma rede.

2. INTRODUÇÃO

A Política de Segurança da Informação, comumente referida como PSI, representa um guia fundamental que estabelece as diretrizes e práticas corporativas da Prefeitura Municipal da Estância Turística de Holambra (PMETH) com o propósito de proteger os ativos de informação e mitigar a exposição à responsabilidade legal para todos os seus usuários. É mandatório que esta política seja rigorosamente obedecida e aplicada em todas as instâncias da PMETH.

A PSI aqui apresentada tem suas bases alicerçadas nas recomendações preconizadas pelas normas ABNT NBR ISO/IEC 27002:2005 e ISO/IEC 27001, amplamente reconhecida como um código de boas práticas para a gestão da segurança da informação em escala global, o Marco Civil da internet e as normas estabelecidas pela Lei Geral de Proteção dos Dados (LGPD).

Com o propósito de fortalecer a segurança da infraestrutura tecnológica que dá suporte aos serviços públicos, visando orientar os servidores da PMETH sobre a utilização responsável dos ativos de tecnologia da informação disponibilizados.

3. OBJETIVO

Por meio de diretrizes e normas aplicadas a todas as áreas da administração pública, a PSI municipal busca mitigar riscos, garantir a continuidade de operações e

proteger contra ameaças diversas, atendendo aos princípios de autenticidade e legalidade das informações provenientes de diferentes fontes.

A implantação deste documento tem como objetivo promover um comportamento ético na utilização de recursos de TI. Adotar-se-ão novas metodologias de trabalho com práticas preventivas, visando à redução de ameaças e vulnerabilidades, assegurando uma gestão eficiente de recursos, zelando pelos equipamentos e ferramentas de trabalho, reduzindo gastos e aprimorando o atendimento aos munícipes, bem como a produtividade dos colaboradores.

Além disso, busca-se estabelecer o controle de níveis de acesso de fornecedores externos a sistemas, gerenciar os acessos de colaboradores em equipamentos remotos, garantir a segurança em dispositivos e supervisionar atividades vinculadas à TI. Estas ações visam seguir padrões de comportamento relacionados à segurança da informação, adequados às necessidades do serviço público, e proporcionar proteção legal à PMETH e aos indivíduos envolvidos.

4. PRINCÍPIOS

Este documento trata novos padrões comportamentais que devem ser levados em consideração, princípios básicos referentes à segurança da informação:

- **Autenticidade –** Os dados deverão ser certificados com relação a sua origem evitando modificações ao longo do processo;

  Exemplo de ferramentas: biometria e certificado digital.

- **Confidencialidade –** Acesso aos dados somente por indivíduos, entidades, órgãos autorizados;

  Exemplo de ferramentas:Criptografia.

- **Disponibilidade –** Os dados e recursos devem estar disponíveis sempre que necessários para órgãos, indivíduos, entidades ou sistemas autorizados;

  Exemplo de ferramentas: backup, firewall e nobreak.

- **Integridade –** Garantir que os ativos de informação estejam protegidos e não sofram alterações não autorizadas ou acidentais.

Exemplo de ferramentas: assinatura digital.

5. DIRETRIZES E REQUISITOS

Essas diretrizes são aplicáveis a todos os colaboradores, incluindo funcionários, indivíduos físicos ou jurídicos que tenham acesso a dados ou informações do município por qualquer meio.

O escopo abrange a Governança de TI, com o objetivo de impulsionar melhorias nos sistemas de informação e na gestão municipal. Além disso, busca-se manter e otimizar processos, assegurando a segurança das informações e comunicações. Para garantir consistência, é fundamental seguir as diretrizes abaixo como referência:

- Qualquer informação gerada ou recebida pelos colaboradores no curso de suas atividades profissionais para a PMETH é considerada propriedade desta instituição. As exceções devem ser claramente definidas e formalizadas por meio de contrato entre as partes.
- A preservação da segurança da informação, por meio da análise de vulnerabilidades e mitigação de riscos, é essencial para a manutenção dos serviços e a proteção da organização.
- Os usuários devem ser autorizados a acessar apenas as informações essenciais para a execução de suas funções. É crucial evitar a disseminação de dados, mídias e informações consideradas confidenciais. Além disso, é recomendável evitar a exposição de materiais impressos, relatórios, processos e documentos em locais de fácil acesso.
- As aquisições, o recebimento de equipamentos e a contratação de serviços de TI devem estar em conformidade com as leis vigentes, sendo supervisionados pela DTI para garantir especificações e verificações apropriadas.
- Esta política comunica a todos os colaboradores que os ambientes nos setores administrativos da prefeitura, bem como sistemas de gestão, redes e computadores, podem ser monitorados sem aviso prévio, com o intuito de garantir a preservação da segurança dos dados da organização.

- Os equipamentos podem ser retirados, desativados para fins de manutenção, sujeitos a auditoria ou realocados conforme as necessidades e padrões da organização, sem aviso prévio.
- A Política de Segurança da Informação (PSI) será periodicamente atualizada e revisada, considerando o surgimento constante de ameaças cibernéticas, propostas de melhorias em sistemas, mudanças comportamentais e fatores relevantes.
- É dever de cada colaborador permanecer ciente e informado sobre os procedimentos e normas desta política, procurando esclarecimentos junto á DTI sempre que surgirem dúvidas relacionadas ao uso de recursos de TI.
- A responsabilidade pela segurança da informação deve ser comunicada durante a fase de contratação dos servidores, acompanhada de orientações sobre os procedimentos de segurança e uso adequado dos ativos para mitigar riscos. Todos os colaboradores devem ter acesso e conhecimento a esta política.
- Incidentes que impactem a segurança da informação devem ser comunicados imediatamente à DTI.
- Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados durante a fase de levantamento de escopo de um projeto ou sistema. Estes requisitos devem ser justificados, acordados, documentados, implementados e testados ao longo da fase de execução.
- A Prefeitura Municipal da Estância Turística de Holambra isenta-se de responsabilidade por uso indevido, negligente ou imprudente de recursos e serviços concedidos aos colaboradores, reservando o direito de analisar dados e indícios com o propósito de obter elementos probatórios para investigações, bem como de adotar as medidas legais cabíveis.
- A implementação da PSI na PMETH ocorrerá por meio de procedimentos específicos obrigatórios para todos os colaboradores, independentemente de cargo ou função, assim como de vínculo empregatício ou prestação de serviço. O descumprimento dos requisitos expostos nessa PSI sujeitará o

usuário a medidas administrativas e legais conforme as regras internas da instituição.

6. RESPONSABILIDADES ESPECÍFICAS

6.1 Dos Colaboradores em Geral

O termo colaborador engloba toda pessoa física, seja contratada por meio de concurso público, comissão, estágio ou serviço prestado através de pessoa jurídica ou não, que realize atividades dentro ou fora da instituição.

Cada colaborador é inteiramente responsável por qualquer prejuízo ou dano causado à Prefeitura Municipal e/ou a terceiros devido à não conformidade com as diretrizes e normas estabelecidas.

É imperativo que zelem pelo patrimônio público e utilizem adequadamente as ferramentas necessárias para o desempenho de suas funções.

É obrigatório ler, compreender e aderir integralmente aos termos estabelecidos na Política de Segurança da Informação - PSI, assim como às demais normas e procedimentos de segurança em vigor. Além disso, é necessário assinar o Termo de Responsabilidade e Confidencialidade da Prefeitura, formalizando o conhecimento e aceitação plena das disposições contidas nesta Política de Segurança da Informação, juntamente com as demais normas e procedimentos de segurança, assumindo total responsabilidade pelo seu cumprimento.

Em caso de desligamento, é fundamental manter o sigilo e confidencialidade das informações, e, se aplicável, devolver as ferramentas utilizadas em bom estado de conservação.

6.2 Dos Gestores

É dever do gestor adotar uma conduta ética exemplar em relação à segurança da informação, servindo como modelo para os colaboradores sob sua supervisão.

Requerer a assinatura do **Termo de Responsabilidade e Confidencialidade** pelos colaboradores, comprometendo-se a seguir as normas estabelecidas e a manter sigilo e confidencialidade sobre os ativos de informação da Prefeitura Municipal da Estância Turística de Holambra, mesmo após o desligamento.

Na contratação de novos colaboradores, o gestor deve abrir um chamado na plataforma *Help Desk* para solicitar a criação de usuário, indicando o setor e se o novo colaborador terá acesso à rede. Antes de conceder o acesso, é fundamental que o gestor solicite a assinatura do **Termo de Responsabilidade e Confidencialidade** por parte dos colaboradores.

Ao integrar novos colaboradores que precisarão utilizar o sistema de gestão, o gestor deve preencher o **Termo de Responsabilidade dos Sistemas de Gestão** para solicitar o acesso necessário, marcando apenas os acessos estritamente essenciais. Além disso, é imprescindível que o gestor colete a assinatura do colaborador no referido termo.

6.3 Do Departamento de Administração e Recursos Humanos

Dado que todos os desligamentos ocorrem por meio do Departamento de Administração e Recursos Humanos, cabe a este departamento comunicar à DTI sobre todas as dispensas. Essa comunicação visa garantir que as credenciais de acesso aos sistemas, contas de e-mail institucional e ambiente de rede dos usuários sejam desativadas devidamente.

Arquivar o termo de responsabilidade e confidencialidade e o termo de responsabilidade dos Sistemas de gestão dos colaboradores em suas respectivas pastas.

6.4 Da Divisão de Tecnologia da Informação

A divisão tem como principais atribuições administrar, planejar, dimensionar e coordenar a execução de projetos e ações, colocando em prática as diretrizes de maneira atualizada e funcional. Além disso, desempenha outras responsabilidades, tais como:

- Implementar ajustes, realizar atualizações e ferramentas adequadas em todos os dispositivos, seguindo os requisitos de segurança estipulados nesta PSI. Colocar em uso exclusivamente os equipamentos livres de ameaças virtuais, equipados com *software* licenciado ou de código aberto.
- Assegurar, mediante solicitação formal do departamento de administração e recursos humanos, o bloqueio imediato do acesso de usuários em casos de

desligamento da empresa, incidentes, investigações ou outras situações que demandem medidas restritivas para a preservação dos ativos da organização.

- Adotar mecanismos de controle que permitam auditoria e investigações por meio de registros (*logs*). É crucial dedicar atenção especial à segurança de sistemas com acesso externo, destinados ao público, visando proteção contra ataques ou possíveis problemas de disponibilidade. Garantir níveis aprimorados de segurança para esses sistemas, mantendo registros que possibilitem a rastreabilidade em situações de auditoria ou investigação.
- Associar cada usuário ou dispositivo de acesso a computadores, sistemas, bases de dados e outros ativos de informação a um responsável identificável como pessoa física, seguindo a seguinte atribuição de responsabilidades:
    - Os usuários individuais (*logins*) de funcionários será de responsabilidade dos próprios funcionários.
    - Os usuários (*logins*) de terceiros ficarão a cargo do gestor da área contratante.
- Dividir as funções administrativas e operacionais com o objetivo de limitar ao mínimo necessário as autorizações de cada indivíduo. Eliminar ou reduzir a presença de pessoas com a capacidade de excluir registros e trilhas de auditoria de suas próprias ações é fundamental.
- Desenvolver perfis de acesso com privilégios de usuários, impedindo o acesso a recursos de administrador para colaboradores não autorizados.
- Preservar cópias seguras e testadas dos sistemas e dados em locais distintos, com acesso restrito. Gerenciar, assegurar e realizar testes nas cópias de segurança dos programas e dados associados aos processos críticos e pertinentes para a PMETH.
- Desenvolver propostas para metodologias e processos direcionados à segurança da informação, incluindo avaliação de riscos e implementação de medidas de mitigação.
- Disseminar e divulgar as versões da PSI.
- Sugerir e apoiar iniciativas voltadas para a segurança dos ativos de informação.

- Implementar ferramentas de monitoramento de ativos, realizando a inclusão ou configuração de novos e a exclusão de obsoletos ou problemáticos.
- Assegurar que todos os servidores, estações de trabalho e outros dispositivos conectados à rede da empresa estejam configurados para manter a sincronização de seus relógios com os servidores temporais designados pelas autoridades governamentais brasileiras.
- Definir diretrizes formais para a implementação de *software* e *hardware* nos dispositivos da prefeitura, incluindo estações de trabalho, notebooks e outros dispositivos similares.
- Os administradores e operadores de sistemas computacionais têm a capacidade, devido aos seus privilégios, de acessar arquivos e dados de outros usuários. Entretanto, tal acesso só será concedido quando necessário para a condução de atividades operacionais sob sua responsabilidade, tais como a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
- Realizar avaliações periódicas da eficácia dos controles de segurança, além de detectar e alertar sobre casos de fraudes quando identificados. Manter os dispositivos de segurança e sistemas constantemente atualizados, acompanhando o surgimento de novas tecnologias para garantir uma postura proativa em relação à segurança da informação.
- Estabelecer e manter registros de auditoria com um nível de detalhamento adequado para rastrear potenciais falhas e fraudes. Ao gerar e manter essas trilhas em formato eletrônico, implementar controles de integridade para conferir a validade jurídica, tornando-as evidências robustas e confiáveis.
- O gestor da informação deve receber uma notificação antecipada sobre o término do prazo de retenção, oferecendo a oportunidade de ajustá-lo antes que a informação seja permanentemente descartada pelo custodiante. Isso visa proporcionar uma gestão ativa e consciente do ciclo de vida da informação.
- Desenvolver um plano abrangente para implementar, fornecer e monitorar a capacidade de armazenamento, processamento e transmissão necessária, assegurando a segurança exigida pelos diferentes departamentos. Esse

processo visa atender de forma eficaz e contínua às demandas específicas de cada setor, garantindo um ambiente seguro e operacionalmente eficiente.

- Monitorar o ambiente de TI de maneira abrangente, produzindo indicadores e registros relativos a diversos aspectos, tais como:
    - Utilização da capacidade instalada da rede e dos equipamentos;
    - Tempo de resposta no acesso à internet e aos sistemas críticos;
    - Períodos de inacessibilidade no acesso à internet e aos sistemas críticos;
    - Ocorrências de segurança, englobando vírus, trojans, furtos, acessos não autorizados, entre outros;
    - Atividades de todos os colaboradores durante os acessos às redes externas, incluindo a internet, como os sites visitados, e-mails recebidos/enviados e atividades de transferência de arquivos.

6.4 Do Monitoramento e da Auditoria

Com o objetivo de assegurar o cumprimento das diretrizes mencionadas nesta Política de Segurança da Informação (PSI), a Prefeitura Municipal da Estância Turística de Holambra reserva-se o direito de:

- Implementar sistemas de supervisão em estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou sem fio, e demais elementos da rede. As informações produzidas por esses sistemas poderão ser utilizadas para identificar usuários, bem como os acessos efetuados e o conteúdo manipulado.
- Tornar divulgadas as informações obtidas pelos sistemas de supervisão e auditoria, quando exigido por via judicial ou mediante solicitação de autoridades superiores.
- Realizar, a qualquer momento, inspeções físicas nas máquinas de sua propriedade.
- Implementar sistemas de salvaguarda, tanto preventivos quanto detectáveis, a fim de garantir a segurança das informações e dos perímetros de acesso.

7. CONTROLE DE ACESSO

7.1 Lógico

Acesso lógico refere-se à entrada em sistemas, redes e recursos que demandam credenciais de identificação, como login, autorizando o colaborador a utilizar determinadas ferramentas da organização. Essas credenciais são pessoais e confidenciais, sendo estritamente proibido o seu compartilhamento.

Se houver login compartilhado por mais de um colaborador, a responsabilidade perante a Prefeitura Municipal e a legislação (código penal art. 307 – falsa identidade) recairá sobre os usuários que o utilizarem.

Essa norma estabelece critérios de responsabilidade sobre o uso dos dispositivos de identificação, aplicando-se a todos os colaboradores. Para mitigar riscos, as seguintes diretrizes devem ser seguidas:

- A solicitação de permissões de acesso a sistemas, redes, ativos e a criação de usuários deve ser feita pelo gestor por meio de um chamado na plataforma *Help Desk*, o gestor deve detalhar os dados do usuário como nome, CPF, localização e se o usuário terá acesso a pastas de rede.
- O solicitante de acesso deverá assinar o Termo de Responsabilidade e Confidencialidade, conforme Anexo I, a ser arquivado pelo Departamento de Administração e Recursos Humanos.
- Quando o acesso às pastas de rede é concedido, este será restrito à rede específica do setor ao qual o usuário está designado.
- Os privilégios concedidos devem estar alinhados com as necessidades específicas das funções desempenhadas pelo usuário.
- As credenciais de acesso são inicialmente geradas de forma padrão, sendo a responsabilidade do colaborador efetuar a substituição por uma credencial forte e pessoal após o primeiro login. Para atender aos critérios mínimos de segurança, é necessário seguir algumas diretrizes, incluindo a utilização de caracteres alfanuméricos diversos (letras maiúsculas, minúsculas e números), um comprimento mínimo de 8 (oito) caracteres e a incorporação de caracteres especiais (@, #, $, %, &). As senhas não devem conter dados pessoais, como

nome, sobrenome, data de nascimento, e não devem ser constituídas de combinações óbvias de teclado, como “abcdefg”, “12345678”, entre outras.

- As senhas não devem ser registradas (em papéis, adesivos) ou armazenadas em documentos eletrônicos (Word, Excel, etc.).
- A senha deve ser renovada periodicamente como medida de garantia de segurança. Em caso de esquecimento, perda ou suspeita de acesso não autorizado por terceiros, os usuários devem solicitar imediatamente a emissão de uma nova senha através de chamado na plataforma *Help Desk*.
- A troca de senhas deve ocorrer a cada 90 (noventa) dias, e as 12 (doze) senhas anteriores não podem ser reutilizadas. O sistema exige a renovação das senhas dentro desse prazo máximo.
- Após 5 (cinco) tentativas de acesso malsucedidas, a conta do usuário será automaticamente bloqueada. Para realizar o desbloqueio, é imprescindível que o usuário entre em contato com a Divisão de Tecnologia da Informação (DTI).
- Os servidores da divisão de TI não mantêm registro das senhas e não têm meios para conhecer a senha atual do usuário.
- Qualquer ação realizada mediante o uso da senha pessoal é de responsabilidade exclusiva do respectivo usuário.
- Todos os acessos devem ser prontamente bloqueados quando se tornarem desnecessários. Portanto, no momento em que um usuário for demitido ou solicitar demissão, o Departamento de Administração e Recursos Humanos deve comunicar imediatamente essa informação à DTI para que as devidas medidas sejam tomadas. Essa mesma prática se aplica a usuários cujos contratos ou prestação de serviços tenham se encerrado, assim como aos usuários de testes e em outras situações similares.
- A detecção de acessos desconhecidos ou a suspeita de acessos aos recursos de TI devem ser prontamente comunicadas à divisão competente para que sejam tomadas as devidas providências.
- O acesso remoto a ativos só é permitido mediante a prévia autorização da divisão de TI. Colaboradores devem solicitar esse acesso, identificando-se e fornecendo informações detalhadas sobre o motivo, local e período de

utilização. Tais solicitações devem ser conduzidas por meios seguros, garantindo a integridade e legitimidade da atividade.

- O acesso de administrador aos recursos de TI é restrito exclusivamente ao setor de TI, salvo em casos excepcionais de extrema necessidade, que devem ser comunicados e autorizados pelo gestor responsável.
- O colaborador solicitante de acesso aos sistemas de gestão deverá assinar o Termo de Responsabilidade dos Sistemas de Gestão, conforme descrito no Anexo II. Este documento será arquivado pelo Departamento de Administração e Recursos Humanos. Adicionalmente, o gestor responsável também deve assinar o termo, indicando seu nome de maneira legível ou através de um carimbo.

7.2 Acesso à Infraestrutura

O acesso à infraestrutura do datacenter está estritamente limitado aos colaboradores da Divisão da Tecnologia da Informação (DTI). Qualquer necessidade de acesso deve ser supervisionada por um membro da equipe da DTI, garantindo assim uma abordagem controlada.

A sala deve ser mantida permanentemente fechada com uma fechadura biométrica para prevenir qualquer acesso não autorizado. Além disso, a temperatura é cuidadosamente controlada para evitar qualquer possibilidade de superaquecimento. Essas medidas visam reforçar a segurança e garantir o funcionamento eficiente e seguro do datacenter.

8. ASSINATURA ELETRÔNICA

Os documentos digitais produzidos na esfera da Prefeitura Municipal da Estância Turística de Holambra poderão ter sua autenticidade e integridade garantidas por meio da aplicação de assinatura eletrônica. Documentos com assinatura digital têm validade equiparada à de documentos assinados fisicamente, conforme regulamentado pelo Decreto Federal nº 10.543, de 13/11/2020 (modificado pelo Decreto Federal nº 10.900/2021).

A assinatura eletrônica ocorrerá por meio de:

- Assinatura eletrônica simples: possibilita identificar o signatário e associar seus dados a outros em formato eletrônico.
- Assinatura eletrônica avançada: emprega certificados não emitidos pela ICP-Brasil ou outros meios aceitos pelas partes para comprovar autoria e integridade de documentos eletrônicos, como é o caso da assinatura GOV.BR.
- Assinatura eletrônica qualificada: utiliza certificado digital ICP-Brasil (infraestrutura de Chaves Públicas Brasileira).

A prática de atos assinados eletronicamente importará a aceitação das normas regulamentares sobre o assunto. A assinatura eletrônica é de uso pessoal e intransferível, sendo de responsabilidade do titular sua guarda e sigilo. A utilização da assinatura eletrônica individual indevida será de responsabilidade exclusiva do titular.

9. INTERNET

As normas da Prefeitura Municipal da Estância Turística de Holambra visam promover um comportamento ético e profissional na utilização da internet. Embora a conexão direta e constante da rede corporativa da instituição com a internet apresenta um vasto potencial de benefícios, ela também acarreta riscos substanciais para os ativos de informação. Considerando isto, a PMETH possui normas a serem seguidas que são detalhadas a seguir:

- Toda informação que é acessada, enviada, recepcionada ou produzida na internet está sujeita a divulgação e auditoria. Em total conformidade com a legislação vigente, a PMETH reserva-se o direito de monitorar e registrar todas as interações realizadas em sua rede.
- Os dispositivos, tecnologia e serviços disponibilizados para a conexão à internet são de propriedade da instituição, que reserva o direito de analisar e, quando necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação de trabalho ou em áreas privadas da rede. Além disso, será efetuado

o monitoramento do volume de tráfego na Internet e na rede, incluindo os endereços web (http://) visitados, com o objetivo de garantir o cumprimento desta política.

- É estritamente proibido o uso das áreas, serviços e ativos de informação para propósitos ilegais ou em desacordo com esta política de uso, causando danos, desativação, sobrecarga, prejuízo a qualquer área, serviço ou conteúdo, assim como interferência no uso e participação de colaboradores.
- A PMETH monitora a rede interna para garantir a integridade dos dados e programas, buscando prevenir tentativas de alteração nos parâmetros de segurança. Qualquer colaborador que realizar tais modificações sem o devido credenciamento e autorização será considerado inadequado, e os riscos relacionados serão comunicados ao colaborador e ao gestor correspondente. O uso de recursos para atividades ilícitas sujeitará o infrator a ações administrativas e penalidades conforme processos civil e criminal, com a instituição colaborando ativamente com as autoridades competentes.
- É responsabilidade do colaborador assegurar que dados confidenciais sejam armazenados exclusivamente nas pastas designadas para cada setor, evitando a pasta “público”.
- Não é permitido tentar obter acesso não autorizado a qualquer área, serviço e conteúdo dos sistemas ou redes de computadores conectados, seja por ações mal-intencionadas, corrupção de credenciais ou outros meios
- O colaborador deve utilizar e acessar a rede, internet e/ou e-mail institucional exclusivamente para fins profissionais, voltados à execução e desempenho dos objetivos da Administração Pública. Qualquer uso fora desses propósitos poderá ser interrompido sem aviso prévio ao colaborador. Os gestores podem requerer a divisão de TI, o bloqueio e a limitação do acesso dos colaboradores, mediante chamado no sistema *Help Desk*.
- A utilização dos recursos computacionais e de comunicação da Administração Pública para navegação em sites das categorias abaixo, bem como a exposição, armazenamento, distribuição, edição e gravação estão estritamente proibidos:

- Conteúdo com teor sexual explícito, especialmente relacionado à proteção da infância, ou qualquer material contrário a princípios éticos e morais;
- Conteúdo impróprio, ofensivo, preconceituoso ou discriminatório;
- Apologia à violência, terrorismo ou uso de drogas;
- Violação de direitos autorais (pirataria);
- Práticas fraudulentas de qualquer natureza;
- Compartilhamento de arquivos não relacionados às atividades da Prefeitura sem autorização do superior hierárquico;
- Sites de streaming, séries, filmes, vídeos e arquivos de entretenimento, como Netflix, HBO Max, Disney Plus e/ou similares, estão restritos, exceto em atividades relacionadas ao departamento com autorização do gestor.

- A utilização de qualquer recurso da PMETH para atividades ilegais constitui motivo para investigação interna por meio de sindicância ou PAD (processo administrativo disciplinar). A Administração Pública cooperará ativamente com as autoridades policiais ou judiciais em tais casos.
- O acesso a sites de proxy não é permitido.
- O acesso a *softwares* ponto a ponto (como Kazaa, uTorrent e similares) não será permitido.
- Colaboradores com acesso à internet estão proibidos de realizar o *upload* de qualquer *software* licenciado à PMETH ou de dados pertencentes à instituição para parceiros e clientes sem expressa autorização do responsável pelo *software* ou pelos dados.
- É vedado o uso dos recursos da PMETH para a propagação deliberada de vírus, *worms*, cavalos de Troia, spam, assédio, perturbação ou programas de controle de outros computadores.
- Os colaboradores não estão autorizados, em hipótese alguma, a utilizar os recursos da PMETH para efetuar o *download* ou distribuição não autorizada de *software*. Fica expressamente proibido o uso, instalação, cópia ou distribuição de *softwares* que possuam direitos autorais, marca registrada ou

patente na internet. Qualquer *software* não autorizado será excluído pela Divisão de Tecnologia da Informação.

- O funcionário que compartilhar informações confidenciais da Administração Pública em fóruns de discussão, conversas, plataformas de mensagens, e-mails, chamadas telefônicas, redes sociais, WhatsApp, entre outros, seja a divulgação intencional ou acidental, estará sujeito às sanções determinadas por lei, processos internos e/ou conforme a legislação vigente, incluindo responsabilidade criminal ou civil.
- Somente os colaboradores devidamente autorizados pela instituição estão autorizados a copiar, capturar, imprimir ou enviar imagens da tela para terceiros. Eles devem observar a norma interna de uso de imagens, a Lei de Direitos Autorais, a proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.
- É proibido a utilização de jogos, inclusive os onlines.
- Apenas os colaboradores devidamente autorizados a representar a PMETH nos meios de comunicação estão autorizados a se manifestar, seja por e-mail, entrevista online, podcast, documento físico, entre outros.
- A transferência de programas, jogos e similares para a rede interna da Administração Pública sem autorização específica do gestor é proibida.
- É vedado o *download* de arquivos com extensões como .exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .d11, e de programas de entretenimento ou jogos, exceto aqueles estritamente relacionados aos serviços inerentes à função do colaborador, com vistas às atividades da Administração Pública.
- É vedado ao colaborador revelar, fora do âmbito profissional/institucional, qualquer fato ou informação de que tenha conhecimento por força de suas atribuições, exceto em decorrência de decisão competente na esfera legal ou judicial.
- Visando o interesse da Administração Pública em manter seus colaboradores bem informados, é permitido o uso de sites ou serviços de notícias, desde que essa utilização não comprometa a largura de banda da rede nem

perturbe o bom andamento das atividades. Em todos os casos, é necessário observar os termos estabelecidos nesta política de uso.

- Exceções e casos omissos devem ser reportados ao gestor ao qual o colaborador está vinculado.

10. E-MAIL INSTITUCIONAL

Essa ferramenta estará disponível exclusivamente para a realização de atividades relacionadas ao cumprimento da função. Cabe ao gestor avaliar a necessidade de utilização por parte do colaborador.

A utilização do e-mail institucional não confere prerrogativas sobre o mesmo, tampouco outorga autoridade para conceder acesso a terceiros, pois engloba informações pertencentes à PMETH.

A seguir, apresentamos as diretrizes para o correto emprego desta ferramenta:

- Cada colaborador é responsável por preservar sua credencial de forma segura, mantendo a conta sempre fechada quando não estiver em uso. Em situações de recebimento de spam ou de mensagens de remetentes desconhecidos, é recomendável excluí-las para prevenir a possibilidade de infecção por vírus e, consequentemente, a propagação de ameaças.
- As mensagens de correio eletrônico devem sempre conter assinatura no seguinte formato:
    - Nome do colaborador;
    - Setor de atuação;
    - Nome da instituição, Prefeitura Municipal da Estância Turística de Holambra;
    - Número(s) de telefone;
    - Endereço de correio eletrônico.
- Adicionalmente, ressalta-se que é terminantemente proibido aos colaboradores o uso do e-mail institucional da PMETH para:

- Enviar mensagens não solicitadas para múltiplos destinatários, a menos que estejam relacionadas a um uso legítimo da instituição;
- Enviar mensagens de correio eletrônico utilizando o endereço de seu departamento ou o nome de usuário de outra pessoa, ou ainda utilizar endereços de correio eletrônico não autorizados;
- Transmitir mensagens eletrônicas que possam tornar seu remetente, a PMETH ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos, e afins sem a devida autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos com o intuito de ocultar a identidade de remetentes e/ou destinatários, visando evitar as penalidades previstas;
- Apagar mensagens relevantes de correio eletrônico durante qualquer investigação envolvendo os departamentos da PMETH;
- Abrir arquivos anexos de remetentes desconhecidos ou inesperados. Em caso de ocorrência acidental, relatar imediatamente a divisão de Tecnologia da Informação;
- Registrar-se em plataformas de entretenimento, comércio online e receber propagandas, assim como para divulgar anúncios publicitários, mensagens encadeadas, vírus, conteúdos prejudiciais, conteúdos ofensivos, obscenos, pornográficos ou que violem qualquer norma legal;
- Produzir, transmitir ou disseminar mensagens que:
    - contenham ameaças cibernéticas, como spam, bombardeio de e-mails e vírus de computador.
    - incluam 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.
    - tenham o propósito de obter acesso não autorizado a outro computador, servidor ou rede.

- busquem interromper serviços, servidores ou redes de computadores por meio de métodos ilícitos.
- tenham a intenção de burlar sistemas de segurança.
- visem vigiar ou assediar outros usuários.
- tenham como objetivo acessar informações confidenciais sem a explícita autorização do proprietário.
- procurem acessar indevidamente informações que possam causar prejuízos a qualquer pessoa.
- incluam imagens criptografadas ou mascaradas de qualquer forma.
- possuam conteúdo considerado impróprio, obsceno ou ilegal.
- tenham caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, religioso entre outros.
- contenham materiais preconceituosos ou discriminatórios baseada em orientação sexual, raça, gênero, incapacidade física ou mental ou outras situações protegidas.
- manifestações de apreço ou desapreço a políticos locais ou nacionais (propaganda política).
- incluam material protegido por direitos autorais sem a permissão explícita do detentor dos direitos.

11. ESTAÇÕES DE TRABALHO E RECURSOS TECNOLÓGICOS

Todo colaborador é responsável por aderir às diretrizes estabelecidas para o adequado uso e preservação dos ativos de TI, garantindo a integridade do patrimônio público. Estes ativos devem ser empregados unicamente como ferramentas de trabalho para a realização das atividades designadas e operando com a seguintes diretrizes:

- Os arquivos devem ser armazenados no servidor de arquivos do setor para possibilitar a realização de cópias de segurança (backup). Arquivos salvos

localmente (entenda-se no disco rígido da estação de trabalho) não são respaldados, sendo de responsabilidade do colaborador em caso de perda ou danos.

- A pasta do servidor de arquivos denominada 'público' é compartilhada por todos os usuários conectados à rede, tornando-a suscetível a modificações ou exclusões sem garantias de segurança. Portanto, é estritamente desaconselhado utilizá-la como meio de armazenamento, devendo ser reservada exclusivamente para arquivos temporários.
- É responsabilidade do colaborador assegurar que dados confidenciais e sensíveis sejam armazenados exclusivamente nas pastas designadas para cada setor, evitando a pasta ‘público’.
- Todos os documentos que forem digitalizados deverão ser transferidos para a pasta de rede da unidade, caso haja a necessidade de salvá-los, pois arquivos digitalizados na pasta de rede ‘scanner’ permanecerão salvos por no máximo 45 dias, podendo ser apagados de maneira automatizada após este período.
- A divisão de Tecnologia da Informação realizará regularmente a limpeza da pasta ‘público’ para garantir a confidencialidade das informações e otimizar o uso dos recursos computacionais.
- É fundamental que, ao se ausentar da estação de trabalho, o colaborador remova suas credenciais de acesso, realizando a desautenticação.
- Em caso de furtos, roubos ou extravios de ativos da PMETH, é imprescindível comunicar imediatamente a DTI para que seja lavrado um Boletim de Ocorrência visando à apuração dos fatos.
- A colocação de adesivos, propagandas ou imãs em equipamentos não é permitida. Apenas etiquetas de identificação ou patrimônio são autorizadas.
- O uso de equipamentos de TI por pessoas sem vínculo com a PMETH não é permitido, exceto nos casos específicos de equipamentos destinados a essa função.
- A execução de qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação está proibida sem o conhecimento prévio e a supervisão de um colaborador da DTI, ou designado

por este. Para testes, os responsáveis devem solicitar autorização antecipada à DTI, assumindo plena responsabilidade jurídica e técnica pelas ações realizadas.

- A utilização de pendrives, mídias removíveis e outras fontes externas deve se restringir exclusivamente à execução de atividades de trabalho.
- É estritamente proibido armazenar arquivos pessoais (fotos, vídeos, documentos) nos equipamentos do município.
- O uso de impressoras de repartições públicas para a impressão de documentos pessoais é expressamente proibido.
- É requisito essencial que os sistemas e computadores estejam equipados com versões atualizadas do software antivírus, devidamente instaladas e ativadas de forma permanente. No caso de suspeita de vírus ou problemas na funcionalidade, solicita-se ao usuário que contate o departamento técnico responsável, registrando um chamado no *Help Desk*.
- É estritamente proibido que colaboradores da PMETH e/ou titulares de contas privilegiadas realizem a execução de comandos ou programas que possam causar sobrecarga nos serviços da rede corporativa, a menos que haja uma solicitação prévia e autorização da divisão de TI.
- Os colaboradores têm a responsabilidade de comunicar ao departamento técnico qualquer identificação de dispositivo desconhecido conectado ao seu computador.
- O colaborador é incumbido de manter a configuração do equipamento fornecido pela divisão de TI, aderindo aos controles de segurança estabelecidos pela Política de Segurança da Informação e pelas normas específicas da instituição. Nesse contexto, assume a responsabilidade como custodiante de informações.
- É obrigatório comunicar a DTI toda movimentação de ativos de TI primeiramente, a fim de avaliar a viabilidade e prevenir possíveis deteriorações financeiras e físicas no patrimônio público.
- É fundamental que os equipamentos mantenham, de forma segura, registros de eventos que incluam a identificação dos usuários, datas e horários de acesso.

- É obrigatório que todas as senhas padrão (*default*) dos ativos tecnológicos adquiridos pela PMETH sejam alteradas imediatamente.
- Proibido tentar ou obter acesso não autorizado a outros computadores, servidores ou redes.
- Vedada a manipulação de sistemas de segurança.
- É expressamente proibido acessar informações confidenciais sem a autorização explícita do proprietário.
- Não é permitido monitorar secretamente outras pessoas por meio de dispositivos eletrônicos ou softwares.
- Está terminantemente proibida a interrupção de serviços, servidores ou redes de computadores por métodos ilícitos ou não autorizados.
- É estritamente vedado utilizar qualquer recurso tecnológico para cometer ou participar de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular.
- Hospedagem de pornografia, material racista ou qualquer conteúdo que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública não é permitida.

12. DISPOSITIVOS MÓVEIS

Com o intuito de otimizar a mobilidade e a troca de informações entre seus colaboradores, a Prefeitura Municipal da Estância Turística de Holambra autoriza o emprego de dispositivos móveis. Considera-se 'dispositivo móvel' todo dispositivo eletrônico dotado de funcionalidades de mobilidade, pertencente à instituição, como notebooks, smartphones e drives portáteis.

Esta norma visa estabelecer diretrizes para a manipulação, prevenção e responsabilidade no uso de dispositivos móveis, sendo aplicável a todos os colaboradores que façam uso desses equipamento:

- A PMETH, como detentora dos equipamentos disponibilizados, reserva o direito de realizar inspeções a qualquer momento, especialmente se for necessário realizar manutenções de segurança.

- O funcionário, portanto, compromete-se a não utilizar, revelar ou compartilhar de forma alguma, seja diretamente ou indiretamente, para benefício próprio ou de terceiros, qualquer informação, seja ela confidencial ou não, à qual tenha acesso em decorrência de suas responsabilidades na PMETH. Este compromisso permanece mesmo após o término de seu vínculo com a instituição.
- É obrigatório que o colaborador empregue senhas de bloqueio automático em seus dispositivos móveis.
- A modificação da configuração dos sistemas operacionais dos dispositivos, especialmente no que diz respeito à segurança e à geração de logs, não será tolerada em nenhuma circunstância, a menos que haja comunicação prévia e autorização da área responsável. Além disso, qualquer alteração deve ocorrer sob a supervisão, assistência ou presença de um colaborador da divisão de Tecnologia da Informação.
- É responsabilidade do colaborador garantir que não mantenha ou utilize programas e/ou aplicativos que não tenham sido instalados ou autorizados por um colaborador da divisão de Tecnologia da Informação.
- Qualquer reprodução não autorizada dos *softwares* instalados nos dispositivos móveis fornecidos pela instituição será considerada uso inadequado do equipamento e uma infração legal aos direitos autorais do fabricante.
- Caso ocorra furto ou roubo de um dispositivo móvel fornecido pela PMETH, é incumbência do colaborador notificar imediatamente seu gestor direto e a divisão de Tecnologia da Informação. Além disso, deve buscar auxílio das autoridades policiais e registrar, o mais rápido possível, um boletim de ocorrência (B.O).
- O colaborador deve ter plena ciência de que a utilização inadequada do dispositivo móvel implicará na aceitação de todos os riscos associados à sua má utilização. Ele será o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que possam causar à PMETH ou a terceiros.

- É estritamente vedada a saída de qualquer equipamento pertencente à Prefeitura Municipal de Holambra por parte do colaborador, a menos que haja uma autorização expressa formalizada por um documento escrito e assinado por um gestor.
- A utilização de equipamentos portáteis, tais como smartphones, tablets e notebooks, que não tenham sido fornecidos pela instituição ao colaborador, não será autorizada para uso e conexão na rede corporativa. Recomenda-se, para esse propósito, o uso dos pontos de wifi disponíveis em vários setores e localidades, identificados como "WFUN". Quaisquer danos, extravios ou problemas decorrentes de equipamentos particulares serão de responsabilidade exclusiva do proprietário.
- Para obter acesso à rede WFUN, o gestor do departamento ou unidade precisa preencher a solicitação de inclusão de usuários na rede WiFi, conforme descrito no anexo III. Ressalta-se que esta rede deve ser utilizada exclusivamente para fins relacionados ao serviço da PMETH e que todos os acessos poderão ser registrados e monitorados.

13. TRATAMENTO DE DADOS

As informações confidenciais e/ou sigilosas presentes em documentos impressos devem passar pelo processo de fragmentação antes de serem descartadas. Somente após essa medida de segurança, os documentos poderão ser eliminados de forma apropriada.

O tratamento de dados deve seguir as diretrizes estabelecidas na ‘Política de Proteção de Dados Pessoais (PPDP)’ da instituição, juntamente com as disposições do Decreto nº 1732/2022, que regulamenta a política de proteção de dados no âmbito do Município de Holambra, e as normas da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018 - LGPD).

14. BACKUP

A PMETH já implementou uma política de backup como parte integrante de suas medidas de segurança da informação. Esta política assegura a preservação e a recuperação eficiente de dados em casos de incidentes, garantindo a continuidade operacional sem perdas significativas. Todos os colaboradores são orientados a seguir as diretrizes estabelecidas nesta política, assegurando a integridade e a disponibilidade dos dados críticos da instituição. Para detalhes específicos, consulte o documento completo da Política de Backup disponível no site institucional do município.

15. ANEXOS

ANEXO I - MODELO DO TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Pelo presente instrumento, eu _____, CPF n.º _____, lotado (a) no cargo _____ em razão de seu vínculo com a PREFEITURA DO MUNICÍPIO DA ESTÂNCIA TURÍSTICA DE HOLAMBRA, firma o presente TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE, mediante as estipulações consignadas neste instrumento:

DECLARO QUE:

1. Tenho conhecimento e acesso à Política de Segurança da Informação (PSI), bem como as demais normas de Segurança da Informação necessárias ao meu trabalho, que se encontram disponíveis para consulta e/ou impressão no website da PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE HOLAMBRA, aos quais li na íntegra, tomando conhecimento e ciência de suas diretrizes;
2. Compreendi completamente os termos, diretrizes, conceitos e condições de uso da Política de Segurança da Informação (PSI), bem como as demais normas de Segurança da Informação necessárias ao meu trabalho, me comprometendo a cumprir integralmente as diretrizes constantes em tais documentos;
3. Estou ciente e de acordo que, tanto os ativos de informação, quanto a infraestrutura tecnológica da PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE HOLAMBRA somente poderão ser utilizados para fins exclusivamente profissionais e relacionados às atividades que exerço neste órgão;
4. Estou ciente que é realizado o monitoramento de todos os acessos e comunicações ocorridos através da infraestrutura tecnológica da PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE HOLAMBRA;
5. Estou ciente que as violações da Política de Segurança da Informação (PSI), bem como das demais normas de Segurança da Informação são passíveis de sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativas, cíveis e penal, nos termos da legislação em vigor;
6. Estou ciente de que, se necessário, o uso de assinatura eletrônica (engloba-se certificado digital) é de minha responsabilidade, incluindo a posse, proteção e os devidos cuidados associados. Reconheço que a assinatura eletrônica é pessoal e intransferível, compreendendo que empréstimos ou transferências a terceiros são estritamente proibidos.
7. Comprometo-me a não revelar, fato ou informações de qualquer natureza a que eu tenha conhecimento e/ou acesso por força das minhas atribuições, mesmo após o encerramento do contrato de trabalho com a PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE HOLAMBRA.

Holambra, ___ de _____ de 20___.

_____

Assinatura do Colaborador/Terceirizado

_____

Assinatura do Gestor Responsável **com Carimbo ou nome legível**

ANEXO II - MODELO DO TERMO DE RESPONSABILIDADE - SISTEMAS DE GESTÃO

TERMO DE RESPONSABILIDADE - SISTEMAS DE GESTÃO

Por meio deste, formalmente solicito a implementação dos acessos ao sistema de gestão de minha unidade. Assumo total responsabilidade pelo acesso às informações, comprometendo-me a utilizá-las de maneira profissional e adequada. Estou ciente de que todas as ações realizadas no sistema são de minha responsabilidade.

Nome Completo:	
CPF:	**Departamento:**
Local de trabalho:	**Telefone para contato:**

Holambra, ___ de _____ de 20___.

_____

Assinatura do Colaborador/Terceirizado

_____

Assinatura do Gestor Responsável **com Carimbo ou nome legível**

ANEXO III - MODELO DA SOLICITAÇÃO DA INCLUSÃO DE USUÁRIOS NA REDE WIFI

SOLICITAÇÃO DE INCLUSÃO DE USUÁRIOS NA REDE WIFI

Venho por meio desta solicitar a inclusão dos seguintes funcionários para acesso à rede WiFi da Prefeitura.

Departamento/Unidade: _____

Holambra, ___/_____/_____

Nome	CPF

Justificativa para fins profissionais:

Declaro estar ciente que todo acesso à rede estará sendo registrado e monitorado, e que a rede WiFi só deve ser utilizada para fins relacionados ao serviço da Prefeitura.

_____

Assinatura do Gestor Responsável **com Carimbo ou nome legível**