Município de

Espírito Santo do Pinhal

-Política de Segurança da Informação-

SUMÁRIO

1. ABREVIAÇÕES E TERMOS

DGPRITI - Departamento de Gestão de Projetos, Relações Institucionais e Tecnologia da Informação

PDTI - Plano Diretor de Tecnologia da Informação

PMESP – Prefeitura do Município de Espírito Santo do Pinhal

PSI - Política de Segurança da Informação

TI - Tecnologia da Informação

Colaborador – Todo servidor com vínculo com a organização sendo contrato temporário, efetivo, comissionado, estágio, prestador de serviço, visitante ou usuários externos de recursos do município.

Gestor – Todo responsável por departamentos ou secretarias do município. No caso da PMESP os diretores, secretários e chefia de gabinete.

Log - Informações que tem por objetivo descrever eventos sobre o funcionamento, utilização dos sistemas por colaboradores ou interações com outros softwares.

Mitigar – Diminuir o impacto, reduzir. Nesse documento é utilizado no sentido de diminuir os impactos causados por riscos conhecidos ou identificados.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Informação é um conjunto de dados que com o passar dos tempos tem se tornado um ativo de valor imensurável para empresas e cidadãos.

A rede de internet e suas derivações tornaram-se meios de distribuição de informações em velocidades cada vez maiores. Nessa mesma velocidade, fraudes e golpes vem se alastrando das mais diversas formas.

Tendo em vista a necessidade de proteção dos dados da organização, dados de colaboradores e munícipes, conservação de equipamentos, preservação dos direitos autorais e diretrizes para uso dos recursos de tecnologia da informação (TI) disponibilizados como ferramentas de trabalhos, foi desenvolvida a Política de segurança da informação (PSI) da Prefeitura do Município de Espírito Santo do Pinhal (PMESP).

Este documento tem como base referências e recomendações das normas da ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO 31000:2018, o Marco Civil da internet e as normas estabelecidas pela Lei Geral de Proteção de dados (LGPD) pertinentes, dentro da realidade da estrutura organizacional da PMESP, para nortear e definir padrões para implementação, operação, monitoramento, revisão, manutenção e outros parâmetros buscando melhorar os níveis de segurança e a mitigação dos riscos ao que tange os recursos de TI do município.

Essa política deverá ser revista e atualizada periodicamente pelo Departamento de Gestão de Projetos, Relações Institucionais e Tecnologia da Informação (DGPRITI) com novas diretrizes e recomendações de padrões de segurança de maneira a garantir uma melhoria contínua nos serviços de TI.

3. OBJETIVO

A PSI municipal através de diretrizes e normas aplicadas a todas as áreas da administração pública busca mitigar os riscos, garantir a continuidade de operações, proteção contra ameaças diversas, atender os princípios de autenticidade e legalidade das informações produzidas ou recebidas provenientes de diferentes fontes.

Com a implantação desse documento espera-se desenvolver um comportamento ético quanto a utilização de recursos de (TI).

Novas metodologias de trabalhos serão adotadas com práticas preventivas visando a redução de ameaças e vulnerabilidades garantindo uma gestão eficiente de recursos, zelando pelos equipamentos e ferramentas de trabalho, reduzindo gastos, melhorando atendimentos a munícipes e produtividade dos colaboradores.

Busca o controle de níveis de acesso de fornecedores externos a sistemas, controle de acessos de colaboradores em equipamentos remotos, segurança em dispositivos e atividades vinculadas à TI.

4. PRINCÍPIOS

O presente documento aborda novos padrões comportamentais que devem ser levados em consideração princípios básicos referentes a segurança da informação:

1. **Disponibilidade –** As informações e recursos deverão estar disponíveis sempre que necessários para qualquer indivíduo, órgão ou sistemas autorizados.
   Exemplos de ferramentas: nobreak, firewall e backup;
2. **Integridade –** Garantia que os ativos de informação estejam protegidos e não sejam alterados de forma não autorizada ou acidental.
   Exemplos de ferramentas: Assinatura digital e backup;
3. **Confidencialidade –** Acesso as informações somente de indivíduos, órgãos, entidades e processos autorizados.
   Exemplos de ferramentas: Criptografia;
4. **Autenticidade –** As informações deverão ser certificadas com relação a sua origem evitando mutações ao longo do processo.
   Exemplos de ferramentas: Biometria e certificado digital;

Seguindo as premissas anteriores outros princípios adotados são citados para que possa se tornar parte de todo desenvolvimento e execução das ações. São importantes para manutenção de qualidade e busca da melhoria contínua na prestação de serviços:

- **Atualidade –** Deverão ocorrer atualizações periódicas dos procedimentos e normas para manutenção da qualidade e segurança dos serviços;
- **Aplicabilidade –** Todos processos de trabalhos deverão ser integrados e aplicados de maneira funcional obedecendo as normas de segurança;
- **Clareza –** Não poderá existir dúvidas relacionadas às responsabilidades, normas, procedimentos e direitos de cada envolvido;

- **Conhecimento –** Deverão ser desenvolvidos materiais informativos bem como capacitações periódicas de servidores com o que diz respeito à segurança da Informação;
- **Simplicidade –** A segurança deverá ser realizada de maneira simples, eficaz e objetiva de forma a evitar erros;
- **Privilégios –** Os recursos disponíveis deverão ser necessários para um bom desempenho das atividades evitando acesso a recursos não condizentes às funções;
- **Auditoria –** Qualquer tipo de processo poderá ser auditado e suas informações rastreáveis através de log;
- **Resiliência –** Deverá ter a capacidade de recuperação rápida em caso de desastre ou perda de informações;
- **Redundância –** Em caso de falhas um outro controle assume o papel evitando transtornos por falta de disponibilidade;
- **Legalidade –** Garantia de que as informações estão de acordo com legislação vigente;
- **Irretratabilidade –** Garante que um usuário não negue a autoria de operação ou serviço específico.

5. DIRETRIZES

As diretrizes deste plano estão em concordância com o Plano Diretor de Tecnologia da Informação (PDTI) do Município de Espírito Santo do Pinhal e deverão ser seguidas por colaboradores sendo eles funcionários, pessoas físicas ou jurídicas que tenham acesso a dados ou informações do município por quaisquer meios.

Abrange a Governança de TI, buscando promover melhorias nos sistemas de informação e gestão municipal, além de manter e otimizar processos garantindo segurança das informações e comunicações. Como referência deverão ser seguidas as diretrizes:

- É de propriedade do órgão qualquer informação gerada por colaboradores utilizando de maneira integral ou parcial ferramentas e recursos do município.
- A segurança da informação, através de análise de vulnerabilidades e mitigação de riscos deverá ser preservada para manutenção dos serviços e proteção da organização.
- Os usuários deverão ter acesso somente às informações que fazem necessárias para desempenhar suas funções. Devem ser evitadas circulação de informações, mídias, dados considerados confidenciais. Evitar deixar materiais impressos, relatórios, processos e documentos em locais de fácil acesso.
- Aquisições e recebimento de equipamentos, contratação de serviços de TI devem seguir as leis vigentes bem como ser acompanhada pelo setor técnico para as devidas especificações e conferências.
- Esta política dá ciência a todo colaborador que os ambientes dos setores administrativos da prefeitura bem como sistemas de gestão, redes, computadores podem ser monitorados ou gravados sem aviso prévio para manutenção da segurança dos dados da organização.
- Equipamentos poderão ser removidos, desligados para manutenção, auditados ou realocados de acordo com as necessidades e padrões da organização, sem aviso prévio.

- A PSI deverá ser atualizada e revisada periodicamente tendo em vista o surgimento constante de ameaças cibernéticas, novas propostas de melhorias em relação a sistemas, mudanças comportamentais ou fatores relevantes.
- É dever de cada colaborador manter ciente e atualizado sobre os procedimentos e normas desta política buscando informações junto ao DGPRITI sempre que houver dúvidas quanto ao uso de recursos de TI.
- Todo colaborador ingressante na organização deverá ter ciência do termo bem como da legislação vigente para proteção de seus direitos e deveres.

6. RESPONSABILIDADES ESPECÍFICAS

6.1. Colaboradores

O colaborador em caráter temporário deverá seguir as mesmas normas adotadas ao colaborador em regime CLT. Em caso de desligamento, deve-se manter sigilo e confidencialidade das informações. As ferramentas utilizadas no desempenho das funções deverão ser devolvidas se for o caso e sempre mantidas em bom estado de conservação para uso.

Serão responsáveis por qualquer tipo de dano que sofrer ou causar em decorrência do não cumprimento das normas e diretrizes do presente documento.

Deverão zelar pelo bem público bem como fazer bom uso das ferramentas utilizadas para o desempenho das funções.

6.2. Gestores

É dever monitorar, atualizar e disseminar aos envolvidos os termos que deverão ser assinados como forma de aceite dos colaboradores.

Todo gestor deve manter conduta ética, com base em princípios morais zelando pelos bens do município, servindo de modelo a ser seguido pelos colaboradores.

6.3. Recursos humanos

Tendo em vista que todo funcionário tem seu contrato assinado ou faz o desligamento no RH, o setor será responsável por comunicar o DGPRITI sobre dispensas ou contratações para setores administrativos do município.

No caso de contratação, o funcionário deverá assinar os termos e ter conhecimento das políticas implantadas. Os recursos serão disponibilizados de acordo com as necessidades apresentadas nas funções.

No caso de desligamento, o setor de TI deverá ser alertado para que credenciais de acesso aos sistemas, equipamentos utilizados, conta de e-mail e

ambiente de rede possam ser bloqueadas. Os arquivos deverão ser armazenados e disponibilizados para o colaborador que assumir as funções.

6.4. Setor de Tecnologia da Informação

O setor tem como principais atribuições planejar, dimensionar e coordenar a execução de projetos e ações. Colocar em prática as diretrizes mantendo sempre atuais e funcionais. Além disso, outras funções são desempenhadas, entre elas:

- Realizar configurações, atualizações, instalações de antivírus e ferramentas adequadas para o desempenho das funções em todos equipamentos, com base nos requisitos de segurança estabelecidos. Colocar em produção somente equipamentos livres de ameaças virtuais, com software licenciado ou software livre.
- Em caso de manutenção, troca de equipamentos ou colaboradores, garantir a integridade das informações.
- Em caso de desligamento de colaborador, fazer bloqueio de contas de acessos restritos e credenciais logo que receber o comunicado.
- Garantir e promover aos colaboradores o conhecimento de ameaças e segurança da informação. Desenvolver e disponibilizar cartilhas, tutoriais e materiais informativos aos colaboradores de maneira periódica.
- Avaliar periodicamente a eficácia dos controles de segurança, bem como alertar sobre casos de engenharia social e fraudes quando identificados. Manter sempre atualizados dispositivos de segurança e sistemas de acordo com surgimento de novas tecnologias.
- Implantar mecanismos de controle que permitam auditoria e investigações através de logs. Sistemas com acesso externo (disponibilizados ao público), deverão ter atenção especial contra ataques ou problemas de disponibilidade.
- Padronizar serviços, sistemas e configurações de acordo com as necessidades da organização.

- Manter pleno funcionamento de ferramentas de monitoramento de ativos. Fazer inserção ou configuração de novos e exclusão de obsoletos ou problemáticos.
- Manter cópias seguras e testadas dos sistemas e dados, em locais diferentes e com acesso restrito.
- Criação de perfis de acessos com privilégios de usuários, não possibilitando acesso a recursos de administrador a colaboradores não autorizados.
- Analisar o ambiente para identificação de possíveis riscos e mitigação dos mesmos.

7. CONTROLE DE ACESSO

7.1. Lógico

O acesso lógico é relacionado a acesso em sistemas, redes, recursos que necessitem de credenciais de identificação como login/ID ou que autorizem o colaborador a fazer uso de determinadas ferramentas da organização. São pessoais e confidenciais, não sendo permitido o seu empréstimo a quem quer que seja.

Os servidores que se utilizarem de códigos de identificação e de credenciais de terceiros poderão ser responsabilizados internamente, sem prejuízo de outras cominações pertinentes. As diretrizes a seguir deverão ser seguidas para evitar riscos:

- Deverá ter privilégio de acordo com as necessidades de suas funções.
- Acesso remoto a ativos só é permitida através de autorização prévia do setor de TI. Colaboradores deverão solicitar acesso, se identificando, informando o motivo, local e período de utilização, mediante meios seguros para tal atividade.
- A criação de conta de e-mail institucional deve ser solicitada através do gestor por meio de ofício, bem como permissão de acesso a sistemas, redes e ativos.
- As credenciais de acesso são criadas de maneira parcial, cabendo ao colaborador a troca por uma credencial forte e pessoal após o primeiro login. Alguns critérios mínimos devem ser seguidos com a utilização de caracteres alfanuméricos variados (letras maiúsculas, minúsculas e números), pelo menos 8 caracteres e utilização de caracteres especiais. Não deve ser usado credencial com dados pessoais como nome, data de nascimento, entre outros.
- As credenciais deverão ser trocadas periodicamente para garantia de segurança. Em caso de esquecimento ou perda, deve-se solicitar uma nova de maneira imediata.

- Acessos desconhecidos ou suspeita de acessos aos recursos de TI devem ser informados com urgência ao setor para providências.
- Somente o setor de TI deverá ter acesso de administrador aos recursos ou em casos específicos de extrema necessidade comunicados pelo gestor interessado.

7.2. Acesso à Infraestrutura

Todo acesso à infraestrutura do datacenter é restrito aos funcionários do setor de TI. Qualquer acesso necessário deverá ser acompanhado pelo funcionário do setor de TI. A sala deve permanecer sempre fechada para evitar acesso indevido.

Deverá ser instalado vídeo monitoramento de segurança e a temperatura controlada para evitar superaquecimento.

7.3. Acesso à rede e recursos

Os recursos são liberados como condição de uso. As áreas, serviços e conteúdos institucionais não poderão ser usados para quaisquer propósitos que sejam ilegais ou proibidos por esta política de uso, de modo a danificar, desativar, sobrecarregar, prejudicar qualquer área, serviço ou conteúdo, interferir no uso e participação de qualquer um dos colaboradores. As normas são tratadas a seguir:

- Não é permitido tentar obter acesso não-autorizado a qualquer área, serviço e conteúdo dos sistemas ou redes de computadores conectados, através de ações mal-intencionadas, corrupção de credenciais ou outros meios.
- O uso e o acesso pelo colaborador à rede, internet e/ou utilização de e-mail institucional, deverão ser exclusivos para uso profissional, para a execução e desempenho dos objetivos da Administração Pública. Exceto esses casos, deverá existir autorização expressa do gestor.

- A Administração Pública reafirma que o uso da Internet é uma ferramenta valiosa para atender suas necessidades. Entretanto, o mau uso dessa facilidade pode ter impacto negativo sobre a produtividade dos colaboradores e a própria reputação da instituição.
- A Administração Pública possuiu softwares e sistemas implantados que podem monitorar o uso da Internet, e-mails, chats, etc., através da rede local e das estações de trabalho da instituição.
- A Administração Pública se reserva o direto de monitorar o volume de tráfego na Internet e na Rede juntamente com os endereços web visitados, visando assegurar o cumprimento desta política.
- O acesso à Internet para propósitos particulares ou estranhos às atividades da Administração Pública poderá ser bloqueado, sem prévia comunicação ao servidor, sem prejuízo das demais sanções aplicáveis.
- Não é permitida a navegação aos sites pertencentes às categorias abaixo, e tampouco a exposição, o armazenamento, a distribuição, a edição, a gravação através do uso dos recursos computacionais e de comunicação da Administração Pública:
    a) Material sexualmente explícito (em especial pedofilia) e, ainda, material contrário a moral ou aos bons costumes;
    b) Material de conteúdo impróprio, ofensivo, preconceituoso ou discriminatório;
    c) Apologia à violência ou ao terrorismo;
    d) Apologia às drogas;
    e) Violação de direito autoral (pirataria);
    f) Execução de quaisquer tipos ou formas de fraudes;
    g) Sites de relacionamentos e bate-papo;
    h) Sites de séries, filmes, vídeos e arquivos de entretenimento (exemplos Netflix, Amazon Prime e/ou similares). Exceto em atividades relacionadas ao departamento com autorização do gestor;

i) Programas de TV na internet. Exceto em atividades relacionadas ao departamento com autorização do gestor;
j) Compartilhamento de arquivos estranhos às atividades da Administração Pública e não autorizados pelo gestor.

- Não é permitida a troca de arquivos de vídeo ou música.
- É proibida a transferência de qualquer tipo de programa, jogo e similares para a rede interna da Administração Pública sem autorização específica do gestor.
- É proibido downloads de arquivos de extensões tipo: .exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .d11, e de programas de entretenimento ou jogos, exceto os estritamente relacionados aos serviços inerentes à função do colaborador com vistas às atividades da Administração Pública.
- Não é permitido o acesso a programas de TV na Internet ou qualquer conteúdo sob demanda (streaming).
- É proibido o uso de jogos, inclusive os da Internet (online).
- O colaborador não poderá revelar, fora do âmbito profissional/institucional, fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial.
- O colaborador que divulgar informações confidenciais da Administração Pública em grupos de discussão, bate-papos, aplicativos de mensagens, e-mail, telefone, não importando se a divulgação foi deliberada ou inadvertida, poderá sofrer as penalidades previstas em Lei e procedimentos internos e/ ou na forma da lei, responsabilidade criminal ou civil.
- Sendo do interesse da Administração Pública que os seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços de notícias é aceitável, desde que o seu uso não comprometa o uso de banda da rede, nem perturbe o bom andamento dos trabalhos, observados em todos os casos os termos desta política de uso.

- A utilização da Internet para atividades não relacionadas com os interesses da Administração Pública é facultada durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política.
- O uso de qualquer recurso da PMESP para atividades ilegais é motivo para a devida investigação interna por meio de sindicância ou PAD e a Administração Pública cooperará ativamente com as autoridades policiais ou judiciais nesses casos.
- A entrada e consequente uso de equipamentos de informática pessoais (notebooks, tablets) na rede de dados municipal é expressamente proibida. Em hipótese alguma a instituição será responsabilizada por danos no equipamento pessoal do servidor ou ainda em casos de furto ou roubo.
- Celulares e ou smartphones de funcionários deverão ser cadastrados no DGPRITI que receberão um termo de aceite para liberação. Em locais com rede de wifi públicos estão liberados para acesso com cadastro no local através de site.
- As excepcionalidades e os casos omissos deverão ser relatados para o gestor a qual o colaborador pertence.
- Tendo necessidade de algum acesso a sites ou serviços que não conste na lista de permitidos, mas que seja necessário para andamento de trabalhos, entrar em contato com DGPRITI.

7.4. E-mail institucional

Essa ferramenta estará disponível para utilização somente às atividades relacionadas ao desempenho da função. Cabe ao gestor definir a necessidade de uso pelo colaborador ou não.

O uso do e-mail institucional não garante direito sobre este, nem confere autoridade para liberar acesso a outras pessoas, pois se constitui de informações pertencentes à Administração Pública.

A seguir seguem as regras para bom uso da ferramenta:

- É expressamente proibido utilizar o e-mail institucional para cadastro em sites de jogos, compras e vendas, propagandas, bem como disseminar por meio dessa ferramenta anúncios publicitários, mensagens tipo corrente, vírus, conteúdos nocivos, conteúdos ofensivos, obscenos, pornográficos ou de qualquer forma contrária à lei.
- Não é permitido o compartilhamento de arquivos de áudio, vídeos ou quaisquer mídias que não condiz com as funções e ferem os princípios dos direitos autorais.
- Não é permitido divulgação de contas ou contatos, informações, imagens, documentos sem autorização do proprietário.
- Todo colaborador deve guardar sua credencial em segurança, manter sempre a conta fechada quando não estiver em uso. Em caso de recebimento de spam ou de remetentes desconhecidos, excluir para evitar a infecção com vírus e até mesmo a propagação.
- Não abrir arquivo anexo de remetente desconhecido ou inesperado, em caso de ocorrência por acidente, relatar o ocorrido imediatamente ao setor de TI.

7.5. Política de uso de Equipamentos de Informática

Todo colaborador deve estar ciente das diretrizes para bom uso e conservação dos ativos de TI. É de responsabilidade zelar e evitar qualquer tipo de dano ao patrimônio público.

Devem ser utilizados somente como ferramenta de trabalho para o desenvolvimento das tarefas pertinentes:

- Os arquivos devem ser armazenados no servidor de arquivos do setor para a possibilidade de cópia de segurança. Arquivos locais (entende-se salvo no disco rígido da estação de trabalho) não são salvos cabendo ao colaborador a responsabilidade em caso de perda ou danos.
- A pasta do servidor de arquivos denominada pública é comum a todos usuários conectados à rede, portanto sem garantia contra

modificações ou exclusão. Não deve ser utilizada como forma de armazenamento, somente para arquivos temporários.

- Atualmente encontra vigente o contrato de locação de computadores que proíbe a manutenção por parte dos colaboradores do setor de TI. Para tal reparo, é necessária abertura de chamado pelo setor e aguardar o técnico responsável de realizar o suporte. Somente o setor de TI pode fazer modificações em configurações.
- Não é permitido o uso de equipamentos particulares como notebooks na rede local da PMESP. Para tais fins, recomenda-se o uso dos pontos de wifi espalhados em diversos setores e localidades, com nome de “CIDADE CONECTADA”. Danos, extravios e problemas gerados em equipamentos particulares serão de responsabilidade exclusiva do proprietário.
- Na ocorrência de furtos, roubos ou extravios de ativos da PMESP deverá ser comunicado ao setor de TI para que possa ser lavrado Boletim de ocorrência para apuração dos fatos.
- Não é permitida colocação de adesivos, propagandas, imãs em equipamentos. Somente etiquetas de identificação ou patrimônio.
- Não é permitido o uso de equipamentos de TI por pessoas sem vínculo com a organização.
- Somente colaboradores do setor de TI estão autorizados a configurar rede, roteadores, switches e alterar endereços de rede IPs bem como modificar/remover ativos.
- Utilização de pendrives, mídias removíveis e outras fontes externas deverão ser utilizadas somente para fins de execução de atividades de trabalho.
- Não é permitido o armazenamento de arquivos pessoais (fotos, vídeos, documentos) em equipamentos do município.
- É proibido o uso de impressoras de repartições públicas para impressões de documentos pessoais. Além disso não é permitida a instalação ou execução de qualquer software em desacordo com

as funções do ambiente de trabalho e, ainda, aqueles que burlam as regras de proteção e segurança para acesso a sites indevidos.

- É proibida a saída de qualquer equipamento de propriedade da Administração Pública pelo colaborador, exceto se houver autorização por expresso neste sentido formalizada por documento escrito e assinado.
- A Administração Pública se reserva o direito de inspecionar, sem a necessidade de aviso prévio, as estações de trabalho e qualquer arquivo armazenado, estejam no disco local da estação ou nas áreas privadas da rede.

8. BACKUP

Procedimento de extrema importância para segurança da informação. A implantação de política de backup assegura que no caso de algum incidente a organização consiga restaurar em sua totalidade sem transtornos ou danos às informações. Para isso, alguns procedimentos são primordiais:

- Todo sistema deve possuir cópia de dados para que em caso de uma eventual indisponibilidade possa ser restaurado com impactos mínimos para a organização.
- As rotinas de backups deverão ser executadas em períodos noturnos, quando há pouco ou nenhum acesso. Os sistemas devem ser automatizados com agendamento para melhor administração e gerência.
- Os backups são armazenados devidamente identificados em localizações diferentes do datacenter, com controle de segurança, de acesso restrito, seco, climatizado. Alguns sistemas utilizados enviam cópias para nuvem com criptografia e disponibilidade.
- Testes de restauração bem como integridade dos dados devem ser periodicamente executados em locais diferentes dos originais (evitando sobreposição) para garantia que as informações se mantenham preservadas e as rotinas funcionais.
- Caso aconteçam erros na criação do backup ou na restauração, as rotinas devem ser revisadas e acondicionadas a novos testes.
- As ferramentas de backup devem estar sempre atualizadas e corrigidas para manter a qualidade dos serviços.
- Mídias de armazenamento devem ser monitoradas e substituídas de acordo com prazo especificado pelo fabricante.
- É importante manter sempre redundância de equipamentos para substituição em caso de emergência.

REFERÊNCIAS

BRASIL. **Marco Civil da Internet. Lei 12.965/14**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 08 de agosto 2021.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2013.**

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. ABNT, 2013.**

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000 – Gestão de Riscos – Diretrizes. ABNT, 2018.**

TERMO DE RESPONSABILIDADE E COMPROMISSO

Com o objetivo de definir as responsabilidades para todos os agentes públicos, estagiários e prestadores de serviços em atividade na Prefeitura do Município de Espírito Santo do Pinhal (PMESP) que tenham acesso aos recursos de tecnologia da informação (TI) ou à rede de computadores da instituição.

Pelo presente termo, declaro ter conhecimento da Política de Segurança da Informação (PSI), com cópia entregue em mãos ao gestor responsável pelo departamento ou secretaria, de acordo com as regras estabelecidas. Também disponível para consulta no portal www.pinhal.sp.gov.br, (link da Carta de Serviços, no botão Gestão de Projetos, relações Institucionais e Tecnologia da Informação) ou pelo link direto:

https://s11.asp.srv.br:445/ouvidoria.pm.espiritosantodopinhal.sp/servlet/com.asp.ouvidoria.externo.wpcartaservicoext

Recebo/utilizo uma conta e equipamento com privilégios adequados ao exercício das atividades que aqui executo, a qual deverá ser utilizada somente para tal fim.

Declaro estar ciente de que minhas ações serão monitoradas de acordo com a (PSI) e qualquer alteração feita sob minha identificação, advinda de minha autenticação e autorização, é de minha responsabilidade e me comprometo a não os disponibilizar ou divulgar a entidades (pessoas, sistemas ou órgãos) não autorizadas. É, meu dever zelar e manter a segurança das informações geradas ou utilizadas em minhas funções.

Estou ciente, ainda, de minha responsabilidade pelo dano que possa causar por descumprimento da (PSI) da (PMESP) ao realizar uma ação de iniciativa própria de tentativa de modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Eu, _____,
colaborador do setor de _____,
Departamento/Secretaria_____,
declaro que li e estou ciente da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO da Prefeitura do Município de Espírito Santo do Pinhal e me comprometo a seguir todos os seus termos, bem como a me atualizar a respeito de eventuais alterações.

Espírito Santo do Pinhal, ____, _____de 202 .

_____
Assinatura e carimbo do colaborador

_____
Assinatura e carimbo do Gestor