Índice

1. Objetivo

Esta Política de Segurança Cibernética ("Política"), tem por objetivo estabelecer diretrizes e orientar os Colaboradores, Parceiros, Clientes e Prestadores de Serviços sobre as regras para assegurar a aplicação de controles e medidas administrativas necessárias para proteger as Informações de propriedade ou responsabilidade do Banco Original S.A. e suas controladas ("Original"), para fins de atendimento as principais normativas vigentes do Banco Central do Brasil e demais Órgãos competentes.

2. Fórum de Aprovação

Esta Política é aprovada pelo Conselho de Administração.

3. Vigência

Esta Política terá vigência de 01 (um) ano, ou, em menor prazo, quando o fórum responsável que a aprovou considerar necessário.

4. Aplicação e Público-Alvo

Esta Política se aplica, no Brasil e no Exterior, ao Original, bem como, a todos os seus administradores e colaboradores, incluindo também qualquer interação com clientes, parceiros, fornecedores e demais públicos de relacionamento.

5. Sumário

Segue abaixo, em ordem alfabética, os principais conceitos referidos nesta Política, de forma a evitar dificuldades de interpretação ou ambiguidades:

- **Ativo de Informação:** qualquer recurso que tenha a condição de processar, armazenar ou transmitir as informações.
- **Antivírus:** *Software* que identifica, previne, detecta e elimina *Malwares* que podem comprometer os ativos, mantendo a integridade do sistema e das informações.
- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para os sistemas ou informações da companhia.

- **Backup:** processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda dos originais.
- **Controle de Acesso:** são barreiras lógicas ou físicas que impedem ou limitam o acesso à informação, bem como protegem as mesmas de modificações não autorizadas.
- **Colaborador**: denominação dada à pessoa contratada cujo vínculo de cunho empregatício é regido pela CLT - Consolidação das Leis do Trabalho.
- **Criptografia**: técnicas utilizadas para transformar a informação da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado.
- **Classificação da Informação:** processo que tem como objetivo identificar e definir níveis e critérios adequados para a proteção das informações, de acordo sua importância para as organizações.
- **CFTV:** sigla utilizada para circuito fechado de TV, é o monitoramento de ambientes através de câmeras analógicas ou digitais.
- **Código-fonte:** um conjunto de arquivos de texto contendo todas as instruções que devem ser executadas pelo computador de forma lógica numa linguagem de programação.
- **Dispositivos Móveis:** equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento.
- **Disponibilidade:** propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados a acessar.
- **Dados Pessoais:** são considerados dados pessoais, para fins de cumprimento desta política, os listados no artigo 5º, inciso I da Lei Geral de Proteção de Dados 13.709/2018.
- **Dados Pessoais Sensíveis:** são considerados dados pessoais, para fins de cumprimento desta política, os listados no artigo 5º, inciso II da Lei Geral de Proteção de Dados 13.709/2018.
- **Dados de Cartão:** são informações relativas ao portador do cartão como nome, número do cartão, data de validade, número de segurança e outros dados transacionais.
- **Dados Financeiros:** qualquer dado transacional, com identificação do usuário, valor da transação, data e horário, histórico de pagamentos, dados de cartão, saldo de recarga, saldo em conta e dados de investimentos.
- **Estação de Trabalho:** computador/recurso fornecido ao colaborador ou prestador de serviços para execução de tarefas relativas ao trabalho.
- **Fornecedor:** empresa que fornece ou venha a fornecer algum tipo de produto e/ou serviço para o Original.

- **Incidente de Segurança:** qualquer evento que resulte em perda ou dano aos ativos da companhia, ou qualquer ação que desrespeite as regras de segurança.
- **Informação:** é um conjunto de dados relacionados entre si que levam a compreensão de algo e que traz um determinado conhecimento. A Informação pode estar na forma escrita, verbal, imagem, meio digital e/ou físico.
- ***Malware*:** qualquer tipo de *software* malicioso projetado para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável.
- **Parceiro:** empresa que participa com o Original no desenvolvimento de seus produtos e serviços.
- **Prestador de Serviço:** parte contratada pelo Original que tem acesso às instalações, recursos e informações necessárias para o cumprimento de suas obrigações profissionais.
- **Proprietário da Informação:** responsável que define quem tem acesso à informação e que tipo de privilégio de acesso deve ser atribuído.
- **Riscos de Cibernéticos**: possibilidade de uma ameaça explorar vulnerabilidades dos ativos, comprometendo a confidencialidade, integridade e disponibilidade das informações.
- **Sistemas de Informação**: todos os sistemas de informação que são utilizados pela empresa para suportar suas operações.
- ***Software*:** um conjunto de instruções lógicas que devem ser seguidas e executadas por um mecanismo, seja ele um computador ou um aparelho eletromecânico.
- **Usuário:** pessoa que utiliza sistemas e/ou demais recursos de tecnologia fornecidos pela companhia.
- **VPN (*Virtual Private Network*):** rede privada (virtual), que tem como objetivo estabelecer uma comunicação segura entre os usuários e os sistemas/aplicações do Original que são acessados por uma rede pública.
- ***Wi-Fi*:** tecnologia de rede sem fio que permite que dispositivos como notebooks, smartphones e similares se conectem à Internet.

6. Diretrizes

Neste capítulo, são apresentadas as diretrizes gerais desta Política. Essas diretrizes constituem os principais pilares da Gestão de Segurança Cibernética, norteando a elaboração de Procedimentos e Manuais, bem como a implementação de controles, seguindo os seguintes princípios:

I. **Confidencialidade:** garantia de que toda Informação estará acessível apenas para pessoas autorizadas, garantindo o conceito de "mínimo privilégio possível".

II. **Integridade:** garantia de que a informação, armazenada ou em trânsito, seja completa, exata e não sofrerá qualquer modificação ou exclusão não autorizada.

III. **Disponibilidade:** garantia de que a Informação sempre estará disponível quando necessário; e

IV. **Autenticidade:** garantia da veracidade da informação, certificando que a Informação é verdadeira e que não sofreu alteração em seu ciclo de vida.

1.1 Gestão de Riscos Cibernéticos

O Original possui processos e mecanismos para identificar, avaliar, corrigir e monitorar os Riscos Cibernéticos que podem trazer impactos para a companhia. Observando, mas não se limitando às seguintes diretrizes:

I. Identificação e registro dos riscos de Segurança, no qual seja possível realizar a sua formalização e ciência;

II. Análise e classificação dos riscos identificados, no qual seja possível mensurar a criticidade e o impacto para a companhia;

III. Tratamento dos riscos de acordo com sua criticidade e relevância para a companhia, independentemente de sua classificação;

IV. Monitoramento e reavaliação periódica dos riscos, a fim de observar a aplicação dos controles e sua eficiência; e

V. Relatório periódico com as tratativas dos riscos identificados, bem como a eficiência do processo.

O detalhamento do processo deve ser consultado por meio do Procedimento de "**Gestão de Riscos Cibernéticos**", disponibilizado no portal de documentações do Original.

1.2 Gestão de Ativos e Tratamento de Informações

O Original possui processos e mecanismos para a Gestão dos Ativos de Informações, a fim de protegê-los de acesso não autorizado, bem como uma metodologia para classificá-los de acordo com o grau de sensibilidade para o negócio, considerando o seu valor e sua necessidade para as operações da companhia. Observando, mas não se limitando às seguintes diretrizes:

I. Todos os ativos de Informação devem ser inventariados e submetidos a um processo de homologação que verifica, entre outros aspectos, os requisitos legais e técnicos para sua utilização;

II. Uma lista com os *Softwares* homologados deve ser criada e mantida regularmente atualizada pela área de Tecnologia;

III. Todas as Estações de Trabalho devem possuir políticas e controles implementados, a fim de garantir que *Softwares* não homologados não sejam instalados. Caso seja identificado, estes devem ser removidos imediatamente;

IV. Todos os Ativos de Informação, sejam eles no formato físico ou lógico, devem ser protegidos, cuidados e gerenciados adequadamente;

V. Devem ser definidos critérios objetivos para a classificação e rotulação das informações de acordo com a relevância e sensibilidade para o negócio;e

VI. Devem ser adotadas ferramentas e medidas administrativas que permitam proteger e monitorar as informações, bem como detectar possíveis violações das regras de proteção estabelecidas.

O detalhamento do processo deve ser consultado por meio dos Procedimentos de "**Gestão de Ativos**" e "**Classificação da Informação**", disponibilizados no portal de documentações do Original.

1.3 Postura de Segurança

Todos os Colaboradores e Prestadores de Serviços tem o compromisso individual de proteger as Informações do Original, por esta razão, são esperados os seguintes comportamentos, mas não se limitando a:

- Todos os Colaboradores e Prestadores de Serviços devem realizar a leitura desta Política, bem como, todos os Procedimentos e Manuais criados a partir dela;
- Todos os Colaboradores e Prestadores de Serviços devem realizar a leitura do termo de responsabilidade sobre a Segurança Cibernética, bem como assiná-lo no ato da contratação;
- Todos os Colaboradores devem compreender os Riscos Cibernéticos inerentes às suas atividades de trabalho e tomar medidas preventivas para mitigá-los;
- Todos os recursos fornecidos pela companhia, devem ser utilizados para suas atividades de trabalho. Quaisquer exceções deverão ser avaliadas e formalizadas;

- Toda Informação produzida e/ou recebida pelos Colaboradores, Fornecedores e Prestadores de Serviços, em resultado da função exercida e/ou atividade profissional, é de propriedade da companhia. Quaisquer exceções devem ser devidamente formalizadas;
- As senhas de usuário bem como seus tokens, do múltiplo fator de autenticação, são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive entre os Colaboradores da própria companhia);
- Todos os Colaboradores e Prestadores de Serviços devem agir de forma ética preservando os princípios de Segurança estabelecidos nesta Política;
- Todas as informações críticas ou de negócios, sejam elas em formato digital ou impresso, devem ser guardadas em lugar seguro (idealmente em cofre, armário, drive corporativo ou outras formas de armazenamento); e
- Todas as estações de trabalho devem ser protegidas de acesso indevido e/ou não autorizado às informações, por meio de (usuário/senha), bem como o bloqueio de tela ou desligamento do dispositivo quando o responsável não estiver presente.

1.4 Controle de Acesso Lógico

Todo acesso às informações e aos ambientes lógicos do Original devem ser controlados, de forma a garantir permissão apenas às pessoas autorizadas pelo respectivo proprietário da informação. Observando, mas não se limitando às seguintes diretrizes:

I. Procedimento formal de concessão e cancelamento de acesso aos sistemas e bases de dados da companhia, bem como outras origens de Informação que precisam ter o seu acesso controlado;

II. Comprovação da autorização do proprietário da Informação para a concessão do acesso aos sistemas sob sua responsabilidade;

III. Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;

IV. Verificação do nível de acesso concedido e se é apropriado ao propósito da atividade exercida pelo colaborador ou prestador de serviço;

V. Remoção tempestiva de autorizações dadas a usuários afastados ou desligados da companhia, ou que tenham mudado de função;

VI. Processo de revisão periódica dos acessos e autorizações concedidas;

VII. Definição de critérios objetivos para a atribuição, manutenção e uso de senhas fortes nas aplicações e sistemas da companhia;

VIII. Estabelecer o princípio do menor privilégio, em que cada usuário deverá possuir o mínimo de privilégios necessários para desempenhar suas atividades; e

IX. Todas as aplicações críticas da companhia devem possuir um duplo fator de autenticação, a fim de mitigar o risco de acesso indevido ou não autorizado.

O detalhamento do processo deve ser consultado por meio do Procedimento de "**Gestão de Acessos Lógicos**", disponibilizado no portal de documentações do Original.

1.5 Controle de Acesso Físico

O Original possui processos e mecanismos para a Gestão de Acesso Físico às suas instalações, de forma a garantir o controle de acesso e os registros necessários para autorização e permanência das pessoas que trafegam pelo ambiente da companhia. Observando, mas não se limitando às seguintes diretrizes:

I. Implementação de barreiras e perímetros de acesso físicos, tais como catracas e segurança patrimonial, a fim de evitar acesso não autorizado às instalações da companhia;

II. Todos os acessos de Colaboradores e terceiros às instalações da companhia, devem ser expressamente autorizados e registrados por meio de controles biométricos e/ou cartão magnético (crachá);

III. Todos os Colaboradores ou terceiros devem possuir identificação, por meio da utilização de crachá, mantendo sempre em local visível;

IV. Todos os acessos de Colaboradores e terceiros às instalações físicas da companhia devem ser monitorados via sistema CFTV; e

V. Todos os acessos às áreas de armazenamento de informações críticas e às instalações de equipamentos sensíveis, devem possuir controles adicionais de segurança.

O detalhamento do processo deve ser consultado por meio do procedimento de "**Gestão de Acesso Físico**", disponibilizado no portal de documentações do Original.

1.6 Monitoramento, Controle e Auditoria

O Original possui processos e mecanismos para garantir a rastreabilidade das informações, bem como o registro das ações que foram realizadas nos sistemas e aplicações da companhia. Observando, mas não se limitando às seguintes diretrizes:

I. Implementação de sistemas de monitoramento em Estações de Trabalho, correio eletrônico, conexões com a internet, dispositivos móveis e outros componentes da rede, de forma que

a Informação gerada ou trafegada por eles permita a sua rastreabilidade, identificando usuários e respectivos acessos efetuados;

II. Instalação de sistemas de proteção, preventivos e/ou repressivos, para garantir segurança das Informações e dos perímetros de acesso das Estações de Trabalho;

III. Todos os Ativos de Informação como (sistemas e aplicações), devem ser capazes de gerar trilhas de auditoria com as informações necessárias (*logs*) para a identificação adequada das ações que foram executadas; e

IV. Todos os registros devem ser mantidos por período definido na Política de Retenção de Informações e Documentos, a fim de atender as regulamentações vigentes.

1.7 Gestão de Ameaças e Incidentes

O Original possui processos e mecanismos que garantam a devida prevenção, detecção e tratamento de ameaças aos ativos e sistemas de Informação da companhia, bem como o Gerenciamento de Incidentes de Segurança que possam comprometer os serviços e operações do Original. Observando, mas não se limitando às seguintes diretrizes:

I. Todos os Ativos de Informação devem possuir mecanismos de detecção e proteção contra ameaças em sua versão mais atual disponível;

II. Implementação de controles para a detecção e inibição de ações e/ou comportamentos maliciosos causados por agentes internos ou externos mal-intencionados;

III. A área de Segurança Cibernética tem autonomia para medidas para combater ou prevenir a disseminação de agentes maliciosos. Além destes mecanismos, devem ser empregados controles que garantam a prevenção e detecção de intrusão;

IV. Todos os Incidentes de Segurança devem ser identificados e registrados a partir do monitoramento do ambiente ou reportado por Colaboradores, Fornecedores ou Prestadores de Serviços, bem como classificado e priorizado de acordo com o impacto para o negócio;

V. Todos os Incidentes de Segurança devem ser investigados, estudados e corrigido, de forma a preservar disponibilidade, integridade, confidencialidade e autenticidade da Informação;

VI. Todos os incidentes que houver indícios de atividade ilícita ou criminal, devem ser avaliados individualmente e constatado o fato ilícito, as autoridades competentes deverão ser acionadas para tomar as medidas cabíveis e criminais; e

VII. Devem ser disponibilizados relatórios periódicos dos incidentes para as partes envolvidas, bem como para fins de investigação e/ou conformidade com as autoridades e entidades reguladoras; e

VIII. Incidentes cibernéticos relevantes, que envolvam vazamento de dados pessoais, serão notificados aos titulares e entidades reguladoras, conforme critérios estabelecidos no procedimento de Gestão de Incidentes de Segurança.

O detalhamento do processo deve ser consultado por meio dos Procedimentos de "**Gestão de Ameaças**" e "**Gestão de Incidentes de Segurança**", disponibilizado no portal de documentações do Original.

1.8 Segurança nas Operações

O Original possui processos e mecanismos para garantir que as operações, produtos e serviços oferecidos pela companhia estejam sempre disponíveis e protegidos de falhas ou indisponibilidades. Observando, mas não limitando-se somente, as seguintes diretrizes:

I. Implementação do uso de criptografia quando envolver dados pessoais, dados pessoais sensíveis, dados de cartão de crédito ou quaisquer outras informações críticas ou confidenciais para o negócio, sejam elas, dados em trânsito ou em repouso;

II. Verificação periódica de vulnerabilidades nos Ativos de Informação de tecnologia da companhia, tais como redes, sistemas e aplicações a fim de identificar necessidades de correção e/ou atualização;

III. Todas as vulnerabilidades identificadas devem ser analisadas e direcionadas para os responsáveis corrigirem dentro do prazo determinado.

IV. Realizar testes de intrusão nas aplicações internas que realizam tratamento de informações da companhia, como processamento, transmissão e armazenamento;

V. Estabelecer uma rotina de Backup das informações, bem como mecanismos que permitam a restauração caso ocorra perda de dados (voluntárias ou acidentais) por erro humano, ataques externos, catástrofes naturais ou outras ameaças;

VI. Realizar testes periódicos de backup, a fim de identificar possíveis falhas na execução do processo e mitigar o risco de perda dos dados;

VII. Monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a Integridade da rede, sistemas e dados internos;

VIII. Os Ativos de Informação fornecidos pela companhia são de propriedade do Original, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança Cibernética; e

IX. Os Ativos de Informação utilizados por terceiros que prestam serviços para o Original, devem ser configurados para acessar as Informações da companhia somente por VPN e deve possuir o agente de segurança instalado para monitoramento das atividades.

1.9 Continuidade de Negócios

O Original possui processos para criar, manter e testar periodicamente uma estratégia de Continuidade dos Negócios, considerando os processos críticos da companhia, bem como para assegurar que o negócio esteja pronto para operar em caso de interrupção total ou parcial de suas atividades operacionais. Observando, mas não limitando-se somente, as seguintes diretrizes:

I. Desenvolver e implementar uma estratégia de Análise de Impacto no Negócio (*BIA - Business Impact Analisys*);

II. Desenvolver procedimentos operacionais que possam reduzir os impactos decorrentes da interrupção de serviços causada por desastres, crises, indisponibilidades, falhas, e eventos adversos;

III. Desenvolver planos de testes operacionais e aplicá-lo periodicamente, a fim de avaliar a eficiência do processo, bem como, identificar e aplicar possíveis melhorias; e

IV. Desenvolver e disponibilizar relatórios periódicos de Continuidade dos Negócios, bem como apresentar possíveis riscos para as áreas envolvidas.

O detalhamento do processo deve ser consultado por meio do Procedimento de "**Gestão de Continuidade de Negócio**", disponibilizado no portal de documentações do Original.

1.10 Gestão de Fornecedores, Prestadores de Serviços e Parceiros

O Original possui processos e metodologia para avaliar seus Fornecedores, Prestadores de Serviços e/ou parceiros de negócio, a fim de serem identificados possíveis Riscos Cibernéticos que possam comprometer a Integridade, Disponibilidade, Confidencialidade e Autenticidade das informações da companhia. Observando, mas não limitando-se somente as seguintes diretrizes:

I. Todos os fornecedores, Prestadores de Serviços e/ou parceiros de negócio, que realizam tratamento de dados confidenciais, devem passar por um processo de avaliação, realizado pela área de Segurança Cibernética, previamente à contratação e, periodicamente, após a contratação;

II. Todos os fornecedores, Prestadores de Serviços e/ou parceiros de negócio, devem ser avaliados considerando os aspectos técnicos como infraestrutura, plataforma ou serviços em nuvem, bem como os seus controles, processos e tecnologias;

III. Deve-se estabelecer critérios objetivos para avaliar e classificar os fornecedores, Prestadores de Serviços e/ou parceiros de negócio, a fim de determinar seu nível de maturidade em relação aos requisitos mínimos de Segurança Cibernética;

IV. As áreas de negócio devem levar em consideração o resultado da avaliação de Segurança para realizar a contratação dos Fornecedores, Prestadores de Serviços e/ou parceiros de negócio. Caso o nível de maturidade seja abaixo do esperado, a área de negócio deve adotar medidas preventivas para seguir com a contratação dos serviços;

V. Deve-se estabelecer critérios objetivos para a suspensão dos acessos e dos serviços aos fornecedores, Prestadores de Serviços e/ou parceiros de negócio que, eventualmente, possam expor os sistemas e as Informações do Original; e

VI. Deve ser realizada uma avaliação de qualidade dos serviços fornecidos pelos Fornecedores e Prestadores de Serviços.

O detalhamento do processo deve ser consultado por meio do Procedimento de "**Gestão Fornecedores, Parceiros e Terceiros**", disponibilizado no portal de documentações do Original.

1.11 Redes e Comunicações

O Original possui processos e medidas técnicas, a fim de assegurar a proteção adequada da rede e meios de comunicações da companhia, bem como monitora e segregar, fisicamente ou logicamente os ambientes, adotando controles e permissões de acesso, em conformidade com a necessidade de uso dos Colaboradores, Prestadores de Serviços, fornecedores e visitantes. Observando as seguintes diretrizes:

I. A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade do Original ou Prestadores de Serviços autorizados, com a finalidade restrita à realização de atividades de trabalho;

II. A Internet sem fio (Wi-Fi) deverá ser segregada, garantindo o isolamento da rede interna da companhia, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os Colaboradores desempenharem suas tarefas;

III. Deve ser criada outras redes sem fio (Wi-Fi) com acesso apenas à Internet para disponibilizar a visitantes e usuários que não precisam ter acesso aos sistemas e dados internos da companhia; e

IV. Toda concessão de acesso à rede do Original, deve ser registrado via chamado, onde passará por análise e aprovação pelos responsáveis.

1.12 Desenvolvimento Seguro e Adoção de Novas Tecnologias

O Original possui processos e medidas técnicas para garantir que durante o ciclo de desenvolvimento de novas aplicações, assim como na adoção de novas tecnologias, existam controles capazes de identificar vulnerabilidades e corrigi-las antes da entrada em produção. Observando as seguintes diretrizes:

I. Os ambientes de desenvolvimento, homologação, qualidade e produção devem ser segregados, a fim de evitar possíveis Riscos Cibernéticos para a companhia;

II. Todos os códigos-fonte desenvolvidos internamente ou obtidos de terceiros, devem passar por um processo de revisão (Code review);

III. Todos os sistemas desenvolvidos internamente ou obtidos de terceiros devem possuir um controle de versionamento, bem como o registro das atualizações;

IV. Todas as mudanças nos sistemas que estiverem em produção devem ser registradas e aprovadas pelos responsáveis; e

V. Todos os sistemas desenvolvidos internamente ou obtidos de terceiros, devem passar pela esteira de desenvolvimento seguro, a fim de garantir que o código esteja aderente aos requisitos de segurança.

1.13 Gestão de Conformidade de Segurança

O Original possui processos definidos para a Gestão de Conformidade com os controles de segurança estabelecidos nesta Política, bem como avaliar possíveis desvios com as boas práticas e regulamentações vigentes. Observando, mas não limitando-se somente, as seguintes diretrizes:

I. Avaliações periódicas dos controles implementados, bem como sua eficiência, considerando aspectos técnicos, legais e contratuais;

II. Todos os casos de desvio de conformidade devem ser registrados e direcionados para a área responsável implementar um plano de ação dentro do prazo estabelecido;

III. A área de Segurança Cibernética é responsável por estabelecer um calendário de avaliação dos controles e executá-lo conforme o planejado; e

IV. Deve ser criado um relatório periódico das avaliações realizadas e disponibilizado para os gestores.

O detalhamento do processo deve ser consultado por meio do Procedimento de “**Gestão de Conformidade de CiberSegurança**”, disponibilizado no portal de documentações do Original.

1.14 Cultura e Conscientização

O Original possui um programa contínuo de educação, treinamentos e ações de conscientização para todos os Colaboradores e Prestadores de Serviços que manipulam informações da companhia. Observando, mas não limitando-se somente as seguintes diretrizes:

I. Desenvolvimento de treinamentos relacionados a conhecimentos gerais sobre segurança cibernética para todos os Colaboradores e Prestadores de Serviços;

II. Desenvolvimento de treinamentos específicos de segurança cibernética para todos os Colaboradores e Prestadores de Serviços que desempenham atividades de maior complexidade e impacto para o Original;

III. Aplicação de testes de conhecimentos, a fim de avaliar a eficiência e o desempenho dos Colaboradores em relação aos treinamentos e as campanhas de conscientização realizadas;

IV. Desenvolvimento de um relatório periódico dos Colaboradores e Prestadores de Serviços que realizaram os treinamentos, bem como daqueles que não realizaram;

V. Remoção de acessos dos Colaboradores que não realizarem os treinamentos dentro do prazo estabelecido pela área de Segurança e Compliance;

VI. Desenvolvimento de um cronograma de conscientização para todos os Colaboradores e Prestadores de Serviços; e

VII. Devem ser aplicadas, regularmente, campanhas de conscientização sobre o tema de Segurança para todos os colaboradores e prestadores de Serviços.

O detalhamento do processo deve ser consultado por meio do procedimento de “**Gestão de Treinamento e Conscientização**”, disponibilizado no portal de documentações do Original.

1.15 Demandas Regulatórias

O Original se compromete a manter arquivados pelo período de 5 (cinco) anos, os documentos citados abaixo, caso venham a ser solicitados pelo Banco Central do Brasil:

I. A presente Política de Segurança Cibernética;

II. Ata de reunião do comitê de diretoria com a aprovação desta Política;

III. Documentação relativa aos planos de ação e resposta a incidentes;

IV. Relatório anual sobre a implementação do plano de ação e de resposta a incidentes;

V. Documentação sobre procedimentos;

VI. Documentação de que trata de serviços prestados no exterior; e

VII. Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem.

1.16 Violação da Política Cibernética e Sanções

O descumprimento ou a inobservância de quaisquer regras ou diretrizes definidas nesta Política e normas complementares, constituem falta grave, sobre as quais o Original poderá aplicar todas as medidas cabíveis nos âmbitos administrativo e judicial.

São considerados comportamentos contrários à Política de Segurança Cibernética do Original, mas não se limitando a:

I. Praticar atos irregulares que causem prejuízo ao Original, com o intuito de obter lucro ou vantagem de qualquer espécie (próprio ou para terceiros);

II. Qualquer comportamento comissivo ou omissivo no tratamento das informações que possam causar vazamento ou acesso indevido;

III. A utilização de qualquer dos recursos fornecidos pela empresa para fins unicamente particulares e que possam gerar algum risco ou perda para a Companhia;

IV. Apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, dados, programas, documentos físicos ou quaisquer outros de forma intencional e/ou não autorizada;

V. Obter, manter ou fornecer a terceiro acesso de forma indevida ou não autorizada a dados, instrução, computador, rede, ambientes ou qualquer meio de identificação, tais como crachás, senhas, logins, entre outros;

VI. Obter segredos, informações sigilosas ou dados pelos quais o usuário não possui acesso, armazenadas em computador, rede, meio eletrônico de natureza magnética, óptica ou similar, bem como documentos físicos, de forma indevida ou não autorizada;

VII. Criar, desenvolver ou inserir dado ou programa, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dados ou programas de computador, ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede;

VIII. Realizar download e upload de jogos, filmes, conteúdo pornográfico, bem como de qualquer outro programa que atende única e exclusivamente aos interesses do usuário e não da companhia;

IX. Distribuir cópia não autorizada de arquivos, informações, *software* ou qualquer outro ativo da companhia sem autorização;

X. Utilizar o serviço de correio eletrônico para envio de mensagens com teor político/partidário, racista, preconceituoso, pornográfico, pejorativo ou com outros fins não pertinentes às atividades do Original;

XI. Utilizar qualquer meio ou subterfúgio para burlar, fraudar, anular ou impedir a ação dos sistemas de segurança da Informação implementados no Original; e

XII. Agir em desacordo com padrões e procedimentos específicos de utilização dos recursos e serviços fornecidos pelo Original.

A área de Segurança Cibernética é responsável por avaliar o grau de criticidade da violação e solicitar o envolvimento de outras áreas como RH, Compliance e Jurídico para a análise das medidas cabíveis de acordo com o Procedimento de "**Gestão de Consequências**".

7. Papéis e Responsabilidades

Comitê de Diretoria

- O Comitê de Diretoria é responsável pela aprovação da presente Política, bem como pela disseminação da cultura de Segurança Cibernética para todos os Colaboradores, Prestadores de Serviços, parceiros, clientes e comunidade em geral.

Diretores Estatutários

- Devem zelar pelo cumprimento das diretrizes estabelecidas nesta Política através de suas alçadas competentes, bem como por comprometer-se, na medida do possível, na dedicação de recursos que permitam a adequada gestão de Segurança Cibernética e o estabelecimento do Plano Diretor de Segurança.

Segurança Cibernética

- A área de Segurança Cibernética é responsável pela adoção e implementação de tecnologias, processos e controles que possam garantir ao Original salvaguardar seus Ativos de Informação, além de ser responsável por orientar e informar os Colaboradores e terceiros sobre a comunicação de possíveis incidentes e/ou violações desta Política.

Governança Cibernética

- A área de Governança Cibernética é responsável por estabelecer e manter um modelo de gestão de segurança cibernética, por meio da adoção de um framework, com intuito de apoiar as estruturas de gestão e processos para garantir a conformidade com as diretrizes de segurança e aderência às regulamentações necessárias.

TI Corporativa

- A área de TI Corporativa é responsável por gerenciar e disponibilizar os ativos de tecnologia para os colaboradores, bem como implementar os controles de segurança de acordo com os critérios estabelecidos nesta Política e demais normas internas. Além de apoiar o time de Segurança Cibernética nas ações de análise e remediação de incidentes que envolvam os sistemas e redes de comunicação da Companhia.

Recursos Humanos

- A área de Recursos Humanos é responsável por apoiar a área de Segurança Cibernética na execução de controles relacionados aos processos de contratação, conscientização, encerramento e modificação dos colaboradores e terceiros que tratam informações da Companhia, bem como atuar em análises dos casos de violação desta Política e demais normas complementares.

Procurement

- A área de Procurement é responsável por envolver, sempre que necessário, a área de Segurança Cibernética em possíveis contratações de novos fornecedores e parceiros de negócios que envolve a manipulação, processamento, armazenamento ou compartilhamento de informações de clientes, negócios ou confidenciais.

Privacidade e Proteção de Dados

- A área de Privacidade é responsável por estabelecer regras de tratamentos de dados com base na legislação vigente, bem como envolver a área de Segurança Cibernética em questões de compartilhamento, processamento e armazenamento de dados pessoais e dados pessoais sensíveis, sempre que necessário.

Gestão de Continuidade de Negócios

- A área de Gestão de Continuidade de Negócios é responsável por estabelecer e operacionalizar um plano de continuidade de negócios, bem como definir critérios mínimos de continuidade nos parceiros e/ou fornecedores, a fim de garantir que as operações do Original permaneçam disponíveis em caso de interrupção parcial ou total dos serviços.

Jurídico

- A área de Jurídico é responsável por envolver, sempre que necessário, a área de Segurança Cibernética no processo de análise contratual de fornecedores, parceiros e terceiros, bem como, apoiar a área em questões jurídicas e análises quando houver descumprimento desta Política e normativos complementares.

Facilities

- A área de Facilities é responsável por estabelecer medidas para proteger as instalações físicas dos escritórios do Original, bem como evitar o acesso não autorizado às instalações da companhia, por meio da implementação de controles que visam registrar e monitorar o ambiente.

Colaboradores, Parceiros e Prestadores de Serviços

- Todos os Colaboradores, Parceiros e Prestadores de Serviços são responsáveis cumprir as diretrizes estabelecidas nesta Política, bem como proteger as informações do Original e por apoiar a área de Segurança Cibernética na disseminação da cultura de Segurança.

8. Alçadas

Não aplicável.

9. Referências e Normativos Internos Vinculados

Esta Política foi desenvolvida com base nos principais Frameworks de Segurança Cibernética, a fim de atender às diretrizes de Segurança estabelecidas pelo Banco Central do Brasil e outras entidades reguladoras.

a) Resolução BCB nº 85/2021;

b) Resolução CMN nº 4.893/2021;

c) LGPD - Lei Geral de Proteção de Dados 13.709/2018;

d) CVM - Instrução de Comissão de Valores Mobiliários nº 35/2021;

e) NIST - National Institute of Standards and Technology;

f) ISO/IEC 27001:2022 e ISO/IEC 27002:2022;

g) PCI DSS - Payment Card Industry – Data Security Standard;

h) ISO/IEC 27005:2023;

i) ISO/IEC 31000:2018.

10. Anexo

Não Aplicável.

11. Histórico de alterações

Tópico alterado	**Detalhamento**	**Data da alteração**
Criação do Documento.	1. Unificação das diretrizes de Segurança Cibernética do Conglomerado Prudencial e suas controladas revogando qualquer Política de Segurança da Informação e Cibernética existente anteriormente.	29/09/2023
Desmembramento da Política	Desmembramento da Política da empresa J&F para o Banco Original.	31/05/2024