Prefeitura Municipal de Miracatu

Supervisão Legislativa

Decretos

PREFEITURA MUNICIPAL DE MIRACATU
Estado de São Paulo
Gabinete
Avenida Dona Evarista de Castro Ferreira nº 360 – Centro
Miracatu-SP - Fone: (13) 3847-7000
Email: gabinete@miracatu.sp.gov.br – site: www.miracatu.sp.gov.br

DECRETO Nº 2.156 DE 19 DE DEZEMBRO DE 2024.

"DISPÕE SOBRE A REGULAMENTAÇÃO DE BACKUPS RESTAURAÇÃO DE DADOS E INFORMAÇÕES NO ÂMBITO DO MUNICÍPIO DE MIRACATU E DÁ OUTRAS PROVIDÊNCIAS".

VINICIUS BRANDÃO DE QUEIRÓZ, ***Prefeito Municipal***, residente e domiciliado neste Município de Miracatu, no uso de suas atribuições legais;

DECRETA:

Art. 1º Fica instituída a regulamentação para a realização de backups de dados e informações nos órgãos e entidades da administração pública municipal, com o objetivo de garantir a integridade, a disponibilidade e a confidencialidade das informações.

Art. 2º Para os fins deste decreto, consideram-se:
I - - **Backup ou Cópia de Segurança**: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo a guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Deve ser identificado a mídia em que a cópia é realizada;
II - **Responsáveis**: Servidores públicos designados para a execução e supervisão dos processos de backup;
III – **PSI**: Política de Segurança da informação Anexo I;
IV - **Recovery Point Objective (RPO)**: ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;
VI - **Recovery Time Objective (RTO)**: tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperante até a restauração de seus dados, após um incidente

Art. 3º Todos os órgãos e entidades da administração pública municipal deverão:
I - Elaborar e implementar uma política de backup que contemple:
a) Frequência de realização dos backups;
b) Tipos de dados a serem copiados;
c) Armazenamento seguro dos backups;
d) Testes regulares de recuperação de dados.

II - Designar servidores responsáveis pela execução e supervisão das atividades de backup.

III - Garantir que os backups sejam realizados em local seguro e que possuam criptografia, quando aplicável.

PREFEITURA MUNICIPAL DE MIRACATU
Estado de São Paulo
Gabinete
Avenida Dona Evarista de Castro Ferreira nº 360 – Centro
Miracatu-SP - Fone: (13) 3847-7000
Email: gabinete@miracatu.sp.gov.br – site: www.miracatu.sp.gov.br

Art. 4º Os responsáveis deverão elaborar relatórios semestrais sobre a execução das políticas de backup, apresentando:

I - Frequência de backups realizados;
II - Ocorrências de falhas ou problemas na execução dos backups;
III - Resultados dos testes de recuperação de dados.

Art. 5º Responsabilidade específica da coordenadoria de Informática:
I - Para as bases de dados que ficam instalados nos servidores do município de posse da coordenadoria de informática e são de responsabilidade do município manter a base de dados com backups diários em mais de 1 local físico diferente.
Art. 6º Responsabilidade de sistemas de terceiros ou contratados:
I - As bases de dados de sistema externos precisam constar em seus respectivos editais ou contratos de renovação que é de responsabilidade da prestadora do serviço (Sistema) externos (entende-se externos aquelas bases de dados que não estão de posse direta da coordenadoria de informática) com as seguintes observações:

a) Deve por regra trimestralmente ser enviado o backup ao município ou assim que solicitados através de mídias digitais com backup full contendo todas as informações incluindo anexos de arquivos caso tenha, e que todos as bases de dados alimentadas terão que ser disponibilizadas ao município para conservação das informações alimentadas nos respectivos sistemas, e os backups diários são de responsabilidade da empresa que presta o serviço ao município para que não se perca informações pois o município não ter acesso direto a essas bases de dados.
b) Sempre que solicitado ser entregues criptografados e enviados a senha sem separado do arquivo para descompactação e utilização do município sem qualquer restrição de informação e que sejam compatíveis com SQLServer e caso possua alguma outra senha de segurança deve ser informada a coordenadoria.
c) Os prestadores de serviços terceirizados que utilizam de sistemas para gestão próprio e que alimentem dados dos munícipes ou do município que são de interesse público ou da gestão pública, sistemas externos deverão ser notificados para que se enquadrem no presente decreto incluindo seu anexo, e estabeleçam rotina para entrega da base de dados a coordenadoria de informática para que se possa manter as informações sem qualquer perca de dados em uma possível alteração ou migração para um novo sistema sem qualquer ônus a prefeitura quer seja financeiro ou perca de informações.

Art. 7º Este decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

VINÍCIUS BRANDÃO DE QUEIROZ
Prefeito Municipal

Registre-se e publique-se

Meire Rolim Camargo de Oliveira
Superv. de Serv. Legislativos

PREFEITURA MUNICIPAL DE MIRACATU
Estado de São Paulo
Gabinete
Avenida Dona Evarista de Castro Ferreira nº 360 – Centro
Miracatu-SP - Fone: (13) 3847-7000
Email: gabinete@miracatu.sp.gov.br – site: www.miracatu.sp.gov.br

ANEXO I

Política de Segurança da Informação e Backup (PSI)

1. Objetivo

Estabelecer diretrizes para proteger as informações e garantir a integridade, confidencialidade e disponibilidade dos dados, além de definir procedimentos para a realização de backups e suas respectivas restaurações assim que necessário com eficácia no menor tempo possível.

2. Escopo ou Abrangência

Esta política se aplica a todos os colaboradores, contratados e parceiros que tenham acesso a informações e sistemas da organização ou contratado por terceiros para melhor eficácia na gestão pública no que se refere a tecnologia de informação.

3. DEFINIÇÃO DA SEGURANÇA DA INFORMAÇÃO

Diariamente, todas as Coordenadorias e Diretorias da Prefeitura Municipal de Miracatu, coletam, processam, armazenam e transmitem informações, não somente pelo meio físico e verbal, mas, também pelo meio digital. Todas essas informações são como Ativos para a organização, e como qualquer outro ativo importante, elas são essenciais para o funcionamento dos serviços públicos, portanto, elas têm valor para a organização e, consequentemente, precisam ser protegidas contra diversos tipos de riscos. Ativos são objeto de ameaças, sejam elas acidentais ou de forma deliberada, além do mais, os processos, sistemas, redes e pessoas possuem vulnerabilidades inerentes. Ambientes de mudanças, internas ou externas a organização (novas leis ou regulamentações, por exemplo), podem criar novas ameaças a estes ativos de tal modo que, inevitavelmente, sempre haverá riscos à segurança da informação. Desta forma, uma boa segurança da informação reduz estes riscos, protege a instituição pública contra essas ameaças e vulnerabilidades e mitiga qualquer impacto aos ativos de maneira eficaz.

4. Princípios da Segurança da Informação

- **Confidencialidade**: Assegurar que a informação é acessível apenas a pessoas autorizadas.
- **Integridade**: Proteger a informação contra modificações não autorizadas.
- **Disponibilidade**: Garantir que a informação esteja acessível e utilizável quando necessário.

5. Diretrizes de Segurança da Informação

- **Acesso Controlado**: O acesso a informações deve ser limitado com base em funções e necessidades.
- **Treinamento**: Todos os colaboradores devem receber treinamento regular sobre segurança da informação.
- **Gestão de Incidentes**: Estabelecer um processo para identificar, reportar e responder a incidentes de segurança.

6. Diretrizes de Backup

- **Frequência**: Realizar backups regulares, com a frequência definida por categoria de dados (diária, semanal, mensal).
- **Tipos de Backup**: Implementar backups completos, incrementais e diferenciais conforme necessário.

PREFEITURA MUNICIPAL DE MIRACATU
Estado de São Paulo
Gabinete
Avenida Dona Evarista de Castro Ferreira nº 360 – Centro
Miracatu-SP - Fone: (13) 3847-7000
Email: gabinete@miracatu.sp.gov.br – site: www.miracatu.sp.gov.br

- **Armazenamento**: Os backups devem ser armazenados em local seguro, e pelo menos 2 locais físicos ou virtuais distintos que não se comuniquem após o backup preferencialmente fora do site principal ou físicos com bom armazenamento e qualidade para evitar perda de dados.
- **Criptografia**: Dados sensíveis devem ser criptografados durante o backup e no armazenamento.
- **Testes de Recuperação**: Realizar testes periódicos de recuperação de dados para assegurar a eficácia dos backups.

7. ATRIBUIÇÃO DE RESPONSABILIDADES PARA O GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

7.1. Dos usuários em geral

Entende-se por usuário toda e qualquer pessoa física, contratada por concurso ou seleção ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Cabe a todos os usuários cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos a sua disposição sejam utilizados apenas para as finalidades aprovadas pela Prefeitura Municipal de Miracatu; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas incluindo a emissão de comentários e opiniões em blogs e redes sociais; não compartilhar informações confidenciais de qualquer tipo; e comunicar imediatamente a Area de Tecnologia da Informação quando do descumprimento ou violação desta política.

7.2. DOS GESTORES

Entende-se por gestores o Prefeito Municipal, o Vice-Prefeito Municipal e todos os Diretores responsáveis pelos Departamentos.

Todos os gestores devem ser um modelo de conduta e manter postura exemplar em relação a segurança da informação para os colaboradores sob a sua gestão; Atribuir aos colaboradores a responsabilidade do cumprimento da PSI da Prefeitura Municipal de Miracatu; Assegurar que todos os colaboradores possuam acesso e conhecimento desta PSI; Identificar os desvios praticados e adotar as medidas corretivas apropriadas; Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI; Avaliar e aprovar os termos e controles desta Política, bem como os ajustes, melhorias, aprimoramentos e modificações desta Política, propostos pelos Custodiantes da Informação.

7.3. Dos Custodiantes da Informação

Entende-se por Custodiantes da Informação toda e qualquer pessoa física, contratada por concurso ou seleção ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade na área de Tecnologia da Informação.

7.3.1. Da Area de Tecnologia da Informação

Cabe a área de Tecnologia da Informação:

1 - Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

2 - Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

3 - Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

PREFEITURA MUNICIPAL DE MIRACATU
Estado de São Paulo
Gabinete
Avenida Dona Evarista de Castro Ferreira nº 360 – Centro
Miracatu-SP - Fone: (13) 3847-7000
Email: gabinete@miracatu.sp.gov.br – site: www.miracatu.sp.gov.br

4 - Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de copias de segurança, auditorias ou testes no ambiente.

5 - Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
6 - Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessária para garantir a segurança requerida pelas áreas de negócio.
7 - Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

a) Os usuários (logins) individuais de colaboradores serão de responsabilidade do próprio colaborador;
b) Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante;

8 - Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado;
9 - Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

10 - Realizar auditorias periódicas de configurações técnicas e análise de riscos.
11 - Garantir, da forma mais rápida possível, após solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
12 - Garantir que todos os servidores, estações e demais dispositivos com acesso a rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
13 - Propor ajustes, melhorias, aprimoramentos e modificações desta Política.
14 - Publicar e promover a PSI aprovada pelos gestores. Promover a conscientização dos colaboradores em relação a relevância da segurança da informação para as atividades da Prefeitura Municipal de Miracatu, mediante campanhas, palestras, treinamentos e outros meios de marketing.
15 - Manter comunicação efetiva com os Gestores sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Prefeitura Municipal de Miracatu. Buscar alinhamento com as diretrizes de governo da instituição.

8. Responsabilidades

- **Gestão de TI**: Responsável por implementar e monitorar a política de segurança da informação e backup.
- **Colaboradores**: Devem seguir as diretrizes estabelecidas e reportar qualquer incidente ou violação.

9. da Revisão
Esta política de Segurança da informação deve ser revisada anualmente ou sempre que ocorrer mudanças significativas nos processos ou na estrutura organizacional.