Linhas Gerais da Política de Segurança Cibernética

1 – Objetivo

Esta política tem como objetivo estabelecer diretrizes, responsabilidades e controles para proteger os ativos de informação da Harmos SA – Sociedade de Crédito, Financiamento e Investimento ("Harmos"), sua reputação e imagem institucional, assegurando a confidencialidade, integridade e disponibilidade dos dados, além de garantir conformidade com a Resolução CMN 4.893/2021, a Lei n° 13.709/2018, Lei Geral de Proteção de Dados Pessoais, e demais leis e normativos aplicáveis a Sociedade.

A política abrange todos os sistemas, aplicações, processos e dados sob responsabilidade da Harmos, bem como os usuários, incluindo funcionários, terceiros, clientes e parceiros comerciais. Aplica-se a todos os dispositivos, seja dentro ou fora das instalações da instituição.

2 - Principais Diretrizes

2.1 - Gestão de Riscos Cibernéticos

Mapeamento dos ativos de informação da Harmos de acordo com o seu valor e a importância para os processos de negócios.

Identificar potenciais ameaças externas e internas, como ataques cibernéticos (*phishing, ransomware*, *malware*), falhas de hardware, erro humano e ações maliciosas internas.

Realizar análises de vulnerabilidades e testes de penetração ao menos anualmente para identificar brechas e vulnerabilidades no ambiente da Harmos.

Mapear as vulnerabilidades que podem ser exploradas pelas ameaças, incluindo falhas em software, falta de treinamento, políticas inadequadas ou falhas na infraestrutura de segurança.

Avaliar a probabilidade de cada risco ocorrer e o impacto potencial, levando em consideração as consequências para os negócios, reputação e dados sensíveis.

Implementar controles corretivos de segurança para mitigar esses riscos de acordo com a priorização da classificação do nível do risco.

2.2 - Gestão de Incidentes Cibernéticos

Os incidentes de segurança da informação devem ser classificados, registrados, tratados e devidamente comunicados.

Deve estabelecer a relevância dos incidentes para que a resposta e mitigação de risco seja adequada ao nível de complexidade que o incidente exige.

O processo deve realizar a contenção, registro, análise do impacto e análise da causa raiz para mitigar definitivamente a vulnerabilidade que deu origem ao incidente.

Ninguém, exceto aqueles que sejam autorizados pela Harmos, devem pronunciar-se publicamente a respeito de qualquer tipo de incidente de Segurança da Informação.

A equipe responsável pela comunicação do incidente, deve avaliar a relevância do incidente e avaliar a necessidade de comunicação ao Banco Central e demais stakeholders, em até 24 horas. Como exemplos podem incluir, ataque ransomware, vazamento de dados e falhas de sistema.

2.3 - Continuidade de Negócios

A Harmos deverá manter um Plano de Continuidade de Negócios (PCN) atualizado, com cenários de desastres que incluam falhas sistêmicas ou cibernéticas e definir procedimentos para recuperação de desastres.

Testes de simulação serão realizados anualmente para avaliar a eficácia do plano, bem como, planejar a resposta a incidentes críticos para garantir a continuidade operacional.

3 - Responsabilidades

Os Colaboradores são responsáveis por cumprir as diretrizes desta política e demais documentos em vigor. O descumprimento ou violação das diretrizes previstas nesta Política e nos demais documentos em vigor poderão resultar na aplicação das sanções previstas em procedimentos internos, contratos e legislação em vigor, conforme regras estabelecidas pela Sociedade.