Política de Segurança da Informação

Sumário

1. Objetivo

Orientar estrategicamente as questões relacionadas à segurança da informação, definindo diretrizes para proteção, preservação e descarte de informação no ambiente convencional ou de tecnologia da EMAE, abrangendo, sem restrições, suas subsidiarias.

2. Referências

2.1 Lei nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD).

2.2 Decreto nº 9.637, de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.

2.3 Portaria nº 93, de 26 de setembro de 2019, Glossário de Segurança da Informação.

2.4 ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

2.5 ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

2.6 000.05.RE.005 - Código de Conduta Ética e Integridade da EMAE.

2.7 000.05.PO.015 – Política de Privacidade de Dados Pessoais da EMAE.

3. Princípios

3.1 Garantia de disponibilidade, para que a informação esteja acessível e utilizável sob demanda a toda empresa.

3.2 Garantia de integridade da informação, para que não seja modificada ou destruída de maneira não autorizada ou acidental.

3.3 Garantia de confidencialidade da informação, para que não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

3.4 Garantia de autenticidade de autoria e origem da informação, para que sejam sempre identificáveis.

4. Diretrizes

4.1. O ativo "informação"

4.1.1 Toda informação utilizada pela EMAE é um ativo que possui valor e deve ser gerenciada adequadamente ao longo de todo seu ciclo de vida, para que esteja disponível para acesso pelo público adequado, protegida contra manipulação indevida, com tratamento adequado ao seu grau de sigilo ou restrição de acesso e passível de rastreamento.

4.2. Proprietário da informação

4.2.1 A EMAE é proprietária e a detentora do direito de uso exclusivo das informações geradas, armazenadas, processadas ou transmitidas no ambiente convencional ou de tecnologia.

4.3. Classificação da informação

4.3.1 As informações utilizadas na EMAE devem ser classificadas a partir de metodologias e critérios definidos em documentos normativos internos específicos, quanto ao seu grau de sigilo ou nível de restrição de acesso, considerando os processos e atividades nas quais estão inseridas, a fim de assegurar que essas informações recebam um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a EMAE.

4.4. Utilização da informação e dos recursos corporativos

4.4.1 O gestor de cada informação deve determinar a autorização de acesso, incluindo os relacionados ao sistema de gestão empresarial, levando em consideração o sigilo adequado e a necessidade de acesso para cada tipo de público, no cumprimento dos objetivos estratégicos da EMAE.
4.4.2 O acesso à informação deve ser autorizado apenas para os colaboradores que dela necessitem para o desempenho de suas atividades profissionais.
4.4.3 Cada colaborador deve acessar apenas as informações ou os sistemas previamente autorizados. Qualquer tentativa não autorizada de acesso à informação ou sistema deve ser considerada uma falta disciplinar.
4.4.4 A credencial (*login* e senha) concedida a um colaborador é de uso individual, intransferível e de seu conhecimento exclusivo.
4.4.5 Todo e qualquer uso dos recursos corporativos da EMAE, sejam recursos físicos, lógicos ou tecnológicos, não deve violar qualquer tipo de legislação e de normativos internos ou externos à Empresa, bem como o Código de Conduta e Integridade da EMAE.
4.4.6 Para garantir o cumprimento desta política, a utilização dos recursos corporativos deve ser registrada e monitorada pela EMAE, não devendo o colaborador ter expectativa de sigilo em sua utilização.

4.5. Proteção da informação

4.5.1 A segurança da informação deve ser obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e sistemas.
4.5.2 Os colaboradores devem preservar a integridade de documentos, registros, cadastros e sistemas de informação da EMAE, em todos os meios utilizados pela EMAE, tanto físico quanto eletrônico.
4.5.3 Os gestores das áreas devem providenciar proteção e controle de acesso físico e lógico aos seus recursos de informação, compatível com o seu nível de criticidade e/ou classificação.
4.5.4 Todo incidente que afetar a segurança da informação deve ser reportado à área de suporte e infraestrutura de TI.
4.5.5 Os riscos de segurança da informação devem ser identificados, quantificados e priorizados para que se adotem medidas de proteção adequada.
4.5.6 A área de suporte e infraestrutura de TI deve manter registros atualizados dos indicadores de segurança da informação, bem como a adequada manutenção da arquitetura, dos ativos tecnológicos, das configurações e das soluções de segurança em uso na EMAE.

4.6. Sigilo da informação

4.6.1 Os colaboradores da EMAE não devem divulgar ou fazer uso de informações corporativas em benefício próprio ou de terceiros, não importando o tipo de mídia ou suporte utilizado.

4.7. Continuidade do uso da informação

4.7.1 Os recursos de ambiente convencional ou de tecnologia utilizados nas atividades de gestão, operacionais e de suporte da EMAE, devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade definidos.
4.7.2 Os gestores das áreas devem definir e implementar medidas de prevenção e recuperação para situações de desastre e contingência, que devem contemplar os colaboradores e os recursos de tecnologia e de infraestrutura necessários.

4.8. Relacionamentos formais com terceiros

4.8.1 Todos os relacionamentos formais com terceiros (contratos, convênios, dentre outros) em que haja o compartilhamento de informações da EMAE e/ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos corporativos devem ser precedidos por termos de confidencialidade e conter cláusulas que tratem especificamente de privacidade e segurança da informação.

4.9. Temporalidade da informação

4.9.1 A EMAE deve garantir que qualquer informação com valor comprobatório para fins de auditorias, de conformidade e judiciais seja preservada na forma e pelos prazos necessários.

4.10. Capacitação

4.10.1 A EMAE deve incluir a segurança da informação em seus programas de capacitação.

4.11. Tratamento de dados pessoais

4.11.1 A EMAE deve assegurar o adequado tratamento de dados pessoais, conforme estabelecido nos termos da Lei nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD).

4.12. Violações e penalidades

4.12.1 O descumprimento de algum dos princípios, bem como a mera tentativa de burla às diretrizes desta política ou aos controles estabelecidos pela EMAE, quando constatada, deve ser tratado como uma violação e pode resultar na adoção de medidas disciplinares, sem prejuízo da adoção de medidas administrativas e/ou judiciais, quando se tratar de infrações contratuais ou legais.

5. Responsabilidades

5.1 **Diretoria Colegiada da EMAE** – aprovar esta política e deliberar sobre as diretrizes estratégicas de segurança da informação para nortear o processo de implementação na EMAE.
5.2 **Área responsável pela segurança da informação na EMAE** – elaborar políticas, normas e procedimentos que padronizem ações de Segurança da Informação na EMAE.
5.3 **Departamento de Tecnologia da Informação** – gerir os processos e planejamento de ações de desdobramento desta política, coordenar o tratamento de incidentes de segurança da informação, apoiar a gestão dos riscos de segurança da informação definindo controles adequados em conjunto com os Proprietários do Risco.
5.4 **Gerentes e coordenadores** – zelar pelas informações produzidas por sua equipe e autorização de acesso e contingência, bem como o mapeamento, implantação e operacionalização de seus controles, fazendo cumprir as diretrizes desta política.
5.5 **Áreas responsáveis pela infraestrutura de tecnologia da automação e de tecnologia da informação** – prevenir e proteger instalações e ativos de informação contra acessos não autorizados, danos ou comprometimento de informações. Compete ainda avaliar regularmente o ambiente e encaminhar relatório das vulnerabilidades encontradas nas medidas de segurança física ao responsável pela segurança da informação.
5.6 **Colaboradores** – cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, por meio do uso de forma responsável, profissional, ética e legal das informações corporativas, respeitando os direitos e as permissões de uso concedidas pela EMAE.
5.7 **Áreas de gestão de pessoas** – promover ações de treinamento e desenvolvimento referentes à segurança da informação, incluindo aspectos técnicos, normativos e comportamentais.