POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

O presente resumo da **Política de Segurança da Informação e Segurança Cibernética** da SLED ("Política") tem como objetivo estruturar os conceitos e os parâmetros da Segurança da Informação e Segurança Cibernética visando à proteção dos ativos de informação com diligência, de modo seguro e transparente, garantindo a confidencialidade, integridade e disponibilidade das informações.

A Política destina-se aos órgãos que compõem o sistema financeiro nacional, instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil ("BACEN"), entidades de classe, público em geral, especialmente clientes, colaboradores, parceiros, administradores, gestores, prestadores ou fornecedores de serviços, estagiários e usuários externos das informações pertencentes ou de alguma forma tratadas pela SLED.

As bases da segurança da informação são norteadas pelos seguintes princípios:

a) Confidencialidade: garantia de que a informação sigilosa não estará disponível de nenhuma forma a terceiros, entidades ou sistemas de aplicação de maneira irregular ou sem autorização.

b) Integridade: garantia de que a informação não tenha sido alterada em seu conteúdo de forma indevida ou não autorizada mantendo a sua integridade, procedência e autenticidade.

c) Disponibilidade: garantia de que a informação seja utilizada somente quando necessária, estando ao alcance de seus destinatários e possa ser acessada no momento oportuno.

As informações de uso corporativo são classificadas de acordo com os riscos e grau de sigilo exigido ao ramo de atuação da empresa, de acordo com os seguintes níveis:

a) Confidencial: é o mais alto grau de sigilo, aplicado às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado às referidas informações podem ter consequências críticas para o negócio, causando possíveis danos à imagem da empresa.

b) Restrito: são informações específicas para uso interno, com circulação exclusiva e irrestrita dentro da empresa. Tais informações podem estar disponíveis a todos os colaboradores e prestadores de serviços e devem ser utilizadas somente para as atividades da SLED. Essas informações, mesmo sendo de circulação livre dentro das empresas, não devem ser divulgadas para entidades externas sem os devidos cuidados,

incluindo, quando necessário, a assinatura de acordos de confidencialidade ou de autorização formal previamente avaliada pela alçada responsável pela informação ou documento em questão.

c) Público: são informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

d) Uso Interno: são informações de nível reduzido de confidencialidade de informações que podem ser divulgadas a toda a empresa e/ou pessoas diretamente interessadas.

Para efeito da presente Política, o incidente de segurança da informação é definido como qualquer evento adverso, decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da segurança da informação.

A SLED, visando a proteção e a prevenção de riscos identificados e avaliados, adota, por meio do seu time de Tecnologia, rotinas padronizadas de prevenção e proteção dos processos e ativos relevantes, conforme previsto na política interna de Gestão de Incidentes, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

A SLED, promove, ainda, o programa capacitação, conscientização e revisão dos normativos, possuindo e mantendo um programa de revisão/atualização que vise garantir que todos os requisitos de segurança técnicos e legais implementados estão sendo cumpridos, atualizados e em conformidade com a legislação vigente, incluindo também a revisão periódica dos planos de ação voltados para segurança da informação.

As **questões de segurança de informação e segurança cibernética** devem ser endereçadas ao Diretor de Tecnologia responsável pela Política de Segurança Cibernética (Resolução CMN 4.658/18 e Circular 3909/18).