POLÍTICA DE SEGURANÇA CIBERNÉTICA
COOPER CARD INSTITUIÇÃO DE PAGAMENTO LTDA.

1. Objetivo

A Política de Segurança Cibernética *(ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético que possam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis)* tem como objetivo estabelecer diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética, visando preservar e garantir a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade (não repúdio), legalidade e conformidade dos dados e informações da Cooper Card e seu Conglomerado Prudencial (doravante denominados apenas "Cooper Card"), ou que estejam em seu poder, observando as regulamentações aplicáveis e melhores práticas de mercado, sejam elas físicas ou eletrônicas.

2. Abrangência

Todos os usuários que estejam sob responsabilidade da Cooper Card, independente de seu vínculo com a empresa: dirigente, colaborador efetivo, estagiário, temporário ou terceiro, fornecedor e prestador de serviço. Conforme art. 4 e 5 da Resolução nº 85/2021 do Banco Central do Brasil ("BCB").

3. Estrutura da Área Responsável

As iniciativas relacionadas à segurança cibernética da Cooper Card são tratadas horizontalmente por toda sua estrutura, ou seja, abrangem todos os departamentos. A área de tecnologia é responsável por diversas iniciativas técnicas, controles e procedimentos que corroboram com a execução desta política.

4. Diretrizes de Segurança Cibernética

As informações da Cooper Card, ou que estejam em seu poder, 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.

Assim, temos que as informações devem ser utilizadas de forma transparente e ética entre as partes relacionadas, mediante consentimento ou fundamentado em base legal, conforme previsão da Lei Geral de Proteção de Dados ("LGPD" – Lei nº 13.709/2018).

5. Da Classificação dos Dados

Para os devidos fins, a Cooper Card classifica as informações recebidas e geradas em:

a) Público (P);
b) Grupo (GN);
c) Interna (I);
d) Departamental (D);

e) Estratégico (E);
f) Confidencial (C).

Uma vez classificada, as informações devem ser rotuladas a fim de que os usuários possam compartilhar, manusear, armazenar e descartar as informações de forma apropriada e segura.

As informações devem ser protegidas contra acesso, modificações, destruição ou divulgação não autorizada, garantindo que os sistemas e as informações sob responsabilidade da Cooper Card, ou suas coligadas, estejam adequadamente disponíveis para a continuidade do processamento das informações críticas de negócios.

A Cooper Card estipula política própria e específica para classificação e gestão dos dados corporativos definindo as diretrizes da mesma.

6. Da Prevenção de Incidentes e de Vazamento de Informações

A Cooper Card possui diversas iniciativas com intuito de prover rotinas e atividades que corroborem com a Prevenção de Incidentes e de Vazamento de informações, incluindo:

- Definição de mecanismos de controle de acesso e autenticação;
- Estabelecimento de um processo de desenvolvimento seguro de software;
- Estruturação de segmentação de rede corporativa;
- Procedimentos de prevenção e detecção de intrusão;
- Utilização de tecnologias de proteção contra software malicioso;
- Estabelecimento de rotinas de monitoramento e rastreabilidade das informações e eventos;
- Monitoramento e segurança física de suas estruturas prediais;
- Estabelecimento de rotinas de backup periódicos;
- Realização de testes de segurança periódicos;
- Rotinas para gerenciamento de vulnerabilidades.

7. Plano de Continuidade de Negócios

A Cooper Card mantém um Plano de Continuidade de Negócios (“PCN”) em conjunto com suas áreas de negócio, a fim de garantir a rápida retomada das atividades no caso de um incidente que interrompa as mesmas.

Referido PCN contempla os serviços e atividades relevantes dos setores envolvidos e seus respectivos tempos de recuperação assim como os tipos de cenários considerados no PCN.

8. Incidentes de Segurança Cibernética

Sendo a segurança da informação e a proteção dos dados uma responsabilidade de todos os colaboradores, fornecedores e prestadores de serviços que possuírem ou manipularem quaisquer dados sob a responsabilidade da Cooper Card, é fundamental que qualquer incidente de segurança cibernética

confirmado ou suspeito seja reportado ao CSI, tempestivamente, a fim de permitir a identificação da causa, objetivando a contenção de danos e de impactos.

A Cooper Card possui procedimentos implementados para tratar incidentes de segurança da informação e notificar os órgãos competentes conforme a necessidade.

Os incidentes serão classificados conforme matriz de relevância definida no Plano de Resposta a Incidentes sempre considerando como diretriz o impacto da exposição dos dados envolvidos no incidente e oportunamente a criticidade da infraestrutura que possa a vir tornar-se indisponível no mesmo.

Os prestadores de serviços de tecnologia da informação, quando atuando em processos críticos do negócio da Cooper Card, devem manter processo próprio de gerenciamento de incidentes que inclua informar a Cooper Card sobre incidentes que envolvam dados em sua posse ou gestão.

9. Treinamentos

A Cooper Card promove a capacitação, reciclagem e aperfeiçoamento de todos seus colaboradores, para garantir a segurança de seus dados e informações, ou que estejam em seu poder, respeitando as melhores práticas de segurança cibernética.

Frequentemente, a área de comunicação e marketing da Cooper Card divulga aos seus titulares dicas e melhores práticas referentes à precaução de fraudes que possam ocorrer na utilização dos produtos e serviços ofertados pela Cooper Card.

10. Relacionamento e Gerenciamento de Fornecedores e Prestadores de Serviços

A Cooper Card se preocupa com o seu relacionamento entre fornecedores e prestadores de serviços, por isso avalia os aspectos de segurança em suas contratações (on-premises e em nuvem), seja na aquisição, contratos ou privacidade de dados, incluindo a avaliação de potenciais fornecedores para o cumprimento das políticas e controles da empresa e finalidade de análise dos controles de segurança.

Os fornecedores e prestadores de serviços serão informados para que comuniquem os incidentes relevantes relacionados às informações da Cooper Card quando armazenadas ou processadas por eles em cumprimento a determinações legais e/ou regulamentares.

11. Considerações Finais

A política de segurança cibernética de uma empresa requer recursos tecnológicos e principalmente pessoas devidamente treinadas. A cultura de segurança da informação é um processo contínuo.

A Cooper Card entende e se compromete com seus clientes, colaboradores e público em geral, na busca pelo atingimento de um nível de segurança adequado, de modo a minimizar os impactos nos negócios e na prestação de serviços aos seus clientes.

12. Legislação

- RESOLUÇÃO BCB Nº 85, DE 08 de ABRIL DE 2021
- LGPD – Lei Nº 13.709/2018