ÍNDICE

1. OBJETIVO 2
2. ABRANGÊNCIA 2
3. DEFINIÇÕES 2
3.1. SIGLAS 2
3.2. TERMINOLOGIA 2
4. DIRETRIZES 2
4.1. PREMISSAS 2
4.2. ESTRUTURA DA ÁREA 2
4.2.1. IMPLEMENTAÇÃO E OPERAÇÃO DA ÁREA DE SEGURANÇA DA INFORMAÇÃO 3
4.3. PAPEIS E RESPONSABILIDADES 5
4.3.1. SEGURANÇA DA INFORMAÇÃO 5
4.3.1.1. *DEFENSIVE SECURITY TEAM* 5
4.3.1.2. *INTEGRATION TEAM* 5
4.3.1.3. *IT CORP TEAM* 5
4.3.1.4. *IDENTITY & ACCESS MANAGEMENT* 6
4.3.1.5. *ADVISORY TEAM* 6
4.3.2. ADMINISTRADORES(AS) E COLABORADORES(AS) 6
4.3.3. DIRETOR RESPONSÁVEL POR SEGURANÇA DA INFORMAÇÃO 7
4.3.4. COMPLIANCE E SEGURANÇA DA INFORMAÇÃO 7
4.3.5. COMITÊ EXECUTIVO E COMITÊ DE SEGURANÇA DA INFORMAÇÃO 7
4.4. ATIVOS DE SEGURANÇA DA INFORMAÇÃO 8
4.5. DIRETRIZES GERAIS 8
4.6. COMPROMETIMENTO DA ALTA DIREÇÃO 10
4.7. TREINAMENTO E CONSCIENTIZAÇÃO 11
4.8. REGISTROS E INFORMAÇÕES 11
4.9. NORMATIVOS DE SEGURANÇA DA INFORMAÇÃO 11
4.10. GESTÃO DE CONSEQUÊNCIAS 12
4.11. CUMPRIMENTO DA POLÍTICA 12
4.12. CONTATO COM GRUPOS ESPECIAIS 13
4.13. VIGÊNCIA DA POLÍTICA 13
5. ASPECTOS REGULATÓRIOS 13
6. REGISTRO DE ALTERAÇÕES 14
7. ANEXOS 14

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 do Brasil
SIEM: Gerenciamento e Correlação de Eventos de Segurança
CLT: Consolidação das Leis do Trabalho
CMN: Conselho Monetário Nacional
PCI: Payment Card Industry

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 Resolução do Banco Central do Brasil Nº 85/2021, 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.

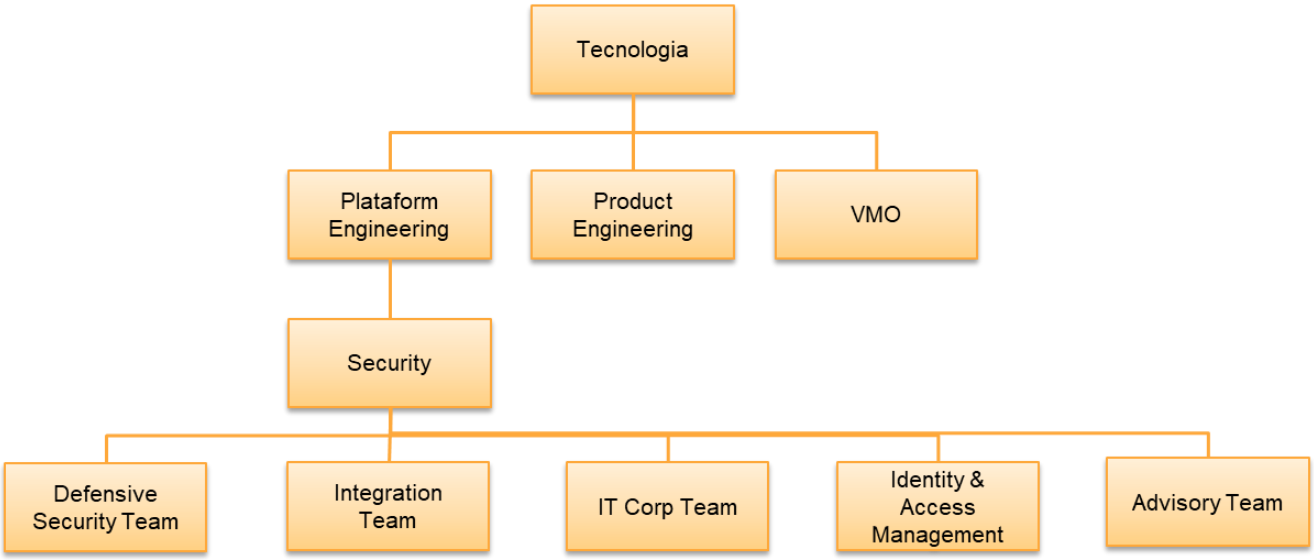
4.2. ESTRUTURA DA ÁREA

Alinhado com as estratégias internas de TI e com as melhores práticas de Segurança da Informação, foram analisados os diversos padrões que poderiam atender às necessidades de proteção das informações da empresa.

Foram eleitas as normas NBR ISO IEC 27001 e 27002, bem como os padrões PCI e requerimentos Bacen, com o objetivo de implementar não apenas os controles tecnológicos, mas também os controles de processo, garantindo assim a governança na implementação do Sistema de Gestão da Segurança da Informação da Zoop.

A estrutura organizacional montada reflete a seleção de controles da gestão de segurança e é baseada no resultado da Avaliação de Riscos, nas orientações dos acionistas, no diagnóstico realizado, nos aspectos culturais da Zoop e na legislação pertinente.

A equipe de Segurança da Informação é uma gerência alocada na estrutura de Tecnologia da Zoop, sob a nomenclatura *Security*, conforme apresentado no organograma a seguir.



4.2.1. IMPLEMENTAÇÃO E OPERAÇÃO DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Com base no Sistema de Gestão da Segurança da Informação, a Zoop:

i. Formula um plano de tratamento de risco que identifica a ação apropriada a ser adotada pela direção, os recursos e as responsabilidades e prioridades para o gerenciamento dos riscos relacionados com a segurança da informação;

ii. Implementa o plano para o tratamento de pontos de auditoria que estejam sob responsabilidade da área, para atender aos objetivos de controle identificados;
iii. Implementa os controles selecionados para atender aos objetivos de controle;
iv. Define como medir a eficácia dos controles ou grupos de controle selecionados e específica como essas medidas são usadas para avaliar a eficácia dos controles, visando produzir resultados comparáveis e reproduzíveis;
v. Define o escopo, os limites da área e os processos envolvidos, em termos das características do negócio, da organização, da localização, dos ativos e da tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo de controles
vi. Implementa tecnologias para identificar tentativas e violações de segurança da informação bem sucedidas ou não, além de incidentes de segurança da informação;
vii. Contribui com tecnologias e processos para detectar eventos de segurança da informação e assim prevenir os incidentes de segurança da informação pelo uso dos indicadores;
viii. Realiza, a cada seis meses, a análise crítica da eficácia dos controles, por meio do Comitê de Segurança da Informação, para garantir que o escopo permanece adequado e que melhorias no processo de gestão de segurança são identificadas e implementadas;
ix. Gerencia as operações de Segurança da Informação;
x. Gerencia os recursos de tecnologia sob sua custódia; e
xi. Implementa Políticas, Padrões e Procedimentos e outros controles que sejam capazes de permitir a pronta detecção de eventos de segurança da informação e a resposta a incidentes de segurança da informação.

A Zoop estabelece, implementa, opera, monitora, analisa criticamente, mantém e melhora continuamente o seu Sistema de Gestão da Segurança da Informação (SGSI) documentado dentro do contexto das atividades de negócios globais e dos riscos a que ela está sujeita. Este processo está baseado no ciclo PDCA, conforme ilustrado na figura a seguir.

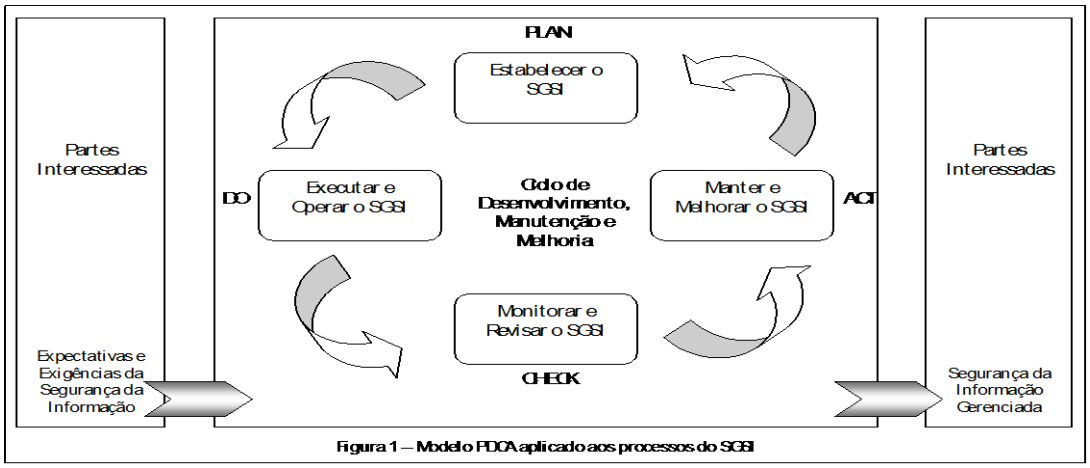


Figura 1 – Modelo PDCA aplicado aos processos do SGSI

4.3. PAPEIS E RESPONSABILIDADES

Os papeis e reponsabilidades relacionados a esta Política estão estabelecidas abaixo.

4.3.1. SEGURANÇA DA INFORMAÇÃO

4.3.1.1. *DEFENSIVE SECURITY TEAM*

Responsável pelo monitoramento de ameaças e comportamentos anômalos, bem como acesso aos dados. Investiga, analisa e responde a incidentes cibernéticos no ambiente Zoop. Gerencia o SOC (Security Operations Center), que monitora o ambiente 24x7x365 e analisa os alertas e as informações de segurança, distribuindo para as equipes apropriadas. Define, documenta e distribui procedimentos de resposta e escalação de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo eficiente.

4.3.1.2. *INTEGRATION TEAM*

Assegura que os requisitos de segurança necessários para proteger a missão e os processos comerciais da organização sejam adequadamente abordados em todos os aspectos da arquitetura sistêmica, incluindo modelos de referência, arquiteturas de segmento e de solução conforme as melhores práticas de segurança.

4.3.1.3. *IT CORP TEAM*

Responsável por todo apoio ao usuário final, desde suporte técnico até orientações para o uso das ferramentas utilizadas na Zoop.

4.3.1.4. *IDENTITY & ACCESS MANAGEMENT*

Responsável pelo ciclo de vida dos acessos de todos os colaboradores e terceiros, bem como pelo cumprimento das melhores práticas. Administra as contas dos usuários, incluindo adições, exclusões e modificações. Controla o acesso aos sistemas e dados por meio de perfis apropriados.

4.3.1.5. *ADVISORY TEAM*

Conduz avaliações de normativas e técnicas quanto aos controles de segurança em âmbito corporativo, gerencia os riscos associados à segurança da informação, pontos de auditorias, projetos de compliance e adequação às leis e gerencia os indicadores de segurança promovendo a melhoria contínua do processo e conscientização. Define, documenta e distribui políticas e procedimentos de segurança.

4.3.2. ADMINISTRADORES(AS) E COLABORADORES(AS)

É dever dos administradores(as) e colaboradores(as) da Zoop:

i. Observar e zelar pelo cumprimento da presente Política, estando ciente formalmente das diretrizes estabelecidas 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;
ii. Cumprir as leis e normas que regulamentem os aspectos de propriedade intelectual e uso de dados, como zelar pela proteção dos dados confidenciais (dados pessoais, sensíveis, financeiros – inclusive dados de cartão, estratégicos ou protegidos por lei) da Zoop ou dados que estiverem sob sua responsabilidade durante o seu tratamento;
iii. Reportar à equipe de Segurança da Informação de forma tempestiva qualquer evento suspeito que possa comprometer o ambiente da Zoop ou que configure uma violação à Política de Segurança da Informação e Cibernética;
iv. Sugerir, recomendar e verificar a implementação das melhores práticas de segurança em todos os processos de sua responsabilidade;
v. Utilizar responsavelmente e para fins de trabalho, de forma profissional, ética e legal os ativos de tecnologia da informação;
vi. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;
vii. Compreender o papel da segurança da informação em suas atividades diárias e participar dos programas de conscientização.

4.3.3. DIRETOR RESPONSÁVEL POR SEGURANÇA DA INFORMAÇÃO

É dever do Diretor responsável por Segurança da Informação:

i. Cumprir e zelar pelo cumprimento das diretrizes desta Política alinhada à Resolução CMN nº 4.658/2018 e à Resolução do Banco Central do Brasil Nº 85/2021, bem como demais normativos internos correlatos e suas respectivas atualizações; e
ii. Atender e cumprir as demandas dos órgãos reguladores relacionadas à Segurança da Informação.

4.3.4. COMPLIANCE E SEGURANÇA DA INFORMAÇÃO

É dever da área de Compliance e Segurança da Informação, em conjunto, realizar a atualização dos normativos internos relacionados à Segurança da Informação, assegurando a sua conformidade com as leis e regulamentações aplicáveis.

4.3.5. COMITÊ EXECUTIVO E COMITÊ DE SEGURANÇA DA INFORMAÇÃO

É dever do Comitê Executivo e do Comitê de Segurança da Informação da Zoop garantir a proteção dos dados de cartão e a conformidade com o Programa PCI DSS, fornecendo os recursos necessários para essa adequação.

Nos casos em que haja necessidade de contato com autoridades (por exemplo, no caso de suspeita de que a lei foi violada), haverá deliberação do Comitê de Segurança da Informação para definir os responsáveis por conduzir as atividades de comunicação.

Ambos os Comitês mencionados acima têm suas diretrizes estabelecidas no Regimento Interno do Comitê de Segurança da Informação, disponível para conhecimento dos colaboradores da Zoop no repositório corporativo de normativos internos.

Os materiais de apresentação aos Comitês, assim como as pautas correspondentes, devem ser repassados à equipe de Compliance com antecedência para organização das reuniões e para a distribuição do material aos integrantes e eventuais convidados.

4.4. ATIVOS DE 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.

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.

Todo ativo de informação de propriedade da Zoop deve ter um responsável devidamente classificado de acordo com os critérios estabelecidos e adequadamente protegido de quaisquer riscos ou ameaças que possam comprometer o negócio.

4.5. DIRETRIZES GERAIS

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

i. Proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;
ii. Adequada classificação das informações e garantia da continuidade do processamento destas, conforme os critérios e princípios indicados nos normativos específicos;
iii. Garantia que os sistemas e dados sob nossa responsabilidade estão devidamente protegidos e estão sendo utilizados apenas para o cumprimento das nossas atribuições;
iv. Zelo 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. Manutenção e gerenciamento de softwares antivírus, firewall e demais softwares de segurança instalados e atualizados e manutenção dos programas de computador instalados no ambiente; e

vi. Atendimento 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, a Zoop adota procedimentos e controles para reduzir a vulnerabilidade à incidentes e para atender aos objetivos de segurança cibernética. Dentre eles:

i. Autenticação, criptografia, prevenção e a detecção de intrusão;

ii. Prevenção de vazamento de informações, realização periódica de testes e varreduras para detecção de vulnerabilidades. proteção contra softwares maliciosos, estabelecimento de mecanismos de rastreabilidade, controles de acesso e de segmentação da rede de computadores e armazenamento de cópias de segurança dos dados e das informações, conforme normativos vigentes;

iii. 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.

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

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

vi. Contribui para a mitigação dos riscos de negócio e cibernéticos conforme a Política de Gerenciamento de Risco Operacional.

vii. 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.

viii. 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;

ix. 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;

x. 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;

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

xii. Adota processo de gestão de continuidade de negócios, conforme a Política Corporativa de Continuidade de Negócios.

xiii. 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.

xiv. 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.

xv. Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na empresa, incluindo a implementação de programa de treinamentos obrigatórios para colaboradores, a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos e o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

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

4.6. COMPROMETIMENTO DA ALTA DIREÇÃO

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, dentre outras iniciativas.

4.7. TREINAMENTO E CONSCIENTIZAÇÃO

O Programa de Treinamento e Conscientização em Segurança da Informação é estabelecido e gerenciado pela equipe de *Advisory*. Um cronograma anual é estabelecido com os tópicos relevantes a serem abordados e podem ser adotados diferentes formatos de treinamento e conscientização, como por exemplo:

- Online através da plataforma de conscientização vigente;
- Online e ao vivo através da plataforma de comunicação vigente, permitindo a interação com os participantes;
- Testes de *phishing* encaminhados ao e-mail dos Zoopers;
- Treinamentos específicos para atender a necessidade de um grupo de Zoopers;
- Comunicados com dicas e materiais de conscientização divulgados aos Zoopers por meio dos canais oficiais de comunicação.

A comprovação da participação e reconhecimento do conteúdo é avaliada por meio de um questionário ou outro método adequado.

As evidências da execução do Programa de Treinamento e Conscientização em Segurança da Informação são armazenadas pelo Segurança da Informação em local protegido.

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. NORMATIVOS DE SEGURANÇA DA INFORMAÇÃO

A equipe de Segurança da Informação mantém suas Políticas, Procedimentos e outras informações relevantes documentadas formalmente no repositório corporativo de normativos internos.

É papel do responsável pelo documento realizar a atualização do normativo pelo menos 1 (uma) vez ao ano, seguindo a diretriz corporativa de atualização de documentos estabelecida pelo time de compliance.

Os documentos devem seguir a nomenclatura especificada abaixo:

POL – Políticas: devem ser classificados como Políticas todos os documentos que contêm diretrizes abrangentes e regras a respeito de um tema.

PROD – Procedimentos: devem ser classificados como Procedimento todos os documentos que contêm instruções detalhadas sobre determinado processo.

Outros documentos: Documentos que não se enquadrem nas categorias Políticas e Procedimentos (por exemplo: formulários, diagramas, etc) devem obedecer à nomenclatura vigente a ser estabelecida pelo time de *Advisory*, conforme a necessidade.

Os documentos que devem ser divulgados para toda a empresa devem ser encaminhados ao time de *Advisory* para revisão, que, por sua vez, encaminhará à equipe de Compliance para aprovação e divulgação nas plataformas corporativas utilizadas na ocasião.

Já os documentos pertinentes somente à equipe de Segurança da Informação devem ser encaminhados somente ao time de *Advisory* para revisão e catalogação.

4.10. GESTÃO DE CONSEQUÊNCIAS

Todos os(as) 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).

4.11. 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.

4.12. CONTATO COM GRUPOS ESPECIAIS

Com o objetivo de ampliar o conhecimento sobre as melhores práticas e nos mantermos atualizados com as informações relevantes sobre Segurança da Informação, estabelecemos contato com grupos especializados no tema.

Os contatos dos fornecedores de Segurança da Informação podem ser visualizados por meio dos links abaixo:

CERT BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. http://www.cert.br/
CVE Mitre	Registro, classificação e divulgação de vulnerabilidades técnicas https://cve.mitre.org/
Fornecedores de Segurança da Informação	https://pag-zoop.atlassian.net/wiki/spaces/SEC/pages/1655898187/Lista+de+Fornecedores
Leis e Regulamentações	https://pag-zoop.atlassian.net/wiki/spaces/SEC/pages/1708687382/Regulamenta%2Bes%2Be%2BLeis

4.13. VIGÊNCIA DA POLÍTICA

Esta Política deverá ser revisada anualmente ou sempre que for necessária sua adequação. É de competência do Comitê de Segurança da Informação e do Conselho de Administração da empresa 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

DS FTL

	observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Resolução do Banco Central do Brasil Nº 85/2021	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 DE 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.
03	14/10/2021	Todos os itens	Alteração da Política para adaptação aos processos atuais e boas práticas

7. ANEXOS

Não aplicável.

Responsável pela Política:

DocuSigned by:
Alessandra Simões
29DCC2A40FB442B...
11/16/2021

Alessandra Simões
Especialista de Segurança da Informação

Aprovador da Política:

DocuSigned by:
Anselmo Gavazzi
5347CB4AD9064CB...
11/16/2021

Anselmo Gavazzi
Gerente de Segurança da Informação
Owner do Comitê de SI

DS FTC