PREFEITURA MUNICIPAL DE TAGUAÍ / SP

PLANO MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO - PSI

N.º: 001 / 2023

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Revisão 1.0

www.taguai.sp.gov.br **ti@taguai.sp.gov.br**

PLANO MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO

Publicação: 2023

N.º 001/23

Redação
Marcio Ricardo Bergamo Bento
Especialista em Gestão de TI

Revisão Jurídica
Dr. Flavio Sérgio Vaz Prado
Procurador Jurídico Municipal

PLANO MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO

Publicação: 2023

I. SUMÁRIO

II. TERMOS E DEFINIÇÕES RELACIONADAS

Ativo: qualquer coisa que possua ou proporcione valor para a organização;

Ativos da Informação: são ativos referente a informação e seu uso, são subdivididos em - primários (informações, processos e atividades) e ativos de suporte, dos quais os primários dependem (hardware, software, rede, pessoal, locais, estruturas);

Confiabilidade: garantia de que apenas usuários autorizados tenham acesso às informações, impedindo que sejam desviadas de seu propósito;

Dados: registros de valores quantitativos ou qualitativos, que de forma isolada não representam informação concreta;

Dados ou Informações Sensíveis: informações que precisam ser protegidas devido a potenciais efeitos adversos;

Disponibilidade: garantia de que as informações estejam acessíveis quando necessário, evitando interrupções indesejadas;

Dispositivos endpoint: são dispositivos que estão conectados à rede e servem como pontos de acesso (podem ser equipamentos como computadores, notebooks, smartphones, dentre outros);

Informação: contextualização ou conjunção de dados de maneira que formem um significado e possam gerar uma mensagem;

Integridade: preservação da exatidão das informações, assegurando que não sejam indevidamente alteradas ou corrompidas;

Parte Interessada: pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade;

Patch: uma modificação aplicada ao código de um programa;

Transferência de dados: compreende o envio e a recepção de dados e informações;

PLANO MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO

PREFEITURA MUNICIPAL DE TAGUAÍ / SP

N.º: 001 / 2023

1. INTRODUÇÃO

1.1 CONTEXTO

Este documento propõem os princípios e organização de um sistema de gestão da segurança da informação, que de maneira adequada ao atual estágio de desenvolvimento organizacional, forneça garantias à administração e às partes interessadas de que suas informações e ativos associados estejam preservados de forma apropriada. Descreve abordagens para o gerenciamento e proteção da informação, seus usos e desusos, visando mitigar riscos e ameaças por meio de ações preventivas e corretivas.

Os princípios são fundamentados na norma NBR ISO/IEC 27002:2022, que versa sobre “Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.”

1.2 OBJETIVO

Promover o entendimento e adoção de políticas, práticas e controles para garantir a confiabilidade, integridade e disponibilidade da informação e de seus ativos.

1.3 ESCOPO

As ações propostas destinam-se à toda administração pública municipal e colaboradores, bem como seus parceiros e fornecedores no que envolva interação em qualquer uma das fases do ciclo de vida da informação, seja em sua produção, troca, armazenamento ou descarte.

1.4 METAS

▪ Instituir o Plano de Segurança da Informação - PSI;	2023
▪ Promover a publicidade e orientação do PSI para as partes envolvidas;	2024
▪ Iniciar a aplicação e observação as atividades de Segurança da Informação;	2024
▪ Monitorar resultados obtidos e avaliar adequações e melhorias do PSI.	Contínuo

Praça Expedicionário Antônio Romano de Oliveira nº 44 Tel. (14) 3386 9040 CEP 18890-091 Taguaí - SP

2. CONTROLES ORGANIZACIONAIS, DE PESSOAS, FÍSICOS E TECNOLÓGICOS

A segurança da informação envolve todas as áreas funcionais da administração pública municipal e seus níveis hierárquicos, desde a alta direção aos serviços operacionais, vai além de controles técnicos ou tão somente da área de Tecnologia da Informação, depende da conscientização e do comprometimento de todos os envolvidos para que as medidas sejam efetivas e consistentes.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O estabelecimento de uma Política de Segurança da Informação visa a definição de regras e o uso de práticas claras para promover a cultura de segurança na administração pública municipal.

Com a instituição do Plano de Segurança da Informação ficam observados princípios para orientar as atividades de segurança da informação e a atribuição de responsabilidades e compromissos legais, estatutários e regulamentares.

TEMAS E PRINCÍPIOS A SEREM OBSERVADOS:

- Controle de acesso;
- Segurança física e do ambiente;
- Gestão de ativos;
- Transferência de informações;
- Configuração e manuseio de dispositivos “*endpoint*”;
- Segurança das redes;
- Gestão de incidentes;
- Backup;
- Classificação e tratamento das informações;
- Gestão de vulnerabilidades.

A. CONTROLE DE ACESSO:

Definição: refere-se à implementação de medidas para garantir que apenas pessoas autorizadas tenham acesso aos recursos e informações.

Propósito: proteger a confidencialidade e a integridade dos dados, prevenindo o acesso não autorizado.

Procedimentos:

i. Todos os usuários devem ser identificados de forma única, por logins e senhas ou outros mecanismos de identificação, para garantir a responsabilização e rastreabilidade das ações realizadas;

ii. Garantir que apenas usuários autorizados acessem sistemas e aplicações específicas, com base nas necessidades de suas funções;

iii. As senhas não devem ser expostas ou compartilhadas e devem incluir requisitos de complexidade, expiração regular e não reutilização em múltiplos locais;

iv. Aos usuários deve-se atribuir apenas os privilégios de acesso necessários para realizar suas funções, seguindo o princípio do menor privilégio;

v. Os administradores devem revisar os privilégios de acesso atribuídos aos usuários, removendo privilégios desnecessários e garantindo a atualização de acordo com as mudanças nas necessidades;

vi. Devem ser observados procedimentos para criação, modificação e exclusão de contas de usuários, garantindo a inabilitação ou remoção imediata de contas inativas ou de usuários que deixaram as funções ou a administração pública municipal;

vii. Devem ser utilizados mecanismos de auditoria para registrar e monitorar atividades de acesso, a fim de identificar e investigar quaisquer atividades suspeitas ou não autorizadas;

viii. O acesso às redes deve utilizar mecanismos de controle para restringir conexões de equipamentos ou softwares não autorizados e delimitar o acesso somente a redes confiáveis e seguras;

ix. Restrições de acesso físico devem garantir o controle de acesso às áreas físicas críticas dos ativos, por meio de medidas de autorizações, fechaduras e vigilância;

x. O acesso remoto deve ser realizado por pessoal autorizado, somente com demandas específicas, ser executado por meio de tecnologias criptografadas e utilizando autenticação forte para evitar o acesso não autorizado;

xi. Todos os usuários devem estar cientes das responsabilidades, da importância e dos riscos associados à violação do controle de acesso.

Praça Expedicionário Antônio Romano de Oliveira nº 44 Tel. (14) 3386 9040 CEP 18890-091 Taguaí - SP

B. SEGURANÇA FÍSICA E DO AMBIENTE:

Definição: envolve a proteção das instalações físicas, equipamentos e recursos da administração pública municipal.

Propósito: contribuir para a proteção dos ativos e garantir a continuidade das operações sem interrupções causadas por eventos adversos.

Procedimentos:

i. Implementar medidas de controle de acesso físico, como o uso de chaves físicas, cartões, sensores de biometria, vigilância por câmeras e registros de visitantes, para garantir que apenas pessoas autorizadas tenham acesso às áreas restritas;

ii. Definir zonas seguras dentro das instalações e prédios públicos para controlar o acesso a áreas críticas, de pessoas não autorizadas conforme suas atribuições;

iii. Tomar medidas e promover ações para prevenir riscos as instalações, cabos, estruturas e ativos, contra ameaças físicas, incêndio, inundações, vandalismo e falhas estruturais;

iv. Fazer uso de sistemas de monitoramento e sensores para detectar e responder a eventos ou condições anormais no ambiente físico das instalações;

v. Utilizar medidas de segurança física para proteger os equipamentos, dispositivos e mídias de armazenamento, através do uso de armários trancados, racks protegidos, cabos de segurança contra roubo e etiquetagem adequada dos equipamentos;

vi. Garantir que as informações confidenciais não sejam visíveis a olhares não autorizados, por meio de documentos, posicionamento de monitores, impressoras e quaisquer outros dispositivos que exibam informações sensíveis, tornando-os acessíveis apenas para os usuários autorizados;

vii. Estabelecer procedimentos para o descarte seguro de ativos físicos, como equipamentos de tecnologia obsoletos, mídias de armazenamento de dados e documentos confidenciais;

viii. Determinar controles físicos e o cumprimento de requisitos de segurança à fornecedores, parceiros ou terceiros que tenham acesso físico às instalações ou equipamentos da administração pública municipal;

ix. Promover a conscientização e alertar regularmente os envolvidos sobre as práticas de segurança física, a identificação de ameaças, medidas preventivas e a organização física, para proteger as informações e os ativos.

C. GESTÃO DE ATIVOS:

Definição: abrange a identificação, o registro, a classificação e a proteção dos ativos de informação da administração pública municipal.

Propósito: criar inventários de ativos, estabelecendo responsabilidades pelo seu uso, manutenção e implementando controles para evitar perdas, danos ou acesso não autorizado.

Procedimentos:

i. Manter um inventário atualizado de todos os ativos de informação, incluindo hardware, software, documentos e recursos físicos relevantes;

ii. Classificar os ativos de informação com base em sua categoria, importância, confidencialidade e integridade;

iii. Atribuir a cada ativo um proprietário responsável por sua proteção e utilização adequada;

iv. Implementar controles físicos e lógicos para proteger os ativos de informação de acesso não autorizado, perda, roubo ou danos;

v. Estabelecer e seguir diretrizes claras para a transferência segura de ativos de informação entre pessoas, departamentos ou organizações;

vi. A manutenção adequada dos ativos deve ser realizada por pessoal autorizado, para garantir o bom funcionamento e os níveis de segurança;

vii. Realizar auditorias periódicas para avaliar a eficácia dos controles de segurança nos ativos de informação;

viii. Estabelecer procedimentos para o descarte seguro dos ativos da informação quando não forem mais necessários, inclusive a remoção ou destruição segura de dados.

D. TRANSFERÊNCIA DE INFORMAÇÕES:

Definição: refere-se à comunicação e ao compartilhamento seguro de dados dentro e fora da administração pública municipal.

Propósito: auxiliar a proteção, a confidencialidade e a integridade das informações durante o envio e o recebimento, minimizando os riscos de interceptação ou manipulação por parte de invasores.

Procedimentos:

i. Garantir que os sistemas e redes utilizados na transferência de informações estejam devidamente protegidos e sejam corretamente utilizados;

ii. Utilizar apenas os meios de comunicação determinados e seguros para transferência de informações;

iii. Somente pessoas identificadas e autorizadas podem ter acesso ao conteúdo das informações durante sua transferência;

iv. Revisar e garantir que os canais e os endereços destinados a transferência da informação estejam corretos antes do envio;

v. Respeitar a classificação de sensibilidade, importância e restrição das informações durante sua transferência;

vi. Observar medidas de segurança para proteção de e-mails e outros meios de comunicação, evitando o acesso, envio e replicação de conteúdos inseguros, de fontes desconhecidas ou não autorizadas;

vii. Implementar mecanismos de registro de transferências de informações, permitindo a detecção e investigação de atividades suspeitas ou não autorizadas;

viii. Em transferências verbais de informações, evitar que assuntos sensíveis, restritos ou confidenciais sejam tratados em ambientes não adequados ou junto de pessoas sem autorização;

ix. Reforçar o entendimento das responsabilidades e papéis das partes envolvidas na transferência de informações, incluindo remetentes e destinatários.

E. CONFIGURAÇÃO E MANUSEIO DE DISPOSITIVOS ENDPOINT:

Definição: a configuração e o manuseio de dispositivos endpoint dizem respeito à proteção dos dispositivos (como computadores, laptops, smartphones) utilizados pela administração pública municipal.

Propósito: realizar as configurações adequadas e estabelecer diretrizes para o manuseio seguro dos dispositivos, visando evitar perdas, roubos ou acesso não autorizado aos dados neles armazenados.

Procedimentos:

i. Restringir a utilização e a conexão de dispositivos endpoint que não estejam devidamente identificados e autorizados;

ii. Implementar mecanismos de registro, monitoramento, e rastreio de atividades dos dispositivos endpoint, incluindo logs de eventos, autenticação, tentativas de acesso não autorizado e uso de aplicativos ou recursos críticos;

iii. Utilizar configurações seguras por padrão em todos os dispositivos endpoint, garantindo a segurança do sistema operacional e aplicativos instalados;

iv. Restringir a instalação de softwares não autorizados ou patches e atualizações nos dispositivos endpoint, sem a indicação ou acompanhamento do setor competente;

v. Estabelecer uma política de senhas fortes para os dispositivos endpoint, incluindo requisitos de complexidade, expiração regular e quando possível autenticação de múltiplos fatores (AMF);

vi. Quando necessário, restringir a conectividade e o uso de dispositivos externos nos dispositivos endpoint, como pen drives USB ou outras conexões e mídias;

vii. Utilizar procedimentos para a remoção segura dos dados em dispositivos endpoint antes de serem reutilizados ou descartados;

viii. Se necessário o uso de um nível de segurança mais elevado, encriptar os dados armazenados nos dispositivos endpoint, especialmente em laptops e dispositivos móveis;

ix. Promover a conscientização sobre a configuração correta e o manuseio seguro dos dispositivos endpoint, destacando os riscos de segurança e boas práticas.

F. SEGURANÇA DAS REDES:

Definição: abrange as medidas para proteger a infraestrutura de rede da administração pública municipal contra ameaças e ataques cibernéticos.

Propósito: garantir a confidencialidade, integridade e disponibilidade das informações transmitidas pela rede, bem como a proteção dos serviços e sistemas conectados a ela.

Procedimentos:

i. Implementar um firewall para monitorar e controlar o tráfego de entrada e saída da rede, filtrando ameaças e ataques externos, e garantindo a segurança do perímetro da rede;

ii. Estabelecer mecanismos de autenticação e autorização robustos para garantir que apenas dispositivos e usuários autorizados tenham acesso à rede;

iii. Dividir a rede em segmentos ou zonas de segurança, com base nas necessidades de segurança;

iv. Implementar medidas de segurança adequadas para redes sem fio (Wi-Fi), como autenticação de usuário, criptografia (como WPA2-PSK ou WPA3), segmentação e isolamento de redes de convidados;

v. Utilizar sistemas de detecção e prevenção de intrusões (IDS/IPS) para identificar e responder a atividades suspeitas na rede, bloqueando automaticamente atividades maliciosas e mitigando possíveis comprometimentos;

vi. Implementar estratégias de backup e recuperação das configurações e dados dos equipamentos de rede para garantir a disponibilidade e a integridade em caso de falhas, desastres ou ataques cibernéticos;

vii. Manter os equipamentos de rede, como roteadores, switches e firewalls, atualizados com as últimas versões de firmware e correções de segurança fornecidas pelos fabricantes;

viii. Promover o uso consciente e responsável dos recursos de rede e deixar claras as obrigações e responsabilidades quanto ao uso inadequado, malicioso ou que possam comprometer a segurança da rede.

G. GESTÃO DE INCIDENTES:

Definição: refere-se à capacidade de identificar, responder e recuperar-se de incidentes de segurança da informação.

Propósito: minimizar os impactos causados por eventos de segurança, investigando e mitigando seus efeitos o mais breve possível.

Procedimentos:

i. Implementar um sistema de classificação e priorização de incidentes com base em sua gravidade, impacto potencial, nível de urgência e risco, permitindo uma resposta adequada e eficiente;

ii. Iniciar procedimentos para uma resposta rápida à incidentes de segurança da informação, com ações ágeis para conter e reduzir os riscos, efeitos e propagação;

iii. Estabelecer um processo para investigar e analisar a causa raiz dos incidentes, identificando as vulnerabilidades, as ações tomadas e as lições aprendidas, para diminuir a probabilidade de ocorrência de incidentes similares futuros;

iv. Ao ser percebido um incidente de segurança da informação por qualquer uma das partes, este deve ser prontamente comunicado à equipe responsável pela gestão de incidentes, assegurando a análise e tratamento;

v. Realizar revisões regulares do processo de gestão de incidentes, analisando e identificando oportunidades de melhoria;

vi. Promover a conscientização sobre a gestão de incidentes de segurança, capacitando a todos para identificar e relatar incidentes com prontidão e fornecer orientações sobre ações corretivas adequadas.

H. BACKUP:

Definição: envolve a realização de cópias de segurança periódicas dos dados e informações críticas da administração pública municipal.

Propósito: definir políticas de backup, escolher métodos de backup adequados, realizar regularmente cópias e armazenamento seguro das mídias de backup.

Procedimentos:

i. Identificar e priorizar os dados críticos e informações importantes que serão incluídos nos backups, levando em consideração a confidencialidade, integridade e disponibilidade desses dados;

ii. Determinar a frequência adequada para a realização dos backups com base na criticidade dos dados, considerando a capacidade de recuperação desejada em caso de incidentes ou desastres;

iii. Selecionar e utilizar mídias de backup confiáveis e seguras, como discos rígidos externos ou sistemas de armazenamento em nuvem confiáveis, levando em conta os requisitos de capacidade, segurança e facilidade de restauração;

iv. Garantir que as mídias de backup sejam armazenadas em local seguro, protegidas contra roubos, danos físicos, incêndios ou eventos adversos, levando em consideração a necessidade de acesso rápido e confiável em caso de recuperação;

v. Realizar regularmente testes de restauração dos backups para verificar a integridade dos dados, garantir a eficácia do processo de backup e a capacidade de recuperação dos dados em caso de necessidade;

vi. Monitorar regularmente os registros de backup para identificar quaisquer erros ou falhas e garantir que os backups estejam sendo realizados corretamente, sem falhas ou incompletos;

vii. Realizar cópias de backup em um local externo, fora das instalações físicas da administração pública municipal, para proteger os dados contra desastres que possam afetar a infraestrutura principal;

viii. Revisar e atualizar regularmente a política de backup, levando em consideração as mudanças nos requisitos, regulamentações e tecnologias, para garantir a eficácia e relevância contínua dos procedimentos.

I. CLASSIFICAÇÃO E TRATAMENTO DAS INFORMAÇÕES:

Definição: referem-se à atribuição de níveis de classificação às informações, de acordo com sua importância, confidencialidade e sensibilidade.

Propósito: garantir que as informações sejam devidamente protegidas, proporcionando um equilíbrio entre a necessidade de acesso e os requisitos de segurança.

Procedimentos:

i. Estabelecer um sistema de classificação para as informações com base em importância, confidencialidade e sensibilidade da informação;

ii. Designar responsáveis pela supervisão e implementação das regras de classificação e tratamento das informações e garantir que haja um ponto de contato designado para questões relacionadas à segurança da informação;

iii. Garantir que a classificação e o tratamento das informações sejam considerados em todas as fases do ciclo de vida da informação, desde sua produção até seu descarte final;

iv. Implementar controles de acesso adequados com base na classificação das informações, garantindo que apenas pessoas autorizadas tenham acesso às informações confidenciais ou sensíveis

v. Estabelecer procedimentos para o tratamento adequado das informações, incluindo requisitos de autenticação, registros de atividades e rastreabilidade;

vi. Estabelecer diretrizes para o armazenamento seguro de informações sensíveis, como criptografia de dados ou restrições físicas de acesso;

vii. Assegurar que as informações sejam adequadamente destruídas ou descartadas quando não forem mais necessárias, seguindo políticas de remoção segura de dados;

viii. Implementar mecanismos de auditoria e monitoramento para garantir o cumprimento das políticas de classificação e tratamento das informações;

ix. Realizar revisões regulares das categorias de classificação e dos controles de tratamento das informações, garantindo sua eficácia contínua e sua conformidade com as regulamentações relevantes;

x. Garantir que os colaboradores sejam devidamente treinados e conscientizados sobre as categorias de classificação e os requisitos de segurança associados a cada uma delas.

J. GESTÃO DE VULNERABILIDADES:

Definição: envolve a identificação, avaliação e tratamento de vulnerabilidades em sistemas, aplicativos e infraestrutura.

Propósito: reduzir a exposição a ameaças, garantindo que as vulnerabilidades sejam identificadas e tratadas de forma oportuna.

Procedimentos:

i. Realizar avaliações regulares de vulnerabilidades em sistemas, aplicativos e infraestrutura, utilizando ferramentas adequadas para identificar possíveis falhas de segurança;

ii. Classificar as vulnerabilidades identificadas com base em sua gravidade, priorizando aquelas que representam um maior risco;

iii. Estabelecer um processo de tratamento de vulnerabilidades, que inclua ações corretivas adequadas para mitigar os riscos identificados;

iv. Implementar medidas preventivas, como a aplicação de patches de segurança e atualizações de software, para corrigir as vulnerabilidades identificadas;

v. Realizar testes de penetração ou avaliações de segurança periódicas, a fim de identificar vulnerabilidades desconhecidas ou potenciais brechas de segurança;

vi. Manter-se atualizado sobre as melhores práticas e as últimas tendências em gestão de vulnerabilidades, utilizando recursos como publicações especializadas, grupos de discussão e comunidades de segurança da informação;

vii. Estabelecer um processo de revisão e melhoria contínua da gestão de vulnerabilidades, levando em consideração as lições aprendidas, as mudanças nas ameaças de segurança e as novas tecnologias disponíveis.

3. CONSCIENTIZAÇÃO E TREINAMENTO

A conscientização e treinamento são os elementos essenciais para garantir a eficácia do Plano de Segurança da Informação e a adoção das boas práticas. Todo pessoal envolvido deve estar ciente do papel que desempenha, de suas obrigações e do impacto de suas ações.

Para promover a conscientização este Plano de Segurança da Informação deve ser apresentado e explicado à todas as partes envolvidas, por meio de comunicação interna, apresentações e reuniões informativas ou outros meios disponíveis. E quando identificada a necessidade de revisão ou esclarecimentos adicionais, ser prontamente fornecidos por pessoal capacitado, junto de cópia deste material.

4. RESPONSABILIDADES

Para a efetivação do Plano de Segurança da Informação - PSI, o compromisso e a responsabilidade de todas as áreas envolvidas devem ser considerados, cada área deve participar e contribuir para o todo e de acordo com suas atribuições.

A alta direção e administração têm a responsabilidade geral de garantir que o PSI seja estabelecido, implementado, mantido e revisado de acordo com as necessidades da administração pública municipal. Devem fornecer apoio e recursos adequados para sua implementação, demonstrar comprometimento com a segurança da informação e garantir que as políticas e diretrizes do PSI sejam seguidas.

A equipe de segurança da informação é responsável por desenvolver, implementar e manter o PSI. Eles são encarregados de realizar avaliações de riscos, identificar e implementar controles de segurança, monitorar e solucionar incidentes e garantir a conformidade com as políticas e diretrizes atualizadas.

Todos os colaboradores e usuários da administração pública municipal têm a responsabilidade de cumprir as políticas e procedimentos do PSI. Eles devem estar cientes e seguir as práticas de segurança estabelecidas, tomar medidas para proteger as informações e ativos associados, relatar incidentes de segurança à equipe de segurança da informação e participar de treinamentos em segurança da informação.

Fornecedores e parceiros que tenham acesso às informações e ativos da administração pública municipal também têm responsabilidades no âmbito da segurança. Eles devem estar em conformidade com os requisitos de segurança da informação, seguir as políticas e diretrizes do PSI e garantir a confidencialidade, integridade e disponibilidade das informações compartilhadas.

5. MONITORAMENTO, AUDITORIA E MELHORIA CONTÍNUA

Os processos de monitoramento e registros de eventos devem ser viabilizados, pois possibilitam o desenvolvimento e a execução de auditorias, que buscam garantir a avaliação dos resultados e a conformidade das ações frente os controles e políticas estabelecidas.

Espera-se com o passar do tempo um aumento da maturidade organizacional e do estágio de desenvolvimento cultural, permitindo a obtenção de resultados mais próximos à conformidade.

A Gestão da Segurança da Informação não deve depender tão somente da avaliação e auditoria dos resultados, mas também dos processos de melhoria contínua, visto a dinâmica compreendida nas áreas de tecnologia.

Padrões, regulamentações e políticas internas estabelecidas podem necessitar de novos ajustes e controles, devido ao desenvolvimento e aplicação de técnicas ou novos equipamentos e funções.

A melhoria contínua deve ser observada e avaliada, desde o momento inicial da implantação das Políticas de Segurança da Informação ao estabelecimento de novas realidades e objetivos políticos, organizacionais e estruturais.

PLANO MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO - PSI

N.º: 001 / 2023

EDER CARLOS FOGACA DA CRUZ:14506312821
Assinado de forma digital por EDER CARLOS FOGACA DA CRUZ:14506312821
Dados: 2023.12.14 08:55:47 -03'00'

EDER CARLOS FOGAÇA DA CRUZ
Prefeito Municipal

MARCIO RICARDO BERGAMO BENTO:28808918840
Assinado de forma digital por MARCIO RICARDO BERGAMO BENTO:28808918840
Dados: 2023.12.14 08:57:58 -03'00'

MARCIO RICARDO BERGAMO BENTO
Responsável pelo Serviços de TI

PLANO MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO - PSI

N.º: 001 / 2023

TERMO DE APROVAÇÃO

Diante do trabalho realizado pela equipe técnica, visando a elaboração e desenvolvimento do Plano Municipal de Segurança da Informação, tendo desenvolvido as etapas necessárias aos estudos e conclusões, bem como diante da revisão realizada por pessoal jurídico, especificamente para tal fim, APROVO O PLANO MUNCIPAL DE SEGURANÇA DA INFORMAÇÃO - N.º 001/2023, para que surta seus legais efeitos.

Publique-se.

Taguaí, 14 de dezembro de 2023.

EDER CARLOS FOGACA DA CRUZ:14506312821

Assinado de forma digital por EDER CARLOS FOGACA DA CRUZ:14506312821
Dados: 2023.12.14 08:55:23 -03'00'

EDER CARLOS FOGAÇA DA CRUZ
Prefeito Municipal