INSTRUÇÃO NORMATIVA COMPLEMENTAR – CDTSIP – 002/2022

ESTABELECE CONCEITOS, CRITÉRIOS E DIRETRIZES PARA A DISPONIBILIZAÇÃO E ADMINISTRAÇÃO DO ACESSO AOS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO, BEM COMO ESTABELECER CRITÉRIOS RELATIVOS ÀS SENHAS DAS RESPECTIVAS CONTAS DOS USUÁRIOS, NO ÂMBITO DA PREFEITURA MUNICIPAL DE ITAGUAÍ – RJ E DÁ OUTRAS PROVIDÊNCIAS.

O PRESIDENTE DO COMITÊ DE DIRETRIZES DE TECNOLOGIA, SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE – CDTSIP, torna público que o Colegiado, em reunião realizada em 30 de novembro de 2022, tendo em vista o disposto no art. 3º, incisos I a IV, do Decreto Municipal Nº. 4.711 de 26 de maio de 2022, nomeado pela Portaria Nº. 659 de 26 de maio de 2022, alterada pelas Portarias Nº. 1.110 de 04 de outubro de 2022 e Nº. 1.213 de 11 de novembro de 2022 e pelo item 7 da Política de Segurança da Informação e Privacidade, instituída pelo Decreto Municipal Nº. 4.706 de 22 de maio de 2022, APROVOU a seguinte Instrução Normativa Complementar:

Art. 1º Esta Instrução Normativa Complementar, estabelece conceitos, critérios e diretrizes para a disponibilização e administração do acesso aos serviços de tecnologia da informação, bem como estabelecer critérios relativos às senhas das respectivas contas dos usuários, a todos os órgãos e entidades da administração pública no âmbito da Prefeitura Municipal de Itaguaí – RJ;

Parágrafo Único. Para fins desta Instrução Normativa complementar, são estabelecidos as seguintes definições:

I - Usuário – servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da PMI, formalizada por meio da assinatura do Termo de Responsabilidade;

II - Senha ou Credencial de Acesso – credencial que concede, de maneira prevista, o direito de acesso, físico ou lógico, a determinado ativo de informação de qualquer natureza, ou local que o

abrigue. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes. É pessoal e intransferível.

III - Credenciais ou Contas de Acesso – permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e lógica como identificação de usuário e senha. É pessoal e intransferível;

IV - Perfil de Acesso – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

V - Recursos Computacionais – recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

VI - Rede Corporativa – conjunto de todas as redes locais sob a gestão da instituição;

VII - Rede Pública – rede de acesso a todos;

VIII - *Log* – é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

XI - *Logon* – procedimento de identificação e autenticação do usuário nos recursos de tecnologia da informação. É pessoal e intransferível;

X - Ativo de Tecnologia da Informação (TI) – são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles tem acesso;

XI - Controle de Acesso – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XII - Bloqueio de Acesso – processo que tem por finalidade suspender temporariamente o acesso aos recursos computacionais;

XIII - Ameaças – conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

XIV - Vulnerabilidades – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

XV - Incidente de Segurança – é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XVI - Tratamento de Incidentes de Segurança em Redes Computacionais – serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XVII - Termo de Responsabilidade – termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

CAPÍTULO I
DIRETRIZES GERAIS

Art. 2º A Conta de Acesso é o instrumento para identificação do usuário na rede corporativa da Prefeitura Municipal de Itaguaí e caracteriza-se por ser de uso individual e intransferível, sua divulgação é vedada sob qualquer hipótese.

Art. 3º Para utilização inicial dos recursos computacionais da rede corporativa da PMI é necessária abertura de chamado na Central de Atendimento do STI, pelo chefe da área a qual o usuário está lotado, solicitando inscrição do funcionário no cadastro de usuários da rede corporativa da PMI.

Art. 4º O cadastro de usuários da rede corporativa da PMI é composto de:

§1º Usuários Internos: são aqueles que acessam sistemas corporativos ou qualquer tipo de aplicação pela rede interna da PMI; e,

§2º Usuários Externos: são aqueles que acessam sistemas corporativos e aplicações da PMI pela rede mundial de computadores fora da rede interna corporativa, ou localmente na rede da PMI por prazo determinado.

Art. 5º A STI tem por objetivo consolidar todos os controles de acesso à rede e sistemas corporativos num diretório de usuários (AD – Serviço *Active Directory*).

Art. 6º Visando a maior segurança dos sistemas corporativos, os usuários internos devem estar devidamente identificados, sem o qual não poderão ser incluídos no sistema de controle de acesso aos sistemas corporativos.

Art. 7º Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas.

CAPÍTULO II
PARÂMETROS PARA A FORMAÇÃO DE SENHA E AUTENTICAÇÃO

Art. 8º Todas as senhas para autenticação na rede corporativa da PMI, devem seguir os seguintes critérios mínimos, para formação de senha e autenticação:

I. Em relação ao comprimento, a senha deverá ter no mínimo 8 (oito) caracteres;
II. Em relação à sintaxe e dentro dos limites de comprimento descritos acima, a senha deve contar no mínimo 1 (um) caractere de pelo 3 (três) das seguintes classes:
    a. Letras em caixa alta: A, B, C, ..., Z;
    b. Letras em caixa baixa: a, b, c, ..., z;
    c. Números arábicos: 0, 1, 2, ..., 0;
    d. Caracteres não alfabéticos: !, $, #, %, etc.
III. A senha tem validade de 60 (sessenta) dias. Ao expirar este prazo, os usuários deverão alterar a senha para evitar o bloqueio de sua conta, podendo fazer a alteração antes do prazo;
IV. A nova senha não poderá ser a mesma palavra passe das 2 (duas) últimas cadastradas/atualizadas;
V. A Será obrigatória a troca da senha ao efetuar o primeiro logon;
VI. A conta será bloqueada em caso de 3 (três) tentativas inválidas de acesso;
VII. Deve-se evitar, na criação da senha, o uso de palavras presentes em dicionários de qualquer idioma, nomes próprios ou de familiares, datas, telefones, placas de carro e endereços;
VIII. Para segurança, é recomendável que a senha seja alterada regularmente.

CAPÍTULO III
INATIVAÇÃO DE USUÁRIO

Art. 9º O usuário que ficar inativado por qualquer motivo deverá, mediante solicitação da chefia imediata, por meio da Central de Atendimento da STI, pedir a sua reativação, justificando o pedido.

Art. 10 Os logins que não forem utilizados por mais de 180 (cento e oitenta) dias serão automaticamente desabilitados e excluídos 90 (noventa) dias após terem sido desabilitados.

Art. 11 O Usuário Interno será inativado nas seguintes situações:

§1º Ficar mais de 90 (noventa) dias sem acessar algum sistema corporativo;
§1º Errar seu login 3 (três) vezes consecutivas.

Parágrafo Único. O Usuário Externo será inativado de acordo com a data de expiração do prazo de concessão;

CAPÍTULO IV
REVISÃO ANUAL DAS CONTAS DE ACESSO

Art. 12 A revisão dos acessos das contas de usuário ocorrerá no segundo semestre de cada ano. Nesta atividade, cada gestor da PMI deve fazer a revisão das contas dos usuários sob responsabilidade de seu setor. O processo é orientado pela STI e está descrito nas etapas seguintes, de forma resumida:

I. Os setores serão comunicados pela STI do início do processo de revisão dos acessos das contas à Rede Corporativa da PMI;
II. A STI irá encaminhar a relação de usuários de cada setor aos seus respectivos gestores, solicitando retorno em até 15 (quinze) dias com expediente;
III. Expirado o prazo para a revisão, os setores que não realizarem a revisão terão as contas dos usuários bloqueadas, ocorrendo o desbloqueio somente a partir do envio da relação devidamente atualizada.

Parágrafo Único. Os casos de mudança de lotação, afastamento temporário ou definitivo e retorno de usuários internos deverão ser comunicados imediatamente à STI pelo órgão competente pela administração destes, através da abertura de solicitação de serviço, na Central de Atendimento da STI.

Art. 13 Os usuários serão responsabilizados por todos os acessos e atividades desenvolvidas através do seu login, inclusive por eventuais danos decorrentes de sua má utilização e responderá por toda e qualquer violação normativa e/ou legal, de natureza administrativa, cível e/ou criminal que o envolva incluindo-se, ainda o ressarcimento pelos danos de natureza material, devidamente observado, o contraditório e a ampla defesa.

CAPÍTULO V
DISPOSIÇÕES GERAIS

Art. 14 Caracterizado o descumprimento de qualquer dos dispositivos desta Norma Complementar, caberá à STI informar o ocorrido:

I. à chefia imediata ou superior do usuário, para fins de eventual apuração de responsabilidades; e
II. aos demais setores competentes para apuração dos fatos verificados.

Art. 15 Os casos omissos serão resolvidos pela Secretaria Municipal de Administração.

Art. 16 Esta Instrução Normativa Complementar entra em vigor na data de sua publicação, revogando as disposições em contrário.

Itaguaí, Palácio Barão de Tefé, 05 de dezembro de 2022, aos 204 anos da Emancipação Político Administrativa do Município

REGIS DE SOUZA DE CARVALHO
Presidente CDTSIP

Membros:
Bruno Oliveira dos Santos
Paulo Luciano Xavier Vianna
Sheila Priscila da Silva Nogueira Honorato
Paulo Roberto Bezerra Júnior
Frederico Antonio Carneiro de Moraes
Wilson Ferreira Santiago
Maria Luciana Pereira de Souza
Sandro Valoura Alves
Thiago da Costa
Alexandre dos Santos Sanchez