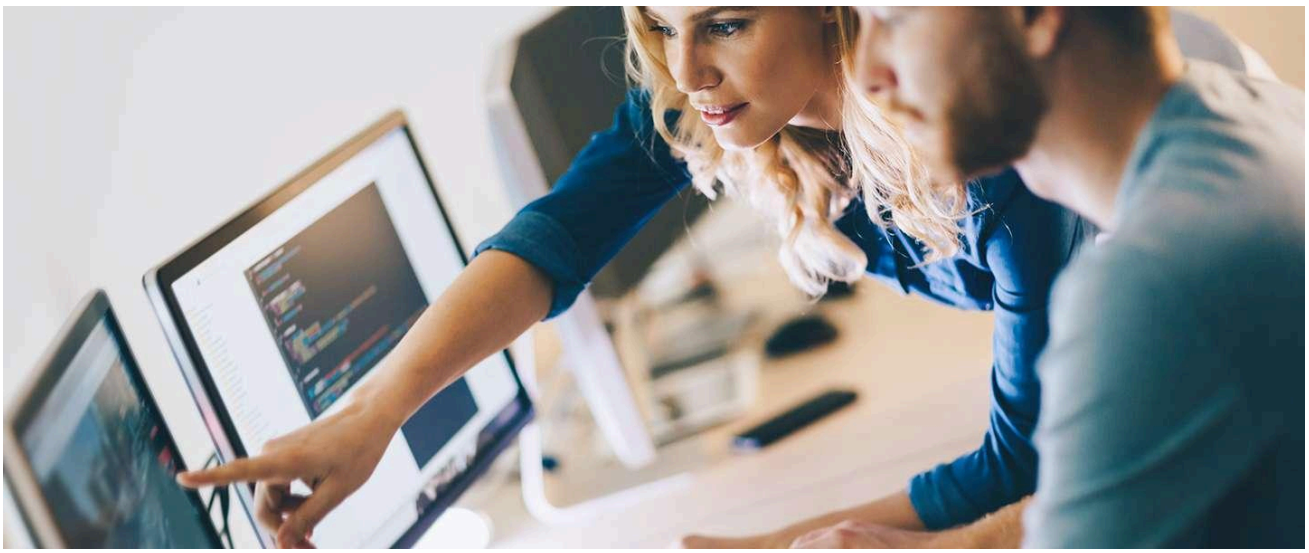
MARINGÁ
PREFEITURA
COMPLIANCE E CONTROLE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Diretrizes para a Proteção de Ativos e Prevenção de Responsabilidades à **SI**

SUMÁRIO



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PREFEITURA MUNICIPAL DE MARINGÁ

SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação – PSI da Prefeitura Municipal de Maringá é o documento que orienta e estabelece as diretrizes e critérios para a proteção dos ativos de informação e a prevenção da responsabilidade relacionada à Segurança da Informação para todos os servidores, estagiários, prestadores de serviços e demais agentes públicos.

Trata-se de uma política com o objetivo de aumentar a segurança da infraestrutura tecnológica direcionada ao uso corporativo e deve ser cumprida e aplicada em todas as áreas da Prefeitura, assim como, deve ser revisada anualmente, podendo ser alterada quando mudanças forem aprovadas.

Este documento está fundamentado nos objetivos de controle elencados pela norma ABNT NBR ISO/IEC 27002, assim como as publicações NIST e seu Framework de Segurança da Informação.

OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

A Política de Segurança da Informação - PSI vem com o objetivo de estabelecer diretrizes e normas que permitam à gestão municipal, servidores, estagiários, prestadores de serviços e demais agentes públicos que possuem algum tipo de relação com a Prefeitura Municipal de Maringá, seguir padrões de comportamento desejáveis e aceitáveis, de acordo com a legalidade e as boas práticas mundiais, a fim de mitigar riscos técnicos e jurídicos.

Neste contexto, complementa com as seguintes finalidades:

- O compromisso da Prefeitura de Maringá com a proteção das informações de sua propriedade e/ou sob sua guarda.
- Nortear a definição dos princípios e diretrizes gerais que visam a preservação da segurança da informação, primando pela legalidade dos processos que amparam a operacionalização e gestão das atividades da instituição, assim como, de procedimentos específicos de segurança da informação e a implementação de controles e processos para o atendimento de seus requisitos.
- Preservar a confidencialidade, a integridade e a disponibilidade das informações da Prefeitura para garantir a confiabilidade das informações e dados pessoais.
- Prevenir possíveis incidentes e responsabilidade legal da Prefeitura de Maringá, bem como da gestão municipal, servidores, estagiários, prestadores de serviços e demais agentes públicos.
- Garantir a normalidade e a continuidade das atividades da Prefeitura, protegendo os processos críticos contra falhas ou desastres significativos.
- Atender aos requisitos legais, regulamentares e contratuais pertinentes à atividade da Prefeitura.
- Minimizar os riscos de danos, perdas financeiras, perda da reputação ou qualquer outro impacto negativo nas atividades da Prefeitura resultante de uma falha de segurança.
- Assegurar o treinamento contínuo e atualizado das políticas e dos procedimentos de segurança da informação na instituição, estabelecendo e enfatizando as obrigações, responsabilidades e limites de atuação, ainda que transitoriamente, da gestão municipal, servidores, estagiários, prestadores de serviços e demais agentes públicos que possuem algum tipo de relação com a Prefeitura Municipal de Maringá em relação à segurança da informação e proteção de dados pessoais, reforçando uma cultura interna baseada em integridade.
- Garantir que todas as responsabilidades da segurança da informação sejam claramente definidas e preservadas.

NORMAS E REFERÊNCIAS PARA FUNDAMENTAÇÃO

Este documento está fundamentado nos objetivos de controle elencados:

- Pela norma:
    - ABNT NBR ISO/IEC 27001:2013 - Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos
    - ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação
    - ABNT NBR ISO/IEC 27701:2019 - Tecnologia da Informação – Técnicas de segurança – Gestão da privacidade da informação — Requisitos e diretrizes
- Publicações do *National Institute of Standards and Technology Framework* - NIST e seu Framework de Segurança da Informação que foi criado para ajudar as organizações a gerenciar e reduzir o risco de segurança cibernética da infraestrutura crítica e dos sistemas de controle industrial.
- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.
- Decreto Estadual nº 6.474, de 14 de dezembro de 2020 – Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo do Estado do Paraná.
- Decreto Municipal n.º 1.547/2023 - Regulamenta a Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Município de Maringá e dá outras providências.

A confidencialidade, integridade e disponibilidade são os 3 (três) pilares da segurança da informação, sendo que cada um desses pilares tem vital importância para os processos de proteção de dados e são essenciais em qualquer política interna de Tecnologia da Informação para garantir que os processos internos fluam corretamente.

CONFIDENCIALIDADE

Trata-se de não permitir a disponibilização, acesso ou exposição da informação a indivíduos, entidades ou processos não autorizados expressamente, seja por contratos ou outros instrumentos formais.

INTEGRIDADE

Vem salvaguardar exatidão e completeza das informações, tal como foram criadas ou recebidas utilizando tecnologias, controle e processos que garantam esse requerimento pelo próprio design dos produtos e sistemas da Prefeitura Municipal de Maringá.

DISPONIBILIDADE

Os sistemas e informações pertencentes ao ecossistema tecnológico da Prefeitura Municipal de Maringá deverão estar disponíveis para seus servidores e cidadãos, atendendo também a confidencialidade das informações e integridade de seu conteúdo, formando, assim, uma tríade de segurança de qualidade superior.

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Os dados pessoais contidos nas informações devem ser protegidos com a adoção de medidas técnicas e organizacionais de segurança da informação, nos termos impostos pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados – LGPD e esta estará disciplinada em conjunto com o procedimento de tratamento de dados pessoais.

APLICAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PELOS SERVIDORES

Segurança da Informação – SI é a proteção da informação contra vários tipos de ameaças, garantindo a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades para a Prefeitura Municipal de Maringá.

A SI é obtida a partir da implementação de um conjunto de controles, incluindo tecnologia, políticas, processos, procedimentos, comportamentos e a própria estrutura organizacional do órgão.

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente, sempre que necessários, e melhorados continuamente para garantir que os objetivos e a segurança da Prefeitura Municipal de Maringá sejam atendidos.

É fundamental que esses controles sejam aplicados à gestão municipal, servidores, estagiários, prestadores de serviços e demais agentes públicos que possuem algum tipo de relação com a Prefeitura Municipal de Maringá, visando a proteção da informação por meio do uso correto de recursos tecnológicos e ações comportamentais.

Internamente, considera-se como informação toda a base de conhecimento, conteúdo, dado, conceito, envio ou recebimento de mensagens, processo ou fato existente, em meio físico ou eletrônico, que compõe documentos e informações de propriedade, interesse ou posse da Prefeitura Municipal de Maringá e inclui, mas não se limita a, qualquer dado, material, procedimento, processo, especificações, inovações e aperfeiçoamento técnicos e comerciais que agreguem valor para o negócio do órgão, assim como todas as informações confidenciais dos servidores e cidadãos sob custódia da Prefeitura.

Esta Política de Segurança da Informação - PSI compromete e responsabiliza cada servidor a se manter atualizado sobre este documento e as normas relacionadas, buscando orientação do(a) Encarregado(a) de Proteção de Dados Pessoais – DPO, do gestor imediato ou da gerência de tecnologia da informação - TI sempre que não estiver absolutamente seguro quanto a qualquer tratamento de dados pessoais, assim como, o descarte desses.

A PSI é um documento com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação para a gestão municipal, servidores, estagiários, prestadores de serviços e demais agentes públicos que possuem algum tipo de relação com a Prefeitura Municipal de Maringá.

PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Os equipamentos de informática, de comunicação, os sistemas e as informações devem ser utilizados para a realização de atividades profissionais, com senso de responsabilidade e preceitos éticos comuns à sociedade e dentro da legalidade.

Deve-se respeitar a privacidade dos usuários, agindo de forma ética e atendendo aos princípios da Lei Geral de Proteção de Dados Pessoais - LGPD.

A Prefeitura Municipal de Maringá se reserva no direito de monitorar e registrar todo e qualquer uso das informações geradas, armazenadas ou veiculadas no órgão. Para tanto, podem ser criados e implantados controles apropriados, trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a Prefeitura julgar necessário para reduzir os riscos, pautando-se na ética e na legalidade de forma a detalhar as ações para conhecimento de todos.

CLASSIFICAÇÃO DAS INFORMAÇÕES

A Informação é tida como um ativo e possui valor diferente dependendo do seu conteúdo.

Os controles de proteção desses ativos podem aumentar de acordo com seu valor. A classificação das informações também pode definir quais controles de proteção precisam ser implementados.

Podemos entender que a classificação da informação também é vista como uma escala de proteção a ser aplicada na mesma, com controles compatíveis em todo o seu ciclo de vida, por meio de implementação de ferramentas e formalização de processos em instrumento específico, nos termos dos Normativos Internos de Segurança da Informação ou legislação prevista para cada tipo de informação tratada no órgão.

Para a Prefeitura Municipal de Maringá, são quatro níveis de classificação da Informação em ordem crescente de importância e sigilo:

Pública

São todas as informações que já sejam de conhecimento público e estejam disponibilizadas para os servidores e para o público em geral através da internet (via site e/ou portal da transparência), ou veiculadas em documentos publicados em jornais, revistas, folders, redes sociais, panfletos, avisos ou palestras autorizadas.

Interna

São informações que estão disponíveis aos servidores por meio das ferramentas aprovadas, com armazenamento interno em servidores da Prefeitura Municipal de Maringá ou em terceiros autorizados (na nuvem, por exemplo).

Qualquer Informação classificada como INTERNA não poderá ser encaminhada, divulgada ou publicada em quaisquer meios para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho da Prefeitura Municipal de Maringá e uso limitado aos servidores ou terceiros (mediante assinatura de contrato com cláusulas de confidencialidade específicas ou termo de confidencialidade), que realmente necessitem ter acesso a tais Informações.

Restrita

Os documentos classificados como RESTRITOS somente poderão ser acessados pela área, departamento, setor ou função dentro da Prefeitura Municipal de Maringá que classificou a informação. Normalmente são informações de uma determinada área que não devem ser acessadas por outros setores da empresa.

Confidencial

Todas as Informações classificadas como CONFIDENCIAIS deverão ser mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis com a relevância da informação, tais como cofres, armários com chaves, diretórios criptografados ou envio dos arquivos somente após a inclusão de mecanismos de segurança (senha ou criptografia).

A transmissão de arquivos confidenciais só deverá ser feita utilizando meios de transmissão seguros, para as partes previamente autorizadas, com contrato de sigilo claro e dentro da validade, sejam as partes: servidores, estagiários, prestadores de serviços, agentes públicos ou qualquer tipo de parceiro de negócios que precisam: criar, armazenar ou processar qualquer tipo de Informação confidencial.

Exemplos de informações confidenciais:

- Processos judiciais.
- Dados cadastrais de servidores e agentes públicos.
- Dados cadastrais dos usuários da Prefeitura Municipal de Maringá.
- Documentos e/ou Informações fornecidas pelos usuários da Prefeitura Municipal de Maringá.
- Contratos firmados pela Prefeitura Municipal de Maringá com terceiros.
- Contratos firmados pela da Prefeitura Municipal de Maringá com seus contratados.
- Entre outros.

TERMOS E DEFINIÇÕES

Para melhor interpretação da presente PSI consideram-se:

Usuários

Todos os envolvidos, independente de cargo ocupado, no manuseio da informação durante as suas atividades diárias.

Prestadores de serviços

Os prestadores de serviços, considerados como trabalhadores autônomos, exercendo, portanto, as suas atividades profissionais, por conta própria, sem vínculo empregatício ou subordinação, deverão garantir a segurança da informação, o sigilo e a confidencialidade dos dados pessoais a que tiverem acesso, mesmo após o término do Contrato de Prestação de Serviços.

Os prestadores de serviços deverão tratar os dados pessoais a que tiverem acesso, de acordo com as orientações da Prefeitura Municipal de Maringá, para as finalidades específicas determinadas por esta e pelo período de duração do Contrato de Prestação de Serviços.

Agentes Públicos *(servidor público e todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função na Prefeitura de Maringá)*

Por consequência do Contrato de Trabalho, os agentes públicos deverão garantir a segurança da informação, o sigilo e a confidencialidade dos dados pessoais a que tiverem acesso, mesmo após o término da relação trabalhista.

Os agentes públicos deverão tratar os dados pessoais a que tiverem acesso, de acordo com as orientações da Prefeitura Municipal de Maringá para as finalidades específicas determinadas por esta e pelo período de duração do vínculo perante à organização.

Dado pessoal

Informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Informação

Qualquer conteúdo que tenha ou traga valor para a empresa ou ao profissional para que alcance seu objetivo.

Risco

Estabelece a relação entre probabilidade e impacto em uma determinada situação ou atividade. Essa análise possibilita determinar como devem ser os investimentos em segurança da informação.

Ameaça

Elemento externo ou interno capaz de explorar vulnerabilidades existentes no ambiente da empresa, o qual pode ocasionar prejuízo ou dano para o seu ambiente organizacional.

Vulnerabilidade

Fragilidade que pode ser explorada por uma ou mais ameaças no ambiente da empresa.

Violação

Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos, políticas e procedimentos operacionais da Prefeitura de Maringá.

Credencial de Acesso

É a identificação do agente público em ambientes lógicos, sendo composta por seu nome de usuário (*login*) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.

Incidente de Segurança da Informação

Eventos indesejados ou inesperados que possam colocar em risco as informações armazenadas em meio físico ou eletrônico sob a guarda da empresa ou que tenham grande probabilidade de comprometer as operações do órgão e ameaçar a segurança da informação.

Classificação da Informação

Processo que compreende a identificação e definição de níveis e critérios de proteção para as informações, de forma a garantir sua confidencialidade, integridade e disponibilidade.

Confiabilidade

Recurso relativo à consistência no comportamento e nos resultados desejados.

Impacto

Trata das consequências esperadas caso as informações protegidas sejam expostas de forma não autorizada.

Probabilidade

Oportunidade de uma vulnerabilidade ser explorada por uma ameaça.

Sigilo profissional

Trata da manutenção de segredo para informação valiosa, cujo domínio de divulgação deva ser fechado, ou seja, restrito a um usuário, a um prestador de serviços e/ou contratado ou a um agente público, uma vez que a ele é confiada a manipulação da informação.

Gestão de Risco

Atividades coordenadas para dirigir e controlar um órgão público em relação ao risco, aplicabilidade de suas políticas de segurança, bem como, monitoramento e revisão dos riscos.

Plano de Continuidade do Negócio

Fornece estratégias para garantir que serviços essenciais ou críticos sejam identificados, garantindo sua preservação após a ocorrência de um desastre e até o retorno da situação normal de funcionamento da empresa. Também prevê quais planos de ação devem ser realizados em cada momento.

Comitê de Segurança da Informação (CSI)

É o comitê composto por uma equipe multidisciplinar, cuja principal função está em assessorar a implementação das ações relacionadas à Segurança da Informação, além de avaliar os controles e incidentes de segurança relacionados.

DEVERES E RESPONSABILIDADES

Comitê de Segurança da Informação - CSI

Aos indicados para participar do Comitê de Segurança da Informação, incluindo representantes da área de Tecnologia da informação, cabe a estes:

- Propor diretrizes e normas de caráter geral, políticas e estratégias em segurança da informação.
- Elaborar o planejamento e gestão da Segurança da Informação.
- Elaborar documentos necessários à Segurança da Informação.
- Elaborar, divulgar para as partes interessadas, manter e aperfeiçoar os indicadores de Segurança da Informação.
- Coordenar, juntamente com a equipe da Secretaria de Gestão de Pessoas (SEGEP), programas de treinamento e de conscientização em Segurança da Informação.
- Analisar os incidentes de Segurança da Informação e recomendar as ações corretivas e preventivas.

- Assegurar que o sistema de gestão da segurança da informação está em conformidade com os requisitos da norma ISO 27001 vigente.
- Relatar o desempenho do sistema de Gestão da Segurança da Informação para o Gestor imediato da Agência Maringá de Tecnologia e Inovação (AMTECH).

Gestão - AMTECH

Em relação à Segurança da Informação, cabe à alta direção:

- Aprovar a Política de Segurança da Informação.
- Patrocinar a implementação da Política de Segurança da Informação.
- Apoiar o processo de melhoria contínua do Sistema de Gestão de Segurança da Informação.

Diretorias, Gerências e equipe do setor de Tecnologia da Informação

Cabe às Diretorias, Gerências e equipe da tecnologia da informação:

- Participar da aprovação da Política de Segurança da Informação e suas atualizações.
- Definir as regras para instalação de *software* e *hardware* na Prefeitura Municipal de Maringá.
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação.
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações.
- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades etc.
- Analisar criticamente incidentes de segurança.
- Manter comunicação efetiva sobre possíveis ameaças e novas medidas de segurança.
- Buscar alinhamento com as diretrizes da organização.
- Apoiar na promoção à conscientização da gestão municipal, servidores, estagiários, prestadores de serviços e demais agentes públicos quanto à relevância da

segurança da informação para as atividades da Prefeitura Municipal de Maringá por meio de campanhas, palestras, treinamentos, entre outros meios.

- Apresentar as atualizações da Política de Segurança da Informação e das Normas de Segurança da Informação ao Comitê, aos superiores para aprovação e posterior publicação.
- Apoiar a avaliação e a adequação dos controles específicos da segurança da informação para novos sistemas ou serviços.
- Desenvolver normas e regras específicas conforme à Lei de Proteção de Dados Pessoais com o apoio do(a) Encarregado(a) de Proteção de Dados Pessoais – DPO.
- Promover adequação dos recursos técnicos e de infraestrutura necessários para atender à Lei Geral de Proteção de Dados Pessoais - LGPD.

Secretaria de Gestão de Pessoas (SEGEP)

Cabe a Secretaria de Gestão de Pessoas (SEGEP):

- Na fase de formalização da admissão dos servidores, estagiários e demais agentes públicos, deve atribuir e formalizar nos contratos individuais de trabalho, por meio eletrônico, a responsabilidade quanto ao cumprimento da Política de Segurança da Informação e sua responsabilidade para com a Confidencialidade e Proteção de Dados Pessoais.
- Colher e arquivar, por meio eletrônico, a assinatura e ciência do Termo de Responsabilidade, **Anexo I,** e da Política de Segurança da Informação dos servidores já contratados e de novas contratações.
- Comunicar formalmente e imediatamente ao setor de Tecnologia da Informação toda e qualquer alteração no quadro funcional da Prefeitura de Maringá, admissões, demissões, alterações de cargos, funções, processos, entre outros, no prazo mínimo de 48 (quarenta e oito) horas, e de imediato em casos específicos, a fim de evitar acessos não autorizados e/ou desnecessários.
- Apoiar e promover com o setor de Tecnologia da Informação ações de conscientização e de capacitação em Segurança da Informação e Proteção de Dados Pessoais para todos os servidores, estagiários e demais agentes públicos do quadro funcional da Prefeitura Municipal de Maringá.
- Zelar e promover a devida proteção de dados pessoais, em conformidade com as políticas internas e legislação pertinentes.

- Promover, com o envolvimento do Comitê de Segurança da Informação, palestras de conscientização do quadro funcional em relação à importância da segurança da informação para as atividades institucionais da Prefeitura Municipal de Maringá.
- Elaborar, em parceria com o Comitê de Segurança da Informação, um plano de comunicação e disseminação da Política de Segurança da Informação.

Servidores, estagiários e agentes públicos – Usuários em geral

Servidores, estagiários e demais agentes públicos pertencentes ao quadro funcional da Prefeitura Municipal de Maringá, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação. Em atenção especial ao compromisso com os critérios legais e éticos que envolvem a instituição.

Será de inteira responsabilidade de servidores, estagiários e demais agentes públicos da Prefeitura Municipal de Maringá:

- Cumprir fielmente políticas, normas e procedimentos de Segurança da Informação, incluindo regras estabelecidas neste documento.
- Buscar orientação do superior quando houver dúvidas relacionadas à segurança da informação.
- Assinar o Termo de Responsabilidade, **Anexo I**, formalizando a ciência da Política de Segurança da Informação e das Normas de Segurança da Informação, bem como assumindo a responsabilidade pelo seu cumprimento.
- Proteger as informações contra o acesso, a modificação, a divulgação ou a destruição não autorizada pela Prefeitura Municipal de Maringá.
- Assegurar que os recursos tecnológicos sejam utilizados apenas para fins profissionais aprovados e de interesse da Prefeitura Municipal de Maringá.
- Prezar pela segurança das informações confidenciais, incluindo todo e quaisquer dados pessoais a que tiverem acesso.
- Atender à Lei Geral de Proteção de Dados Pessoais - LGPD, protegendo os dados a que tiver acesso ou que venha a manuseá-los, sempre em conformidade com os princípios previstos em Lei (qual a finalidade e dados necessários), procedimentos e medidas de segurança definidas pela Prefeitura Municipal de Maringá.
- Sanar dúvidas com o(a) Encarregado(a) de Proteção de Dados – DPO quando essas houver na aplicabilidade dos princípios previstos na Lei Geral de Proteção de Dados Pessoais.

- Encaminhar ao(a) Encarregado(a) de Proteção de Dados – DPO os fluxos de trabalhos com tratamento de dados para que estes sejam adequados à proteção de dados e analisadas as medidas de segurança para futura mitigação de riscos.
- Comunicar imediatamente ao superior direto sobre qualquer descumprimento ou violação da PSI e/ou de suas Normas e Procedimentos, assim como, quando se tratar de infrações administrativas causadas por servidores, estagiários e demais agentes públicos pertencentes ao quadro funcional da Prefeitura Municipal de Maringá, além de outras áreas, quando for necessário.
- Realizar o descarte adequado de documentos de acordo com seu grau de classificação.
- É de responsabilidade dos servidores, estagiários e demais agentes públicos o uso de senha de forma segura, devendo alterá-la conforme periodicidade determinada pela Prefeitura Municipal de Maringá.

Gestores de Pessoas e/ou Processos e/ou Contratos de Terceiros

Em relação à Segurança da Informação, cabe aos gestores de pessoas e/ou processos:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores, estagiários e agentes públicos sob sua gestão.
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da Política de Segurança da Informação da Prefeitura Municipal de Maringá.
- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação, assim como, observar e zelar pela aplicação das regras e legislação de Proteção de Dados Pessoais.
- Atender à Lei Geral de Proteção de Dados Pessoais, protegendo os dados a que tiver acesso ou que venha a manuseá-los, sempre em conformidade com os princípios previstos em Lei (qual a finalidade e dados necessários), procedimentos e medidas de segurança definidas pela Prefeitura Municipal de Maringá.
- Sanar dúvidas com o(a) Encarregado(a) de Proteção de Dados – DPO quando essas houverem na aplicabilidade dos princípios previstos na Lei Geral de Proteção de Dados Pessoais.
- Encaminhar ao(a) Encarregado(a) de Proteção de Dados – DPO os fluxos de trabalhos com tratamento de dados para que estes sejam adequados à proteção de dados e analisadas as medidas de segurança para futura mitigação de riscos.
- Solicitar ao(a) Encarregado(a) de Proteção de Dados – DPO a elaboração em contratos com prestadores de serviços, terceirizados e parceiros, quando estes

necessitarem ter contato com informações da Prefeitura Municipal de Maringá, de cláusula de responsabilidade, de proteção de dados pessoais, da ciência da Política de Segurança da Informação e de confidencialidade, exigindo o repasse das obrigações a seus próprios empregados e servidores.

- Elaborar, com o apoio da Secretaria de Gestão de Pessoas e de Tecnologia da Informação, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados.
- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade.
- Solicitar previamente a permissão de acesso ao setor de Tecnologia da Informação elencando os ativos de informação que serão oferecidos a terceiros.
- Garantir a implementação de mecanismos necessários para o descarte seguro das informações.
- Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender à Política de Segurança da Informação e as regras pertinentes à legislação de Proteção de Dados Pessoais com suporte, quando necessário, do(a) Encarregado(a) de Proteção de Dados - DPO.
- Comunicar imediatamente ao setor de Tecnologia da Informação toda e qualquer violação de segurança da informação, incluindo violação de dados pessoais, que deverá informar ao(a) Encarregado(a) de Proteção de Dados - DPO a ocorrência de infrações provenientes de servidores, estagiários, prestadores de serviços e demais agentes públicos, bem como, informar as demais áreas quando houver necessidades específicas.
- Tomar as decisões administrativas referentes aos descumprimentos da Política de Segurança da Informação da Prefeitura Municipal de Maringá.
- Colher e arquivar a assinatura do Termo de Responsabilidade, **Anexo II,** e ciência da Política de Segurança da Informação aos prestadores de serviço contratados e de novas contratações.

DESCRIÇÃO DAS ATIVIDADES

Diretrizes

As diretrizes e normas referentes à presente PSI são estabelecidas a seguir.

Interpretação

Esta PSI e seus documentos complementares devem ser interpretados dentro do contexto de uso de informações e recursos de TI. Tudo o que não estiver expressamente permitido

apenas poderá ser realizado após prévia autorização do Comitê de Segurança da Informação (CSI), devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

Propriedade

As informações geradas, acessadas, manuseadas, transmitidas, compartilhadas, armazenadas ou descartadas por servidores, estagiários prestadores de serviços e agentes públicos no exercício de suas atividades profissionais com a Prefeitura Municipal de Maringá, bem como os demais recursos tangíveis e intangíveis disponibilizados pelo órgão a esses atores são de sua propriedade exclusiva, as quais devem ser empregadas exclusivamente em atividades de interesse da empresa.

Proteção da Informação

As informações geradas, adquiridas, armazenadas, processadas, transmitidas e descartadas pela Prefeitura Municipal de Maringá devem ter mecanismos de proteção adequados, de forma a resguardar sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Os mecanismos de proteção devem estar em conformidade com a legislação vigente, e com a versão vigente das normas de Segurança da Informação da ISO 27001 para as informações tratadas pela empresa e da ISO 27701 para informações que envolvam dados pessoais.

Controle de Acesso às Informações

Toda informação utilizada pelas áreas, aplicações ou sistemas da Prefeitura Municipal de Maringá deve ter seu acesso controlado e monitorado e concedido apenas aos usuários que realmente necessitam do acesso aos dados para execução de suas atividades, sendo proibido os acessos não autorizados dos demais profissionais ao acervo físico e lógico da empresa.

Privacidade e Proteção de Dados

A Prefeitura Municipal de Maringá respeita a privacidade dos titulares de dados e garante a proteção e segurança dos dados pessoais em todo o seu ciclo de vida até o seu descarte final.

Responsabilidade em Relação a Segurança da Informação Tratadas

- O usuário é responsável pela segurança das informações a que tenha acesso.
- Os usuários devem notificar à equipe de Tecnologia da Informação os casos de violação das regras e eventuais falhas de Segurança da Informação mediante registro de incidente de segurança.
- Os gestores das áreas devem conscientizar usuários e visitantes da importância da Segurança das Informações na Prefeitura Municipal de Maringá do cumprimento ao disposto nesta política.

Gestão de Continuidade do Negócio

A Prefeitura Municipal de Maringá é responsável por elaborar e manter um plano de continuidade de negócios, de acordo com a sua necessidade, de forma a reduzir os impactos decorrentes da interrupção de serviços causada por desastres ambientais ou não, bem como falhas da segurança. Deve existir para cada situação um plano de continuidade, contendo informações mínimas para recuperação do serviço e integridade das informações.

Gestão de Riscos

A Prefeitura Municipal de Maringá é responsável por implementar e manter um processo para análise e gestão dos riscos, objetivando minimizar possíveis impactos nas informações tratadas e mantidas no ambiente da empresa.

O processo de gestão de riscos deve definir os ativos a serem protegidos, bem como os dados pessoais mantidos pela empresa.

O processo de gestão de risco deve definir e implantar controles para a identificação e tratamento de problemas relacionados à segurança e proteção de dados pessoais.

Tratamento de Incidentes

Devem ser estabelecidos procedimentos formais para notificação de incidentes de segurança da informação, bem como procedimentos de resposta a incidentes, sendo obrigatória a notificação desses incidentes por todos que possam estar envolvidos.

REQUISITOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação – PSI deve ser comunicada para a gestão municipal, servidores, estagiários, prestadores de serviços e demais agentes públicos que possuem algum tipo de relação com a Prefeitura Municipal de Maringá, visando a efetividade e a real cultura de uso ético e legal dos recursos tecnológicos, bem como, a segurança da informação da Prefeitura.

Sempre que um convênio ou contratação de empresa terceirizada envolver acesso a informações e/ou recursos tecnológicos da Prefeitura, os gestores do contrato devem comunicar ao(a) Encarregado(a) de Proteção de Dados – DPO para providenciar as cláusulas contratuais de proteção de dados e para a Agência Maringá de Tecnologia e Inovação - AMTECH tomar as devidas providências técnicas necessárias.

A PSI e as Normas serão revisadas e atualizadas com periodicidade mínima de um ano ou sempre que houver um fato novo e relevante de ser detalhado, conforme análise e aprovação administrativa.

Todos os contratos da Prefeitura Municipal de Maringá devem constar cláusulas relacionadas à proteção de dados pessoais e confidencialidade para garantir a aplicabilidade dos requisitos solicitados na Lei Geral de Proteção de Dados, sendo estes os princípios e embasamento legal previstos.

A responsabilidade em relação à segurança da informação deve ser atribuída na fase de contratação do funcionário, de forma a ser incluída nos contratos e monitorada durante a sua vigência.

Para gestão municipal, servidores, estagiários, prestadores de serviços e demais agentes públicos, sendo estes contratados em período anterior à publicação desta política e que não tenham assinado os respectivos documentos, deverá ser entregue um Termo de Ciência e Responsabilidade da PSI para a respectiva assinatura de forma física ou eletrônica.

A gestão municipal, assim como, todos os servidores, estagiários, prestadores de serviços e demais agentes públicos que possuem algum tipo de relação com a Prefeitura Municipal de Maringá devem passar por treinamento e conscientização sobre os procedimentos de segurança e o uso correto dos ativos oferecidos pela instituição. A finalidade é minimizar possíveis riscos de segurança, explicitar as responsabilidades e comunicar os procedimentos para a notificação de incidentes.

Todos os requisitos de segurança da informação e os aspectos legais, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de um projeto ou sistema. Também devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução.

Sempre que a Prefeitura Municipal de Maringá julgar necessário a aplicação de ações para reduzir os riscos dos ativos de informação, serão criados e implementados controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas.

Nos ambientes de produção e de desenvolvimento tecnológico devem ser segregados e rigidamente controlados.

Um plano de contingência e continuidade do negócio deverá ser implementado e testado. O objetivo é reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, por meio da combinação de ações de prevenção e recuperação.

Os ativos críticos ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas aos riscos identificados, além de ter o acesso controlado, registrado e monitorado.

Todo ativo de informação deve ser protegido de divulgação, modificação, furto ou roubo por meio da aplicação de controles.

Devem ser estabelecidas e comunicadas normas e responsabilidades pela propriedade e custódia dos ativos de informação. Bem como a instauração de procedimentos e responsabilidades específicas para o uso e o gerenciamento dos ativos de informação

oferecidos pela Prefeitura Municipal de Maringá, quando estiverem fora das instalações da instituição.

Os dados coletados e armazenados devem ser segmentados a fim de que sejam aplicados controles especiais e sejam adequados às legislações pertinentes sobre a proteção de dados pessoais.

UTILIZAÇÃO DE REDE E INTERNET

A Prefeitura Municipal de Maringá poderá permitir acesso à Internet e a navegação em sites de conteúdo, sempre de acordo com a sua Política de Segurança da Informação e bloqueios de sites classificados como inseguros ou não confiáveis.

É explicitamente proibido a transferência de arquivos por meio de quaisquer protocolos, aplicativos ou ferramentas que não forem previamente e explicitamente aprovados pelo departamento de Tecnologia da Informação.

A Prefeitura Municipal de Maringá se reserva no direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos.

Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade da Prefeitura Municipal de Maringá, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Internet disponibilizada pela Prefeitura Municipal de Maringá aos seus servidores, estagiários e agentes públicos, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que seja autorizada e não prejudique o andamento dos trabalhos nos setores/unidades.

Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

PARTICULARIDADES DO USO DE *E-MAIL*/CORREIO ELETRÔNICO

O correio eletrônico (*e-mail*) é uma das principais formas de comunicação. No entanto, é considerada uma das principais vias de disseminação de *malwares*. Diante disso, surge a necessidade de normatização da utilização deste recurso, tais como:

1) O *e-mail* corporativo é destinado a fins profissionais, relacionados às atividades dos servidores.
2) Os *e-mails* enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear *spams*, *malwares* ou outros conteúdos maliciosos que violem a Política de Segurança da Informação.

3) É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções.

4) É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas.

5) É proibido enviar qualquer mensagem por meios eletrônicos que torne a Prefeitura Municipal de Maringá vulnerável a ações civis ou criminais.

6) É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários.

7) Produzir, transmitir ou divulgar mensagem que:

    - Contenha ameaças eletrônicas, como: *spam*, *phishing*, *mail bombing*, *malwares*.
    - Contenha arquivos com código executável (*.exe, .cmd, .pif, .js, .hta, .src, cpl, .reg, .dll, .inf*) ou qualquer outra extensão que represente um risco à segurança.
    - Visa obter acesso não autorizado a outro computador, servidor ou rede.
    - Visa interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
    - Visa burlar qualquer sistema de segurança.
    - Visa vigiar secretamente ou assediar outro usuário.
    - Visa acessar informações confidenciais sem a explícita autorização do proprietário.
    - Tenha conteúdo considerado impróprio, obsceno ou ilegal.
    - Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros.
    - Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

8) O uso de *e-mails* pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:

    - Não contrariar as normas aqui estabelecidas.
    - Não interferir, negativamente, nas atividades profissionais individuais ou de outros servidores.

- Não interferir, negativamente, na Prefeitura Municipal de Maringá e na sua imagem.

PROTEÇÃO DE *MALWARE* E GERENCIAMENTO DE SI

Detecção e remoção de *malware* nos equipamentos, estações de trabalho e servidores com antivírus.

Realizado monitoramento de rede através de Firewall NGFW combinada a solução de antivírus corporativa, com gerenciamento pelo departamento de Tecnologia da Informação, com detecção automática para tomada de decisões, bloqueando o ataque ou movendo para quarentena.

Relatórios para acompanhamento de ambiente e aplicação dos devidos controles.

UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHOS

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os servidores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

1) É de responsabilidade do servidor do equipamento zelar por ele, mantendo-o em boas condições.
2) Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio.
3) É vedada a abertura de computadores para qualquer tipo de reparo pelos servidores. Caso seja necessário, o reparo deverá ser feito pela equipe competente.
4) As estações de trabalho só estarão acessíveis aos servidores através de contas de usuário limitadas.
5) É proibida a instalação de *softwares* ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe competente.
6) É proibida a instalação ou uso de softwares que não possuam licença e/ou não sejam homologados pela equipe competente.
7) As estações de trabalho devem permanecer bloqueadas (*logoff*) nos períodos de ausência dos servidores.
8) Os documentos e arquivos relativos à atividade desempenhada pelos servidores deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de *backup* e controle de acesso adequado.

9) Documentos críticos, com dados pessoais e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina.

10) É proibido o uso de estações de trabalho para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular.
- Hospedar ou consumir pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

11) O técnico de informática não se responsabiliza por prestar manutenção ou instalar *softwares* em computadores que não sejam os da instituição.

12) As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

BRING YOUR DEVICE – BYOD (USO DO EQUIPAMENTO PARTICULAR E DISPOSITIVO MÓVEL)

A utilização de dispositivos móveis, tais como, *smartphones*, *notebooks* e *tablets* pessoais deve ser solicitada e formalizada pelo gestor da área ou superior, através de abertura de chamado junto à TI, informando quais recursos ou dados corporativos o dispositivo terá acesso na rede corporativa da Prefeitura Municipal de Maringá, conforme diretrizes citadas abaixo:

a) Não é permitida a instalação de licenças corporativas em dispositivos móveis BYOD.

b) Apenas os dispositivos móveis BYOD homologados pela área de tecnologia da informação da Prefeitura Municipal de Maringá poderão ter acesso à rede de dados corporativos.

c) A área de tecnologia da informação da Prefeitura Municipal de Maringá é responsável pela gestão dos dispositivos móveis BYOD, inclusive quanto ao monitoramento e controle.

d) Em caso de desligamento do servidor que possua dispositivo móvel BYOD incorporado à rede corporativa Prefeitura Municipal de Maringá, o gestor da área ou superior deve comunicar, através de abertura de chamado técnico, e solicitar que toda informação da Prefeitura no dispositivo seja salva em ativos físicos corporativos e removida do referido dispositivo.

e) A Prefeitura Municipal de Maringá não se responsabilizará pelo reembolso ou porcentagem do dispositivo móvel BYOD incorporado à rede corporativa da Prefeitura Municipal de Maringá, nos casos de roubo, dano, furto, uso indevido e condutas assemelhadas.

f) Sempre que a necessidade puder ser atendida através de equipamentos corporativos, sem prejuízos significativos ao usuário, resguarda-se a equipe de TI o direito de orientar o uso do equipamento do município, não necessitando então do ingresso do equipamento BYOD na rede corporativa.

DESCARTE DE MÍDIAS

O descarte adequado de mídias deve estar de acordo com seu grau de classificação e diretrizes citadas abaixo:

a) As mídias contendo informações sensíveis e confidenciais, a exemplo das mídias que contém dados pessoais, devem ser guardadas e destruídas de forma segura e protegida, como por exemplo, por meio de incineração ou trituração, ou pela remoção dos dados para uso por outra aplicação dentro da organização.

b) A depender da situação pode ser mais fácil implementar a coleta e o descarte seguros de todas as mídias a serem inutilizadas do que tentar separar apenas aquelas contendo informações sensíveis e confidenciais, a exemplo das mídias que contém dados pessoais.

c) Existem empresas especializadas que oferecem serviços de coleta e descarte de mídias. Recomenda-se que sejam tomados os devidos cuidados na seleção destas empresas, exigindo referências, experiências e controles adequados de descarte.

d) Equipamentos que contenham dados que precisem de um armazenamento de maior tempo, conforme exigências legais, deverá ser feito descarte de forma segura, podendo até mesmo inutilizar o disco (HD).

Como exemplos de dados com maior tempo de armazenamento temos:

a) Folha de Pagamento: *10 (dez) anos – art. 225, I, § 5º do Decreto 3.048/99*.

b) PCMSO, PPP, PPRA, LTCAT: *20 (vinte) anos - IN INSS 99/2003, Art. 148, § 11o; Portaria SST 24/94, item 7.4.5.1; Portaria MTE 25/94, item 9.3.82*.

c) Exames médicos admissionais, periódicos, retorno, mudança de função e demissional, incluindo avaliação clínica e exames complementares: *20 (vinte) anos - NR7, subitens 7.4.1, 7.4.2, 7.4.5 e 7.4.5.1*.

d) FGTS, GFIP, GRFP: *30 (trinta) anos - Lei 8.036/90, Art. 23, § 5o - Súmula 362, TST*;

e) Livro de atas da CIPA, livro de inspeção do trabalho, livro ou ficha de registro de empregado: *prazo indeterminado*.

TRABALHO REMOTO

Os servidores que estão trabalhando fora do ambiente da Prefeitura Municipal de Maringá, no modelo de trabalho remoto (*home office*), devem exercer a modalidade de trabalho remoto apenas quando houver prévia e expressa autorização da chefia imediata. Os servidores devem seguir as regras de confidencialidade, sigilo e não divulgação de qualquer dado pessoal a que tenha acesso em decorrência de suas funções, sejam eles relativos a cidadãos, outros servidores, prestadores de serviços, terceiros, agentes públicos ou quaisquer outras pessoas envolvidas com a Prefeitura Municipal de Maringá.

Compete aos servidores:

a) Tratar apenas os dados pessoais necessários às suas funções, salvo autorização expressa da Prefeitura Municipal de Maringá.

b) Jamais utilizar dados pessoais, documentos ou materiais a que tenha acesso para finalidades alheias à prestação de serviço para o qual foi admitido.

c) Cuidar e proteger dos dispositivos eletrônicos, documentos e quaisquer outras ferramentas utilizadas no trabalho remoto da mesma forma como no trabalho presencial.

POLÍTICA DE SENHA

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do servidor, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

a) A senha é de total responsabilidade do servidor, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação.

b) A senha inicial é fornecida ao próprio servidor e deve ser modificada no seu primeiro acesso. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade dos servidores.

c) É proibido o compartilhamento de *login* para funções de administração de sistemas.

d) As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor etc.).

As senhas deverão seguir os seguintes pré-requisitos:

a) Tamanho mínimo de 08 (oito) caracteres.

b) Existência de caracteres pertencentes aos seguintes grupos: letras maiusculas, letras minúsculas, números.

c) Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge etc.).

O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:

a) Desligamento do servidor.

b) Mudança de função do servidor.

c) Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

Para os cancelamentos acima mencionados, o departamento responsável por admissões e exonerações da Secretaria de Gestão de Pessoas (SEGEP) ficará responsável por informar prontamente ao departamento competente acerca dos desligamentos e mudança de função dos servidores e agentes públicos.

MÉTODO DA MESA LIMPA

Todos os servidores deverão obedecer às regras de limpeza e organização do ambiente de trabalho a fim de não expor desnecessariamente informações classificadas.

Os documentos impressos e anotações que precisem estar em um papel (impresso ou anotações) devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados disponíveis em seu departamento ou qualquer dependência da empresa que forneça segurança e proteção a esses materiais.

Toda informação que permanecer nas mesas poderá e deverá ser destruída pelo servidor responsável ou por qualquer outro servidor que for designado. Desta forma, será praticada as boas práticas de proteção de dados pessoais da Prefeitura Municipal de Maringá.

SEGURANÇA DO AMBIENTE DE TECNOLOGIA DA INFORMAÇÃO - TI

Estrutura Física do Datacenter

As máquinas (servidores) que armazenam sistemas da Prefeitura Municipal de Maringá estão em área protegida – Datacenters localizados nessa instituição ou em ambiente em nuvem.

Todos os sistemas ou equipamentos classificados como críticos devem ser mantidos em áreas seguras do *Datacenter*.

A entrada aos *Datacenters* tem acesso devidamente controlado e monitorado. As permissões de acesso físico às áreas restritas do *Data Center* devem ser revisadas mensalmente.

As áreas do *Datacenter* devem ser protegidas com barreiras de segurança ou mecanismos de acesso, de forma a impedir o acesso não autorizado.

A porta do *Datacenter* deve permanecer fechada, com mecanismo de autenticação individual, quando possível.

O acesso às dependências dos *Datacenters* com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de segurança e mediante supervisão.

O acesso ao *Datacenter* sem as devidas identificações só poderá ocorrer em emergências, quando a segurança física deste for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Caso haja necessidade do acesso não emergencial, o solicitante deverá requisitar a autorização com antecedência a qualquer servidor responsável pela administração de liberação de acesso.

O *Datacenter* deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração dos servidores designados para a limpeza.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do *Datacenter* somente se dará com o preenchimento da solicitação de liberação pelo servidor solicitante.

Estrutura Lógica do *Datacenter*

Na política de segurança da Informação estabelecida pela Prefeitura Municipal de Maringá, define-se que o departamento de TI deve ser o único a ter permissão para ler/editar as informações, obedecendo às atribuições de sua área de atuação.

O objetivo da segurança lógica no *Datacenter* é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados.

Somente os servidores credenciados e autorizados pela administração podem ter acesso aos dados armazenados.

Os *logs* dos ativos de rede devem ser monitorados constantemente a fim de evitar acessos indevidos.

Estrutura Organizacional

O Departamento de Tecnologia da Informação terá como competências:

- Coordenar, executar e acompanhar as atividades de tratamento e resposta a incidentes na rede corporativa da Prefeitura Municipal de Maringá.
- Coordenar, executar e acompanhar a análise dos sistemas comprometidos buscando, causas, danos e responsáveis.
- Coordenar, executar e acompanhar a avaliação, auditoria e testes das condições de segurança da rede corporativa da Prefeitura Municipal de Maringá.
- Coordenar, executar e acompanhar a análise dos ativos de informação e estruturas constitutivas dos ambientes de tecnologia da informação, presentes na Prefeitura Municipal de Maringá.
- Apoiar o desenvolvimento de um Plano de Conscientização em segurança da informação e comunicações a fim de que todos os Servidores da Prefeitura Municipal de Maringá tenham ciência do assunto.
- Manter em condições adequadas de segurança o acervo de informações relativas aos incidentes da rede corporativa da Prefeitura Municipal de Maringá.
- Participar da definição e acompanhar os indicadores de incidentes na rede corporativa da Prefeitura Municipal de Maringá.
- Prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicações.
- Participar na proposição de recursos necessários às ações de segurança da informação e comunicações.
- Executar outras atividades correlatas que lhe forem demandadas.

CONTROLE DE ACESSO

Todos os sistemas de informação da Prefeitura Municipal de Maringá devem estar integrados a um sistema de controle de acesso definido pelo Departamento de Tecnologia da Informação.

As informações e os serviços utilizados pelos usuários são de exclusiva propriedade da Prefeitura Municipal de Maringá, não podendo ser interpretados como de uso pessoal.

Todos os profissionais e servidores da Prefeitura Municipal de Maringá devem ter ciência de que o uso das informações e dos sistemas de informação podem ser monitorados, e que os registros assim obtidos poderão ser utilizados para detecção de violação da Política e das Normas de Segurança da Informação.

Para acessar os serviços de rede (servidor de arquivos, internet, impressão), ao sistema ERP, *e-mail* e outros, o usuário recebe um “nome de usuário” e “senha”, de uso privativo, utilizados na sua identificação e que não devem ser divulgados a terceiros.

O usuário assume todas as responsabilidades decorrentes de seus atos e de sua conduta como usuário dos serviços, respondendo, ainda, pelos atos que terceiros praticarem em seu nome, por meio de uso de seu “nome de usuário” e “senha”.

A concessão de acessos (recursos ou sistemas) deve ser aprovada pelo gestor da informação. Além disso, deve ser instituída a segregação de função de acordo com nível funcional ou responsabilidade assim como uma revisão periódica dos acessos concedidos, a fim de evitar acessos indevidos. Para mais informações, consulte a Política de Segurança da Informação - Controle de Acesso.

O acesso a sala do *Datacenter* onde estão todos os servidores, *switches*, links de internet entre outros ativos da Prefeitura Municipal de Maringá, é feito através de sistema biométrico. Apenas servidores da TI e diretoria poderão obter acesso a esta sala.

O cadastro no sistema de acesso ao *Datacenter* deverá ser feito pelo Departamento de TI através do *software W-Access*. Todos os acessos são registrados e poderão ser analisados e auditados posteriormente.

BACKUP

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de *Backup* (cópia de segurança).

Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra.

Caso um incidente de perda de dados venha a ocorrer, estabelecem-se as regras:

a) Todo sistema ou informação relevante para a operação dos negócios da Prefeitura Municipal de Maringá deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição.

b) As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e provocar o departamento competente sobre a necessidade de *backup* deles, sugerindo o tempo de retenção destas cópias.

c) Todos os *backups* devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informação.

SEGURANÇA FÍSICA DO AMBIENTE

É necessário estabelecer o perímetro de segurança física de modo a preservar o acesso somente a pessoas autorizadas. Além disso, deve ser instituído de modo obrigatório o uso de identificação visual (crachá) para visitantes, clientes, fornecedores e prestadores de serviço.

Para controle e liberação de acesso de servidores, deve-se utilizar sistema de registro de acesso físico por meio de sistemas de catracas, torniquetes e biometria.

TRATAMENTO DE INCIDENTES

Todo e qualquer servidor deve estar ciente que o tratamento de incidentes visa minimizar os impactos de um incidente nos processos em curso na Prefeitura Municipal de Maringá, sendo assim voltado à redução e contenção dos efeitos causados por eventos técnicos indesejáveis e seu monitoramento.

Quaisquer falhas, anomalias, ameaças ou vulnerabilidades observadas devem ser notificadas o mais rápido possível para o Departamento de Tecnologia da Informação.

Devem-se obter informações, inclusive quantitativas, acerca dos incidentes ocorridos, pois estes servem como indicadores da eficácia das políticas e da relação custo-benefício dos controles de segurança. São elas:

- Natureza
- Causas
- Data da ocorrência
- Frequência
- Custos resultantes.

Após o levantamento dos dados, o incidente deverá ser tratado e documentado, visando manter um histórico dos incidentes e ainda uma cultura acerca deles.

Os ataques de rede distribuídos muitas vezes são chamados de ataques de negação de serviço distribuído (DDoS) e o monitoramento e a detecção deste tipo de ataques são realizados com *Firewall***.** Na detecção de um ataque DDoS, o sistema irá bloquear os principais endereços de origem.

O sistema está preparado para mitigar ataques, assim como, monitorar internamente seus arquivos contra ataques de código maliciosos. Quando um ataque é detectado pelo

sistema, o administrador é notificado e este irá avaliar se foi de fato um ataque ou um falso positivo.

Caso sejam detectados códigos maliciosos, eles são imediatamente interrompidos e suas origens isoladas até a avaliação do administrador.

Tipos de tratamento de incidentes:

Serviços Reativos

Comporta neste tipo de serviço o tratamento de Incidentes de Segurança em Redes Computacionais, tratamento de Artefatos Maliciosos e tratamento de Vulnerabilidades.

Serviços Proativo

Comporta neste tipo de serviço a detecção de Intrusão.

VIOLAÇÃO DA POLÍTICA E PENALIDADES

As violações de segurança devem ser informadas à área de Segurança da Informação, seguindo o fluxo de comunicação e, eventualmente, uma matriz RACI – matriz de responsabilidades definida pela Prefeitura Municipal de Maringá.

Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

a) Uso ilegal de *software*.
b) Introdução (intencional ou não) de vírus de informática.
c) Tentativas de acesso não autorizado a dados e sistemas.
d) Compartilhamento de informações sensíveis ou não com terceiros não autorizados.
e) Divulgação de informações internas e não públicas da Prefeitura de Maringá.

Os princípios de segurança estabelecidos na presente política possuem total aderência da administração da Prefeitura Municipal de Maringá e devem ser observados por todos na execução de suas funções.

A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma, quando couber, sujeita os servidores às sanções previstas na Lei Complementar n.º 239/1998, Estatuto do Servidor Público do Município de Maringá.

Em caso de dúvidas quanto aos princípios e responsabilidades descritas nesta norma, o servidor deve entrar em contato com o canal de atendimento da segurança da informação (departamento de TI).

CONSCIENTIZAÇÃO E CAPACITAÇÃO

Os usuários devem ser instruídos para a correta utilização das informações, dos recursos computacionais, sistemas, aplicações e serviços disponibilizados pela Prefeitura Municipal de Maringá.

A Prefeitura deverá manter um plano de capacitação em segurança da informação e proteção de dados pessoais voltada aos trabalhadores, cujas atividades sejam correlatas aos assuntos citados anteriormente.

CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas por meio do e-mail ***segurancainformacao@maringa.pr.gov.br*** ao setor de Tecnologia da Informação - TI para avaliação e decisão.

Esta entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão da Administração, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento ou, categoricamente, deverá ser revista no prazo máximo de 12 (doze) meses.

Esta PSI, bem como os demais documentos que a complementam, encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao Departamento de Tecnologia da Informação.

O não cumprimento da Política de Segurança da Informação sujeitará o servidor, estagiário, prestador de serviço e outros agentes públicos que possuem vínculo com a Prefeitura de Maringá, às sanções previstas na Lei Complementar n.º 239/1998, Estatuto do Servidor Público do Município de Maringá, bem como as sanções cíveis e penais oportunamente cabíveis.

HISTÓRICO DE REVISÕES

Versão	Data	Responsável	Controle de modificações
1.0	23/08/2023	FIA	Criação do Documento
2.0	20/03/2024	SECCOMPLIANCE e AMTECH	Correção/Revisão do Documento