Índice

1. Objetivo

Esta Política de Segurança Cibernética ("Política") tem por objetivo definir as diretrizes para o uso, a segurança e o bom gerenciamento dos recursos de TI do Banco Original S.A. e suas controladas ("Banco Original"), garantindo que as informações sejam protegidas, os ativos tecnológicos sejam utilizados de forma eficiente e em conformidade com as normas e regulamentos aplicáveis sejam mantidas, ainda que também divulgada ao público em geral, além de adotar uma visão de abordagem baseada em risco e rastreabilidade de auditoria, conforme determina as principais normativas vigentes do Banco Central do Brasil e demais Órgãos competentes.

2. Fórum de Aprovação

Esta Política é aprovada pelos Comitês de Diretoria e pelo Conselho de Administração ("CA").

3. Vigência

Esta Política terá vigência de 03 (três) anos, ou, em menor prazo, quando o fórum responsável que o aprovou considerar necessário.

4. Aplicação e Público-Alvo

Esta Política se aplica a todos os seus administradores e colaboradores, incluindo também qualquer interação com clientes, parceiros, fornecedores e demais públicos de relacionamento do Banco Original S.A. e demais empresas controladas.

5. Sumário

Segue abaixo, 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 do Banco Original S.A.
- **Backup:** processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda das informações 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, sendo o detentor da "chave secreta", impossibilitando 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 com 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:** é um conjunto de linhas de instruções em uma linguagem de programação que define como um programa de computador deve funcionar. É a forma legível por humanos, antes de ser compilado ou interpretado em código de máquina, que o computador possa executar.

- **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 LGPD - 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 LGPD - 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 Banco Original S.A. e demais empresas controladas.

- **Incidente de Segurança:** qualquer evento que resulte em perda ou danos aos ativos, 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 Banco Original S.A. e demais empresas controladas no desenvolvimento de seus produtos e serviços.

- **Prestador de Serviço:** parte devidamente contratada pelo Banco Original S.A. e demais empresas controladas 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 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, dividido em duas categorias, Software de sistema e Software de aplicação.

- **Usuário:** pessoa que utiliza sistemas e/ou demais recursos de tecnologia fornecidos pelo Banco Original S.A e demais empresas controladas.

- **VPN (Virtual Private Network):** rede privada (virtual), que tem como objetivo estabelecer uma comunicação segura entre os usuários e os sistemas/aplicações do Banco Original S.A. e demais empresas controladas, 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

As 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;

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

6.1 Gestão de Riscos Cibernéticos

O Banco Original S.A. e demais empresas controladas, possui processos e mecanismos para identificar, avaliar, corrigir e monitorar os Riscos Cibernéticos que podem trazer impactos. 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;

iii. Tratamento dos riscos de acordo com sua criticidade e relevância, independentemente de sua classificação;

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

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 na Intranet do Banco Original S.A.

6.2 Gestão de Ativos e Tratamento de Informações

O Banco Original S.A. e demais empresas controladas, 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.
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;

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”, disponibilizado na Intranet do Banco Original S.A.

6.3 Postura de Segurança

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

i. Todos os Colaboradores e Prestadores de Serviços devem realizar a leitura desta Política, bem como, todos os Procedimentos e Manuais criados a partir dela;

ii. 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;

iii. Todos os Colaboradores devem compreender os Riscos Cibernéticos inerentes às suas atividades de trabalho e tomar medidas preventivas para mitigá-los;

iv. Todos os recursos fornecidos, devem ser utilizados para suas atividades de trabalho. Quaisquer exceções deverão ser avaliadas e formalizadas;

v. 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 do Banco Original S.A. e demais empresas controladas. Quaisquer exceções devem ser devidamente formalizadas a área de Segurança Cibernética;

vi. As senhas de usuário bem como seus tokens, do múltiplo fator de autenticação, são pessoais e intransferíveis, não podendo ser compartilhadas, emprestadas, divulgadas a terceiros, inclusive entre os seus Colaboradores do Banco Original S.A. e demais empresas controladas;

vii. Todos os Colaboradores e Prestadores de Serviços devem agir de forma ética preservando os princípios de Segurança estabelecidos nesta Política;

viii. 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);

ix. 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.

6.4 Controle de Acesso Lógico

Todo acesso às informações e aos ambientes lógicos do Banco Original S.A. e demais empresas devem ser controladas, de forma a garantir permissão apenas às pessoas autorizadas pelo respectivo proprietário da informação.
É importante observar, mas não se limitar às seguintes diretrizes:

i. Procedimento formal de concessão e cancelamento de acesso aos sistemas e bases de dados do Banco Original S.A. e demais empresas controladas, 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, 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;

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

ix. Todas as aplicações críticas 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 na Intranet do Banco Original S.A.

6.5 Controle de Acesso Físico

O Banco Original S.A. e demais empresas controladas 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. 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;

ii. Todos os acessos de Colaboradores e terceiros às instalações, devem ser expressamente autorizados e registrados por meio de controles biométricos.

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

iv. 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 na Intranet do Banco Original S.A.

6.6 Monitoramento, Controle e Auditoria

O Banco Original S.A. e demais empresas controladas possui processos e mecanismos para garantir a rastreabilidade das informações, bem como o registro das ações que foram realizadas nos sistemas e aplicações. 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;

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

6.7 Gestão de Ameaças e Incidentes

O Banco Original S.A. e demais empresas controladas possui processos e mecanismos que garantam a devida prevenção, detecção e tratamento de ameaças aos ativos e sistemas de Informação, bem como o Gerenciamento de Incidentes de Segurança que possam comprometer os serviços e operações do Banco Original S.A. e demais empresas controladas.
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;

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;

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 na Intranet do Banco Original S.A.

6.8 Segurança nas Operações

O Banco Original S.A. e demais empresas controladas possui processos e mecanismos para garantir que as operações, produtos e serviços oferecidos 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, 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, 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 são de propriedade Banco Original S.A. e demais empresas controladas, 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;

ix. Os Ativos de Informação utilizados por terceiros que prestam serviços para o Banco Original S.A. e demais empresas controladas, devem ser configurados para acessar as Informações somente por VPN e deve possuir o agente de segurança instalado para monitoramento das atividades.

6.9 Continuidade de Negócios

O Banco Original S.A. e demais empresas controladas possui processos para criar, manter e testar periodicamente uma estratégia de Continuidade dos Negócios, considerando os processos críticos, 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;

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 na Intranet do Banco Original S.A.

6.10 Gestão de Fornecedores, Prestadores de Serviços e Parceiros

O Banco Original S.A. e demais empresas controladas 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.
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 Banco Original S.A. e demais empresas controladas;

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 na Intranet do Banco Original S.A.

6.11 Redes e Comunicações

O Banco Original S.A. e demais empresas controladas, possui processos e medidas técnicas, a fim de assegurar a proteção adequada da rede e meios de comunicações, bem como monitorar 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 Banco Original S.A. e demais empresas controladas 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, 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;

iv. Toda concessão de acesso à rede do Banco Original S.A. e demais empresas controladas, deve ser registrado via chamado, onde passará por análise e aprovação pelos responsáveis.

6.12 Desenvolvimento Seguro e Adoção de Novas Tecnologias

O Banco Original S.A. e demais empresas controladas 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;

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 de infraestrutura ou em sistemas, que estiverem em produção devem ser registradas e aprovadas pelos responsáveis seguindo o Procedimento de GMUD;

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.

6.13 Gestão de Conformidade de Segurança

O Banco Original S.A. e demais empresas controladas 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;

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 Ciber Segurança”, disponibilizado na Intranet do Banco Original S.A.

6.14 Cultura e Conscientização

O Banco Original S.A. e demais empresas controladas possui um programa contínuo de educação, treinamentos e ações de conscientização para todos os Colaboradores e Prestadores de Serviços que manipulam informações. 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 Banco Original S.A. e demais empresas controladas;

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;

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 na Intranet do Banco Original S.A.

6.15 Demandas Regulatórias

O Banco Original S.A. e demais empresas controladas 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 conselho de administração 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;

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

6.16 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 Banco Original S.A. e demais empresas controladas, poderão aplicar todas as medidas cabíveis nos âmbitos administrativo e judicial.

São considerados comportamentos contrários à Política de Segurança Cibernética do Banco Original S.A. e demais empresas controladas, mas não se limitando a:

i. Praticar atos irregulares que causem prejuízo ao Banco Original S.A. e demais empresas controladas, 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 financeira;

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;

ix. Distribuir cópia não autorizada de arquivos, informações, software ou qualquer outro ativo sem prévia 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 suas atividades;

xi. Utilizar qualquer meio ou subterfúgio para burlar, fraudar, anular ou impedir a ação dos sistemas de segurança da Informação implementados;

xii. Agir em desacordo com padrões e procedimentos específicos de utilização dos recursos e serviços fornecidos.

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.

7. Papéis e Responsabilidades

Conselho de Administração

- O Conselho de Administração 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 da gestão de Segurança Cibernética.

Segurança Cibernética

- A área de Segurança Cibernética é responsável pela adoção e implementação de tecnologias, processos e controles que possam garantir ao Banco Original S.A. e demais empresas controladas salvaguardar seus Ativos de Informação, além de ser responsável por treinar, 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.

Área de TI

- A área de TI 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.

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 incluindo os devidos treinamentos no processo 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 a área de Segurança Cibernética em possíveis contratações de novos fornecedores de sistemas, ferramentas, parceiros de negócios que envolva a manipulação, processamento, armazenamento ou compartilhamento de informações de clientes, negócios ou de informações 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.

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 Banco Original S.A. e demais empresas controladas e suas controladas, bem como evitar o acesso não autorizado às instalações, 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 Banco Original S.A. e demais empresas controladas 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.

i. Resolução BCB nº 85/2021;
ii. Resolução CMN nº 4.893/2021;
iii. LGPD - Lei Geral de Proteção de Dados 13.709/2018;
iv. CVM - Instrução de Comissão de Valores Mobiliários nº 35/2021;
v. NIST - National Institute of Standards and Technology;
vi. ISO/IEC 27001:2022 e ISO/IEC 27002:2022;
vii. PCI DSS - Payment Card Industry – Data Security Standard;
viii. ISO/IEC 27005:2023;
ix. ISO/IEC 31000:2018.

10. Anexos

Não aplicável

11. Histórico de alterações

Tópico alterado	Detalhamento	Data da alteração
Criação do Documento.	Primeira versão da Política de Segurança Cibernética	22/09/2024
Revisão geral do documento	Revisão geral do documento após a segregação das empresas com troca do nome da área responsável no cabeçalho e vários tópicos alterados.	01/12/2025