PREFEITURA DE SOBRAL

SECRETARIA DE OUVIDORIA, CONTROLADORIA E GESTÃO - SECOG

COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

Sumário

OBJETIVO

Estabelecer os conceitos e diretrizes de segurança da informação, visando proteger as informações da Prefeitura Municipal de Sobral e do público em geral.

ABRANGÊNCIA

Esta Política aplica-se a todos os funcionários, terceirizados, estagiários, prestadores de serviços e dos demais órgãos vinculados a PMS.

CONCEITOS

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- **Confidencialidade**: Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;
- **Disponibilidade**: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;
- **Integridade**: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

ESTRUTURA NORMATIVA

A estrutura normativa da Segurança da Informação da Prefeitura Municipal de Sobral é composta por um conjunto de assuntos, relacionados a seguir.

- **Política**: define a estrutura, as diretrizes e os papéis referentes à segurança da informação;
- **Normas**: estabelecem regras, definidas de acordo com as diretrizes da Política, a serem seguidas em diversas situações em que a informação é tratada;
- **Procedimentos**: instrumentam as regras dispostas nas normas, permitindo a direta aplicação nas atividades da PME.

DIRETRIZES

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação da PMS. Tais diretrizes devem nortear a elaboração das Normas e dos Procedimentos.

Aspectos gerais

- As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da PMS, não podendo ser interpretados como de uso pessoal;
- Todos os funcionários, terceirizados, estagiários e prestadores de serviços devem ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação, podendo estas servir de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais;
- Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de uma pessoa ou equipe.

Tratamento da informação

- Para assegurar a proteção adequada às informações, deve existir um método de classificação da informação de acordo com o grau de confidencialidade e criticidade para a PMS;
- As informações devem ser atribuídas a um proprietário, formalmente designado como responsável pela autorização de acesso às informações sob a sua responsabilidade;
- Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da PMS em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

Gestão de acessos e identidades

- O acesso às informações e aos ambientes tecnológicos da PMS deve ser controlado de acordo com sua classificação, de forma a garantir acesso apenas às pessoas autorizadas, mediante aprovação formal;
- Os acessos aos funcionários, terceirizados, estagiários e prestadores de serviços devem ser solicitados e aprovados somente às informações necessárias ao desempenho de suas atividades.

Gestão de incidentes de segurança da informação

- Em casos de violação desta Política e Normas de Segurança da Informação, o gestor da coordenadoria de tecnologia da informação realizará deliberações somente nos incidentes classificados com alta criticidade. Os demais casos serão tratados pelo fluxo normal de resposta a incidentes.

PARTES EXTERNAS

- Os contratos entre a PMS e empresas prestadoras de serviços com acesso às informações, aos sistemas e/ou ao ambiente tecnológico da PMS devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram a Política e as Normas de Segurança da Informação.

RESPONSABILIDADES

De forma geral, cabe a todos os funcionários, terceirizados, estagiários e prestadores de serviços:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da PMS;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela PMS;
- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela PMS;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.) incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente à área de tecnologia da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

Área de gestão de segurança da informação

Cabe à área de Gestão de Segurança da Informação:

- Prover todas as informações de gestão de Segurança da Informação;
- Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os funcionários, terceirizados, estagiários e prestadores de serviços;
- Promover ações de conscientização sobre Segurança da Informação para os funcionários, terceirizados, estagiários e prestadores de serviços;
- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da PMS;
- Estabelecer procedimentos relacionados à instrumentação da segurança da informação da PMS.

AÇÕES EM CASOS DE NÃO CONFORMIDADE

As regras que estabelecem o controle e o tratamento de situações de não conformidade relativas à Política e às Normas de Segurança da Informação da PMS devem ser tratadas em acordo com o coordenador de tecnologia da informação da PMS.

Na ocorrência de violação desta Política ou das Normas de Segurança da Informação, poderá adotar, com o apoio das coordenadorias Jurídica e de Recursos Humanos, sanções administrativas e/ou legais, que poderão culminar com o desligamento e eventuais processos criminais, se aplicáveis.

DEFINIÇÕES

- **Ativos de Informação**: conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a PMS.
- **Informação**: resultado do processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema. É composta por dados, mas um conjunto de dados não necessariamente é considerado uma informação.
- **Sistemas de informação**: de maneira geral, são sistemas computacionais utilizados pela PMS para suportar suas operações.
- **Segregação de funções**: consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que nenhum funcionário, terceirizado, estagiário ou prestador de serviço detenha poderes e atribuições em desacordo com este princípio.