ÍNDICE

1. LISTA DE SIGLAS

- **PSI** – Política de Segurança da Informação
- **TI** – Tecnologia da Informação
- **SI** – Segurança da Informação
- **EMAP** – Empresa Maranhense de Administração Portuária

2. DOCUMENTOS DE REFERÊNCIA

- Lei nº 12.527, de 18 de novembro de 2011 - Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.
- Lei nº. 9.610, de 18 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.
- Lei nº. 9.279, de 14 de maio de 1996, que regula direitos e obrigações relativas à propriedade industrial.

- Decreto nº 7.845, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
- Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.
- Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- Norma Complementar nº 07/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
- ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação – Requisitos.
- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação -Técnicas de segurança - Código de prática para controles de segurança da informação.
- ABNT NBR ISO/IEC 22301:2013 - Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos.

3. DEFINIÇÕES

- **Segurança da informação:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade das informações.
- **Empregados:** todo aquele que por força de lei, faz parte do quadro de funcionários efetivos da EMAP, sendo em regime permanente ou temporário.
- **Prestadores de serviço:** todo e qualquer funcionário de empresa contratada pela EMAP que utiliza um ou mais ativos de informação de propriedade da EMAP, ou sob sua responsabilidade, para realização de suas atividades.
- **Setores:** todas as áreas da estrutura organizacional da EMAP.
- **Cópia de segurança:** uma cópia exata de um documento eletrônico, programa de computador ou disco, feito para fins de arquivamento ou para salvaguardar arquivos, na eventualidade de danificação ou destruição do original.
- **Integridade:** característica de que a informação não sofreu alterações ou

exclusões de maneira não autorizada ou acidental.

- **Confidencialidade:** característica de que a informação não esteja disponível ou divulgada a pessoa física, sistema, órgão ou entidade não autorizada.
- **Disponibilidade:** característica de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- **Ativos de informação:** os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal;
- **Inventário de Ativos de Informação:** é um processo interativo e evolutivo, que dentre outras etapas prevê a identificação e classificação de ativos de informação.
- **Dispositivos móveis:** equipamentos portáteis dotados de capacidade computacional, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets.
- **GETIN:** Gerência de Tecnologia da Informação.
- **Infraestrutura interna:** conjunto de ativos de informações interligados localmente com o objetivo de disponibilizar serviços aos usuários de TI da EMAP.
- **Usuários de TI:** Todos os empregados, prestadores de serviço, estagiários ou pessoas que no exercício de suas atividades na empresa tenham acesso as informações e aos ativos de informação.
- **Dispositivos móveis:** equipamentos portáteis dotados de capacidade computacional, entre os quais se incluem, não se limitando a estes: notebooks, netebooks, smartphones, tablets.
- **Trabalho remoto:** Possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc. da infraestrutura interna, sem estar fisicamente na EMAP, utilizando-se de sistema de informação do tipo VPN.
- **Sistema de informação:** Programa de computador composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual.
- **Continuidade de Negócios:** capacidade estratégica e tática da empresa de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

- **Resiliência:** poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.
- **Ciclo de vida da informação:** período de tempo entre a criação ou aquisição da informação, passando por sua manutenção, armazenamento, transporte e descarte.
- **Algoritmo:** função matemática utilizada na cifração e na decifração de informações restritas.
- **Algoritmo Assimétrico:** função matemática que utiliza chaves criptográficas distintas para cifração e decifração de informações restritas.
- **Algoritmo Simétrico:** função matemática que utiliza a mesma chave criptográfica tanto para a cifração quanto para a decifração de informações restritas.
- **Certificado Digital:** funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas por um gestor, associa uma entidade (pessoa ou sistema informatizado) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.
- **Cifração:** ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis por pessoas não autorizadas a conhecê-la.
- **Chave ou chave criptográfica:** valor que trabalha com um algoritmo criptográfico para cifração ou decifração.
- **Controle criptográfico:** sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.
- **Credencial:** permissões, concedidas por gestor competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.
- **Decifração:** ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.
- **Gestão de Riscos:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que

estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

- **ICP-Brasil:** Instituído pela Medida Provisória nº 2.200-2, de 24 de Agosto de 2001, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual de pessoas físicas, pessoas jurídicas ou sistemas informatizados associados a pessoas físicas ou jurídicas.
- **VPN:** Virtual Private Network. Rede privada construída sobre uma infraestrutura de rede pública, com recursos para proteção dos dados transmitidos contra interceptações e capturas.

4. OBJETIVO

A informação é um dos principais bens de qualquer organização. Assim, a EMAP estabelece a presente Política de Segurança da Informação, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações da organização, dos clientes e do público em geral.

5. ESCOPO

Esta Política de Segurança da Informação da EMAP:

- estabelece regras que direcionam a Gestão da Segurança da Informação na Empresa, subscrevendo princípios de confidencialidade, integridade e disponibilidade das informações de sua propriedade ou sob sua custodia, com vistas a garantir a continuidade nos processos imprescindíveis, preservação e valores institucionais e qualidade na prestação dos seus serviços.
- deve ser observada em todos os Setores por todos os empregados e prestadores de serviço, sendo diretrizes de conduta para a Segurança da Informação dentro da Empresa.
- está em conformidade com a legislação vigorante, as normas técnicas relacionadas a temática e as melhores práticas de Segurança da Informação.
- praticar a melhoria contínua do Sistema de Gestão da Segurança da Informação.

6. PRINCÍPIOS

Os princípios que direcionam a Política de Segurança da Informação da EMAP

são os descritos abaixo:

- **Confidencialidade:** característica de que a informação não esteja disponível ou divulgada a pessoa física, sistema, órgão ou entidade não autorizada.
- **Integridade:** característica de que a informação não sofreu alterações ou exclusões de maneira não autorizada ou acidental.
- **Disponibilidade:** característica de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
- **Legalidade:** Característica de que a PSI e todas as políticas técnicas correlatas estão em acordo com a legislação e regulamentações vigentes.
- **Normatização:** Característica de que a PSI e todas as políticas técnicas correlatas tem estabelecida em si regras e normas institucionalmente sobre segurança da informação.
- **Responsabilidade:** Característica de que a PSI e todas as políticas técnicas correlatas possuem definições de imputabilidades definidas em relação à segurança da informação.
- **Transparência:** Característica de que a PSI e todas as políticas técnicas correlatas estão em acordo com os princípios legais da transparência pública.
- **Efetividade:** Característica de que a PSI e todas as políticas técnicas correlatas produzem o efeito desejado com o melhor resultado possível por intermédio de suas determinações, com vistas a apoiar as atividades internas no que se refere à segurança da informação, de maneira que sejam exercidas com rapidez, correção e alto rendimento funcional.
- **Ética:** Característica de que a PSI e todas as políticas técnicas correlatas estão em acordo com a correta conduta que deve ser seguida no serviço público, observando os valores morais e de boa fé.
- **Impessoalidade:** Característica de que a PSI e todas as políticas técnicas correlatas servem a todos os empregados, prestadores de serviços, fornecedores e todo e qualquer que tenha relação institucional com a empresa, sem preferências de cunho pessoal, partidário, racial e ideológico.
- **Publicidade:** Característica de que a PSI e todas as políticas técnicas correlatas terão ampla publicidade institucional, sendo levadas ao conhecimento geral da empresa com vista a garantir a divulgação efetiva a todos os empregados, prestadores de serviços e qualquer que possua relação institucional com a empresa e que tenha necessidade do conhecimento sobre os documentos.

- **Aplicação prática:** Característica de que a PSI e todas as políticas técnicas correlatas possuem aplicações reais e práticas no dia a dia dos empregados e prestadores de serviços da empresa.
- **Institucionalização:** Característica de que a PSI e todas as políticas técnicas correlatas são instrumentos de caráter institucional, devendo ser observada para a realização de todas e quaisquer atividades referente ao manejo de informações.

7. DIRETRIZES GERAIS

A Segurança da Informação na Instituição estabelece os principais controles, denominados diretrizes:

- As informações da empresa, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.
- O acesso às informações e recursos só deve ser feito se devidamente autorizado.
- Os riscos às informações da empresa devem ser reportados à Gerência de Tecnologia da Informação.
- As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes.
- A segurança da informação deve ser considerada no gerenciamento de projetos, independentemente do tipo do projeto.

7.1. Tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da EMAP em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

Toda e qualquer informação produzida, recepcionada, classificada, utilizada, acessada, reproduzida, transportada, transmitida, distribuída, arquivada e armazenada pelos empregados ou prestadores de serviços no exercício de suas funções públicas na empresa, são de propriedade da EMAP, e devem ser tratadas de acordo com as definições da legislação vigente e das diretrizes definida nessa Política de Segurança

da Informação.

- As informações da empresa podem ser cedidas a terceiros por força da Lei de Acesso a Informação, mas deve passar por análise do gestor da informação com o apoio do setor jurídico para providência da documentação formal relativa à cessão da informação.

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Pública, Restrita ou Sigilosa. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações, conforme procedimento EMAP-PC-89 Classificação da Informação.

7.2. Tratamento de Incidentes de segurança da informação

Todo e qualquer incidente de segurança da informação deve ser obrigatoriamente informado pelos empregados e prestadores de serviços ao Setor de TI no momento em que tomarem conhecimento do incidente.

7.3. Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Instituição, para que sejam recomendadas as proteções adequadas.

7.4. Auditoria e Conformidade

A EMAP possui direito legal de realizar o monitoramento, controle e registro de acesso às informações que trafegam em sua rede interna e nos ativos de informação de propriedade da empresa.

- A EMAP se reserva ao direito de realizar auditorias nos ativos de informação de sua propriedade que estejam sob a custódia de qualquer empregado ou prestador de serviço sem prévio aviso quando identificadas possíveis quebras de segurança da informação.

A EMAP deve instituir mecanismo de segurança que possibilite que apenas ativos de informações homologados e previamente autorizados pelo setor de TI sejam conectados a sua rede interna.

- Ativos de informação não autorizados na rede interna devem ter seus acessos bloqueados sem prévio aviso.
- O setor de TI não tem responsabilidade em realizar cópias de segurança

de estações de trabalho e notebooks dos empregados e prestadores de serviços da EMAP.

A EMAP deve realizar avaliações internas contínuas de forma a verificar o cumprimento e necessidades de adequações dessa política e das políticas técnicas correlatas.

7.5. Controle de Acesso

O acesso, utilização e manuseio das informações e dos ativos de informação da EMAP por parte dos empregados e prestadores de serviço são controlados e limitados ao cumprimento de suas atividades internas.

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da empresa.

Os acessos podem ser rastreados, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações.

Os empregados e prestadores de serviço que utilizam ativos de informação e a rede interna da EMAP devem possuir uma conta de acesso de usuário.

- A conta de acesso dos usuários deve ser única e intransferível.
- A implantação de perfis de acesso aos usuários deve ser realizada com base no princípio de privilégio mínimo.

7.6. Uso de e-mail

O correio eletrônico disponibilizado aos empregados e prestadores de serviços deve ser utilizado somente para realização de atividades profissionais de interesse estritamente da Empresa.

A EMAP se reserva ao direito de realizar auditorias nas caixas de correio eletrônico de qualquer empregado sem prévio aviso quando identificadas possíveis quebras de segurança da informação.

7.7. Acesso à Internet

O acesso à Internet concedido aos empregados e prestadores de serviço que utilizam a rede interna da EMAP deve ser utilizado prioritariamente para os interesses e negócios da Empresa.

A EMAP consente na utilização cuidadosa da Internet para interesses particulares, desde que não exceda os limites da razoabilidade, ética e bom senso.

- O uso da Internet para interesses particulares não deve intervir na

produtividade pessoal nem consumir recursos computacionais significativos da EMAP.

- É vetado o acesso a sites de conteúdo de jogos, crimes, rádios, tvs, apostas, eróticos, pornográficos e blogs. A EMAP irá restringir os acessos a sites que, considerar alheios aos objetivos da Empresa, e monitorar consultas de usuários com o objetivo de garantir segurança e adequação no uso deste recurso.

A EMAP se reserva ao direito de realizar auditorias nas conexões de Internet de qualquer empregado ou prestador de serviços sem prévio aviso quando identificadas possíveis quebras de segurança da informação.

- Todos os acessos à internet serão armazenados em log, para posterior pesquisa, se necessário;

7.8. Monitoramento

Todos os ativos de informação de propriedade da EMAP são suscetíveis a monitoramento contínuo dentro dos limites da legislação vigente.

Toda e qualquer pessoa que acessa as dependências da EMAP deve portar identificação física visível demonstrando qual sua função/atividade.

- A identificação dos empregados e prestadores de serviços deve ser pessoal e intransferível.

Os ativos de informação de visitantes podem ser retidos temporariamente para verificações em relação aos processos de gestão de segurança da informação da EMAP.

7.9. Propriedade Intelectual

Tecnologias, marcas, metodologias e quaisquer informações que pertençam à EMAP não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

7.10. Controles Criptográficos

A confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou sob processo de transporte físico ou de transmissão eletrônica, assim como de sistemas disponíveis em redes públicas, deverão ser assegurados por meio de controles criptográficos.

7.11. Mesa Limpa e Tela Limpa

Todos os empregados e prestadores de serviços são responsáveis pelas informações armazenados em seus postos de trabalho (mesa e computador) e devem garantir a segurança das mesmas.

7.12. Disposições Finais

- Os casos não previstos nesta Política deverão ser encaminhados para o setor de TI.
- Os casos omissos serão resolvidos pelo setor de TI.

8. PENALIDADES

O descumprimento dos itens descritos na PSI e nas políticas técnicas correlatas será considerado ato infracional de indisciplina, sujeito a penalizações administrativas internas e a penalizações previstas na legislação vigente.

As penalizações podem variar de acordo com a gravidade do ato infracional, ficando os infratores sujeitos às seguintes penalidades:

- Advertência verbal;
- Advertência por escrito na ficha funcional;
- Suspensão;
- Demissão e/ou outras medidas judiciais cabíveis.

Em caso de suspeita de ato infracional à PSI e às políticas técnicas correlatas, o setor de TI fará uma investigação, ficando a seu critério suspender temporariamente o serviço afetado sem prévia autorização.

- Nos casos em que o infrator for empregado da EMAP, o setor de TI comunicará imediatamente os resultados das investigações para o superior imediato e para o empregado investigado para manifestação da defesa.
- Nos casos em que o infrator for prestador de serviços, o setor de TI comunicará imediatamente os resultados das investigações para o gestor do contrato para que este comunique o ocorrido à empresa do prestador para manifestação da defesa.

9. COMPETÊNCIAS E RESPONSABILIDADES

Deverá ser instituída uma estrutura de gestão de segurança da informação na

EMAP. A estrutura deve ser formada, no mínimo, por:

- Gestor de Segurança da Informação.
- Equipe de Resposta e Tratamento a Incidentes.

A estrutura de gestão de segurança da informação será responsável pela promoção, manutenção e coordenação dos aspectos de segurança da informação.

- A implementação efetiva e o acompanhamento da aplicabilidade dessa política e das políticas técnicas correlatas são de responsabilidade dessa estrutura.

Todos empregados e prestadores de serviços são responsáveis pelo cumprimento integral dessa Política de Segurança da Informação.

10. DOCUMENTOS RELACIONADOS

- EMAP-DSGSI-07 Política Técnica de Controle de Acesso
- EMAP-DSGSI-08 Política Técnica de Suporte a Infraestrutura Interna e a Usuários de TI
- EMAP-DSGSI-09 Política Técnica de Computação Móvel e Trabalho Remoto
- EMAP-DSGSI-10 Política Técnica de Responsabilidade Operacional
- EMAP-DSGSI-11 Política Técnica de Cópias de Segurança
- EMAP-DSGSI-12 Política Técnica de Conformidade Legal
- EMAP-DSGSI-13 Política Técnica de Aquisição, Desenvolvimento e Manutenção Segura de Sistemas de Informação
- EMAP-DSGSI-14 Política Técnica de Aspectos da Gestão da Continuidade de Negócio
- EMAP-DCSGSI-XX Política Técnica de Controles Criptográficos
- EMAP-DCSGSI-XX Política de Mesa Limpa e Tela Limpa
- EMAP-PC-07 Normas de Segurança da Informação
- EMAP-PC-72 Gerenciamento de Serviços e Infraestrutura de TI e Desenvolvimento de Sistemas
- EMAP-PC-89 Classificação da Informação
- EMAP-PC-52 Metodologia Gerenciamento de Riscos
- EMAP-PC-73 Metodologia Gerenciamento de Incidentes
- EMAP-PC-74 Gestão de Problemas
- EMAP-PC-75 Gestão de Mudanças
- EMAP-PC-76 Plano de Continuidade de Negócios

- EMAP-PC-77 Papéis, Responsabilidades e Autoridades Referentes ao Sistema de Gestão da segurança da Informação - SGSI
- EMAP-PC-79 Auditoria Interna do SGSI
- EMAP-PC-78 Tratamento de Não Conformidade e Ação Corretiva – SGSI

11. REVISÕES E ATUALIZAÇÕES

Versão	Data	Item	Revisões
0	XX/03/2020	7.10	Inclusão de Controles Criptográficos
0	XX/03/2020	7.11	Inclusão de Mesa Limpa e Tela Limpa