



RESUMO DA POLÍTICA DE SEGURANÇA E INFORMAÇÃO

Decreto nº 13.129/2023 - Política de Segurança da Informação (PSI)

O Decreto nº 13.129/2023, de 3 de julho de 2023, institui a **Política de Segurança da Informação (PSI)** no âmbito da Administração Pública Municipal de Alegre, estabelecendo que a utilização dos recursos de tecnologia da informação e comunicação fica sujeita às normas e diretrizes constantes em seu anexo.

1. Conceitos Fundamentais da Política de Segurança da Informação

Para fins de aplicação da PSI, são definidos os seguintes conceitos:

- **Informação:** Conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado, independentemente do meio ou suporte utilizado.
- **Ativo:** Engloba todos os elementos que possuam valor para a Prefeitura Municipal de Alegre, tais como informações, microcomputadores e seus acessórios, notebooks, impressoras, servidores, dispositivos de armazenamento de dados, sistemas de informática e meios de transmissão. Todos os documentos e informações sob custódia da Prefeitura constituem ativos e são de sua propriedade.
- **Incidente de Segurança da Informação:** Qualquer ocorrência, indício de fraude, falha ou evento adverso que represente ameaça à segurança da informação ou que possa comprometer as operações institucionais.
- **Usuários Internos:** Servidores públicos e estagiários que utilizam os recursos de tecnologia da informação disponibilizados pela Prefeitura.
- **Colaboradores Externos:** Prestadores de serviços terceirizados ou quaisquer outros profissionais que, de forma autorizada, façam uso dos recursos de tecnologia da informação da Prefeitura.
- **Integridade:** Garantia de que a informação seja mantida em seu estado original, protegida contra alterações indevidas, sejam elas intencionais ou acidentais.
- **Confidencialidade:** Garantia de que o acesso às informações seja restrito a usuários ou processos devidamente autorizados.
- **Autenticidade:** Garantia de que a informação provenha de fonte legítima e confiável, preservando sua origem e validade.

2. Competências e Responsabilidades do Núcleo de Tecnologia da Informação (NTI)

O **Núcleo de Tecnologia da Informação (NTI)** é o setor responsável pela implementação, gestão e manutenção da **Política de Segurança da Informação (PSI)** no âmbito da Administração Municipal de Alegre, cabendo-lhe as seguintes competências:

- **Definir e implementar** políticas institucionais referentes à utilização, aquisição, padronização e controle de equipamentos, sistemas e programas de informática;
- **Manter e administrar** a infraestrutura tecnológica do Município, incluindo a rede, sub-redes e equipamentos associados;
- **Gerenciar** os serviços de infraestrutura de rede, tais como **IP, DNS e DHCP**, bem como os equipamentos de conectividade, como **switches e roteadores**;



- **Administrar** os sistemas de contas de usuários, compreendendo o **correio eletrônico corporativo**, o **Active Directory** e demais serviços correlatos;
- **Executar auditorias de segurança** nos servidores, **monitorar o tráfego de rede** e **identificar vulnerabilidades** relacionadas à segurança física e lógica dos sistemas;
- **Elaborar, implementar e supervisionar** as diretrizes da PSI, avaliando periodicamente sua eficácia e propondo ações de **melhoria contínua**;
- **Promover ações permanentes de capacitação**, divulgação, treinamento e conscientização voltadas à adoção de **boas práticas de segurança da informação** por parte dos usuários internos e colaboradores externos.

3. Responsabilidades dos Usuários e Gestores

Os **usuários internos** e **colaboradores externos** que utilizam os recursos de tecnologia da informação da Prefeitura Municipal de Alegre são corresponsáveis pela aplicação e observância das diretrizes estabelecidas na **Política de Segurança da Informação (PSI)**, incumbindo-lhes:

- **Cumprir integralmente** as normas e diretrizes da PSI, zelando pela **integridade, disponibilidade, autenticidade e legalidade** dos ativos de informação;
- **Abster-se de utilizar** os ativos de tecnologia para fins particulares, pessoais ou que possam causar **prejuízos, danos ou riscos** à Prefeitura Municipal;
- **Manter a confidencialidade** de todos os dados, documentos e informações a que tiverem acesso, sendo **vedada sua comercialização, reprodução, cessão, compartilhamento ou divulgação** a pessoas não autorizadas.

Compete aos **gestores das unidades administrativas**:

- **Promover a conscientização** e o alinhamento dos usuários e colaboradores sob sua responsabilidade quanto às normas e boas práticas de segurança da informação;
- **Incorporar e reforçar** as práticas de segurança da informação nos processos de trabalho e nas rotinas operacionais de sua unidade;
- **Adotar as medidas administrativas cabíveis** para a aplicação de ações corretivas e mitigatórias sempre que ocorrer ou for identificado **comprometimento da segurança da informação**.

4. Regras Específicas e Políticas de Uso

A **Política de Segurança da Informação (PSI)** estabelece normas específicas que disciplinam a utilização dos recursos tecnológicos da Prefeitura Municipal de Alegre, conforme descrito a seguir:

- **Política de Aquisição e Hardware:** Todos os processos de **aquisição de sistemas, softwares e equipamentos** deverão ser previamente submetidos à análise do **Núcleo de Tecnologia da Informação (NTI)** e à **aprovação da Comissão de Modernização Tecnológica (CMT)**.
- **Política de Aplicativos e Softwares:** É **terminantemente proibida** a utilização de softwares não licenciados ("piratas"). O NTI deverá **sugerir e recomendar** a adoção de **softwares livres** — tais como *WPS Office*, *Zabbix* e *pfSense* — sempre que existirem alternativas equivalentes às versões pagas, visando à **redução de custos** e à **legalidade do uso de licenças**. O **controle de acesso**, incluindo a **criação e**



exclusão de usuários em todos os aplicativos, é de **responsabilidade exclusiva do NTI**.

- **Área de Trabalho no Servidor de Arquivos:** Todos os arquivos relacionados às atividades laborais devem ser **armazenados na pasta institucional** do servidor, de modo a garantir **rotinas regulares de backup**. É **proibido o armazenamento** de materiais alheios às atividades institucionais, especialmente conteúdos **pornográficos, profanos, obscenos ou difamatórios**. O uso de **dispositivos de armazenamento móvel** (como *pendrives* ou *HDs externos*) depende de **autorização expressa da CMT**. A Prefeitura **reserva-se o direito de auditar**, a qualquer tempo e **sem aviso prévio**, as pastas e discos rígidos utilizados em sua infraestrutura.
- **Política de Correio Eletrônico:** O uso do **correio eletrônico institucional** deve restringir-se a **assuntos de interesse da Prefeitura**. É **vedado** o envio de **correntes, piadas, mensagens festivas** ou comunicações de natureza **comercial, religiosa ou político-partidária**. O **envio de informações sigilosas** somente poderá ocorrer mediante **autorização expressa**. A Prefeitura poderá **auditar o conteúdo das caixas postais ativas**, sem aviso prévio, para fins de segurança e conformidade.
- **Política de Estação de Trabalho:** O usuário é responsável pela **conservação dos equipamentos** sob seu uso. É **proibida a instalação ou remoção de softwares**, bem como a **alteração de configurações de hardware**, sem a prévia autorização do NTI. Ao ausentar-se de sua estação de trabalho, o usuário deverá **bloquear ou desligar o equipamento**, garantindo a proteção das informações.
- **Política de Interferências:** É **estritamente proibido** violar mecanismos de segurança de contas, redes ou servidores, **interferir no funcionamento de equipamentos de rede**, ou **utilizar programas com finalidade maliciosa ou destrutiva**.
- **Política de Acesso Remoto:** O **acesso remoto** é disponibilizado e gerenciado exclusivamente pelo NTI, sendo as **credenciais pessoais, intransferíveis e de uso restrito**. O uso de **ferramentas de acesso remoto não autorizadas** (tais como *TeamViewer*, *AnyDesk*, entre outras) é **vedado**.
- **Política de Internet:** O acesso à internet é **concedido mediante autorização** do respectivo **Secretário Municipal**. A Prefeitura poderá **monitorar e auditar os acessos**, bem como **bloquear conteúdos incompatíveis** com as atividades institucionais. É **proibido o acesso** a sites de conteúdo **pornográfico, de bate-papo, jogos ou relacionamento**, salvo quando **estritamente necessário** para o desempenho das funções. Também é **vedado o uso de softwares de comunicação instantânea** (*WhatsApp Web*, *Messenger*) e **serviços de streaming** (*rádio online*, *vídeos*), exceto em situações justificadas por **necessidade de trabalho**.
- **Política de Senhas:** As senhas de acesso são **pessoais e intransferíveis**. Devem conter **no mínimo oito caracteres**, incluindo **letras maiúsculas, letras minúsculas, números e símbolos especiais**, em conformidade com os **padrões de segurança** definidos pelo NTI.

5. Termo de Aceite e Penalidades

- O **acesso à rede corporativa e aos recursos tecnológicos da Prefeitura Municipal de Alegre** está condicionado à **assinatura prévia do Termo de Aceite das Condições de Segurança da Informação**, o qual constitui requisito indispensável para utilização dos sistemas e equipamentos institucionais.



- O referido Termo estabelece que **os recursos de informática e comunicação** são **ferramentas de trabalho de propriedade exclusiva** da Prefeitura Municipal de Alegre, que **reserva-se o direito de monitorar, auditar e registrar as atividades dos usuários**, sempre que necessário, a fim de **proteger seus ativos, informações e interesses institucionais**.
- A **violação das diretrizes e normas previstas na Política de Segurança da Informação (PSI)** sujeitará o infrator à **restrição de acesso aos recursos tecnológicos**, bem como à **aplicação das penalidades disciplinares cabíveis**, nos âmbitos **administrativo, civil e criminal**, sem prejuízo da **obrigação de ressarcimento integral dos danos eventualmente causados**, decorrentes de **dolo, negligência, imprudência ou imperícia**.
- Qualquer **incidente de segurança da informação, real ou suspeito**, deverá ser **comunicado imediatamente ao Núcleo de Tecnologia da Informação (NTI)**, para fins de registro, investigação e adoção das medidas corretivas pertinentes.