INSTRUÇÃO NORMATIVA – CDTSIP – 001/2022

ESTABELECE NORMAS PARA REGULAR O USO DOS RECURSOS COMPUTACIONAIS 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 05 de agosto 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 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:

CAPÍTULO I

DOS RECURSOS COMPUTACIONAIS

Art. 1º. Consideram-se recursos computacionais da rede corporativa da Prefeitura Municipal de Itaguaí-RJ (PMI):

I- Hardwares (computadores servidores, estações, periféricos e equipamentos de rede);

II- Softwares (sistemas operacionais, aplicativos ou sistemas corporativos);

III- Canais de comunicação de dados, de uso exclusivo, que interligam a sede da PMI - Palácio Barão de Tefé aos Anexos, Escolas, hospitais, creches e demais Órgãos da Prefeitura Municipal de Itaguaí-RJ;

IV- Serviços corporativos de correio eletrônico e acesso à internet;

V- Bases de dados de sistemas corporativos.

§ 1º. A Subsecretaria de Tecnologia da Informação (STI) é a responsável pela gestão dos recursos computacionais da PMI;

§ 2º. A necessidade de uso de recursos computacionais da rede corporativa por outros órgãos públicos ou privados será individualmente analisada e autorizada pela STI;

§ 3º. O desenvolvimento ou implantação de qualquer sistema ou aplicativo que utilize recursos computacionais da rede corporativa deverá ser feito pela STI ou por terceiro, desde que supervisionado pela STI.

Art. 2º. Os recursos computacionais disponíveis no âmbito da rede corporativa, têm por finalidadeas atividades precípuas e sendo de propriedade da PMI, não devendo ser utilizados para outro fim.

CAPÍTULO II

DA IDENTIFICAÇÃO DO USUÁRIO E SENHA DE ACESSO

Art. 3º. Cabe à STI elaborar, e após aprovação da CDTSIP, implementar e divulgar políticas e boas práticas na utilização de senhas, visando prevenir o acesso não autorizado de usuários ao ssistemas de informação corporativos.

Parágrafo único. A STI, através de ato próprio, aprovado pela CDTSIP, divulgará os critérios para criação padronizada de logins.

Art. 4º. 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. 5º. O cadastro de usuários de rede da PMI é composto de usuários internos e usuários externos.

§ 1º. Usuários Internos são aqueles que acessam sistemas corporativos ou qualquer tipo de aplicação pela rede interna do PMI;

§ 2º. Usuários Externos são aqueles que acessam sistemas corporativos e aplicações do PMI pela

rede mundial de computadores fora da rede interna corporativa, ou localmente na rede da PMI por prazo determinado;

Art. 6º. A STI tem por objetivo consolidar todos os controles de acesso a rede e sistemas corporativos num diretório único de usuários (AD - Serviço Active Directory).

Art. 7º. 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. 8º. Após a inclusão do usuário interno na rede corporativa, o acesso a qualquer sistema corporativo específico, deverá ser pedido pelo seu superior hierárquico, mediante solicitação na Central de Atendimento da STI.

Art. 9º. O usuário interno será inativado nas seguintes situações:

Ficar mais de 90 (noventa) dias sem acessar algum sistema corporativo;

Errar seu login ou senha 3 (três) vezes consecutivas.

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

Art. 10. O Usuário Externo terá um login criado no AD (Active Directory), identificado na sua descrição do cadastro a área a qual é vinculado, com a respectiva validade contratual ou prazo da sua respectiva atividade.

Parágrafo único. O login do usuário externo será sempre limitado especificamente ao sistema ou aplicação a qual for concedido o acesso corporativo.

Art. 11. O login (nome de usuário) e respectiva senha serão atribuídos a um único usuário, de forma individual e intransferível, de uso exclusivo do seu titular, não devendo ser compartilhado com outros usuários.

Parágrafo único. 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.

Art. 12. É vedada a apropriação de login e senha de outros usuários.

Art. 13. 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.

§ 1º. 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.

§ 2º. Caberá ao superior hierárquico do usuário interno ou externo, pedir a sua inclusão, alteração ou exclusão de acesso a um sistema corporativo.

Art. 14. 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.

Parágrafo único. Para segurança, é recomendável que a senha seja alterada regularmente.

CAPÍTULO III
DO USO DAS ESTAÇÕES DE TRABALHO E SERVIDORES CORPORATIVOS

Art. 15. É vedada a instalação ou desinstalação de recursos computacionais de qualquer procedência, na rede corporativa do PMI, sem a prévia autorização da STI.

Parágrafo único. A utilização, por parte de qualquer usuário da rede, de software não autorizado ou não adquirido legalmente, caracteriza infringência à Lei Federal nº 9609/1998.

Art. 16. A inclusão de equipamentos de terceiros na rede corporativa do PMI estará sujeita à aprovação por parte da STI.

§ 1º. A STI deverá conferir as configurações do equipamento e avaliar se o mesmo oferece os requisitos necessários para atender às necessidades de processamento e segurança, durante seu uso na rede corporativa;

§ 2º. Equipamentos de terceiros deverão estar em conformidade com as normas e configurações impostas aos demais equipamentos conectados à rede corporativa da PMI;

§ 3º. Os equipamentos estarão sujeitos a reavaliações a serem realizadas pela STI, para garantir que estejam adequados às novas necessidades, decorrentes da atualização dos sistemas e aplicativos utilizados no âmbito da rede corporativa.

Art. 17. É vedado instalar, manter e acessar nas estações de trabalho e nos servidores corporativos, arquivos de conteúdo pornográfico, discriminatório, ofensivos aos direitos humanos, entretenimentos, jogos, e outros não relacionados às atividades precípuas da PMI.

Art. 18. A fim de evitar exposição ou furto de informação, computadores, terminais de computador e impressoras não devem permanecer ligados quando não assistidos e, no caso decomputadores e terminais, devem ser bloqueados quando não estiverem em uso.

Parágrafo Único. É recomendável que seja configurada a ativação automática da proteção de tela com senha após determinado tempo de inatividade.

Art. 19. É vedado o compartilhamento de diretórios, arquivos e demais recursos computacionais, sem prévia autorização da STI.

Parágrafo único. A detecção de compartilhamentos e diretórios não autorizados que ponham emrisco a segurança, implicará a desconexão imediata da estação até a apuração da responsabilidade e adoção de providências cabíveis.

Art. 20. Os usuários deverão zelar pela conservação, integridade, correta utilização e segurançados recursos computacionais sob sua responsabilidade.

Parágrafo único. Qualquer intervenção na estação de trabalho somente poderá ser efetuada por funcionário da STI obrigatoriamente assistido pelo usuário.

Art. 21. O usuário deverá exigir a identificação do técnico designado para atendimento de manutenção ou verificação dos recursos computacionais e a apresentação da ordem de serviço verificando a autenticidade, se necessário, junto à chefia responsável na STI.

Art. 22. A realização de backups (cópias de segurança) dos dados contidos nas estações de trabalho é de responsabilidade do usuário.

Art. 23. A realização de backups (cópias de segurança) dos dados contidos nos servidores, incluindo o servidor de arquivos, é de responsabilidade da STI.

Parágrafo único. O Servidor de arquivos será usado exclusivamente para armazenamento e manutenção de arquivos de trabalho pertencentes as respectivas áreas organizacionais, pelas suas características de inviolabilidade e segurança. Este serviço será disponibilizado somente aos usuários autorizados pela STI.

Art. 24. Para diagnóstico de problemas nos recursos computacionais, inclusive em caso de suspeita de violação de regras, a STI poderá acessar arquivos nos servidores e estações de trabalho.

Art. 25. O acesso remoto às estações de trabalho, com o objetivo de suporte e manutenção dos recursos computacionais, só poderá ser realizado por equipe autorizada da STI, sempre com prévia permissão do usuário, do chefe do órgão ou da Administração Superior.

Art. 26. É vedado ao usuário e ao chefe da área impedir que procedimentos técnicos realizados por pessoal autorizado pela STI, devidamente identificado e de posse de ordem de serviço, sejam executados nas estações de trabalho sob sua responsabilidade.

CAPÍTULO IV

DO USO DA INTRANET

Art. 27. Considera-se intranet da Prefeitura Municipal de Itaguaí-RJ os recursos computacionais disponíveis nos segmentos da rede corporativa, conceituados no art. 1º e seus incisos, excetuando-se o acesso à internet.

Art. 28. Cabe à STI identificar e ajustar a capacidade dos canais de comunicação, a fim de adequá-los à demanda, bem como estabelecer e revisar periodicamente os critérios de priorização.

Art. 29. O acesso à intranet é permitido a todos os usuários da rede corporativa do PMI, previamente autorizados e através de login.

CAPÍTULO V

DO USO DA INTERNET

Art. 30. O acesso dos usuários da rede corporativa à Internet deve ser feito exclusivamente por meio do *serviço de proxy* da PMI para comunicação com a rede mundial (internet).

Art. 31. Conexões com a internet, através de linha discada e/ou modem, somente poderão ser adotadas nas estações não interligadas à rede corporativa do PMI, enquanto permanecerem totalmente isoladas e com autorização da STI.

§ 1º. É vedada a conexão e/ou acesso à internet através de rede sem fio (wireless) disponibilizada por terceiros, dentro ou fora das dependências da PMI;

§ 2º. A detecção de comunicações independentes entre a internet com a sede da Prefeitura Municipal de Itaguaí e demais Órgãos da Prefeitura Municipal de Itaguaí, implicará a desconexão imediata da estação, até a apuração de responsabilidades e adoção das providências cabíveis;

Art. 32. O acesso à internet através da rede corporativa é permitido somente aos usuários previamente autorizados, através de login.

§ 1º. A concessão do acesso a internet se dará após a análise da disponibilidade de recursos pela STI e mediante abertura de solicitação de chamado pelo chefe imediato do usuário, através da Central de Atendimentos da STI.

§ 2º. A STI poderá complementarmente implementar uma política de concessão de acesso visando racionalizar o uso da internet.

Art. 33. É vedado o acesso a sites da internet de conteúdo não autorizado, tais como os de conteúdo pornográfico, entretenimento, jogos, sites ofensivos aos direitos humanos, comunicação em salas de bate-papo (chats), bem como recursos do tipo FTP, ICQ e programas de cópia de arquivos (download) ponto a ponto (Ex.: Kazaa, Limewire, bit torrent).

§ 1º. A vedação disposta no caput deste artigo é extensiva ao webmail de provedores externos a

rede corporativa da PMI;

§ 2º. Comprovada a imperiosa necessidade de serviço, o acesso poderá ser autorizado temporariamente pela STI, mediante solicitação por escrito assinada pelo chefe imediato do órgão no qual o usuário está lotado;

§ 3º. A STI poderá, sem prévio aviso, bloquear o acesso a sites que potencialmente ameacem a segurança da rede corporativa da PMI.

Art. 34. A execução de cópia de arquivo via internet (download) será passível de priorização durante o expediente, de modo a não concorrer com as atividades precípuas da PMI.

Art. 35. Os acessos à internet são passíveis de monitoração e identificação quanto a login, endereço da máquina do usuário e site acessado.

Art. 36. Não serão permitidos acessos simultâneos à internet com um mesmo login. Caso sejam detectados acessos simultâneos, por medida de segurança, o login e a senha serão desativados. A reativação do login poderá ser feita através de abertura de uma solicitação de serviço e a liberação de acesso à internet se dará mediante solicitação do chefe imediato do respectivo usuário.

Art. 37. É vedada a utilização de softwares de mensagens instantâneas e voz sobre IP (VoIP) não homologados e não autorizados pela STI.

CAPÍTULO VI

DO USO DO CORREIO ELETRÔNICO

Art. 38. É responsabilidade da STI definir, revisar e atualizar regras, elaborar e divulgar políticas e manuais de melhores práticas na utilização do correio eletrônico a fim de reduzir os riscos gerados na utilização deste meio de comunicação.

Art. 39. A caixa postal de correio eletrônico, que poderá ser individual ou institucional, será disponibilizada somente aos usuários ou órgãos previamente autorizados.

§ 1º. A STI, através de ato próprio, divulgará os critérios para concessão de caixa postal de correio

eletrônico individualizada ou institucional;

§ 2º. A concessão atenderá aos critérios aprovados e se dará após a análise da STI da disponibilidade de recursos e mediante abertura de solicitação de serviço pelo chefe imediato.

Art. 40. As caixas postais de correio eletrônico são de propriedade da PMI, passíveis de monitoração pela STI em caso de fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços, com a prévia autorização do chefe imediato, da CDTSIP e do Prefeito da PMI.

Art. 41. É vedado o envio, replicação ou encaminhamento de mensagens, por meio do correio eletrônico, de conteúdo não relacionado às atividades precípuas da PMI.

Parágrafo único. Só será permitido o uso do correio eletrônico para veiculação de campanhas internas, de caráter social, mensagens informativas ou outras que eventualmente possam ter conteúdo vedado, mediante autorização da Administração Superior.

Art. 42. Para os órgãos autorizados pela Prefeitura Municipal de Itaguaí a utilizar as listas de distribuição existentes, convêm que o encaminhamento de uma mesma mensagem do correio eletrônico para várias caixas postais, simultaneamente, seja feito através de cópia oculta ou pelas referidas listas.

Parágrafo único. O envio de uma mesma mensagem eletrônica, para todas as caixas postais da rede corporativa do PMI, deverá ser feito com apoio da STI e autorização da Administração Superior.

Art. 43. O tamanho da caixa postal de correio eletrônico é limitado para todos os usuários da rede corporativa do PMI e é responsabilidade do usuário cuidar para que sua caixa postal mantenha-se dentro dos limites estabelecidos.

Parágrafo Único. As caixas postais que excederem ao limite estabelecido pela STI receberão mensagens de alerta do administrador de correio e ficarão automaticamente impossibilitadas de enviar e receber mensagens.

Art. 44. O tamanho máximo dos arquivos anexados às caixas postais fica limitado pela STI. A liberação de arquivos recebidos que excedam ao limite estabelecido poderá ser autorizada pela STI, mediante abertura de solicitação de serviço, comprovada a imperiosa necessidade de serviço.

Art. 45. Os arquivos anexados em mensagens recebidas serão bloqueados caso sejam arquivos que

potencialmente possam conter softwares maliciosos. A lista de tipos de arquivos bloqueados poderá ser consultada na página da Intranet da PMI.

§ 1º. Em caso de necessidade de recebimento de mensagens através do correio eletrônico, com arquivo anexado descrito no caput deste artigo, o usuário deverá solicitar o desbloqueio através da abertura de solicitação de serviço.

§ 2º. A STI providenciará a verificação do arquivo e seu encaminhamento no caso de inexistência de vírus ou desinfecção com sucesso.

Art. 46. O recebimento de mensagens será filtrado para bloqueio de spam (mensagens geralmente com finalidades comerciais), hoaxes (mensagens contendo boatos maliciosos) e outros tipos de mensagens indesejáveis.

Art. 47. Por questão de segurança, recomenda-se ao usuário não abrir mensagens de remetente ou conteúdo suspeito. Em caso de dúvida, solicite suporte à STI através da abertura de solicitação de chamado.

Art. 48. A fim de reduzir o problema com spam, é vedado o cadastramento de e-mail corporativo em formulários de empresas e/ou sites de relacionamento, compras, anúncios ou qualquer outro que solicite o preenchimento de um endereço eletrônico.

CAPÍTULO VII

DO CONTROLE DOS SOFTWARES MALICIOSOS

Art. 49. São considerados softwares maliciosos: vírus, worms (vermes), trojan horses (cavalos de tróia), spywares (programas espiões), programas de invasão, e todos aqueles que possam prejudicar ou danificar os recursos computacionais e tornar vulneráveis informações corporativas da PMI.

Art. 50. É vedado remover ou desabilitar softwares de controle e remoção de softwares maliciosos, licenciados para a rede corporativa, bem como instalar qualquer outro não licenciado pela PMI.

Art. 51. Arquivos em mídias removíveis (pendrive, HD externo, CD, DVD) ou recebidos através da internet, devem, antes do uso, ser analisados a fim de detectar contaminação por softwares maliciosos.

Art. 52. A STI deve ser imediatamente comunicada, através da central de atendimentos, caso sejam identificados na rede corporativa do PMI, computadores sem antivírus ou com antivírus desatualizado.

CAPÍTULO VIII

DO USO DE DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

Art. 53. Cabe à STI, a elaboração de políticas e normativas para controlar o trabalho remoto e o uso de dispositivos móveis, visando reduzir os riscos de roubo de equipamentos e de informações e o acesso não autorizados aos sistemas internos da PMI, com a aprovação da CDTSIP.

Art. 54. Consideram-se dispositivos móveis equipamentos tais como: notebooks, netbooks,palmtops, smartphones e telefones celulares com interface com computador.

Art. 55. É vedada a conexão de quaisquer dispositivos móveis na rede corporativa sem a prévia verificação contra softwares maliciosos e sem a adequada atualização do software antivírus e do sistema operacional.

§ 1º. Caso seja identificado dispositivo móvel infectado por vírus ou malware, a STI prestará o suporte necessário a correta desinfecção e atualização do dispositivo;

§ 2º. A STI recomenda que os dispositivos móveis, de propriedade da PMI, cedidos a funcionários, sejam conectados a rede corporativa pelo menos uma vez por mês, a fim de que se mantenham atualizados e operacionais ao uso.

Art. 56. É vedada a conexão de dispositivos móveis particulares na rede corporativa da PMI sem prévia análise de viabilidade técnica e autorização da STI.

Art. 57. A verificação de softwares maliciosos, atualização do antivírus e sistema operacional deverá ser observada também fora da rede da PMI com o objetivo de evitar o acesso não autorizado e a divulgação de informações armazenadas nos dispositivos móveis.

Parágrafo único. Por se tratar de equipamentos facilmente transportáveis é importante que cuidados especiais sejam tomados com o objetivo de evitar o furto/roubo do equipamento e a exposição ou

furto de informação corporativa.

CAPÍTULO IX

DO USO DE SISTEMAS CORPORATIVOS E COMERCIAIS

Art. 58. Caberá a unidade ou usuário solicitante de um sistema corporativo, a responsabilidade pela inserção, alteração, exclusão, manutenção, fidedignidade, publicidade e se for o caso, confidencialidade dos dados.

§ 1º. Será de responsabilidade do chefe da área a qual o usuário é vinculado ou da Administração Superior solicitar a STI que conceda, altere ou retire acesso de qualquer usuário interno ou externo, se for o caso, no respectivo sistema;

§ 2º. Usuários externos de outros Órgãos ou Poderes Públicos que venham a ter acesso a sistemas corporativos deverão ter autorização também de seu superior hierárquico.

Art. 59. As alterações de banco de dados decorrentes de migrações, atualizações de versões, ou mau funcionamento de alguma rotina de sistema corporativo, que não seja solicitada pelo usuário, deverá ser corrigida diretamente pela STI, sob autorização do respectivo responsável da unidade.

Parágrafo Único. A STI deverá registrar e controlar as solicitações e respectivas autorizações.

Art. 60. A STI não se responsabilizará por qualquer tipo de manutenção ou suporte a bancos de dados criados a sua revelia, seja qual for a aplicação utilizada.

Art. 61. A STI poderá fornecer suporte apenas aos sistemas comerciais aprovados e utilizados de forma corporativa nos servidores ou estações de trabalho da Prefeitura Municipal de Itaguaí-RJ.

CAPÍTULO X

DO DESCUMPRIMENTO

Art. 62. Esta Resolução é de observância geral e o seu cumprimento, obrigatório. O descumprimento, sujeitará o infrator às penalidades disciplinares, administrativas e/ou criminais.

Art. 63. Além das vedações e infrações individualizadas nos artigos anteriores, é **expressamente**

vedado ao Usuário Interno e/ou Externo, acessar, transmitir, difundir ou disponibilizar a terceiros, informações, dados organizacionais, dados pessoais, sob qualquer suporte de materialização, físico ou digital, que de alguma forma:

§ 1º. Contrariem, menosprezem ou atentem contra os direitos fundamentais e as liberdades constitucionais;

§ 2º. Induzam, incitem ou promovam atos contrários à lei ou à ordem pública;

§ 3º. Induzam, incitem ou promovam atos discriminatórios em razão de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico;

§ 4º. Incorporem, ponham à disposição ou permitam acessar conteúdos, elementos, mensagens e/ou serviços ilegais, violentos, pornográficos, pedófilos, perseguidores ou, de qualquer forma, contrários à lei ou à ordem pública;

Art. 64. Em caso de descumprimento a qualquer das disposições contidas nesta Norma, observar-se-á, o disposto no Parágrafo Único do Artigo 11.

CAPÍTULO XI

DISPOSIÇÕES FINAIS

Art. 65. Os usuários deverão notificar seus superiores ou à STI quaisquer fragilidades ou ameaças, ocorridas ou suspeitas, na segurança dos sistemas, serviços ou informações, mesmo que estes não estejam diretamente sob sua responsabilidade. Para sua própria proteção, em nenhuma hipótese deve ser feita uma averiguação de fragilidade por conta própria, pois a atividade poderá ser interpretada como potencial uso impróprio do sistema.

Parágrafo único. Todas as políticas e normas referidas neste ato ficarão disponíveis na página da STI na intranet e serão passíveis de atualização, devendo ser consultados periodicamente ou sempre que houver dúvida quanto à sua aplicação.

Art. 66. Os casos de desrespeito às normas estabelecidas neste ato serão encaminhados a CDTSIP para a adoção das providências cabíveis, nos termos da legislação vigente.

Art. 67. As solicitações para auditoria de segurança, análise ou informação quanto ao uso indevido dos recursos computacionais, deverão ser solicitados formalmente a STI por expediente, processo

administrativo, solicitação de serviço ou e-mail e autorizados pelo chefe imediato ou pela Administração Superior quando for o caso.

Art. 68. A STI deverá emitir parecer técnico quando houver aquisição de serviços, sistemas e equipamentos relacionados à Tecnologia da Informação, bem como, de qualquer tipo de software, mesmo que o pedido de contratação seja originado por outro órgão do PMI.

Art. 69. Esta Instrução Normativa entra em vigor na data de sua publicação, revogando as disposições em contrário.

Itaguaí, Palácio Barão de Tefé, 05 de agosto 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
Robens Fonseca Pedrosa Júnior
Paulo Roberto Bezerra Júnior
Leonardo Rodrigues de Abreu
Maria Luciana Pereira de Souza
Sandro Valoura Alves
Thiago da Costa
Alexandre dos Santos Sanchez