1. FINALIDADE

1.1. Estabelecer diretrizes e regras aplicáveis à Segurança Física e Patrimonial, bem como da Segurança da Informação e Comunicações visando proteger as instalações da empresa, os processos de negócio, os empregados e demais pessoas que atuam no âmbito da Casa da Moeda do Brasil - CMB, bem como o sigilo das informações para garantir a continuidade dos negócios da empresa.

2. ABRANGÊNCIA

2.1. Se aplica aos colaboradores da CMB, inclusive terceirizados;

2.2. Também é aplicável a qualquer pessoa física ou jurídica que produza ou manipule informação da CMB.

3. CONCEITOS

3.1. Política de Segurança: documento elaborado com base nos princípios da administração da CMB, no qual são estabelecidas as diretrizes, critérios e suportes administrativos aptos à implementação da Segurança Física e Patrimonial e da Segurança da Informação e Comunicações, bem como sua estrutura e competências; Segurança da Informação e Comunicações: conjunto de ações visando garantir a disponibilidade, integridade e confidencialidade das informações organizacionais em meio físico ou lógico, contra acesso não autorizado, uso indevido, divulgação, destruição, modificação ou interrupção. A segurança de informação abrange:

3.1.1. A segurança cibernética;

3.1.2. A defesa cibernética;

3.1.3. A segurança física das infraestruturas críticas responsáveis pela segurança da informação;

3.1.4. A proteção de dados organizacionais; e

3.1.5. As ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

3.2. Segurança Física e Patrimonial: conjunto de ações e métodos estabelecidos visando promover a proteção de pessoas, bens e instalações com atuação preventiva e/ou reativa visando garantir a continuidade dos negócios;

3.3. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

3.4. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

3.5. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

3.6. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados;

3.7. Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

3.8. Gestor de Segurança da Informação e Comunicações: responsável pelas ações de Segurança da Informação e Comunicações;

3.9. Gestor de Segurança Patrimonial: responsável em planejar, organizar, dirigir e controlar as atividades da segurança patrimonial da CMB;

3.10. *Computer Security Incident Response Team - CSIRT*: equipe de tratamento e resposta a incidentes em redes computacionais com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

4. PRINCÍPIOS

4.1. Quanto à Segurança Física e Patrimonial

4.1.1. As ações de segurança física e patrimonial são norteadas pelos seguintes princípios:

I. Aplicação da prevenção, detecção e reação das ameaças;

II. Adoção de práticas de segurança preventiva;

III. Buscar gerar um estado no qual o patrimônio da CMB esteja livre de danos, interferências e perturbações;

IV. Garantir a incolumidade física das pessoas;

V. Garantir a integridade do patrimônio;

VI. Buscar a melhoria contínua.

4.2. Quanto à Segurança da Informação e Comunicações

4.2.1. As ações de segurança da informação e comunicações são norteadas pelos seguintes princípios:

I. Responsabilidade: todos devem conhecer e respeitar as normas de segurança;

II. Ética: todos os direitos e interesses legítimos de usuários, intervenientes e colaboradores devem ser respeitados sem comprometer a segurança da informação e comunicações;

III. Proporcionalidade: o nível, a complexidade e os custos dos processos de segurança devem ser apropriados e proporcionais ao valor e à necessidade de confiança nos sistemas de informação considerando a severidade, a probabilidade e a extensão de um dano potencial ou atual;

IV. Celeridade: as ações de resposta a incidentes e de correções de falhas de segurança devem ser tomadas o mais rápido possível;

V. Menor Privilégio: usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa;

VI. Buscar a melhoria contínua.

5. DIRETRIZES

5.1. Quanto à Segurança Física e Patrimonial

5.1.1. A CMB manterá em sua estrutura organizacional, permanentemente, órgãos nos níveis estratégico, tático e operacional responsáveis pelas ações e manutenções de segurança a longo, médio e curto prazo;

5.1.2. As demais áreas da CMB deverão elaborar procedimentos complementares às diretrizes instituídas pelos órgãos responsáveis pela segurança na CMB, quando se fizer necessário;

5.1.3. O órgão responsável pela segurança deve estabelecer diretrizes para disciplinar o controle do acesso físico e lógico na CMB, objetivando:

I. Proteger as instalações e as informações com ações preventivas;

II. Garantir a segurança dos empregados e demais pessoas em casos de ações que venham a ameaçar a CMB;

III. Manter contingência dos ativos de serviço e de logística, contra tipos de risco, sinistro ou intrusão, mesmo na presença de condições ambientais adversas e/ou de agentes maliciosos;

IV. O compromisso de estar de acordo com as políticas de transações com as partes relacionadas e de conformidade com as partes interessadas consideradas relevantes para o Sistema de Gestão de Segurança - SGS.

5.2. Quanto à Segurança da Informação e Comunicações

5.2.1. Toda informação criada, adquirida ou custodiada pela CMB possui valor e, portanto, deve ser protegida conforme as diretrizes de segurança dispostas nos normativos da empresa e demais regulamentações em vigor;

5.2.2. O Comitê de Segurança da Informação e Comunicações – COSIC, é o órgão responsável por assessorar a implantação e gestão desta Política;

5.2.3. A CMB deverá dispor do CSIRT, para dar tratamento e resposta a incidentes em redes computacionais;

5.2.4. Deverá ser preservada as informações pessoais, proprietárias e os segredos comerciais, garantindo a disponibilidade, integridade, confidencialidade e autenticidade das informações;

5.2.5. Todos os sistemas de informação da CMB são passíveis de monitoramento de segurança a qualquer momento, devendo ser observado os limites impostos pela legislação em vigor;

5.2.6. As hipóteses de monitoramento de segurança da informação deverão ser motivadas e autorizadas pelo Gestor de Segurança da Informação e Comunicações;

5.2.7. Constitui infração a esta Política qualquer ato que exponha a CMB a danos financeiros, efetivos ou potenciais à sua imagem, à segurança da informação, de recursos materiais ou humanos para propósitos não autorizados por lei.

6. RESPONSABILIDADES

6.1. Compete ao Presidente da CMB

6.1.1. Zelar para que o COSIC esteja em permanente funcionamento;

6.1.2. Designar o Gestor de Segurança da Informação e Comunicações;

6.1.3. Designar o Gestor de Segurança Patrimonial.

6.2. Compete à Diretoria Executiva

6.2.1. Garantir a disponibilidade de recursos necessários à institucionalização desta Política.

6.3. Compete ao COSIC

6.3.1. Propor os normativos referentes a Segurança da Informação e Comunicações, inclusive atualizações, quando necessário.

6.4. Compete ao Gestor de Segurança da Informação e Comunicações

6.4.1. Instituir o CSIRT.

6.5. Compete ao Departamento de Segurança – DESEG

6.5.1. Elaborar os instrumentos normativos relativos à segurança física e patrimonial;

6.5.2. Promover ações de segurança a longo, médio e curto prazo, propiciando a melhoria contínua do sistema de gestão de segurança.

6.6. Compete ao Departamento de Pessoas – DEGEP

6.6.1. Incluir o tema segurança em programa de integração de novos empregados, bem como em programas internos de educação continuada.

6.7. Compete ao Departamento de TI Corporativo e Comunicação – DETIC

6.7.1. Observar as diretrizes de segurança visando à proteção dos ativos de Tecnologia da Informação – TI da CMB;

6.7.2. Elaborar normativo para a utilização dos ativos de TI visando à disponibilidade do ambiente tecnológico da CMB para as atividades corporativas.

6.8. Compete a qualquer pessoa física ou jurídica que produza ou manipule informação da CMB

6.8.1. Proteger as informações sob sua responsabilidade;

6.8.2. Zelar pelos bens sob sua custódia;

6.8.3. Comunicar imediatamente ao DESEG qualquer ação ou omissão, intencional ou acidental que resulte no comprometimento da segurança da empresa.