ÍNDICE

1. OBJETIVO

Estabelecer diretrizes que permitam à Zoop proteger seus ativos de informação, nortear a definição de normas e procedimentos específicos de Segurança da Informação e Cibernética.

2. ABRANGÊNCIA

Todos os Zoopers, parceiros e prestadores de serviço terceirizados.

3. DEFINIÇÕES

3.1. SIGLAS

Bacen ou BC: Banco Central

SIEM: Gerenciamento e Correlação de Eventos de Segurança

CLT: Consolidação das Leis do Trabalho

CMN: Conselho Monetário Nacional

3.2. TERMINOLOGIA

Zoopers: são os colaboradores e/ou funcionários que possuem contrato de trabalho vigente com a Zoop.

4. DIRETRIZES

4.1. Premissas

Esta política foi elaborada com base na Resolução CMN nº 4.658/2018 e na Circular Bacen nº 3.909/18, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.

4.2. Segurança da Informação

Para garantir a segurança das informações, os seguintes pilares devem ser respeitados e considerados em toda tomada de decisão:

i. Confidencialidade – garantia de que as informações são acessadas somente por aqueles expressamente autorizados.
ii. Integridade – garantia de que as informações estão íntegras durante o ciclo de criação processamento e descarte.
iii. Disponibilidade – garantia de que as informações estejam disponíveis sempre que necessário para o andamento de processos de negócio.

Consideram-se ativos de informações todas as informações geradas ou desenvolvidas para o negócio que podem estar presentes de diversas formas, tais como: arquivos digitais, equipamentos, mídias externas, documentos impressos, sistemas, dispositivos móveis, bancos de dados e conversas.

Determina que independentemente da forma apresentada, compartilhada ou armazenada, os ativos de informação devem ser utilizados apenas para a sua finalidade devidamente autorizada, sendo sujeitos a monitoramento e auditoria.

Estabelece que todo ativo de informação de propriedade da Zoop tenha um responsável, seja devidamente classificado de acordo com os critérios estabelecidos e adequadamente protegido de quaisquer riscos ou ameaças que possam comprometer o negócio.

4.3. Diretrizes Gerais

Com relação à segurança cibernética, a Zoop dispõe das seguintes diretrizes gerais:

i. Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;
ii. Realizar a adequada classificação das informações e garantir a continuidade do processamento destas, conforme os critérios e princípios indicados nos normativos específicos;
iii. Garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;
iv. Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados e tratados os dados. Adotando as medidas necessárias para prevenir ameaças lógicas, como: vírus, programas nocivos ou outras falhas que possam

ocasionar acessos, manipulações ou usos não autorizados a Dados restritos e confidenciais;

v. Dentre outros aspectos: manutenção e gerenciamento de softwares antivírus, firewall e demais softwares de segurança instalados e atualizados; da manutenção dos programas de computador instalados no ambiente; e

vi. Atender às leis e normas que regulamentam as atividades realizadas pela Zoop.

Em vistas ao cumprimento das diretrizes acima elencadas, a Zoop:

Possui como objetivo de segurança cibernética: prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Com relação às medidas de segurança, adota procedimentos e controles para reduzir a vulnerabilidade a incidentes e atender aos objetivos de segurança cibernética. Dentre eles: autenticação, criptografia, prevenção e a detecção de intrusão. A prevenção de vazamento de informações, realização periódica de testes e varreduras para detecção de vulnerabilidades. proteção contra softwares maliciosos, estabelece mecanismos de rastreabilidade, mantém controles de acesso e de segmentação da rede de computadores e armazena cópias de segurança dos dados e das informações, conforme normativos vigentes.

Controla, monitora, restringe o acesso aos ativos de informação à menor permissão e privilégios possíveis.

Aplica os procedimentos e controles citados anteriormente, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da Zoop.

Possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis.

Realiza o registro, análise da causa e do impacto, bem como, controle dos efeitos de incidentes relevantes para as atividades da Zoop, que abrangem inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

Elabora inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança considerados nos testes de continuidade de serviços prestados e os testa anualmente para garantir a eficácia dos processos, além de produzir anualmente um relatório de resposta a incidentes no ambiente tecnológico da Zoop.

Classifica os incidentes de segurança conforme sua relevância de acordo com a classificação das informações envolvidas e o impacto na continuidade dos negócios da Zoop.

Realiza a avaliação periódica de empresas prestadoras de serviço que efetuam o tratamento de informações relevantes à Zoop com objetivo de acompanhar o nível de maturidade de seus controles de segurança para a prevenção e o devido tratamento dos incidentes.

Possui critérios para classificação da relevância dos serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior.

Adota processo de gestão de continuidade de negócios relativo à segurança da informação.

Estabelece regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância. Toda informação possui um proprietário, é obrigatoriamente classificada e recebe os devidos controles que garantam a confidencialidade desta, condizendo com as boas práticas de mercado e regulamentações vigentes.

Realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o ambiente tecnológico da Zoop e que possam ocasionar o comprometimento dos pilares de segurança da informação ou trazer risco reputacional, financeiro ou operacional.

i. Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na Companhia, incluindo:

ii. A implementação de programa de treinamentos obrigatórios para colaboradores;
iii. A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e
iv. O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

Adota iniciativas para compartilhamento de informações sobre os incidentes relevantes através de filiação em fóruns de discussão e pelo compartilhamento da plataforma de SIEM.

4.4. Gestão de Consequências

Todos os Zoopers, fornecedores, parceiros e clientes que observarem quaisquer desvios em relação às diretrizes desta política, deverão relatar o fato através do Canal Ético Zoop.

O descumprimento das diretrizes desta Política resultará na aplicação de medidas de responsabilização dos agentes envolvidos, conforme a respectiva gravidade do descumprimento podendo estas incluírem a responsabilização administrativa, cível ou penal, processos disciplinares e sanções previstas na Consolidação das Leis do Trabalho (CLT).

4.5. Responsabilidades

<u>Administradores e Colaboradores</u>

Observar e zelar pelo cumprimento da presente Política e, quando assim se fizer necessário, acionar o responsável pela área de segurança da informação para consultas sobre situações que envolvam conflito com esta Política ou mediante a ocorrência de situações nela descritas. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias e participe dos programas de conscientização.

<u>Diretor Responsável por Segurança da Informação</u>

i. Cumprir e zelar pelo cumprimento das diretrizes desta Política alinhada à Resolução CMN nº 4.658/2018 e à Circular Bacen nº 3.909/18, bem como demais normativos internos correlatos e suas respectivas atualizações; e

ii. b) Atender e cumprir as demandas dos órgãos reguladores relacionadas à Segurança da Informação.

Compliance e Segurança da Informação

Realizar a atualização dos normativos internos relacionados à Segurança da Informação assegurando a sua conformidade com as leis e regulamentações aplicáveis;

4.6. Cumprimento da política

Além da avaliação de efetividade desta Política realizado pelo time de Segurança da Informação, os mecanismos de segurança devem ser avaliados periodicamente pela auditoria interna da Zoop e pelas auditorias realizadas por entidades que regulamentem as atividades realizadas pela Zoop.

4.7. Comprometimento da Alta administração

O comprometimento da Alta Administração com a efetividade e a melhoria contínua desta Política, dos procedimentos e dos controles relacionados à segurança da informação e cibernética são percebidos através da constante transformação e aprimoramento da governança em ações relativas aos pilares mencionados anteriormente e pela disponibilização de recursos compatíveis com a complexidade da Zoop, avaliação e aprovação de políticas e procedimentos entre outras iniciativas.

4.8. Registros e Informações

As informações relacionadas a incidentes de segurança da informação e cibernética são de caráter confidencial, não devendo, em hipótese alguma, serem disponibilizadas às partes envolvidas.

Todos os documentos referentes a investigação incluindo coleta de evidências devem ser arquivados pelo prazo mínimo de 10 (dez) anos.

4.9. Disposições gerais

Esta política deverá ser revisada anualmente ou sempre que for necessária sua adequação. É de competência do Comitê de Compliance e do Conselho de Administração aprovar qualquer alteração desta Política sempre que se fizer necessário.

Esta Política entra em vigor na data de sua aprovação pelo Conselho de Administração e revoga quaisquer documentos em contrário.

5. ASPECTOS REGULATÓRIOS

Resolução CMN nº 4.658/2018	Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Circular Bacen nº 3.909/18	Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.
Circular Bacen nº 3.681/13	Dispõe sobre o gerenciamento de riscos, os requerimentos mínimos de patrimônio, a governança de instituições de pagamento, a preservação do valor e da liquidez dos saldos em contas de pagamento, e dá outras providências
ABNT NBR ISO 27001	Norma padrão e a referência Internacional para a gestão da Segurança da informação.

6. REGISTRO DAS ALTERAÇÕES

REVISÃO		ITEM ALTERADO	DESCRIÇÃO RESUMIDA DA ALTERAÇÃO
Nº	DATA		
01	25/03/2020	-	Elaboração da Política
02	05/10/2020	Todos os itens	Revisão da Política em atendimento a regulamentação de Circular BACEN nº 3.909/18.

7. ANEXOS

Não aplicável

Elaborado por:	Aprovado por:	Aprovado por:	Aprovado por:
Luiz Pires	Ygor Moretti	Rodrigo Miranda	Fabiano Cruz Rodrigo Miranda Luciana Carvalho Patrick Hruby Diego Barreto
Segurança da Informação	Coordenador de Segurança da Informação	CTO	Conselho de Administração
06/10/2020	06/10/2020	20/10/2020	05/11/2020