**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

***Cria a Política Geral de Segurança da Informação no município de Guará.***

**VINICIUS MAGNO FILGUEIRA,** Prefeito do Município de Guará, Estado de São Paulo, no uso de suas atribuições legais que lhe são conferidas por Lei Orgânica,

**D E C R E T A:**

**Art. 1º** Fica criada a Política Geral de Segurança da Informação no município de Guará, nos seguintes termos:

## Política Geral de Segurança da Informação

**Sumário**



### 1. Introdução

A **PREFEITURA DE GUARÁ** tem a missão em colaborar na construção das políticas públicas saudáveis de forma participativa e articulada por meio dos diferentes representantes.

A **PREFEITURA DE GUARÁ** entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados à população em geral.

A **PREFEITURA DE GUARÁ** compreende que a manipulação de informação da população em geral, servidores e prestadores de serviços, passa por diferentes etapas de utilização, e podem ficar vulneráveis a fatores externos e internos que podem comprometer a confidencialidade, integridade e disponibilidade da informação.

Dessa forma, a **PREFEITURA DE GUARÁ** estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão administrativo, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

## 2. Objetivo

Esta política tem por objetivos:

- Estabelecer diretrizes de Segurança da Informação que permitam aos servidores e prestadores de serviços da **PREFEITURA DE GUARÁ** adotarem padrões de comportamento seguro, adequados às metas e necessidades da **PREFEITURA DE GUARÁ**;
- Orientar quanto à adoção de controles de segurança e padronização de processos para atendimento dos requisitos para Segurança da Informação;
- Proteger as informações tratadas pela **PREFEITURA DE GUARÁ,** sendo da população em geral, servidores e prestadores de serviços, por meio de controles de segurança, para garantir a confidencialidade, integridade e disponibilidade da informação;
- Prevenir e comunicar possíveis causas de incidentes de responsabilidade legal da instituição e seus de seus servidores, população em geral e prestadores de serviços;
- Ajudar a minimizar os riscos de perdas financeiras, desempenho de suas atribuições públicas e administrativas, da confiança da população em geral ou de qualquer outro impacto negativo na administração pública da **PREFEITURA DE GUARÁ** como resultado de falhas de segurança.

## 3. Escopo

Esta Política de Segurança da Informação e outras políticas, normas e procedimentos complementares da **PREFEITURA DE GUARÁ** abrange todos os sistemas, dados, informações e recursos relacionados à organização, independentemente do formato ou meio em que são armazenados, processados, transmitidos ou acessados.

## 4. Público Alvo

Esta política se aplica a todos os servidores, usuários sem vínculo empregatícios, conveniados com a Prefeitura e prestadores de serviços que sejam usuários da informação tratados pela **PREFEITURA DE GUARÁ,** incluindo mas não se limitando a qualquer indivíduo ou organização que possui ou possuiu vínculo com a **PREFEITURA DE GUARÁ,** tais como servidores, ex-servidores, prestadores de serviço, ex-prestadores de serviço, que possuíram, possuem ou e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura **PREFEITURA DE GUARÁ**.

## 5. Termos e Definições

- **Ameaça:** Causa potencial de um incidente, que pode vir a prejudicar a organização;
- **Ativo:** Tudo aquilo que possui valor para a organização;
- **Ativo de informação:** Patrimônio intangível da organização, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, administrativo, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a organização por parceiros, população em geral, servidores e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da organização ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.
- **Confidencialidade:** Controles dos ativos da informação da organização de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

- **Controle:** Medida de segurança adotada pela organização para o tratamento de um risco específico.
- **Disponibilidade:** Controles dos ativos da informação da organização, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.
- **Gestor da Informação:** Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.
- **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da organização.
- **Integridade:** Controles dos ativos da informação da organização, de serem exatos e completos.
- **Risco de segurança da informação:** Efeito da incerteza sobre os objetivos de segurança da informação da organização.
- **Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da organização.
- **Usuário da informação:** Servidores de qualquer área da organização ou terceiros alocados na prestação de serviços a organização, indiferente do regime jurídico a que estejam submetidos, assim como indivíduos ou organizações devidamente autorizados a utilizar manipular qualquer ativo de informação da organização para o desempenho de suas atividades profissionais.
- **Vulnerabilidade:** Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da organização.

## 6. Diretrizes

O objetivo da gestão de Segurança da Informação da **PREFEITURA DE GUARÁ** é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos na instituição.

O chefe do Poder executivo, Secretários e a Comissão de trabalho de LGPD estão comprometidos com uma gestão efetiva de Segurança da Informação. Desta forma, adotarão todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas desta políticas e outras complementares poderão ser realizadas para garantir sua devida adequação às necessidades da **PREFEITURA DE GUARÁ**.

### 6.1. É Política da PREFEITURA DE GUARÁ

- Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da **PREFEITURA DE GUARÁ** sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
- Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: servidores, terceiros contratados e, onde pertinente, à população em geral;
- Garantir a educação e conscientização sobre as práticas adotadas pela **PREFEITURA DE GUARÁ** de segurança da informação para servidores e prestadores de serviços e, quando pertinente, a população em geral e parceiros;

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

- Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
- Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;
- Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
- Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

6.2 **Política de Dispositivos Móveis**

A menos que especificamente autorizado, somente dispositivos móveis autenticados pela **PREFEITURA DE GUARÁ** devem ser usados para manter ou processar informações internas em nome da organização.

Caso necessite utilizar equipamentos móveis, será entregue um dispositivo adequado para cumprir as políticas da organização. O auxílio será fornecido pela Assessoria de Tecnologia, que pode, às vezes, precisar de acesso ao seu dispositivo para resolução de problemas e manutenção.

Os usuários deverão observar:

1. Deve-se garantir que o dispositivo seja transportado de maneira segura e não seja exposto a situações nas quais possa ser danificado.

2. O usuário não deve deixar o dispositivo à vista do público, como na parte de trás de um carro ou em uma sala de reunião, por exemplo.

3. O usuário não deve remover nenhuma marca de identificação no dispositivo, como uma etiqueta de patrimônio da **PREFEITURA DE GUARÁ** ou um número de série.

4. Deve verificar se o dispositivo está bloqueado, quais informações estão sendo armazenadas e se a chave de acesso pode ser facilmente identificada.

5. Não poderá adicionar hardware periférico ao dispositivo sem a aprovação da Assessoria de Tecnologia.

6. Deverá certificar-se de que a tela do dispositivo "trave" após um curto período de inatividade e que exija um código de acesso ou senha para desbloqueá-lo.

7. As senhas usadas devem ser fortes e criadas de acordo com a Política interna da organização. Login não seguro, ou seja, aqueles que não exigem uma senha não devem ser configurados no dispositivo sob nenhuma hipótese.

8. O dispositivo fornecido pela organização é apenas para uso para atividades da administração pública, ou seja, para ser utilizado apenas durante a jornada de

trabalho. Para os casos de urgência que o servidor público necessite utilizar o dispositivo fora do horário estabelecido de sua jornada de trabalho deverá ter aprovação do seu superior imediato.

9. O dispositivo não deve ser compartilhado com familiares ou amigos ou usado para atividades pessoais.

10. O usuário pode receber uma solicitação para devolver o dispositivo à assessoria de TI a qualquer momento para inspeção e auditoria.

11. O usuário não deve instalar nenhum software não autorizado ou alterar a configuração do dispositivo sem antes consultar a assessoria de TI.

12. As alterações nos arquivos contidos no dispositivo podem não sofrer backup regularmente se não estiverem conectados à rede da Prefeitura por um período de tempo. O usuário deverá agendar dentro de um mês um tempo para fazer isso, de forma regular.

13. Uma proteção contra vírus será instalada no dispositivo pela organização. O usuário deverá verificar se o dispositivo está conectado à rede interna da Prefeitura regularmente para permitir a atualização das assinaturas de vírus. Não podendo desabilitar a proteção contra vírus no dispositivo.

14. O dispositivo não deve estar conectado a redes que não pertencem à Prefeitura, como as sem fio, a menos que uma VPN (Rede privada virtual) seja usada. Quando estiver em locais públicos, deverá certificar-se de que é uma rede privada, de modo que pessoas não autorizadas não possam ver (ou tirar fotos ou filmar) a tela.

**6.3 Uso aceitável de mensagens eletrônicas**

Todo o uso de recursos de mensagens deve ser consistente com as políticas e procedimentos de segurança da **PREFEITURA DE GUARÁ**.

- As contas de recursos de mensagens devem ser usadas exclusivamente para fins relacionados aos processos de trabalho da **PREFEITURA DE GUARÁ**.
- A utilização para assuntos pessoais não é permitida. Todos os dados das empresas, pessoas físicas ou quaisquer dados pessoais contidos nas mensagens de e-mail ou anexos devem ser protegidos.
- As contas dos recursos de mensagens eletrônicas não devem ser usados para a criação ou distribuição de mensagens perturbadoras ou ofensivas, incluindo comentários ofensivos sobre raça, gênero, deficiências, orientação sexual, pornografia, crenças e práticas religiosas, crenças políticas ou outros assuntos preconceituosos. Os servidores públicos que receberem quaisquer mensagens com este conteúdo de qualquer servidor da **PREFEITURA DE GUARÁ** devem relatar o assunto ao gestor do seu setor.

- Os usuários estão proibidos de usar recursos de mensagens eletrônicas fornecidos por terceiros e outros servidores de armazenamento, como Yahoo, MSN e Hotmail, etc.,

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

para realizar suas atividades de trabalho na **PREFEITURA DE GUARÁ**. Tais comunicações e transações devem ser conduzidas por meio de canais apropriados usando ferramentas aprovadas pela organização.

- Os servidores públicos da **PREFEITURA DE GUARÁ** não devem ter expectativa de privacidade no armazenamento, envio ou recebimento de informações nos e-mails de propriedade da **PREFEITURA DE GUARÁ,** podendo esta monitorar mensagens sem aviso prévio.

- Todas as mensagens enviadas de uma conta da instituição permanecem como propriedade da instituição e são consideradas parte do registro administrativo. Todas as mensagens da instituição devem ser consideradas como comunicações oficiais da instituição e tratadas de acordo.

- A **PREFEITURA DE GUARÁ** mantém seu direito legal de monitorar e analisar tecnicamente o uso de mensagens eletrônicas pelos usuários para avaliar a conformidade com essa política. Isso será feito de acordo com as políticas internas da organização e da legislação pertinente.

- A exclusão de uma mensagem de uma conta individual não significa necessariamente que ela foi permanentemente removida dos sistemas de TI da instituição e que essas mensagens ainda não estejam sujeitas a inspeção e revisão.

- Os usuário deverão tomar os seguintes cuidados ao enviar mensagens eletrônicas:

    - Não realizar o envio de mensagens para a distribuição de material comercial ou publicitário não solicitado pelo destinatário da mensagem ou lixo eletrônico de qualquer tipo, para outras organizações ou pessoas;

    - Não realizar o envio de material que infrinja os direitos autorais ou direitos de propriedade intelectual de outra pessoa ou organização;

    - Não realizar atividades que corrompam e/ou destruam os dados de outros usuários ou, de outra forma, interrompam o trabalho de outros usuários;

    - Não realizar a distribuição de imagens, dados ou outros materiais ofensivos, obscenos ou indecentes;

    - Não realizar o envio de qualquer conteúdo que possa causar aborrecimento ou inconveniência desnecessária;

    - Não realizar a transmissão de mensagens abusivas ou ameaçadoras para outros;

    - Não realizar a transmissão de material que discrimine ou incentive a discriminação com base em raça, genêro, orientação sexual, estado civil, deficiência, crenças políticas ou religiosas;

    - Não realizar a transmissão de material difamatório ou falsas alegações de

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

natureza enganosa;

- Não realizar atividades que violem a privacidade de outros usuários;
- Não realizar o envio de mensagens anônimas - ou seja, sem uma identificação clara do remetente;
- Não realizar o envio de mensagens para quaisquer outras atividades que tragam ou possam trazer descrédito à **PREFEITURA DE GUARÁ**;
- Ao endereçar mensagens por meios eletrônicos, o usuário deve se certificar de que os destinatários estão corretamente inclusos, para impedir a transmissão acidental a destinatários não autorizados;
- O usuário deve tomar cuidado com o recurso de preenchimento automático de texto em que o sistema sugere palavras ou frases com base nos caracteres digitados.
- Os usuários devem evitar o envio de mensagens desnecessárias para listas de distribuição, particularmente aquelas com ampla circulação, como a "lista global" de todos os servidores públicos. Quando necessário, essas mensagens devem ser enviadas pelo setor responsável de emitir as comunicações da instituição.
- Caso o Colaborador receba mensagens indesejadas, não solicitadas ou spam, é recomendável excluí-las sem lê-las. Essas mensagens não devem ser respondidas, pois isso pode confirmar a existência de um endereço válido para o remetente, resultando em mais comunicações indesejadas.

1. **Uso de e-mail**

Todos os e-mails enviados dos endereços da instituição para destinatários externos terão automaticamente o seguinte aviso:

*"Esta mensagem é uma correspondência reservada. Se você a recebeu por engano, por favor desconsidere-a. O sistema de mensagens da Internet não é considerado seguro ou livre de erros. A **PREFEITURA DE GUARÁ** não se responsabiliza por opiniões ou declarações veiculadas através de e-mails. Esta mensagem pode conter informação confidencial e/ou privilegiada. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não pode usar, copiar ou divulgar as informações nela contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu esta mensagem por engano, por favor avise imediatamente ao remetente, respondendo o e-mail e em seguida apague-o. Agradecemos sua cooperação."*

Se o usuário acredita que recebeu um e-mail que pode conter vírus, deverá informar à assessoria de Informática. Não deverá abrir anexos que acredite que possam conter vírus.

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

Se dados pessoais confiados à **PREFEITURA DE GUARÁ** forem deliberadamente ou acidentalmente enviados para outra organização ou pessoa, a **PREFEITURA DE GUARÁ** poderá ser responsabilizada nos termos da legislação aplicada de acordo com os danos causados aos destinatários mediante possível violação de dados.

1.1. Monitoramento de utilização de mensagens eletrônicas

O uso de mensagens eletrônicas dentro do sistema da instituição é monitorado e registrado para:

- Planejar e gerenciar sua capacidade de recursos de forma eficaz;
- Avaliar a conformidade com políticas e procedimentos;
- Garantir que os padrões sejam mantidos;
- Prevenir e detectar crimes;
- Investigar o uso não autorizado.

O monitoramento será realizado pela assessoria de TI. Procedimentos de monitoramento consistentes serão aplicados a todos os usuários e podem incluir a verificação do conteúdo das mensagens.

No caso de haver suspeita que os meios de comunicação disponibilizados pela **PREFEITURA DE GUARÁ** estão sendo utilizados para fins diversos do estabelecido por essa política, deve-se entrar em contato com a Assessoria de TI. Todos esses relatórios serão investigados de acordo com procedimentos documentados e, quando for o caso, evidências serão geradas. Essas informações podem ser fornecidas aos órgãos reguladores ou fiscalizadores de acordo com determinações legais ou requisitos específicos dos meios de comunicação utilizados.

Os usuários não devem acessar a conta de mensagens eletrônicas de outro usuário, a menos que tenham obtido permissão do proprietário da conta e de seu superior imediato. Em tais casos, isso deve ser monitorado e o acesso deve ser realizado apenas para mensagens que possam ser consideradas relevantes.

6.4 **Acesso à Internet**

Durante o acesso à Internet não será permitido o download, o upload, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo relacionado com as categorias abaixo nos dispositivos disponibilizados pela **PREFEITURA DE GUARÁ**:

- Qualquer espécie de exploração sexual;
- Qualquer forma de conteúdo adulto, erotismo, pornografia;
- Qualquer tipo de Pornografia infantil;
- Qualquer forma de ameaça, chantagem e assédio moral ou sexual;
- Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;
- Preconceito baseado em cor, sexo, opção sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

- Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam estas lícitas ou não;
- A prática e/ou a incitação de crimes ou contravenções penais;
- A prática de propaganda política nacional ou internacional;
- O desrespeito a imagem da **PREFEITURA DE GUARÁ;**
- A disseminação de códigos maliciosos e ameaças virtuais;
- Tentativa de expor a infraestrutura computacional da **PREFEITURA DE GUARÁ** a ameaças virtuais;
- Divulgação não autorizada de qualquer informação da **PREFEITURA DE GUARÁ** classificada como confidencial ou de uso interno;
- Tentativas de acesso à Dark/Deep Web através de navegador com tecnologia para acesso à rede Tor.

1.1. Comportamento em mídias e redes sociais

- A publicação de conteúdo referente à **PREFEITURA DE GUARÁ** em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização;

Quando no uso de suas mídias e redes sociais particulares, servidores públicos, Prestadores de Serviço e Terceiros contratados devem observar as seguintes restrições:

- Não é permitido o uso da logomarca, bem como de qualquer parte da identidade visual da **PREFEITURA DE GUARÁ** sem autorização prévia e expressa;
- Não é permitida a criação, participação ou interação com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos da **PREFEITURA DE GUARÁ**, excetuando-se os canais oficiais da organização;
- Não é permitida a publicação de conteúdos ou comentários diretamente relacionados à **PREFEITURA DE GUARÁ**, seus servidores públicos, Terceiros contratados e Prestadores de serviço que desonrem ou atentem contra a imagem da **PREFEITURA DE GUARÁ** ou de seus parceiros diretos ou indiretos.
- Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente das atividades da **PREFEITURA DE GUARÁ** sem a expressa autorização da organização, excetuando-se material divulgado em canais oficiais;
- Fica permitido aos servidores públicos promoverem empresas parceiras ou a **PREFEITURA DE GUARÁ** em redes corporativas profissionais com o viés de promoção positiva das marcas.

1.2. Monitoramento de uso da Internet por Servidores Públicos

### 1.2.1. Monitoramento do site

A assessoria de TI deverá monitorar o uso da Internet de todos os computadores e dispositivos conectados à rede interna da organização. Para todo o tráfego, o sistema de monitoramento deve registrar o endereço IP de origem, a data, a hora, o protocolo e o site ou servidor de

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

destino. Sempre que possível, o sistema deve registrar o ID de usuário da pessoa ou conta que iniciou o tráfego. Os registros de uso da Internet devem ser preservados por 1 ano.

6.5 Política de Senha, Gestão de Identidade e Controle de Acesso

**6.1. Diretriz de Construção e Proteção de Senha**

### 6.1.1. Criação de senha

• As senhas associadas às contas de acesso à ativos/serviços de informação ou recursos computacionais da **PREFEITURA DE GUARÁ** são de uso pessoal e intransferível, sendo dever do Usuário zelar por sua guarda e sigilo.

• Todas as senhas de nível de Usuário e de sistema devem estar em conformidade com um padrão forte de construção de senha.

• A equipe de tecnologia da informação será responsável por fornecer senhas de acesso inicial ao Usuário, que deverá proceder com a troca imediata da mesma;

• É considerado como padrão forte de construção de senha:

• Aplicações de uso interno, mínimo 8 Caracteres, incluindo letras maiusculas e minúsculas, números e caracteres especiais:

• Infraestruturas, mínimo 18 caracteres, incluindo letras maiusculas e minúsculas, números e caracteres especiais:

Considera-se como aplicações de uso interno as plataformas e ferramentas utilizadas pelos servidores públicos no dia-a-dia, tais como, email, bloqueios de tela, gestão de processos, gestão de recursos, web sites entre outros.

Considera-se aplicações críticas como banco de dados, servidores, dispositivos de rede e usuários com permissão de Administrador.

• Os Usuários devem usar uma senha separada e exclusiva para cada uma de suas contas relacionadas ao trabalho. Os Usuários não podem usar nenhuma senha relacionada ao trabalho para suas próprias contas pessoais.

• As contas de Usuário que têm privilégios de nível de sistema concedidos por meio de associações de grupo ou programas devem ter uma senha exclusiva de todas as outras contas mantidas por esse Usuário para acessar privilégios de nível de sistema.

• Após 03 (três) tentativas de acesso com senhas inválidas, a conta do Usuário será bloqueada, assim permanecendo, por no mínimo, 20 (vinte ) minutos;

Quando criada uma nova senha, Usuários devem estar atentos às seguintes recomendações:

• Não utilizar nenhuma parte de sua credencial na composição da senha;

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

- Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;

- Não utilizar repetição ou sequência de caracteres, números ou letras;

- Qualquer parte ou variação do nome da **PREFEITURA DE GUARÁ**;

- Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

**TABELA RESUMO DA PARAMETRIZAÇÃO DE SENHA SEGURA**

| Parâmetro | Valor |
|---|---|
| Comprimento mínimo | 8 |
| Comprimento máximo | 16 |
| Caracteres necessários | Pelo menos uma letra maiúscula<br>Pelo menos um símbolo<br>Pelo menos um número |
| Semelhança de senha | A nova senha não pode compartilhar mais de três caracteres na mesma posição que a senha antiga |
| Mudar a frequência | Pelo menos a cada 180 dias |
| Bloqueio de conta | Em 3 tentativas incorretas de logon |
| Ação de bloqueio de conta | A conta deve ser reativada pelo TI |
| Outros controles | A senha não pode conter o nome do usuário |

Quaisquer exceções a estas regras devem ser autorizadas pela área de Tecnologia da Informação.

### 6.1.2. Proteção de senha

- As senhas não devem ser compartilhadas com ninguém, incluindo Supervisores e colegas de trabalho;

- Todas as senhas devem ser tratadas como informações confidenciais da **PREFEITURA DE GUARÁ**;

- As senhas não devem ser inseridas em mensagens de e-mail ou outras formas de comunicação eletrônica, nem reveladas por telefone a ninguém;

- Não deve-se anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas definidas no item abaixo ;

- Não é permitido o recurso "Lembrar senha" de aplicativos (por exemplo, navegadores da web) que não sejam de uso dos serviços públicos;

- Qualquer usuário que suspeite que sua senha possa ter sido comprometida deve relatar o incidente a Assessoria de Tecnologia da Informação e alterar todas as senhas;

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

### 6.1.3. Mudança de senha

As senhas devem ser alteradas quando for comprometida. Troca periódica de senha a cada 180 dias.

6.2. Acesso a Ativos e Sistemas de Informação

A **PREFEITURA DE GUARÁ** fornece a seus Usuários Autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa.

As referidas contas de acesso são fornecidas exclusivamente para que os Usuários possam executar suas atividades laborais;

Toda conta de acesso é de uso individual de cada colaborador e intransferível. Desta forma, o Usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo ou empresa de posse de sua conta de acesso, desde que tenha ocorrido comprovadamente mediante ação ou omissão por parte do Usuário. A situação será devidamente apurada e documentada pela Assessoria de Tecnologia da Informação acompanhada pela Divisão de Gestão de Pessoas.

Os Usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

• Não utilizar sua conta em sistemas que não tem acesso, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pela **PREFEITURA DE GUARÁ**;

• Não compartilhar a conta de acesso e senha com outro Usuário, Colaborador e/ou terceiro;

• Informar imediatamente a equipe de segurança/TI caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais da **PREFEITURA DE GUARÁ**;

• Usuários que têm acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia;

• O Usuário não pode acessar suas contas através de equipamentos ( Desktops, Notebook) que não sejam de propriedade da **PREFEITURA DE GUARÁ**, a menos que expressamente autorizado e que essa autorização deverá ocorrer por escrito, sempre que possível, ou logo após formalizada, ainda que por chat.

6.3. Autorização de Acesso (privilégios de acesso)

A autorização e o nível permitido de acesso ativos/serviços de informação da **PREFEITURA DE GUARÁ** é feita com base em perfis que definem o nível de privilégio dos Usuários.

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

O acesso à ativos/serviços de informação é fornecido a critério da **PREFEITURA DE GUARÁ**, que define permissões baseadas nas necessidades de execução das atividades de negócio dos Usuários;

Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos Gestores de cada Colaborador. Solicitações deverão ser encaminhadas a equipe de tecnologia da informação.

Os Usuários devem ainda observar as seguintes diretrizes:

• A seu critério exclusivo, a **PREFEITURA DE GUARÁ** poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem). Caso o Usuário necessite de mais espaço, deverá realizar uma solicitação à assessoria de TI;

• É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse da **PREFEITURA DE GUARÁ** tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);

• Usuários não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) da **PREFEITURA DE GUARÁ**.

6.5 **Uso de equipamentos pessoais**

É estritamente proibido o uso de equipamentos próprios, incluindo, mas não se limitando a, computadores, notebooks, smartphones, tablets, dispositivos de armazenamento externo (pen drives, HDs externos) e quaisquer outros dispositivos de tecnologia pessoal, durante a execução de atividades profissionais dentro da prefeitura municipal.

O uso de equipamentos pessoais não monitorados pode comprometer a segurança da informação da **PREFEITURA DE GUARÁ**, expondo sistemas e dados a riscos de vazamento, malware, acesso não autorizado e outros incidentes de segurança.

7. Papéis e Responsabilidades

**7.1. Comissão de trabalho de LGPD**

Fica constituída a Comissão de trabalho da LGPD, contando com a participação de um representante de um membro das seguintes áreas de TI, Administração, Jurídico, Secretaria de Governo, Educação, Assistência social, Divisão Tributária e Saúde.

É responsabilidade da Comissão:

- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;
- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;
- Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI;

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

- Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da **PREFEITURA DE GUARÁ.**
- Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e normas e procedimentos de segurança;
- Elaborar e propor as políticas, normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PGSI;
- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- Tomar as ações cabíveis para se fazer cumprir os termos desta política;
- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

### 7.2. Gestores da Informação:

É responsabilidade dos Gestores da Informação:

- Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a coleta, utilização, armazenamento, compartilhamento e descarte conforme as normas estabelecidas pela **PREFEITURA DE GUARÁ**;
- Identificar, classificar e rotular as informações sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela **PREFEITURA DE GUARÁ** ;
- Periodicamente revisar as informações sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;
- Autorizar e revisar os acessos de servidores ou prestadores de serviço à informação e sistemas de informação sob sua responsabilidade de acordo com função e cargo;
- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela **PREFEITURA DE GUARÁ** .

7.3. Usuários da Informação

É responsabilidade dos Usuários da Informação:

- Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Comissão de trabalho da LGPD;
- Comunicar à Comissão de trabalho da LGPD qualquer evento que viole esta Política ou que possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da **PREFEITURA DE GUARÁ**;

7.4 Outras políticas, normas e procedimentos

Para garantir uma abordagem abrangente e eficiente, esta política deve ser lida e aplicada em conjunto com outras políticas específicas, normas e procedimentos internos relacionados à Segurança da Informação, Proteção de Dados e Privacidade tais como, mas não se limitando a:

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

- Política de Proteção de Dados Pessoais;
- Aviso de Privacidade do site;
- Política do CFTV;
- Plano de atendimento ao Titular dos Dados
- Plano para resposta a incidente de segurança;
- Política de Computação em Nuvem;
- Política de Descarte de Equipamentos Tecnológicos;
- Política de e-service;
- Política de instalação de Software;
- Política de monitoramento de internet;
- Política de registro de log e monitoramento;
- Política de segurança e Backup de dados;
- Decreto nº 3.822/2024;

Outras Políticas, normas e procedimentos de Segurança da Informação, Proteção de Dados e Privacidade podem ser criadas conforme a necessidade de adequação, sendo de responsabilidade da Prefeitura manter atualizada a lista mestra dos documentos relacionados ao tema.

Todas as políticas desenvolvidas e implementadas pela **PREFEITURA DE GUARÁ**, devem atender aos requisitos exigidos pela família da ISO 27001.

## 8. Penalizações

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem mas não se limitam a advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

As recomendações de sanções e punições serão realizadas conforme a análise da Comissão de trabalho da LGPD, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas em legislações específicas como CLT e Código Civil, além de cláusulas contratuais. O CGSI ficará responsável em encaminhar as recomendações de penalizações à Diretoria ou departamento responsável, para assim deliberar sobre a ação cabível de acordo com a infração.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a **PREFEITURA DE GUARÁ** , o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens anteriores desta política.

### 8.1. Casos Omissos

Os casos omissos serão avaliados pela Comissão de trabalho da LGPD para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da **PREFEITURA DE GUARÁ** adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da **PREFEITURA DE GUARÁ** .

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

**Art. 2º** Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

PREFEITURA MUNICIPAL DE GUARÁ, em 17 de dezembro de 2024.

**VINICIUS MAGNO FILGUEIRA**
Prefeito Municipal

Registrado, publicado e arquivado na Secretaria de Governo, data supra.

**CARLOS ALBERTO VIEIRA DUTRA**
Procurador Jurídico

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

**ANEXO I**

**TERMO DE RESPONSABILIDAE DE USO DOS RECURSOS DA TECNOLOGIA DA INFORMAÇÃO**

**CONSIDERANDO** que a Prefeitura de Guará disponibiliza aos seus servidores, usuários sem vínculo empregatícios, conveniados com a Prefeitura e prestadores de serviços recursos computacionais para uso exclusivo em suas atividades profissionais;

**CONSIDERANDO** que a Prefeitura de Guará é a única proprietária de todos os recursos computacionais disponibilizados aos seus servidores, usuários sem vínculo empregatícios, conveniados com a Prefeitura e prestadores de serviços, não existindo portanto qualquer tipo de expectativa de privacidade aos servidores;

**CONSIDERANDO** que a Prefeitura de Guará poderá ser seriamente impactada pela má utilização de seus recursos computacionais;

**DECLARO QUE:**

1. Tenho conhecimento e acesso à Política Geral de Segurança da Informação, bem como as demais normas e procedimentos sobre Segurança da Informação, Proteção de Dados e Privacidade, que são necessárias à execução do meu trabalho, aos quais li na íntegra, tomando conhecimento e ciência de suas disposições;
2. Compreendo os termos, diretrizes, conceitos e condições de uso da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação necessárias ao meu trabalho, me comprometendo a cumprir integralmente as disposições constantes em tais documentos;
3. Estou ciente e de acordo que, tanto os ativos de informação, quanto a infraestrutura tecnológica da Prefeitura de Guará somente poderão ser utilizados para fins exclusivamente profissionais e relacionados às atividades da Prefeitura;
4. Estou ciente que é realizado o monitoramento de todos os acessos e comunicações ocorridos através da infraestrutura tecnológica da Prefeitura de Guará;
5. Estou ciente que violações da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação, Proteção de Dados e Privacidade são passíveis de sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativa, cível e penal, nos termos da legislação em vigor;
6. Comprometo-me a não revelar fato ou informações de qualquer natureza a que tenha conhecimento por força das minhas atribuições, sem permissão legal, mesmo após o encerramento da execução de minhas atividades na Prefeitura de Guará.

Guará, ____ de _____ de 2024.

_____

Nome:

Cargo/empresa/convênio:

CPF:

**DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.**

**ANEXO II**

# Solicitação de Acesso

| I – IDENTIFICAÇÃO DO SOLICITANTE | | |
|---|---|---|
| **Orgão** (Secretaria/departamento) | | |
| **Unidade** (Divisões/serviços): | | |
| **IDENTIFICAÇÃO DO SUPERIOR** | | |
| Nome do chefe: | | Matrícula: |
| E-mail: | | Telefone/Celular: |
| **II – IDENTIFICAÇÃO DO SERVIDOR** | | |
| Nome: | CPF: | Matrícula: |
| Cargo/Função: | Regime: | Telefone/Celular: |
| Solicito a habilitação do servidor identificado para os seguintes serviços e softwares de gestão: | | |
| Acesso à Internet<br>Caixa postal de e-mail funcional<br>Mensageiro Instantânio<br>Acesso ao Servidor de Arquivos (Pasta do Secretaria/Departamento/Divisão)<br>Software de Gestão da Prefeitura | | |
| **III – ATENDIMENTO DA SOLICITAÇÃO** | | |
| Declaro estar de acordo com os perfis solicitados. (Chefe imediato)<br>_____ | Declaro que nesta data o cadastramento foi efetuado. (para uso da ATI)<br>_____ | |
| Data/Assinatura | Data/Assinatura | |

# DECRETO Nº 3.974, DE 17 DE DEZEMBRO DE 2024.

| INSTRUÇÕES |
| --- |
| Este formulário deverá ser preenchido pelo chefe imediato do servidor até o quadro II – IDENTIFICAÇÃO DO SERVIDOR e encaminhado a Assessoria de Tecnologia da Informação.<br>O TERMO DE RESPONSABILIDADE deverá ser datado e assinado pelo servidor para que seja efetuado o cadastro. O preenchimento deverá ser efetuado em letra de forma ou digital, sem rasuras e conforme especificações a seguir:<br><br>**QUADRO I**<br>IDENTIFICAÇÃO DO SOLICITANTE: preencher com os dados do chefe imediato ou titular responsável pelo órgão/unidade.<br>**QUADRO II**<br>IDENTIFICAÇÃO DO SERVIDOR: preencher com dados do servidor que terá acesso ao(s) serviço(s). HABILITAÇÃO PARA SERVIÇO: assinalar cada uma das alternativas necessárias.<br><br>**QUADRO III**<br>ATENDIMENTO DA SOLICITAÇÃO: autorização do responsável imediato.<br>CONFIRMAÇÃO DO ATENDENTE: responsável (Técnico da ATI) pelo cadastramento dos dados. |