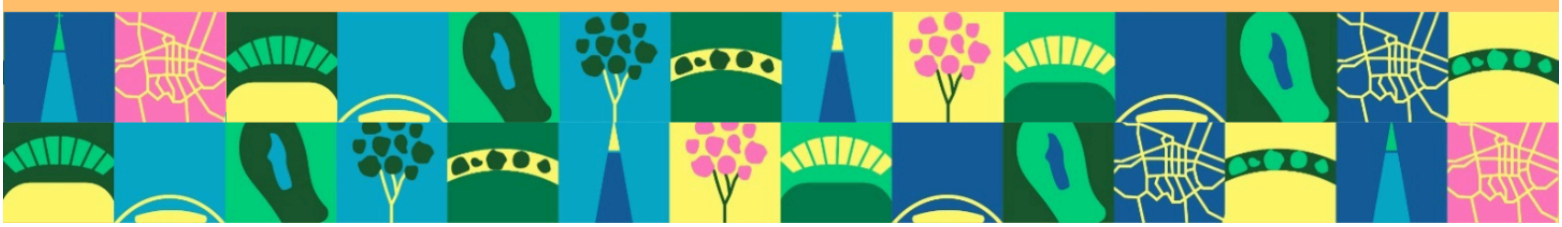
MARINGÁ
PREFEITURA
COMPLIANCE E CONTROLE

POLÍTICA DE CONTROLE DE ACESSO DA PREFEITURA MUNICIPAL DE MARINGÁ

2024



SUMÁRIO

SOBRE A POLÍTICA DE CONTROLE DE ACESSO 3

ESCOPO 4

DEFINIÇÕES 4

REFERÊNCIA LEGAL E DE BOAS PRÁTICAS 4

DECLARAÇÕES DA POLÍTICA DE CONTROLE DE ACESSO 5

ANEXO I 12

Termo de Compromisso com a Política de Controle de Acesso da Prefeitura Municipal de Maringá 12

POLÍTICA DE CONTROLE DE ACESSO DA PREFEITURA MUNICIPAL DE MARINGÁ

SOBRE A POLÍTICA DE CONTROLE DE ACESSO

A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações da Prefeitura Municipal de Maringá, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Sem controles de autorização, identificação e autenticação, existe o risco potencial de que os sistemas de informação possam ser acessados ilicitamente e que a segurança desses sistemas de informação seja comprometida.

Considera-se, portanto, que as credenciais: crachá de identificação funcional e *logins* de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Cabe ressaltar que os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação.

ESCOPO

Esta política se aplica a todas as informações pertencentes à Prefeitura Municipal de Maringá e está voltada para o agente de tratamento, o meio utilizado para este tratamento, o formato de armazenamento - seja este digital ou físico e as dependências físicas desta organização, bem como, a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional desses meios de tratamento mesmo que eventualmente.

Especificamente, inclui:

- Todos os funcionários, sejam servidores efetivos ou temporários.
- Todos os contratados e terceiros que trabalham para a Prefeitura Municipal de Maringá.
- Todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação da Prefeitura Municipal de Maringá.

DEFINIÇÕES

- **ACESSO**

  Ato de ingressar, transitar, conhecer ou consultar a informação, bem como, a possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

- **CONTROLE DE ACESSO**

  Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.

REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Orientação	Secção
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	Capítulo VII - Seção I – Art. 46, Seção II Art. 50
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	Capítulo I - Art.2, Incisos III e IV Capítulo II - Art.3, Inciso XI Capítulo VI - Seção IV – Art.15
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea f
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação	Itens 9 – 11.2.9 (Páginas 23 - 47)
CIS V8	Capítulo 6
Guia do Framework de Segurança – LGPD	Páginas 24 - 26
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

DECLARAÇÕES DA POLÍTICA DE CONTROLE DE ACESSO

- **ACESSO LÓGICO**

  O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso, sendo que este deve ser concedido e mantido pelo setor de Tecnologia da Informação - TI, baseado nas responsabilidades e tarefas de cada usuário.

Consequentemente, terão direito a acesso lógico aos recursos da rede local os usuários voltados para atividades que necessitam de recursos de tecnologia da informação.

Para fins desta aplicação, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade na Prefeitura Municipal de Maringá.

• CONTA DE ACESSO LÓGICO E SENHA

Para utilização das estações de trabalho da Prefeitura Municipal de Maringá, será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pelo setor de Tecnologia da Informação - TI, mediante solicitação formal pelo titular da unidade do requisitante com a devida aprovação do seu gestor imediato.

Os privilégios de acesso dos usuários à rede local devem ser definidos pela área requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas, conforme definição de perfis de acesso estruturado para cada setor e/ou atividades.

Na necessidade de utilização de perfil diferente do disponibilizado, o usuário deverá encaminhar solicitação para seu gestor imediato o qual deve realizar uma análise e, diante de aprovação esta deve encaminhar para o setor de Tecnologia da Informação - TI que examinará, podendo negá-la, com a devida justificativa, nos casos em que entender que não se aplica.

O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo setor de Tecnologia da Informação - TI quando constatada qualquer irregularidade

O padrão adotado para o formato da senha é o definido pelo setor de Tecnologia da Informação - TI, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

Formação da senha da identificação (*login*) de acesso à rede local

- Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números.
- Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &, #).
- Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações.

- Não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system*.
- Não reutilizar as últimas 05 (cinco) senhas.

O setor de Tecnologia da Informação - TI fornecerá uma senha temporária para cada conta de acesso criada, no momento da liberação para o usuário, sendo que esta deverá ser alterada pelo mesmo quando do primeiro acesso à rede local.

As senhas de acesso serão renovadas a cada 90 (noventa) dias, devendo o usuário ser informado automaticamente, a fim de que ele próprio efetue a mudança.

- **BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO**

A conta de acesso será bloqueada nos seguintes casos:

- Após 5 (cinco) tentativas consecutivas de acesso errado.
- Solicitação formalizada do gestor imediato do usuário com a devida justificativa.
- Quando da suspeita de mau uso dos serviços disponibilizados pelo setor de Tecnologia da Informação - TI ou descumprimento da Política de Segurança da Informação e normas correlatas em vigência.
- Diante das orientações formalizadas e encaminhadas para o setor de Tecnologia da Informação – TI pelo setor de Recursos Humanos, após exoneração do servidor público ou do término de contrato com cargo comissionados, ocupantes de emprego público em exercício e estagiários.
- Quando no término contratual de empresas prestadores de serviços com acessos liberados para terceiro, sendo solicitado formalmente ao setor de Tecnologia da Informação - TI pela área responsável da gestão do contrato.
- Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido formal do gestor imediato ao setor de Tecnologia da Informação - TI ou este será realizado pelo próprio setor de Tecnologia da Informação - TI baseado em informações formalizadas pelo setor de Recursos Humanos.

O desbloqueio da conta de acesso à rede local será realizado apenas após solicitação formal do gestor imediato do usuário, ou do setor de Recursos Humanos ou pelo responsável da gestão contratual ao setor de Tecnologia da Informação - TI.

A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

- **MOVIMENTAÇÃO INTERNA**

Quando houver mudança do usuário para outro setor, os direitos de acesso à rede local devem ser readequados, conforme solicitação formal do novo gestor imediato ao setor de Tecnologia da Informação - TI ou este será realizado pelo próprio setor de Tecnologia da Informação - TI baseado em informações formalizadas pelo setor de Recursos Humanos.

Neste caso, é primordial que os direitos de acesso anteriormente concedidos sejam imediatamente cancelados. Esta ação deve ser executada pelo setor de Tecnologia da Informação, seguindo como base uma solicitação formal do gestor imediato do antigo setor de trabalho do usuário ou conforme informações formalizadas pelo setor de Recursos Humanos.

O setor de Tecnologia da Informação deve-se basear nos padrões definidos internamente de perfis de acesso voltados para setores e atividades existentes da Prefeitura Municipal de Maringá.

- **PERFIL DE ACESSO COM PRIVILÉGIOS DE ADMINISTRADOR**

A utilização de identificação (*login*) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

Somente os técnicos do setor de Tecnologia da Informação - TI, devidamente identificados, habilitados e controlados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

Na necessidade de utilização de *login* com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o setor de Tecnologia da Informação - TI, que poderá negar os casos em que entender que não se aplica.

Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal do setor de Tecnologia da Informação - TI.

Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

A identificação (*login*) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (*login*) com privilégio de

administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

- **RESPONSABILIDADES**

É de responsabilidade do gestor imediato do usuário ou do setor de Recursos Humanos comunicar formalmente o setor de Tecnologia da Informação - TI o desligamento ou saída definitiva do usuário do departamento para que as permissões de acesso à rede local sejam canceladas.

Assim como, cabe à área responsável pela gestão de um contrato de prestação de serviços comunicar formalmente ao setor de Tecnologia da Informação - TI o término ou a saída definitiva de um terceirizado para o cancelamento de seu acesso à rede local.

Caberá ao setor de Recursos Humanos da Prefeitura Municipal de Maringá a comunicação imediata ao setor de Tecnologia da Informação - TI sobre férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

É responsabilidade da área responsável pela gestão de um contrato de prestação de serviços a comunicação imediata ao setor de Tecnologia da Informação - TI da Informação sobre férias e licenças de terceirizados para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

O setor de Tecnologia da Informação – TI é responsável pelo monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como, bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica.

O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à rede local e a recursos de tecnologia custodiados ou de propriedade da Prefeitura Municipal de Maringá.

Para preservar a segurança da rede local, os serviços serão filtrados por programas de antivírus, *anti-phishing* e *anti-spam* e, caso for detectado a violação de alguma regra de configuração, esses serviços serão bloqueados ou excluídos automaticamente.

Preservando a proteção de dados e aplicabilidade do controle de acesso aos arquivos e dados constantes nos equipamentos dos servidores, cabe ressaltar que nenhum técnico poderá ter acesso ao conteúdo das informações armazenadas no recurso do usuário.

Obrigações pertinentes aos usuários do uso dos recursos tecnológicos da Prefeitura Municipal de Maringá:

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação para coibir acessos indevidos.

II. A utilização simultânea da conta de acesso à rede local em mais de uma estação de trabalho ou *notebook* deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à rede local.

IV. O usuário deve informar ao setor de Tecnologia da Informação - TI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

V. É dever do usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

- Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros e outras formas.
- Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros para não gerar indisponibilidade de informações internas e externas.
- Interromper a conexão e adotar medidas que bloqueiem o acesso de terceiros nos equipamentos de informática e aos sistemas sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo.
- Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso.
- Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas.
- Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas.
- Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis.
- Assinar o Termo de Responsabilidade, **Anexo I**, referente a Política de Segurança da Informação da Prefeitura Municipal de Maringá quanto a utilização da respectiva conta de acesso.

HISTÓRICO DE REVISÕES

Versão	Data	Responsável	Controle de modificações
1.0	23/08/2023	FIA	Criação do Documento

ANEXO I

Termo de Compromisso com a Política de Controle de Acesso da Prefeitura Municipal de Maringá

Eu, ..., servidor público da Prefeitura Municipal de Maringá, e portador(a) da Identidade funcional nº ....., declaro que assumo a responsabilidade por:

1. Tratar o(s) ativo(s) de informação como patrimônio da Prefeitura Municipal de Maringá.
2. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da Prefeitura Municipal de Maringá.
3. Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da Prefeitura Municipal de Maringá.
4. Responder, perante a Prefeitura Municipal de Maringá, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.
5. Acessar a rede corporativa, computadores, internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa do gestor imediato, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Política de Controle de Acesso que rege o acesso à rede corporativa, computadores, internet e/ou utilização de e-mail.
6. Utilizar o correio eletrônico (e-mail) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa do gestor imediato, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Política de Controle de Acesso que rege o acesso à rede corporativa, computadores, internet e/ou utilização de e-mail.
7. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior.
8. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que esses venham a ser expostos para pessoas não autorizadas.
9. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (*browser*), bloquear estação de trabalho, bem como, encerrar a seção de correio eletrônico (e-mail), garantindo assim a impossibilidade de acesso indevido por terceiros
10. Não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento.

11. Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam colocar em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação de advertências e penalidades a serem definidas pela Prefeitura Municipal de Maringá.

....., ... de ..... de 20..... .

_____

[NOME FUNCIONÁRIO]