DECRETO Nº 16.039, DE 19 DE MARÇO DE 2025.

Dispõe sobre a Política de Segurança da Informação e Comunicação no âmbito do Poder Executivo Municipal de Taubaté, sendo integrado por três anexos.

SÉRGIO LUIZ VICTOR JÚNIOR, PREFEITO MUNICIPAL DE TAUBATÉ, no uso de suas atribuições legais, nos termos dos artigos 56, VIII, e 58, §1º, I, 'a', da Lei Orgânica do Município, CONSIDERANDO

1) a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação e comunicação no âmbito da Prefeitura Municipal de Taubaté, promovendo a proteção dos usuários, dos equipamentos, dos softwares, dos dados dos contribuintes e da própria Administração Pública;

2) a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito da Administração Municipal, de forma a atender aos princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

3) que os servidores públicos devem zelar pelas informações que lhes são confiadas no exercício de suas funções;

4) que as ações de segurança da informação e comunicação reduzem custos e riscos e aumentam os benefícios prestados aos cidadãos, ao permitir a oferta de processos, produtos e serviços suportados por sistemas de informações mais seguros;

D E C R E T A:

Art. 1º Fica instituída nos termos deste Decreto e seus respectivos anexos I, II e III, a Política de Segurança da Informação e Comunicação no âmbito da Prefeitura Municipal de Taubaté, tendo como objetivo principal a normatização e a adequada utilização dos recursos da tecnologia da informação e comunicação.

Art. 2º A Política de Segurança da Informação e Comunicação constitui um conjunto de diretrizes e normas que estabelecem o princípio de proteção, controle e monitoramento das informações processadas, armazenadas e custodiadas pela Administração Municipal, aplicando–se a todos os órgãos do Poder Executivo Municipal, inclusive à administração pública municipal indireta, respeitada a autonomia legal.

Art. 3º Compete à Secretaria de Desenvolvimento, Inovação e Turismo, por meio do Departamento de Tecnologia da Informação, a coordenação das políticas de segurança da informação e comunicação no Município.

Art. 4º Fica revogado o Decreto 14.815/2020, de 15 de setembro de 2020.

Art. 5º Fazem parte integrante deste Decreto o Anexo I, contendo as Diretrizes Comportamentais de Segurança; o Anexo II, contendo as Diretrizes da Gestão de Acesso a Sistemas de Informação; eu Anexo III, contendo a Política de Segurança da Informação.

Art. 6º Este Decreto entra em vigor na data de sua publicação.

Prefeitura Municipal de Taubaté, 19 de março de 2025, 386º da fundação do Povoado e 380º da elevação de Taubaté à categoria de Vila.

SÉRGIO LUIZ VICTOR JÚNIOR
Prefeito Municipal

DANILO VELLOSO
Secretário de Desenvolvimento, Inovação e Turismo

Publicado na Secretaria de Governo e Relações Institucionais, 19 de março de 2025.

ANTONIO CARLOS OZÓRIO NUNES
Secretário de Governo e Relações Institucionais

HUGO DE OLIVEIRA VIEIRA BASILI
Diretor de Assuntos Legislativos

ANEXO I

DAS DIRETRIZES COMPORTAMENTAIS DE SEGURANÇA

1. Introdução

1.1 Objetivo

A prática da Segurança da Informação deve ser compreendida por toda a Prefeitura como um instrumento fundamental para salvaguardar os ativos de informação, garantir sua confidencialidade, integridade e disponibilidade e prover suporte para mitigar riscos e impactos de imagem, financeiro, legal e operacional.

A disciplina de segurança da informação abrange diversos aspectos do ambiente corporativo como comportamento, gestão de acessos aos recursos tecnológicos da entidade e infraestrutura dos recursos.

Apoiado nos parâmetros legais e em princípios éticos, este documento estabelece as diretrizes de Segurança da Informação, referentes a questões comportamentais dos colaboradores no uso de recursos de tecnologia e manipulação de ativos de informação, que devem ser seguidas por todas as áreas da Prefeitura de Taubaté. Sua utilização resulta em minimização dos riscos de vazamento de informação, que serão acompanhados através de indicadores pelos quais terão seus desempenhos analisados.

1.2 Conceitos de Segurança da Informação

Segurança da informação é uma disciplina corporativa que tem como objetivo a salvaguarda de três pilares fundamentais que regem o ciclo de vida dos ativos de informação: Confidencialidade, Integridade e Disponibilidade.

- **Confidencialidade:** atributo de segurança que assegura que a informação seja acessada somente por usuário autorizado.

- **Integridade:** atributo de segurança que assegura que a informação não foi modificada de forma não autorizada ou imperceptível.

- **Disponibilidade:** atributo de segurança que assegura que a informação esteja disponível para uso por seus usuários autorizados.

A defesa destes três atributos é obrigação de todo colaborador da Prefeitura de Taubaté, e reforçada via área de Tecnologia da Informação, que deve estabelecer e garantir que as melhores práticas estão sendo seguidas pelo município, tanto via monitoramento do ambiente tecnológico, quanto através de conscientização dos colaboradores.

Nos capítulos subsequentes, será explicado como os colaboradores devem manipular ativos de informação no ambiente da Prefeitura de Taubaté, tanto utilizando recursos tecnológicos quanto físicos.

1.3 Área de Tecnologia da Informação

São responsabilidades da área de Tecnologia da Informação:

- Estabelecer regras na gestão da Segurança da Informação, visando a atribuição de responsabilidades a todos os colaboradores com relação a salvaguarda dos ativos de informação da Prefeitura;
- Manter atualizadas as políticas, diretrizes e procedimentos da Prefeitura de Taubaté no que diz respeito à Segurança da Informação;
- Garantir que os sistemas de informação utilizados respeitem os requisitos mínimos de segurança estabelecidos para a Prefeitura de Taubaté nas suas camadas de gestão de acessos e infraestrutura durante a fase de aquisição, desenvolvimento e manutenção dos projetos.

1.4 Principais Referências

- ENS – 008345 (Política de Segurança da Informação);
- Lei n.º12.965/2014 (Marco Civil da Internet);
- Lei n.º 12.846/2013 (Lei Anti-Corrupção);
- Lei nº 12.850/2013 (Provas Eletrônicas);
- Decreto n.º 7962/2013 (Regulamentação do Comércio Eletrônico);
- Leis de nº 12.735 e 12.77/2012 (Leis sobre Crimes Eletrônicos);
- Decreto n.º 7.845/2012 (Regulamenta o tratamento da informação classificada);
- Lei nº 12.551/2011 (Lei sobre o Home Office e o Teletrabalho);
- Lei nº 12.527/2011 (Lei Acesso à Informação);

- ISO/IEC 27001:2005 (Sistemas de Gestão de Segurança da Informação);
- Lei nº 9.610/1998 (Lei de Direitos Autorais)
- Lei nº 9.609/1998 (Lei de Software)
- Lei n.º 9.296/1996 (Lei sobre Interceptação de Comunicações Telefônicas)
- Lei nº 9.279/1996 (Lei de Propriedade Industrial)
- Constituição Federal de 1988

1.5 Definição

- **Ativos de Informação:** Incluem, mas não se limitam a bancos/bases de dados, documentações de sistemas e softwares, contratos, políticas, procedimentos operacionais, planos e informações diversas.

- **Ativos de Software:** Incluem, mas não se limitam a sistemas operacionais, softwares adquiridos de terceiros e desenvolvidos na Prefeitura de Taubaté e utilitários.

- **Ativos Físicos:** Incluem, mas não se limitam a computadores, servidores, celulares, smartphones, tablets, rádios, mídias removíveis e outros equipamentos.

- **Serviços:** Incluem, mas não se limitam a serviços de computação e comunicações e serviços que gerem disponibilidade e comodidade aos colaboradores da Prefeitura de Taubaté, como ar condicionado e energia elétrica.

- **Perfil de Acesso:** Atributo de contas de acesso que especificam a quais informações determinado colaborador terá no ambiente tecnológico da Prefeitura de Taubaté.

- **Segregação de Funções:** Necessidade ligada a cadeia de processos de negócio, onde funções conflitantes, como de comprador e aprovador de compras, devem ser segregadas.

- **Perfil de acesso à Internet:** conjunto de categorias de sites, protocolos e regras de acesso associado a um grupo de usuários. São classificados nas categorias global, estendido e amplo.

- **Filtro de Conteúdo Web:** solução utilizada para implementar os perfis de acesso à Internet e bloquear o acesso a sites que tragam risco legal ou de segurança lógica para a Prefeitura de Taubaté.

- **URL:** endereço que identifica a localização de um determinado recurso disponibilizado em uma rede de computadores.

- **Passphrase:** evolução do conceito de Password onde, em vez de definir como senha uma palavra com caracteres especiais, numerais, maiúsculas e minúsculas, define-se uma frase de acesso, cuja tendência é mais fácil de lembrar para o proprietário desta e mais difícil de ser quebrada via ataques cibernéticos.

- **Incidente de segurança da informação:** qualquer ocorrência que comprometa os atributos de segurança da informação no ambiente de TI.

- **Cadeia de Custódia:** A Cadeia de Custódia é um processo usado para manter e documentar a história cronológica de evidências, visando garantir a idoneidade e o rastreamento das mesmas. Ela é utilizada para rastrear a posse e o manuseio destas. Este rastreio passa pela cópia (aquisição) dos ativos de informação, o transporte, o recebimento, o armazenamento e a análise. É um documento muito importante que registra tudo o que aconteceu com uma evidência, quem e quando trabalhou com os arquivos durante seu ciclo de vida.

2 Diretrizes Comportamentais

A seguir, serão listadas as diretrizes comportamentais de Segurança da Informação. Estas se aplicam a todos os colaboradores da Prefeitura de Taubaté, sem exceções.

2.1 Utilização de Recursos Tecnológicos

Atualmente, todo conhecimento e informação de uma corporação nascem em suas redes privadas de dados, onde ficam armazenados e protegidos. Para garantir esta proteção, cuidados são necessários, uma vez que más práticas executadas por colaboradores podem comprometer os perímetros de segurança tecnológicos criados pela entidade, por mais caros e complexos que estes sejam. Assim, seguem as práticas que todos colaboradores devem seguir na utilização destes recursos.

2.1.1 Ativos Físicos

Todo colaborador, durante suas atividades no ambiente da Prefeitura de Taubaté, terá acesso a um ou mais ativos físicos, através dos quais acessarão os recursos de tecnologia e informações armazenadas nestes. Abaixo, estão listadas as regras na utilização destes dispositivos:

1. Todo colaborador que utilizar os ativos de TI da Prefeitura de Taubaté deverá estar ciente sobre sua responsabilidade ao utilizá-los. Todos os colaboradores que tenham acesso aos ativos de TI da Prefeitura de Taubaté, deverão saber sobre a correta forma de utilização dos ativos, assim como seus limites de uso.
2. As regras na utilização de microcomputadores (desktops, laptops e tablets) devem ser aceitas explicitamente pelo usuário do dispositivo, que assinará um termo de aceite ao receber o acesso a uso dos equipamentos. Este é responsável jurídico pelo uso correto deste ativo.
3. Dispositivos de armazenamento são de uso proibido. Qualquer exceção deverá ser previamente aprovada pelo Secretário Municipal da área solicitante e avaliada pelo Departamento de Tecnologia da Informação, antes que qualquer dispositivo seja conectado a microcomputadores da Prefeitura de Taubaté, e serão monitorados.
4. A instalação de softwares nos sistemas operacionais da Prefeitura de Taubaté é controlada. Somente softwares devidamente autorizados pelas áreas de tecnologia da informação podem ser instalados nestes dispositivos.
5. Modificações (upgrades e downgrades) destes ativos devem ser realizadas apenas por equipes autorizadas pela área de TI. O mesmo vale para atualizações de sistemas operacionais, aplicativos e formatações de equipamentos.
6. A realização de instalações de softwares licenciados nos sistemas operacionais da Prefeitura de Taubaté é realizada apenas por equipes autorizadas pela Área de Tecnologia da Informação.
7. Ao utilizar ativos físicos da Prefeitura de Taubaté fora de suas dependências, todo colaborador deve avaliar se o ambiente físico e a infraestrutura de acesso aos meios de comunicação oferecem os requisitos mínimos de segurança para acesso seguro às informações e sistemas de provisionamento e processamento de dados.
8. A captura remota com controle de ativos físicos é exclusiva para fins de manutenção da TI e equipes autorizadas com análise prévia dos riscos envolvidos.

2.1.2 Contas de Acesso

Todo acesso a sistemas da Prefeitura de Taubaté, desde a rede até aplicações corporativas, é feito através de contas de acesso. Abaixo, seguem diretrizes na solicitação, aprovação e uso destas contas:

1. Toda conta de acesso criada é pessoal e intransferível. O titular desta conta é responsável jurídico pelo seu correto uso.
2. É permanentemente proibido o empréstimo de contas de acesso para outros colaboradores.
3. Toda conta de acesso deve ser aprovada por um colaborador com cargo de liderança (Diretor, Secretário Adjunto, Secretário, Chefe de Gabinete ou Prefeito). A aprovação atesta que o solicitante necessita das funções solicitadas na conta para realizar suas atividades.
4. Todos os colaboradores devem substituir senhas de suas contas, periodicamente.
5. Ao indício de comprometimento na confidencialidade de sua senha, o colaborador deve substituir sua senha imediatamente.
6. Todos os aprovadores devem participar e executar as revisões de acesso nas campanhas de revalidação das contas de acesso promovidas pela TI.
7. Caso a área possua soluções que são geridas por ela, é de obrigação dos gerentes desta área a promoção de campanhas internas de revisão das contas de acesso destes sistemas.
8. Cargos de liderança são responsáveis diretos pela segregação de funções nos acessos dos colaboradores de sua área. Caso ocorra problema com essa questão, a liderança é obrigada a resolver o quanto antes, assim que for detectado, envolvendo as áreas necessárias para o ajuste do perfil de acesso.
9. Toda Secretaria deve solicitar o encerramento e bloqueio de acessos desnecessários do colaborador conforme mudem suas atribuições na Prefeitura de Taubaté.
10. Nenhum colaborador deve utilizar conta de acesso destinada ao uso exclusivo por sistemas, incluindo usuários de sistemas operacionais, aplicações e sistemas de manutenção e provisionamento de dados.

2.1.3 Utilização de E-mail Corporativo

O e-mail é um dos meios mais utilizados por agentes maliciosos para captura de informações e execução de ataques, além de ser um recurso finito na organização. Isso exige que todos os colaboradores sigam algumas regras específicas na utilização deste recurso, garantindo sua disponibilidade e integridade. Abaixo, seguem estas diretrizes:

1. O serviço de correio eletrônico deverá ser utilizado somente para assuntos profissionais.
2. Todas as mensagens geradas pelos colaboradores da Prefeitura de Taubaté deverão respeitar a legislação vigente, especialmente, a Lei de Direitos Autorais.

3. As mensagens eletrônicas deverão possuir o seu assunto claramente indicado.
4. Todo correio eletrônico enviado por colaboradores da Prefeitura de Taubaté deverá estar identificado com os dados do colaborador (assinatura).
5. Todos os anexos do correio eletrônico deverão estar claramente descritos no corpo da mensagem.
6. É proibido o encaminhamento de correntes ou outros tipos de mensagens de entretenimento em massa.
7. Todo colaborador, em caso de suspeita de ser alvo de um ataque direcionado por e-mail (spam solicitando dados bancários, e-mail de funcionário perguntando de dados de determinado projeto que não está envolvido, etc.) deve reportar imediatamente o caso para sua chefia direta e/ou Departamento de Tecnologia da Informação.
8. É proibida a utilização de qualquer mecanismo de redirecionamento de mensagens internas para correios eletrônicos externos não integrantes do ambiente da Prefeitura de Taubaté.
9. Ao enviar mensagem para um grupo grande de destinatários, coloque os endereços no campo “cópia oculta”.

2.1.4 Utilização de Internet

Assim como o e-mail, a conexão de internet é um recurso finito na Prefeitura de Taubaté que exige alguns cuidados especiais, por ser um dos principais canais de entrada do mundo externo ao ente.

A fim de garantir a disponibilização deste recurso com desempenho satisfatório, proteger as informações confidenciais do município e evitar desperdícios em gastos com a capacidade do link de comunicação, as diretrizes no uso deste recurso devem ser compreendidas e cumpridas, sendo as seguintes:

1. O acesso à Internet somente deve ser utilizado para finalidades relacionadas aos interesses e assuntos profissionais da Prefeitura de Taubaté, sendo que, o acesso a páginas da internet cujo conteúdo seja inapropriado é proibido como pornografia, pedofilia, atividades criminais, discriminatórias em razão de raça, cor, origem ou qualquer outra, bem como atividade não éticas.
2. O colaborador, estando dentro das dependências da Prefeitura de Taubaté e utilizando ativo físico da mesma, deve obrigatoriamente acessar a Internet via a rede interna.
3. É proibido o acesso à Internet via modem estando conectado na rede interna da Prefeitura.

4. Todo colaborador está ciente que a Internet é monitorada e controlada no ambiente da Prefeitura de Taubaté, com registros dos acessos executados nos últimos 90 dias.
5. As chefias possuem autonomia para solicitar o histórico de utilização deste recurso dos colaboradores de sua área via Departamento de Tecnologia da Informação.
6. O colaborador é responsável jurídico pelo acesso, e pode ser responsabilizado caso seu comportamento de acesso crie brechas que intencionalmente comprometam a segurança lógica da informação da Prefeitura de Taubaté e/ou a confidencialidade dos dados internos (por exemplo publicação de informação corporativa em páginas da Internet sem a autorização expressa da Prefeitura), nos termos da legislação trabalhista, civil ou criminal aplicável.
7. O uso do e-mail pessoal não é permitido na Prefeitura de Taubaté, pois, aumenta o nível de exposição da informação corporativa e não possui rastreabilidade; aumenta também o risco de contaminação por vírus; e pode comprometer o acesso a páginas de Internet relacionadas às atividades inerentes aos serviços da Prefeitura, uma vez que o webmail concorre em nível de performance com outros acessos.
8. O acesso à Internet pela rede corporativa deve ser feito através de um navegador homologado pela área de Tecnologia da Informação da Prefeitura.
9. É proibida a conexão com redes não indexadas (Deep Web) e P2P a partir de ativos da Prefeitura de Taubaté, com exceção para áreas de análise forense e inteligência.
10. O Upload e Download de informações devem ser executados apenas a partir de conexões seguras e autorizadas. As ferramentas para troca deste tipo de informação via Internet podem ser usadas apenas com autorização do Departamento de Tecnologia da Informação.

2.2 Tratamento de Informações

As informações sensíveis da Prefeitura de Taubaté, classificadas como “Confidenciais”, estão espalhadas tanto no ambiente tecnológico quanto físico da Prefeitura. Estas exigem cuidados especiais em sua criação, identificação, manipulação e descarte. Assim, diretrizes na manipulação de todas as informações do município são necessárias para garantir a integridade e rastreabilidade das informações sensíveis.

Abaixo, segue lista de diretrizes que todos os colaboradores da Prefeitura de Taubaté devem estar cientes e cumprir para garantia da proteção adequada dos dados corporativos:

1. Todo colaborador deve estar consciente e preparado para lidar com as ameaças e preocupações relativas à segurança da informação. Caso não esteja, deve solicitar apoio a sua

chefia imediata com relação a treinamento apropriado em conscientização e manutenção da segurança da informação.

2. Classificar todas as informações criadas.
3. Líderes devem garantir que o armazenamento das informações seja rigorosamente adequado à classificação dos documentos.
4. O acesso a informações de defesa e segurança pode ocorrer apenas mediante credenciamento de pessoas físicas ou jurídicas.
5. Tirar fotos e realizar gravações de áudio e vídeo em áreas com informação confidencial ou secreta pode ocorrer apenas mediante autorização.
6. Assim como contas de acesso ao ambiente tecnológico, o acesso físico a áreas confidenciais e secretas deve ser revisado pela chefia da área, periodicamente.
7. Nenhuma informação classificada da Prefeitura de Taubaté como CONFIDENCIAL ou RESERVADA pode ser discutida em locais inapropriados, como lugares públicos, na presença de terceiros ou pessoas não diretamente relacionadas ao assunto, ou diante daqueles sem autorização para conhecimento dessa informação.
8. Para apresentar ou enviar informações com classificação “Reservada”, ou acima, fora das dependências da Prefeitura de Taubaté, o colaborador deve solicitar autorização expressa do responsável pela geração ou guarda da informação.
9. O registro da cadeia de custódia de informações confidenciais ou secretas deve ser respeitado por todo colaborador da Prefeitura de Taubaté.

2.3 Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação

As atividades técnicas de aquisição, desenvolvimento e manutenção de sistemas da informação exigem uma atenção especial. É possível garantir que os sistemas utilizados pela Prefeitura irão zelar pelos três pilares de segurança da informação, isso apenas através do alinhamento e cumprimento das melhores práticas destas disciplinas por todos os colaboradores envolvidos nestas atividades. Deste modo, seguem as diretrizes para execução deste tipo de atividade:

1. Todo colaborador que está envolvido em processos de aquisição, desenvolvimento ou manutenção de sistemas da informação deve garantir que todas as diretrizes da Gestão de Acesso a Sistemas de Informação estão sendo cumpridas.
2. Toda solução de tecnologia adquirida pela Prefeitura de Taubaté deve passar por processo de seleção competitivo com múltiplos fornecedores. Casos de exceção são aceitos apenas através de assinatura de justificativa de compra direta pelo diretor da área interessada e submetida à aprovação.

3. Em processos de aquisição, soluções que não atendem às diretrizes de segurança da Prefeitura de Taubaté devem ser reprovadas tecnicamente pelos colaboradores envolvidos na avaliação técnica.
4. Caso seja detectado que um sistema de informação já implementado não satisfaça as diretrizes da Gestão de Acesso a Sistemas de Informação, o colaborador deve informar a chefia para avaliar se a exceção será aceita perante as vantagens competitivas que este sistema traga às atividades inerentes à administração pública de competência da Prefeitura de Taubaté.
5. Colaboradores podem executar modificações em sistema de informações apenas com Requisições de Mudança aprovadas.
6. Com exceção de mudanças emergenciais, nenhuma mudança de sistema deve causar a indisponibilidade de dados.

2.3 Tratamento de exceções às diretrizes de Segurança da Informação

Devido à diversidade dos serviços e processos da Prefeitura de Taubaté, em alguns casos a abertura de exceções é necessária. Uma vez que estas aberturas impactam diretamente os riscos corporativos da entidade, as seguintes práticas são obrigatórias para estes casos:

1. Toda exceção referente às diretrizes contidas nos procedimentos da Prefeitura de Taubaté deve ser solicitada via documento físico ou digital dirigido ao Diretor do Departamento ou, na ausência deste, à liderança de hierarquia superior.
2. Se aprovada ou se desaprovada a solicitação, deve-se descrever informações sobre a exceção, incluindo descrição do impacto desta para os riscos da Prefeitura de Taubaté.
3. A aprovação ou desaprovação deve ser registrada em documento físico ou digital assinado pelo Diretor do Departamento ou, na ausência deste, por liderança de hierarquia superior, e arquivado por no mínimo três anos pela equipe de segurança da informação para subsidiar resposta a eventuais auditorias.

2.4 Prevenção e denúncia de Incidentes de Segurança da Informação na Prefeitura de Taubaté

Incidentes de segurança não possuem local nem hora para ocorrerem. Por este motivo, os entes públicos devem incentivar a prática de denúncias e alertas a partir de seus colaboradores. Assim, seguem abaixo as diretrizes da Prefeitura de Taubaté para a comunicação de incidentes de segurança da informação por parte de seus colaboradores:

1. Todo colaborador deve entrar em contato com o canal de denúncias o mais breve possível ao perceber um possível Incidente de Segurança da Informação.

2. Em caso de detecção de riscos relacionados à Segurança da Informação, devido a processos ou práticas da área, o colaborador deve contatar o Departamento de Tecnologia da Informação, que irá avaliar e prover soluções relacionadas à prevenção de incidentes de Segurança da Informação.

ANEXO II

DAS DIRETRIZES DA GESTÃO DE ACESSO A SISTEMAS DE INFORMAÇÃO

1 OBJETIVO

Definir diretrizes da gestão de acessos a sistemas de informação da Prefeitura de Taubaté.

2 REFERÊNCIAS

ISO27001 - Sistema de Gestão da Segurança da Informação (SGSI).

Diretrizes Comportamentais de Segurança da Informação.

Política de Segurança da Informação.

3 DEFINIÇÕES

Identidade: identificador pessoal e único nos sistemas.

Trilha de auditoria: registro de rastreabilidade suficiente para os acessos e suas solicitações.

Usuário: qualquer pessoa que possua acesso a sistemas corporativos.

4 RESPONSABILIDADES

4.1 Usuário: zelar pelos acessos aos quais tiver permissão de uso.

4.2 Solicitante: registrar as solicitações de acesso de acordo com a necessidade do usuário.

4.3 Aprovador: certificar-se que o acesso solicitado é coerente ao mínimo necessário.

4.4 Tecnologia da Informação: manter as trilhas de auditoria das solicitações, aprovações, concessões e revogações de acesso dos sistemas que fazem parte de seu escopo de trabalho.

4.5 Segurança da Informação: definir as diretrizes que regem gestão de acessos.

5 GESTÃO DE IDENTIDADES E ACESSOS

É uma disciplina corporativa que rege a administração de identidades e acessos nos sistemas. Ela se subdivide em 5 passos:

1 - Toda Solicitação deve:

- ser formalizada;
- identificar o que se pede e para quem;
- aprovada, quando necessário;
- possuir trilha de auditoria.

2- Concessão:

• A identidade só pode ser criada e o acesso liberado após formalizada a solicitação;

• Identidades já utilizadas não podem ser atribuídas a outros usuários;

• Usuários que já receberam uma identidade não podem receber outra.

3 - Utilização

• Os sistemas devem conter um requisito mínimo de segurança para senhas;

• As senhas devem ser alteradas, periodicamente.

4 - Revisão:

• A necessidade de acesso deve ser revisada, formal e periodicamente.

5 - Remoção:

• Em caso de término de vínculo de trabalho do usuário, o RH ou o gestor do fornecedor deve informar à TI, imediatamente;

• A TI tem um dia útil para realizar a remoção de acessos;

• Acessos também devem ser removidos quando não forem mais necessários;

• Identidades devem ser preservadas para registro das trilhas de auditoria e correta atribuição em caso de retorno do usuário.

ANEXO III

DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Estabelecer a Governança de Segurança da Informação da Administração Pública Municipal – na Prefeitura de Taubaté e em todas as suas extensões, inclusive na administração indireta, respeitada a autonomia legal. Esta política visa proteger e preservar os ativos de informação associando os objetivos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade, Responsabilidade e Conformidade ao sistema normativo brasileiro, incluindo, sem dúvidas, normas municipais.

2. PRINCÍPIOS

O Comitê de Segurança da Informação, instituído por esta Política, conduz a apreciação e as deliberações sobre o tema e os seus membros são:

- Prefeito;
- Secretário de Governo;
- Secretário de Desenvolvimento, Inovação e Turismo; e
- Diretor de Tecnologia da Informação.

A Prefeitura de Taubaté adota práticas de Segurança da Informação seguindo as melhores práticas internacionais e em conformidade com ISO/IEC 27.005:2011, a Lei n.º 12.527/2011 (Lei de Acesso à Informação) e ao Procedimento de Classificação e Controle dos Ativos de Informação, de modo que:

- A Segurança da Informação adota medidas específicas de proteção e preservação devido à importância para o munícipe de Taubaté.
- A Segurança Cibernética é controlada a partir do conjunto de tecnologias, processos e práticas para proteger redes, computadores, dispositivos, programas e dados contra qualquer ataque, dano, acesso não autorizado, sabotagem ou movimentos ativistas de qualquer natureza.
- Atendimento a todos os requisitos legais e de certificação dos produtos e serviços da Prefeitura de Taubaté ligados ao tema Segurança da Informação.
- Cumprimento de obrigações contratuais estabelecidos entre a Prefeitura de Taubaté e seus servidores, fornecedores, parceiros e cidadãos.
- Atuação de forma ética de acordo com a legislação vigente a qual a Prefeitura Municipal de Taubaté está subordinada.

3. DIRETRIZES

- Praticar o princípio de privilégio de acesso mínimo necessário. Cada indivíduo ou sistema deve deter apenas o acesso necessário para o desempenho de sua função.
- Adotar o princípio de seguro por padrão para todos os Ativos de informação. O acesso à informação deve ser negado até que seja explicitamente permitido.
- Adotar o princípio de acesso legitimado. O acesso à informação somente poderá ser concedido a indivíduos com necessidade e direito de conhecimento da informação.
- Garantir a confidencialidade, integridade e disponibilidade do Conhecimento Sensível da Prefeitura de Taubaté, prevenindo qualquer falha ou vazamento das informações, bem como prevenindo qualquer comprometimento de sistemas de informações corporativos e de produtos da Prefeitura de Taubaté.
- Segregar as funções e acessos das pessoas na execução de suas rotinas e processos de trabalho de forma a evitar o uso indevido de informação privilegiada ou de autoridade de aprovação, coibindo conflitos de interesse.
- Garantir a classificação, proteção e controle dos Ativos de Informação em conformidade com o seu valor, requisito legal, sensibilidade e criticidade para as atividades de competência da Prefeitura de Taubaté.
- Disseminar aos servidores, fornecedores, parceiros e cidadãos suas responsabilidades por proteger os Ativos de Informação a que tiverem acesso em decorrência de suas atividades com a Prefeitura de Taubaté.
- Identificar e reportar qualquer suspeita que represente desvio ou descumprimento de qualquer legislação aplicável.
- Manter conduta aderente com a legislação vigente e com os princípios éticos aos quais a Prefeitura encontra-se subordinada.
- Considerar, sem prejuízo do previsto nesta Política, os critérios normativos e os riscos no momento de concessão, renovação e revogação de acessos de servidores, fornecedores, parceiros e cidadãos.

4. CONTROLE E APRENDIZADO

- O cumprimento desta política é de responsabilidade de todos os colaboradores da Prefeitura de Taubaté.
- O Comitê de Segurança da Informação fará o acompanhamento das ações decorrentes desta política através de reuniões com periodicidade mínima trimestral.
- Esta política será **analisada criticamente e, potencialmente, revisada**, com periodicidade mínima bianual.

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 0A53-6372-4BEE-A2F2

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

- HUGO DE OLIVEIRA VIEIRA BASILI (CPF 331.XXX.XXX-63) em 19/03/2025 16:25:13 GMT-03:00
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- ANTONIO CARLOS OZÓRIO NUNES (CPF 050.XXX.XXX-62) em 19/03/2025 16:35:56 GMT-03:00
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- DANILO VELLOSO (CPF 275.XXX.XXX-01) em 19/03/2025 17:55:53 GMT-03:00
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- SÉRGIO LUIZ VICTOR JUNIOR (CPF 372.XXX.XXX-76) em 21/03/2025 14:53:07 GMT-03:00
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://taubate.1doc.com.br/verificacao/0A53-6372-4BEE-A2F2