moneycorp
Banco de câmbio

Moneycorp Banco de Câmbio Information Security Policy

Directorate of Risk and Compliance

Revisada em 29 de novembro de 2024

SUMÁRIO

CONTROLE DE DOCUMENTO

Controle de Documento	Política de Segurança de Informação do Grupo	
Autor do documento:	David Cripps – CISO	
Detentor da Política Executiva:	Diretor de Risco e Compliance	
Revisão:	COMITÊ DE R&C	Data da revisão: 20 de abril de 2022
Aprovação:	SMT	Data de aprovação: 25 de abril de 2022
Ratificação:	Comitê de Riscos	Data de Aprovação: 27 de abril de 2022
Atualização aprovada por:	CISO	Data de Aprovação: 7 de dezembro de 2022
Versão:	2.1.1	

CONTROLE DE VERSÃO

Versão	Autor	Revisado por	Data	Data
1.0	29/03/2017	Adam Altounyan	Kenneth Byrne	
1.1	28/09/2018	Ray Jackson	Kenneth Byrne	
1.2	22/10/2018	Ray Jackson	Kenneth Byrne	
1.3	13/112019	Ray Jackson	Kenneth Byrne	
V1.4.01	Agosto de 2021	David Cripps		Reestruturado
V1.4.04	Dezembro de 2021	David Cripps		Atualização do diagrama de políticas
V1.4.05	Janeiro de 2022	David Cripps		Comentários sobre Criptografia
V1.4.06	Fevereiro de 2022	David Cripps		Apêndice de monitoramento removido
V2.0	Maio de 2022	David Cripps	SMT	V1.4 aprovado pela RiskComm
V2.1	Agosto de 2022	Anthony Wong	ISSG	Governança atualizada para incorporar ISF e ISSG recém-criados
V2.1.1	Dezembro de 2022	Jayson Scheib	CISO	Compromisso de Gestão
V2	Novembro de 2024	Elaine Santos		Atualizado e revisado

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO GRUPO

1.1. Introdução

As informações do Moneycorp Banco de Câmbio (nesta Política também podem ser referidas como “Moneycorp”, “Banco”, “MBdC”, “empresa”, instituição, “nós” ou “nosso”) são de extrema importância para a instituição e, naturalmente, requerem uma abordagem “sem compromisso” para proteger nossa infraestrutura e tecnologias, a fim de garantir que estejam disponíveis quando necessário e que nossas informações não sejam divulgadas, perdidas, roubadas ou alteradas inadvertidamente ou de forma maliciosa.

Esta Política de Segurança da Informação (doravante denominada “Política”) corrobora com o nosso objetivo estratégico de manter um ambiente operacional eficiente e robusto e a nossa capacidade de fornecer um serviço aos clientes, apesar de eventos adversos, com a segurança de nossas informações. É promovida também pela implementação de sistemas e controles apropriados que são definidos em nossas políticas, padrões e procedimentos. Eles estão disponíveis na intranet.

Esta Política segue as mais recentes normas internacionais de segurança da informação (ISO 27001:2013), resoluções e normas do Banco Central e define os princípios necessários para manter a confidencialidade, integridade e disponibilidade de nossas informações.

1.2. Objetivo desta política

Esta Política estabelece as bases para o programa de segurança da informação da Moneycorp (denominado pela ISO27001 como "Sistema de Gestão de Segurança da Informação" ou ISMS) e prevê uma estrutura de Segurança da Informação apropriada, econômica e eficiente à instituição que está de acordo com o apetite de riscos do Conselho da Moneycorp.

A Diretoria Executiva e a alta administração da Moneycorp estão comprometidas com o programa de Segurança da Informação da instituição, por meio de engajamento regular entre a administração, comitês
e o Conselho;

Os principais objetivos desta Política são:

a) Garantir que as informações e sistemas dos escritórios, edifícios e salas de dados da Moneycorp estejam protegidos de acordo com o apetite de Riscos da Moneycorp;
b) Garantir que a Moneycorp seja capaz de fornecer um ambiente operacional resiliente que nos permita: antecipar; detectar; responder e nos recuperar de eventual incidente, possibilitando a continuação da prestação de serviço aos nossos clientes, ainda que com condições operacionais adversas, seguindo os objetivos de tempo de recuperação da instituição;
c) Garantir que as informações da Moneycorp recebam um nível adequado de segurança, considerando o valor das informações, o impacto de sua perda ou divulgação (classificação de dados);
d) Auxiliar os colaboradores (definido no parágrafo 7.1 abaixo) a protegerem a confidencialidade, integridade e disponibilidade das informações e sistemas da empresa (sensibilização);
e) Identificar as partes relevantes interessadas no programa de segurança da Moneycorp;
f) Garantir e promover a conformidade de acordo com as legislações e regulamentos relevantes em relação aos nossos ativos e operações de informações; e

g) Garantir que o programa de segurança da Moneycorp seja mantido e continuamente melhorado, assegurando assim, que permaneça relevante para as operações da instituição.

Esta Política aborda o risco de falha na proteção das informações, sistemas e infraestrutura da Moneycorp, o que pode resultar, por exemplo:

- em danos à reputação (levando a uma perda de confiança do cliente e dos negócios);
- em ações de execução por parte dos reguladores (multas e processos);
- em prejuízos financeiros;
- em responsabilização criminal; e
- em risco direto para nossos clientes de roubo de identidade e crime financeiro.

1.3. Aprimoramento contínuo

- O Programa de Segurança da Moneycorp será mantido e continuamente melhorado, garantindo assim, que permaneça relevante para as operações e estratégia da instituição.

a) O Fórum de Segurança da Informação (ISF), que incluirá a participação de partes internas interessadas que representam a organização, se reunirá regularmente (pelo menos trimestralmente), para analisar o funcionamento operacional do Sistema de Gestão de Segurança da Informação. Ele incluirá a eficácia do ISMS, análises de risco, aprovações de políticas e melhorias contínuas.

b) O Grupo Diretor de Segurança da Informação (ISSG), que compreende-se: (**i**) CRCO; (**ii**) CTO; (**iii**) CISO; e (**iv**) o Diretor de transformação de TI, se reunirá regularmente (pelo menos trimestralmente) para analisar o Sistema de Gestão de Segurança da Informação,bem como pararatificar quaisquer políticas e aprovar a solicitação de recursos para melhorias pelo ISF.

c) O CISO informará mensalmente o progresso atualizado ao Comitê de Risco e Conformidade (R&C) da Moneycorp, a respeito da operação e gestão do Programa de Segurança.

d) O Comitê de Risco (subcomitê do Conselho) garantirá que as análises do Programa de Segurança sejam realizadas e as ações tomadas.

e) A Equipe de Gerência Executiva da Moneycorp (SMT) irá analisar, pelo menos anualmente, a eficácia dos encontros, além de buscar melhorar o Programa de Segurança no contexto das metas de negócios e do plano de tratamento de riscos.

- A SMT garantirá que o registro de risco e o plano de tratamento sejam atualizados para considerarem as descobertas das atividades de monitoramento e revisão.

2. ESCOPO E PÚBLICO

Esta Política se aplica a todas as informações e sistemas que a Moneycorp possui, processa ou gerencia, incluindo, mas não apenas:

- Todas as informações da Moneycorp armazenadas em qualquer formato (incluindo, entre outros, físico e eletrônico);
- Todas as informações da Moneycorp processadas em qualquer plataforma (incluindo, entre outros,
  laptops, PCs, celulares, servidores corporativos, “serviços em nuvem”, etc.);
- Todas as informações da Moneycorp transmitidas de qualquer forma (serviço postal, e-mail, transferência de arquivos, etc.);
- Sistemas físicos que protegem as informações da Moneycorp (arquivos, cofres, sistemas de controle de acesso, etc); e
- Comunicação escrita, verbal ou outro tipo de formato (por exemplo, chamadas telefônicas, fax, scanners, e-mail, internet, vídeo ou conferências e reuniões de voz, etc.).

Estes termos aplicam-se ao uso dos Sistemas de Informação da Moneycorp pelos colaboradores, bem como ao uso de outros equipamentos de informática (por exemplo, equipamentos pessoais) sempre que estiverem a serviço da instituição ou processando dados da Moneycorp, seja em qualquer escritório da Moneycorp ou em trabalho remoto/teletrabalho.

O escopo desta Política refere-se a todas as partes dos negócios da Moneycorp e em todas as competências que a instituição opera, levando em consideração quaisquer variações específica sob as leis e regulamentos das várias jurisdições legais. Esta Política representa os controles mínimos para todos os negócios da Moneycorp. Se aplicável, controles adicionais que reflitam os requisitos regulatórios ou legais locais em países específicos devem ser seguidos.

As Políticas da Empresa se aplicam a todos os colaboradores.

Orientações específicas são fornecidas a equipe na Política de Uso Aceitável, que está disponível na intranet.

2.1. Problemas internos e externos, fatores e determinantes

- O comitê de R&C analisará todos os problemas internos e externos relevantes (Anexo 2) semestralmente ou após incidentes ou alterações significativas, com vistas a identificar qualquer impacto potencial na estratégia de negócios, operações ou Programa de Segurança da Moneycorp.

- O comitê de R&C considerará todos os requisitos legais e dados do cliente em sua análise anual do programa de segurança.

2.2. Partes interessadas

- A Moneycorp identificará quaisquer partes interessadas na gestão do Programa de Segurança da Moneycorp e na proteção de nossos ativos. Essas partes são identificadas e serão mantidas no Anexo 3.

3. DECLARAÇÕES DA POLÍTICA

O programa de Segurança da Informação da Moneycorp se baseia na norma internacional ISO27001. As seguintes declarações de política são concebidas para estabelecer a estrutura para a proteção de ativos de informação em todos os negócios da Moneycorp:

3.1. Gestão de Riscos

- Uma avaliação de risco operacional será realizada anualmente, seguindo uma metodologia reconhecida.

3.2. Políticas de segurança da informação

- Há políticas aprovadas relevantes em vigor para fornecer direcionamento gerencial e suporte para a segurança da informação e resiliência cibernética, de acordo com os requisitos de negócios, tolerância ao risco e leis e regulamentos relevantes.

3.3. Organização da segurança da informação

- A Moneycorp está alinhada com o modelo de “três linhas de defesa” para gerenciar os riscos do negócio, incluindo riscos de tecnologia, informação e resiliência:
    1. A Primeira Linha de Defesa (1LoD) compreende todo o Pessoal com acesso a sistemas ou informações e os chefes de Departamento ou Função que são responsáveis por identificar, possuir e mitigar quaisquer riscos operacionais, e promover a manutenção do ambiente de

controle;

2. A Segunda Linha de Defesa (2LoD) engloba as equipes de Segurança da Informação e Proteção de Dados, no âmbito da disciplina de Risco e Conformidade, que são responsáveis pela geração de políticas, desafiando, analisando e relatando a exposição ao risco, eventos e questões emergentes; e
3. A Terceira Linha de Defesa (3LoD) é a "Auditoria", que é responsável pela garantia/revisão independente. A condução do processo pode se dar por auditoria interna ou externa.

3.4. Recursos Humanos

- É responsabilidade de cada Gerente de Linha garantir que sua equipe e Pessoal, e quaisquer terceiros com os quais eles lidem, entendam suas responsabilidades quanto à redução do risco de roubo, fraude ou uso indevido de nossas informações ou infraestrutura de TI antes, durante ou após seu emprego ou contratação. Em particular, ao deixar a Moneycorp, o Pessoal deve devolver todos os dispositivos, informações e materiais impressos fornecidos pela Moneycorp.
- O Pessoal da Moneycorp deve passar por exames pré-admissionais, quando permitido pelas leis, regulamentos e ética relevantes, antes de ser designado, bem como receber termos e condições que indiquem claramente suas responsabilidades e deveres com relação à segurança das informações da Moneycorp. Novos exames serão realizados, na medida do previsto em requisitos regulatórios e de negócios.

3.5. Controle e classificação de ativos

- Todos os ativos e sistemas de informação devem receber um nível de proteção e controle apropriado ao valor para a Moneycorp (considerando o valor da informação ou o impacto de sua perda ou divulgação).
- Todos os ativos e sistemas de informações devem ser identificados, e um inventário de repositórios de informações deve ser mantido (incluindo, entre outros, computação do usuário final, servidores corporativos, "serviços em nuvem" etc.).
- A Moneycorp entende implementou o seguinte esquema de classificação dos dados:
  Dados Públicos: Informações sem restrições de divulgação
  Dados Internos: Informações para uso interno.
  Dados Confidenciais: Informações sensíveis que precisam de proteção
  Dados Restritos: Informações altamente sensíveis que exigem alta segurança.

- Os ativos de informação devem ter um titular designado, com a responsabilidade de garantir que a informação seja adequadamente protegida, definindo claramente os requisitos de proteção e o uso apropriado do ativo.
- A relevencia de cada incidente, seus paramêtros e a área que deverá ser contatada consta no "Critério de classificação de Incidentes cibernéticos relavantes"

3.6. Controle de acesso

- O acesso à informação e aos sistemas de informação devem ser controlados e gerenciados com base em uma necessidade comercial demonstrada e empregando o princípio de "privilégio mínimo" e "necessidade de saber"
- Um processo formal para conceder (e revogar) o acesso deve ser documentado para garantir que os direitos e privilégios de acesso às redes e sistemas sejam restritos, controlados, atribuídos e revogados em conformidade.
- A segregação de funções deve ser implementada para reduzir o risco de uso indevido acidental ou deliberado dos ativos de informação da organização.

3.7. Criptografia

- As informações confidenciais devem ser protegidas por controles criptográficos apropriados, tanto "em repouso" quanto "em trânsito", para garantir que mantenhamos a confidencialidade, integridade

e disponibilidade dessas informações. Nesse sentido, devem haver processos e procedimentos de gerenciamento de chaves criptográficas que sirvam a esse propósito.
- A Moneycorp usará técnicas e algoritmos criptográficos reconhecidos e suportados pelo segmento.
- O nível de criptografia deve ser proporcional aos nossos requisitos de negócios, realizado de acordo com as nossas políticas e de acordo com as leis e regulamentos relevantes.

3.8. Segurança física e ambiental

- A segurança física é um componente essencial da segurança da informação, portanto, controles físicos e ambientais apropriados devem ser implementados para garantir que as instalações, áreas de trabalho e ativos de informação da Moneycorp sejam adequadamente protegidos.

3.9. Procedimentos operacionais e responsabilidades

- Os principais procedimentos operacionais devem ser documentados e estarem disponíveis para as partes necessárias. Esses procedimentos devem incluir a gestão de mudanças, gestão de capacidade de serviços de TI e gestão de ambiente de TI.
- Controles para detectar, prevenir e habilitar a recuperação de atividades maliciosas ou inadvertidas devem ser implementados. As ferramentas de segurança devem permanecer no suporte do fabricante e os arquivos de detetive/assinatura mais recentes implementados dentro dos prazos acordados.

3.10. Segurança das comunicações

- Nossas redes de comunicações (voz e dados) devem ser protegidas contra falhas acidentais, maliciosas ou tecnológicas, interceptação, interrupção do serviço ou degradação com níveis de serviço acordados com os fornecedores.

3.11. Aquisição, desenvolvimento e manutenção de sistema

- A segurança apropriada será incorporada a todos os sistemas e à infraestrutura de suporte como parte do processo de concepção/construção/execução do sistema e quaisquer alterações serão conduzidas de maneira a preservar o nível de confidencialidade, integridade e disponibilidade das informações e da infraestrutura de TI.

3.12. Relações com fornecedores

- Qualquer terceiro, fornecedor ou prestador de serviços que armazene, processe ou acesse nossas informações ou sistemas devem ser previamente aprovados, identificados e registrados.
- A devida diligência de segurança apropriada deve ser realizada e os requisitos de controle resultantes acordados, documentados e implementados, em conjunto com acordos e/ou contratos apropriados, antes das contratações ou acesso às informações da Moneycorp serem concedidos.

3.13. Gestão de incidentes de segurança da informação

Todos os funcionários têm a responsabilidade de estar cientes e identificar os incidentes à medida que eles ocorrem e de seguir o procedimento de Ação e Evento de Risco (REACT) para escalonar imediatamente qualquer incidente que possa custar à empresa uma quantia e/ou afetar negativamente nossos clientes e funcionários, que possa causar uma violação regulamentar ou que possa prejudicar significativamente nossa reputação.

- Information Security incidents must be reported through the REACT process as effectively and quickly as possible to minimize potential impacts.
- Cada incidente deve ser documentado de forma sistemática, permitindo a coleta de dados essenciais para a compreensão do ocorrido.
- Processos e procedimentos apropriados devem ser implementados para responder a esses incidentes de maneira rápida e eficaz, incluindo o encaminhamento como um evento de risco.

- Para garantir uma resposta eficaz a incidentes, o processo REACT da organização define parâmetros claros para avaliar a relevância de cada incidente.
  Os parâmetros são: Gravidade do impacto, escopo do incidente, duração da interrupção e probabilidade de recorrência. Mais informações são fornecidas nos procedimentos REACT disponíveis na Intranet.

3.14. Aspectos de segurança da informação da gestão de continuidade dos negócios

- Os processos de gestão de continuidade dos negócios devem ser documentados e testados para minimizar os riscos residuais para nossa infraestrutura e sistemas, bem como reduzir o efeito de possíveis interrupções causadas por desastres, falhas de controle ou incidentes cibernéticos.

3.15. Conformidade regulatória e legislativa

- Os requisitos legais, regulamentares e contratuais relevantes aplicáveis à manutenção da segurança dos registros de informações da Moneycorp, devem ser identificados e registrados. Esses requisitos de segurança incluem o uso legal de criptografia, a manutenção de quaisquer direitos de propriedade intelectual, o uso de software exclusivo e a privacidade de informações pessoais.

3.16. Compartilhamento de informações sobre os incidentes relevantes

- Como parte da gestão de incidentes e em conformidade com a Resolução 4893 de 2021 do Banco Central do Brasil (BACEN), a organização implementa processos de comunicação para garantir que incidentes relevantes sejam adequadamente reportados e compartilhados, tanto no âmbito interno quanto com órgãos reguladores e parceiros externos, quando aplicável.

- A organização reconhece a importância do compartilhamento de informações sobre incidentes de segurança como uma prática essencial para fortalecer as defesas contra ameaças e promover uma cultura de segurança colaborativa. Portanto, são adotadas iniciativas que garantem a comunicação adequada de incidentes relevantes, tanto internamente quanto com partes externas, conforme necessário.

- A organização mantém diretrizes claras sobre quais incidentes devem ser compartilhados e com quem, respeitando os princípios de confidencialidade, integridade e disponibilidade da informação. O compartilhamento de informações é conduzido de acordo com as políticas de proteção de dados, respeitando leis e regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD), garantindo que apenas informações pertinentes e necessárias sejam divulgadas.

- O procedimento para compartilhar o incidentes com outras instituições financeiras deverá ser realizado com a plataforma MISP (Malware Information Sharing Platform). Plataforma esta que é utilizada para o compartilhamento de incidentes com outras instituições financeiras.

4. MONITORAMENTO E RELATÓRIOS

A conformidade com esta Política será monitorada pela Equipe de Risco e Conformidade, com encaminhamento de não conformidade para o comitê de R&C, o SMT e, quando apropriado, notificado ao Comitê de Risco

5. FUNÇÕES E RESPONSABILIDADES

- Titular Executivo
  - O Diretor de Risco e Conformidade é o Titular Executivo desta política de Segurança da Informação.
- Detentor da Política
  - O Diretor de Segurança da Informação (CISO) é o Detentor da Política.

- Gerentes
  - Pelo menos anualmente, os gerentes devem revisar e registrar a conformidade com todas as políticas e procedimentos relevantes dentro de sua área de responsabilidade.
- Todo o Pessoal da Empresa
  - Todo o pessoal deve permanecer ciente do que é necessário e garantir que as soluções de segurança sejam usadas adequadamente.
- Exceções à Política
  - Em geral, não serão permitidas exceções a esta Política. No entanto, em certas circunstâncias em que um indivíduo ou departamento não seja capaz de atender a um requisito desta política, eles devem inicialmente buscar orientação do CISO com uma justificativa documentada e o pedido de exceção acordado com o Titular Executivo e o Detentor da Política.
- Acompanhamento
  - O CISO tem responsabilidade pela supervisão desta política de Segurança da Informação e da articulação com grupos e autoridades de interesses especiais relevantes.

6. VIOLAÇÕES

Quaisquer violações materiais ou persistentes devem ser relatadas ao CISO para registro como um Evento Operacional no Registro de Riscos e Problemas da Moneycorp.

7. CONTRATOS DE SERVIÇOS TERCEIRIZADOS

Esta seção tem como objetivo definir as diretrizes para a elaboração de contratos de prestação de serviços terceirizados, garantindo a segurança efetiva dos dados e informações da instituição.

7.1 Indicação de Países/Regiões de Prestação de Serviços

Todos os contratos de serviços terceirizados devem incluir uma cláusula que indique explicitamente os países ou regiões onde os serviços serão prestados.

7.2 Medidas de Segurança Aplicáveis

Os contratos devem estabelecer as medidas de segurança que o provedor de serviços terceirizados deve adotar para proteger os dados e informações da instituição. Isso pode incluir requisitos específicos de criptografia, proteção de dados pessoais, políticas de acesso e controle de segurança física e lógica.

7.3 Procedimentos de Acesso a Informações

É essencial que os contratos especifiquem os procedimentos de acesso às informações por parte do provedor de serviços terceirizados. Isso pode incluir restrições de acessos baseadas em necessidades de conhecer auditorias de acesso, proteção de senhas e credenciais, e políticas de segurança de informações confidenciais.

7.4 Responsabilidades e Responsabilidade Legal

Os contratos devem definir claramente as responsabilidades do provedor de serviços terceirizados em relação à segurança cibernética e proteção de dados. Isso pode incluir cláusulas de responsabilidade por violações de segurança, notificação de incidentes, e conformidade com as leis e regulamentações de proteção de dados aplicáveis.

7.5 Procedimentos de Segurança para Fornecedores

Todos os prestadores de serviços devem cumprir os seguintes procedimentos e controles: Acordos de Nível de Serviço (SLAs), notificação de incidentes, investigação e resposta a incidentes, auditorias e treinamentos. Os fornecedores devem implementar e manter procedimentos robustos para a gestão de incidentes de segurança da informação. Isso inclui a identificação, notificação e resolução de incidentes de forma rápida e eficaz. Os prestadores

de serviços devem relatar imediatamente qualquer incidente ao ponto de contato designado na empresa, fornecer relatórios detalhados sobre a natureza e o impacto do incidente, e colaborar na investigação e mitigação dos efeitos. Além disso, devem realizar revisões periódicas de seus controles de segurança para garantir a conformidade contínua com as políticas da empresa.

8. GESTÃO DE SERVIÇOS TERCEIRIZADOS NO EXTERIOR

Esta seção estabelece os procedimentos e diretrizes para a contratação e gestão de serviços terceirizados prestados no exterior, garantindo conformidade com a norma da CMN 4893 e mitigação de riscos associados.

8.1 Definição Prévia de Países e Regiões

Antes da contratação de qualquer serviço terceirizado no exterior, é obrigatória a definição prévia dos países e regiões onde os serviços serão prestados e os dados armazenados. Esta definição deve considerar aspectos de segurança cibernética, regulamentações locais e geopolíticas.

8.2 Alternativas para Continuidade dos Negócios

Devem ser estabelecidas alternativas para garantir a continuidade dos negócios em caso de impossibilidade de manutenção do contrato com o provedor de serviços terceirizados no exterior. Isso inclui planos de contingência, possíveis realocações de serviços e a identificação de outros fornecedores que possam assumir as responsabilidades necessárias.

8.3 Avaliação de Fornecedores

Antes da contratação de serviços terceirizados no exterior, é fundamental realizar uma avaliação minuciosa dos fornecedores potenciais. Isso inclui análise de sua reputação, histórico de segurança cibernética, conformidade regulatória e capacidade de fornecer serviços de acordo com os requisitos estabelecidos pela instituição.

8.4 Monitoramento e Auditoria

Uma vez contratados, os serviços terceirizados no exterior devem ser constantemente monitorados e auditados para garantir conformidade contínua com os padrões de segurança cibernética, regulamentações locais e requisitos contratuais. Isso pode incluir auditorias regulares, revisões de desempenho e avaliações de risco.

9. CONTROLES DE RASTREABILIDADE

A política de segurança da informação reconhece a importância dos controles de rastreabilidade como um componente fundamental para a integridade e segurança dos dados da instituição. Esses controles têm como objetivo garantir que todas as ações realizadas nos sistemas sejam devidamente monitoradas e registradas, permitindo uma visão clara sobre quem acessou ou manipulou informações sensíveis.

Além disso, a política estabelece que os registros gerados pelos controles de rastreabilidade serão utilizados para auditorias e avaliações contínuas, facilitando a detecção de padrões de comportamento e potenciais vulnerabilidades. A implementação eficaz dos controles de rastreabilidade permitirá à instituição demonstrar seu compromisso com a proteção dos dados e a manutenção de um ambiente seguro.

As ações para controlar a rastreabilidade são: registro de eventos e incidentes de segurança, controle de acesso, salvaguarda de logs, coleta de evidências e gestão de incidentes.

10. DEMAIS INFORMAÇÕES

Esclarecimentos ou interpretações desta política devem ser solicitados ao seu gerente de linha ou Departamento de Segurança da Informação.

10.1. Definições

- Pessoal:
  - Trabalhadores em regime integral, parcial ou temporários;
  - Equipe contratada/consultores/agência; e
  - Diretores Executivos e Não Executivos da Empresa.
- Informações:
  - Aplicações;
  - Software;
  - Código fonte;
  - Propriedade Intelectual
  - Segredos industriais ou comerciais; e
  - Dados comerciais.

10.2. Documentos e Procedimentos Relacionados ou Relevantes

- Esta Política de Segurança da Informação é respaldada por um conjunto de Políticas e Normas que são desenvolvidas e mantidas pela equipe de Segurança da Informação e TI. Este conjunto de Políticas se concentra em três áreas:
  - Políticas focadas no usuário
  - Políticas focadas em "negócios"
  - Políticas focadas em "TI"

- Conforme estabelecido no Anexo 1, são revisadas anualmente pelo comitê de R&C e aprovados pelo SMT. O Comitê de Riscos deve ratificar todas as Políticas que satisfaçam um requisito legislativo ou regulatório ou que tenham um impacto material na gestão de riscos da empresa.

10.3. Treinamento associado

- Todo o pessoal deve receber educação e treinamento iniciais e contínuos de conscientização sobre Segurança da Informação, conforme apropriado para sua função.

- Os treinamentos para colaboradores e terceiros devem ser realizados anualmente.

10.4. Mudanças na Política

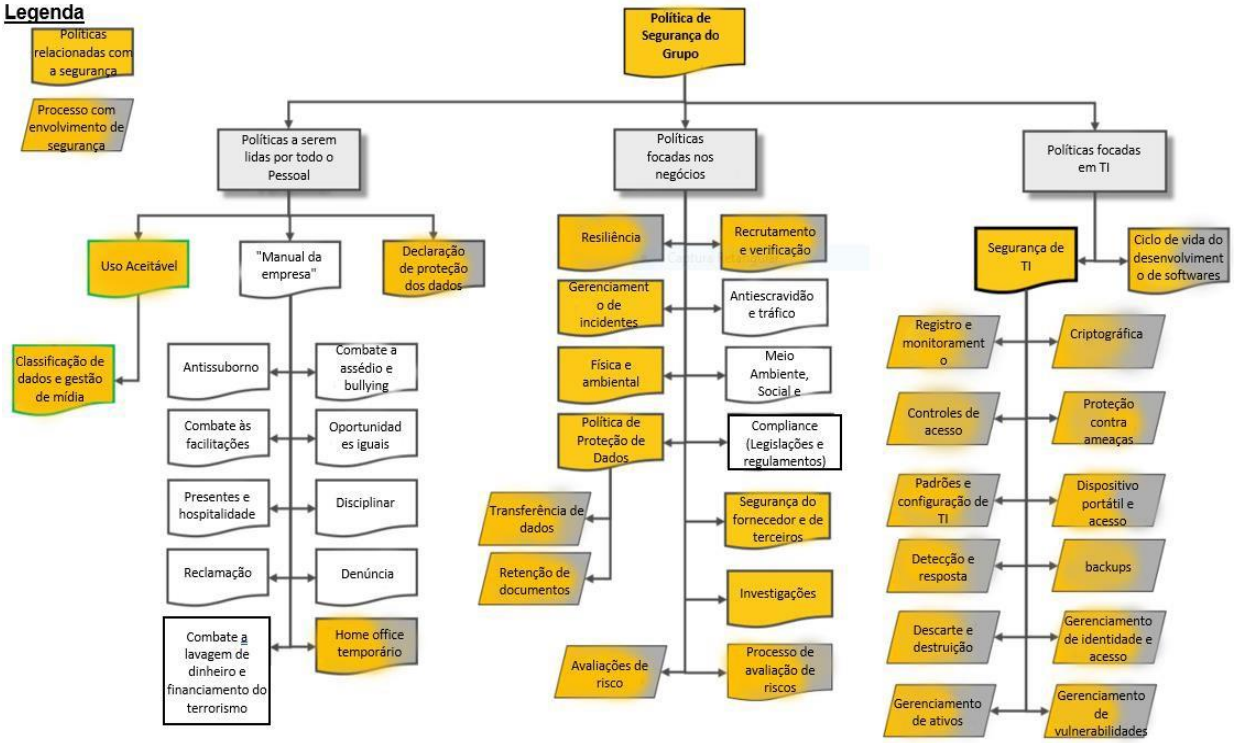
- Quaisquer alterações ou atualizações desta política serão comunicadas pelo CISO.

ANEXO 1 – POLÍTICAS RELACIONADAS À SEGURANÇA DA INFORMAÇÃO DA MONEYCORP

- É política da Moneycorp garantir que todas as informações recebam um nível de proteção apropriado ao valor das informações para a empresa ou ao dano que poderia ocorrer se tais informações fossem comprometidas. Tendo isso em vista, implementamos uma estrutura de políticas baseada em risco que inclui:
  - Políticas relacionadas ao usuário, que foram concebidas para orientar como nosso pessoal opera ao acessar nossos sistemas e informações.
  - Políticas relacionadas a negócios, que foram concebidas para orientar como nossas unidades de negócios tratam nossos ativos de informação.
  - Políticas relacionadas a TI, que foram concebidas para orientar o departamento de TI da Moneycorp e qualquer empresa terceirizada relevante, no projeto, operação e manutenção da tecnologia usada para processar, armazenar ou transmitir nossas informações (a

"Tecnologia da Informação" ou TI).

- A seguir estão identificados os tipos de políticas que são exigidos pela Moneycorp. Observe que a lista a seguir não é abrangente, servindo apenas de indicativo das políticas que as análises de risco podem exigir.
- Cada Política e processo/norma dentro da estrutura tem como alvo uma área específica, com objetivos específicos:



ANEXO 2 - PROBLEMAS INTERNOS E EXTERNOS OU DETERMINANTES

Questões	Requisitos	Responsável
Geopolíticas	O SMT da Moneycorp revisará constantemente os eventos geopolíticos para entender o impacto potencial.	R&C, CISO
Sociais	O SMT e o CISO da Moneycorp analisarão as mudanças sociais.	R&C, CISO
Regulatórias	A equipe jurídica da Moneycorp revisará todas as novas legislações e regulamentos para identificar qualquer impacto potencial nas operações da Moneycorp ou no Programa de Segurança.	Jurídicas
Agências de classificação de risco	A Moneycorp precisa estar ciente dos requisitos e metodologias das Agências de classificação de risco (S&P, Moody's, BitSight, etc.) com relação às operações do nosso Programa de Segurança	CISO, Diretor de TI, Diretor Financeiro
Atores de ameaças	A Moneycorp trabalhará com provedores de inteligência de ameaças para identificar possíveis ameaças às operações da Moneycorp	CISO
Tecnológicas	O Diretor de TI e CISO ajudarão a identificar possíveis mudanças na tecnologia que possam afetar a estratégia, o Programa de Segurança ou os produtos da empresa.	CISO Diretor de TI

Ambientais	A Moneycorp analisará o potencial impacto ambiental em nossas instalações, edifícios, operações e manutenção.	Diretor de TI, CISO
Grupos de Interesse Especial/Setor	A Moneycorp manterá contato com instituições do setor e grupos de interesse para identificar ameaças e tendências que possam afetar o Programa de Segurança.	CISO
Culturais	O CISO trabalhará com o RH e o SMT para monitorar quaisquer possíveis mudanças culturais dentro da empresa que possam afetar o programa de segurança	RH, SMT, CISO
Estratégicas	O CISO trabalhará com o SMT para entender quaisquer mudanças na estratégia da empresa que possam afetar o programa de segurança.	SMT, CISO

ANEXO 3 – PARTES INTERESSADAS

Parte interessada	Requisitos	Responsável
Clientes pessoa física e jurídica	Garantir que fornecemos uma solução confiável, escalável e resiliente que satisfaçam aos seus requisitos de negócios.	CEO CTO
Investidores/Proprietários	Garantir que a Moneycorp ofereça uma solução robusta e segura que proteja a marca, a reputação e a receita da empresa.	CEO
Conselho de Administração	Garantir que o programa de segurança seja abrangente, mantido e seu status seja apresentado regularmente.	Diretor Não Executivo
Comitê de Gestão Executiva	Garantir que o programa de segurança seja abrangente, mantido e seu status seja apresentado regularmente.	CISO
Agentes reguladores	Garantir que cumprimos todas as leis e regulamentos relevantes de segurança da informação/continuidade de negócios.	CRCO
Mídia	Garantir que as informações sobre nossa tecnologia sejam precisas e atualizadas.	CEO
Pessoal	Garantir que suas informações pessoais sejam mantidas confidenciais, que a triagem seja conduzida de maneira transparente e legítima; que os requisitos das políticas sejam adequados à finalidade e que o treinamento apropriado seja oferecido com regularidade. Garantir que os dados pessoais sejam processados de acordo com o Regulamento Geral de Proteção de Dados.	RH/CISO Jurídico DPO
Seguro	Garantir que contamos com políticas, procedimentos e normas adequadas e que os notificamos de quaisquer alterações nas circunstâncias ou incidentes	Jurídico CISO
Equipes de resposta a incidentes e aplicação da lei	Garantir a articulação com departamentos, organizações e equipes apropriadas (ANSSI, NCSC, NCA, etc.) para relatar ameaças e ataques contra a empresa.	CISO Diretor de TI
Fornecedores e revendedores	Fornecedores e revendedores precisam estar cientes dos requisitos, políticas e procedimentos da Moneycorp com relação à confidencialidade, disponibilidade e integridade das informações e sistemas da Moneycorp.	CISO/ Diretor de TI
Parceiros/Revendedores	Revendedores e parceiros, como contrapartes que dependem de nossos sistemas para reservar, processar ou concluir o processamento de FX e pagamento e, portanto, exigem garantia do gerenciamento eficaz da Moneycorp de nossas informações e sistemas.	CISO, Diretor de TI

Proprietários dos escritórios da Moneycorp	Os proprietários precisam estar cientes dos requisitos de segurança da Moneycorp, em especial do cabeamento elétrico e de telecomunicações, alarmes e supressores de incêndio, proteção e detecção de intrusos, manejo de visitantes e gravação de CFTV.	CTO Chefe de Segurança Instalações
Agências de classificação de risco	A Moneycorp precisa estar ciente dos requisitos e metodologias das Agências de classificação de risco (por exemplo, S&P, Moody's, BitSight, etc.) com relação às operações do Programa de Segurança	Diretor Financeiro CISO, Diretor de TI