Banco Paulista

Política de Segurança da Informação e Cyber Security

GRC-11

ÁREA RESPONSÁVEL	PUBLICAÇÃO	VIGÊNCIA	VERSÃO
SEGURANÇA DA INFORMAÇÃO	abr.25	abr.27	v.14

Resumo
Consolida as definições básicas, formaliza diretrizes e relaciona os procedimentos específicos dos mecanismos para garantia dos atributos de segurança dos Ativos de Informação: disponibilidade, integridade, autenticidade, não repúdio e sigilo das informações.

Sumário

1. Objetivo ... 2
2. Público-alvo ... 2
3. Diretrizes Gerais ... 2
4. Conceitos e regras básicas de Segurança da Informação ... 3
4.1 Conceito de Informação ... 3
4.2 Intervenientes da Segurança da Informação e responsabilidades ... 3
4.3 Ativos de Informação ... 4
4.4 Princípios da Segurança da Informação ... 4
4.5 Ciclo de vida da Informação ... 4
4.6 Classificação da Informação ... 5
4.7 Sistema de Gestão da Segurança da Informação ... 6
5. Incidentes de Segurança da Informação ... 7
6. Identificação de Riscos (risk assessment) ... 8
7. Ações de Prevenção e Proteção ... 8
8. Proteção e privacidade da informação de identificação pessoal ... 10
9. Desenvolvimento Seguro de Aplicações e Sistemas ... 11
10. Segurança física e do ambiente ... 11
11. Backup ... 11
12. Monitoramento e Testes ... 12
13. Arquivamento de Informações ... 12
14. Responsabilidade ... 12
15. Referência Cruzada com Outros Normativos Internos ... 12
16. Alinhamento com Órgãos Reguladores e Legislações ... 13
17. Informações de Controle ... 14

1. Objetivo

Formalizar os conceitos e as diretrizes da Segurança da Informação e *Cyber Security* [1] do Banco Paulista que visam à proteção dos ativos de informação com eficiência e eficácia, de modo seguro e transparente, garantindo a confidencialidade, integridade e disponibilidade das informações.

Adicionalmente, essa política tem por objetivo contemplar todas as ações geradas e/ou implementadas pelo Banco Paulista, visando prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados ao ambiente cibernético.

2. Público-alvo

Público em geral, especialmente clientes e parceiros, gestores, colaboradores, prestadores ou fornecedores de serviços, e usuários externos das informações pertencentes/custodiadas ao/pelo Banco Paulista.

3. Diretrizes Gerais

a) Deve ser assegurado pelo Departamento de Compliance que esta Política, normas complementares e as responsabilidades quanto à Segurança da Informação estejam amplamente divulgadas ao público-alvo, visando à sua disponibilidade para todos que se relacionam com o Banco Paulista e que, direta ou indiretamente, são impactados.

b) Esta Política e suas normas complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, no qual os usuários têm acesso somente aos ativos de informação imprescindíveis para o pleno desempenho de suas atividades. Ou seja, tudo que não estiver expressamente permitido só poderá ser realizado após prévia autorização do Departamento de Compliance ou do Departamento de Segurança da Informação e Tecnologia da Informação, devendo ser levado em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

c) A informação deve ser utilizada de forma transparente e apenas para execução de sua atividade profissional. A gestão da informação e dos ativos deve ser assegurada por meio de medidas efetivas que proporcionem acesso e divulgação devidamente autorizados e de acordo com a legislação vigente e com o seu nível de classificação (**v. item 4**).

d) O Banco Paulista é detentor de todos os direitos patrimoniais relativos às suas marcas, nomes comerciais e qualquer informação produzida através do uso dos Recursos de Tecnologia da Informação e Comunicação (RTICs), portanto proíbe o uso não autorizado de suas logomarcas, identidade visual e quaisquer outros sinais distintivos, atuais e futuros, em qualquer forma ou mídia, inclusive na Internet.

e) Sempre que considere necessário, o Departamento de Compliance ou o Departamento de Segurança da Informação e Tecnologia da Informação podem inspecionar quaisquer RTICs (**v. item 4.3**) que porventura interajam com seus ambientes, lógicos ou físicos e/ou suas informações, incluindo aqueles de propriedade de terceiros, serviços de computação e nuvem quando autorizada a sua vinculação ao do Banco Paulista, independentemente da interação com seus ambientes e informações.

f) O Departamento de Segurança da Informação deve manter a segurança dos ativos de informação provendo ferramentas que permitam aplicar as melhores práticas de segurança no ambiente físico ou lógico, para garantir o sigilo e integridade no ciclo de vida da informação, desde a sua recepção, produção, registro, classificação, controle, acesso, manuseio, reprodução, transmissão, guarda e descarte com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques cibernéticos;

g) O Diretor responsável pela política de segurança cibernética nomeado junto aos órgãos reguladores “, além do Departamento de Segurança da Informação e Tecnologia da Informação, são os responsáveis por definir, zelar, aperfeiçoar e garantir a aderência do Banco Paulista às diretrizes de Segurança da Informação e *Cyber Security*[1] com o apoio das demais linhas de defesa da organização (Compliance e Auditoria Interna);

[1] *Cyber* é o diminutivo da palavra *cybernetic*, que em português significa alguma coisa ou algum local que possui uma grande concentração de tecnologia avançada, em especial computadores com grande capacidade de processamento de dados, internet e etc.

h) As ocorrências que podem ser consideradas violações desta Política de Segurança da Informação e *Cyber Security* devem ser avaliadas não só pelas linhas de defesa da organização, mas principalmente pelo Departamento de Segurança Informação e Tecnologia da Informação e, constatado como um incidente (**v. item 4.7**), este deve ser registrado nas

ferramentas de registro definidas pela organização, dependendo de sua gravidade e tema, deverá ser encaminhada para os Comitês internos (ex.: Comitê de Compliance e Comitê de Riscos) para deliberação quanto ao curso de ação a ser tomada.

i) As situações não previstas nesta política serão arbitradas pelo Diretor de Segurança da Informação e Segurança Cibernética, com assessoria dos Departamentos de Compliance e de Tecnologia da Informação e Segurança da Informação;

j) Cabe ao Diretor de Segurança da Informação e Segurança Cibernética aprovar esta normativo e suas diretrizes, assim como, avaliar sua efetividade a qualquer tempo.

4. Conceitos e regras básicas de Segurança da Informação

4.1 Conceito de Informação

Segundo a ISO/IEC 27002:2005(2005), informação é o conhecimento produzido como resultado do processamento de um conjunto de dados (representações de fatos, medidas, valores, ideias ou conceitos), por exemplo:

Informações pertencentes ou relacionadas aos clientes;

a. Informações relacionadas ao Banco Paulista;
b. Estratégias e decisões da alta administração;
c. Informações contábeis do Banco Paulista;
d. Processos e metodologias internos do Banco Paulista;
e. Marcas, logotipos e nomes relacionados aos negócios conduzidos pelo Banco Paulista;
f. Sistema de Instrumentos Normativos Internos do Banco Paulista; e
g. Informações disponibilizadas na Intranet do Banco Paulista.

Assim, considerando que a informação é o resultado de um processamento de dados, cuja operacionalização exige investimento e esforço por parte do Banco Paulista, deve ser tratada como um ativo que deva ser protegida e mantida por meio de regras e procedimentos desta política.

4.2 Intervenientes da Segurança da Informação e responsabilidades

Para efeitos desta política, é algo ou alguém que faz parte dos processos de Segurança da Informação ou pode afetá-los. São classificados em:

a) **Proprietário da informação**: administrador ou gestor de área que possui a responsabilidade de classificar a informação quanto à sua necessidade de sigilo e definir os perfis de acesso. O termo “proprietário” não significa que a pessoa tenha realmente qualquer direito de propriedade sobre a informação, que por essência, pertence ao Banco Paulista.

b) **Custodiante da informação:** indicado pelo “Proprietário da Informação”, é o colaborador, a unidade organizacional ou o fornecedor contratado responsável pela guarda, proteção e defesa das informações produzidas, adquiridas ou custodiadas pelo Banco Paulista e deve observar os critérios e controles definidos no tratamento e classificação da informação.

c) **Usuário da informação:** é a pessoa, a unidade organizacional, a entidade ou o recurso computacional (por exemplo, programas computacionais ou dispositivos) que está autorizado (a) a acessar e fazer uso da informação, de acordo com os privilégios a ele atribuído.

d) **Departamento de Segurança da Informação e Tecnologia da Informação:** é o departamento responsável pelo Sistema de Gestão da Segurança da Informação (v. **item 5**).

Os gestores, colaboradores e prestadores de serviços devem aderir aos termos e condições desta Política de Segurança da Informação, formalizado pelo **Termo de Adesão à Política de Segurança da Informação (Anexo A1 – versão impressa e A versão digital).**

4.3 Ativos de Informação

Entende-se por **Ativos de Informação** qualquer componente de sustentação de processos de negócio capaz de criar, atualizar, alterar, processar, armazenar, transmitir e até excluir a **informação**.

Os Ativos de Informação podem ser classificados como Recursos de Tecnologia da Informação e de Comunicação (**RTICs**), que incluem:

a. Estações de trabalho;

b. Sistema de telefonia;

c. Sistemas de comunicação de dados (*e-mail*, FTP);

d. Acessos à *Internet*;

e. Serviços de rede local (*wireless* e repositórios de dados);

f. "*Data center*";

g. Sistemas aplicativos de processamento de dados;

h. Dispositivos de computação móvel (celulares, *notebooks* e *tablets*);

i. Computação em nuvem; e

j. *Softwares*, que englobam também pacotes aplicativos, extensões e complementos.

Os Ativos de Informação são de propriedade e direito de uso exclusivo do Banco Paulista, e devem ser empregados unicamente para fins profissionais, limitado às atribuições de cargo e/ou função desempenhadas pelo colaborador/prestador de serviço, que deve cumpri-las dentro do padrão de conduta ética estabelecida pelo Banco Paulista e em observância a sua obrigação legal de sigilo profissional, sendo que o mesmo responde diretamente por qualquer dano causado, por ação ou omissão, resultante de sua postura e/ou comportamento, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

O Departamento de Segurança da Informação e Tecnologia da Informação controla o acesso físico e lógico aos seus RTICs, para fins de mitigação do risco de conflito de interesses e acessos não autorizados. Também deve orientar sobre uso de credenciais e coibir o compartilhamento indevido de informações. Desse modo, deve garantir que cada colaborador possua uma credencial de uso individual, intransferível, de conhecimento exclusivo e qualificando-o como responsável pelas ações realizadas.

4.4 Princípios da Segurança da Informação

- **Confidencialidade**: objetiva garantir que a informação não seja disponibilizada ou divulgada a indivíduos, entidades ou aplicativos sem autorização. Em outras palavras, é a garantia do sigilo das informações fornecidas, o que gera proteção contra a sua revelação não autorizada.
- **Integridade:** garantir que a informação não tenha sido alterada em seu conteúdo original e, portanto, é íntegra, autêntica, procedente e fidedigna. Uma informação íntegra é a que não foi alterada de forma indevida ou não autorizada.
- **Disponibilidade**: permite que a informação seja utilizada quando necessária, portanto, esteja ao alcance de seus usuários e destinatários e possa ser acessada no momento pertinente ao uso.

4.5 Ciclo de vida da Informação

Para efeito desta política, será considerado o seguinte ciclo de vida da informação:

- **Manuseio**: é a etapa onde a informação é criada e manipulada.
- **Armazenamento**: consiste na guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.
- **Transporte**: ocorre quando a informação é transportada para algum local, não importando o meio no qual a mesma está armazenada.

- **Descarte**: essa fase refere-se à eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

4.6 Classificação da Informação

A classificação das informações deve ser avaliada em razão do teor do conteúdo, relevância do conhecimento externo e pelos elementos intrínsecos do documento.

O acesso, divulgação e tratamento de documento (físico ou digitalizado), dado ou informação do Banco Paulista são restritos aos colaboradores que tenham necessidade de conhecê-los em razão de suas atividades profissionais, pautados pela regulamentação existente e pelos princípios de pertinência, utilidade e relevância.

Cabe ao Departamento de Segurança da Informação e Tecnologia da Informação estabelecer procedimentos internos e regras específicas quanto ao acesso às informações confidenciais, reservadas ou privilegiadas, concedendo o acesso e controlando as pessoas autorizadas e não autorizadas a receber essas informações, inclusive nos casos de mudança de atividade dentro do Banco Paulista ou desligamento do profissional.

Toda informação de uso corporativo deve ser classificada de acordo com o grau de sigilo para o negócio da empresa, considerando-se os três níveis descritos a seguir:

Classificação da Informação	Quando usar	Público alvo	Impacto
Informação Pública	A informação será divulgada para fora da instituição, sem distinção de público.	Informação acessível e livre para todo e qualquer indivíduo ou meio de comunicação comum e social, sem distinção de público.	**Impacto Baixo:** Revelação destas informações podem causar pouco ou nenhum impacto
Informação Restrita	A informação será divulgada para fora da instituição, com distinção de público.	Informação será compartilhada com um grupo específico e seleto para fora da nossa instituição.	**Impacto Médio:** A revelação não autorizada pode ocasionar dano colateral não desejável.
Informação Interna	A informação será divulgada para todos os colaboradores e prestadores de serviços do Banco Paulista.	Informação acessível para todos os colaboradores e prestadores de serviços do Banco Paulista.	**Impacto Médio:** A revelação não autorizada pode ocasionar dano colateral não desejável.
Informação Confidencial	A informação será divulgada de forma exclusiva com o menor número de colaboradores do Banco Paulista.	Informação acessível exclusivamente para uma pequena quantidade de pessoas internas do Banco Paulista.	**Impacto Alto:** A revelação não autorizada pode causar danos ao negócio, gerar prejuízo financeiro, dano à imagem da instituição, impactar nas operações e viabilizar objetivos estratégicos.

a) Confidencial

É o mais alto grau de sigilo, aplicadas às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. Informação acessível exclusivamente para uma pequena quantidade de pessoas internas do Banco Paulista. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem da empresa.

b) Restrito

A informação será divulgada para fora da instituição, com distinção de público. Informação será compartilhada com um grupo interno de pessoas específicas e previamente definido e com um grupo seleto de pessoas fora da nossa instituição.

Essas informações, mesmo sendo de circulação livre dentro do Banco Paulista, não devem ser divulgadas para entidades externas sem os devidos cuidados e autorização, incluindo, quando necessário, a assinatura de acordos de confiden cialidade ou de autorização formal previamente avaliada pela alçada responsável pela informação ou documento em questão.

c) Uso Interno

São informações de nível reduzido de confidencialidade onde qualquer informação que possa ser divulgada a toda a empresa, bem como pessoas vinculadas. Geralmente tais informações ficam disponíveis na intranet.

d) Público

São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

4.7 Sistema de Gestão da Segurança da Informação

O Sistema de Gestão da Segurança da Informação (SGSI) é um conjunto de disciplinas, deveres e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação visando a coordenação de ações em quatro grandes frentes de atuação:

I. Governança das políticas e procedimentos de segurança da informação

II. Recursos e componentes de segurança da informação

III. Monitoramento contínuo do ambiente de tecnologia da informação

IV. Gestão de crises e continuidade de negócios

Visando à estruturação e coordenação das ações de atendimento das necessidades de segurança da informação, nas visões dos órgãos reguladores (normas e regulamentos), público-alvo (modelo comportamental, conscientização de pessoas no tratamento e uso seguro das informações), ambientes (acessos físicos e proteção ao ambiente de trabalho) e processos de negócios, foram considerados nesta política os seguintes componentes do ambiente de tecnologia da informação, ordenados dos aspectos mais gerais aos mais específicos:

a) Órgãos reguladores

b) Continuidade de negócios

c) Governança e controles de acesso

d) Prevenção dos ataques internos, conscientização dos usuários e diálogos com as partes externas

e) Gestão de vulnerabilidades e processo de investigação

f) Internet

g) Dispositivos de rede

h) Controles tecnológicos e físicos

i) Estação de trabalho e telefonia

j) Servidores internos

k) Servidores externos

l) Dispositivos móveis e BYOD - “Bring Your Own Device”

m) Acesso à informação

5. Incidentes de Segurança da Informação

Para efeito desta política, um incidente de segurança é definido como qualquer evento adverso, decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da Segurança da Informação, descritos no **item 4.4**.

São exemplos de incidentes de segurança:

- Desrespeito a esta política de segurança;
- Tentativas de ganhar acesso não autorizado a sistemas ou dados lógicos ou físicos;
- Indisponibilidade de informações e dados para a execução de rotinas e processos;
- Ataques de negação de serviço;
- Uso ou acesso não autorizado a um sistema;
- Modificações em um sistema, sem conhecimento, instruções ou consentimento prévio do seu gestor; e
- Compartilhamentos de login e senhas.

Cabe a área de segurança da informação estabelecer procedimentos internos e regras específicas para tratar de casos de vazamento de informações confidenciais, reservadas ou privilegiadas, mesmo que oriundos de ações involuntárias (**SCI-11 – Procedimentos de Segurança da Informação).**

Caberá ao Departamento de Segurança da Informação do Banco Paulista a identificação e avaliação de riscos residuais a que os processos e ativos relevantes da instituição estejam sujeitos, em virtude das vulnerabilidades e possíveis cenários de ameaça atribuídos a cada processo ou ativo (**SCI-11 – Procedimentos de Segurança da Informação).**

Toda e qualquer ocorrência que cause risco financeiro ou não, devem ser registradas no Sistema de Gerenciamento do Riscos Controles (SGRC).

- **Vulnerabilidades**

  Vulnerabilidade é uma fragilidade ou fraqueza que pode ser explorado por uma ameaça para concretizar um ataque, roubo ou danos. Vulnerabilidade está associada ao próprio ativo de informação.

  As vulnerabilidades estão associadas ao próprio ativo de informação e podem ser classificadas conforme abaixo:

  a) Ausência de Segregação de Funções (inclui o conflito de interesse e alto número de exceções de acesso)

  b) Hardware;

  c) Software;

  d) Rede;

  e) Recursos Humanos;

  f) Local ou instalações;

  g) Organização (inclui a ausência de classificação da informação e parâmetros fracos de senhas).

- **Ameaças**

  Evento ou atitude indesejável que, potencialmente, remove, desabilita, danifica ou destrói um ativo de informação. As ameaças podem ser classificadas conforme segue:

  a) Dano Físico;

  b) Eventos naturais;

  c) Indisponibilidade de infraestrutura (inclui Internet, Energia, Telefonia);

  d) Código Malicioso / Vírus / Malwares;

  e) Comprometimento da informação;

f) Vazamento de Informações;

g) Falhas técnicas;

h) Ações não autorizadas;

i) Comprometimento de funções (inclui DDOS);

j) Pirataria;

k) Criminosos digitais Terroristas / Espiões / Hacker / Cracker (inclui Main in the Middle);

l) Lixo Informático / Phishing;

m) Furto de Dados / Fraude / Extorsão na Internet;

m) Pessoas: mal treinadas, insatisfeitas, mal-intencionadas, negligentes, imprudentes, desonestas, demitidas;

n) Roubo de Credenciais.

6. Identificação de Riscos (risk assessment)

O Banco Paulista, em especial no âmbito de suas atividades de administração fiduciária, a qual conta com a devida segregação lógica e operacional em relação às demais áreas do Banco Paulista, conforme exigido pela regulamentação em vigor, identificou que os riscos indicados abaixo necessitam de maior resguardo, incluindo, mas não se limitando a:

a. Sistemas: Isso inclui dados sobre os sistemas empregados pelo Banco Paulista e as tecnologias desenvolvidas internamente e por terceiros, juntamente com suas possíveis ameaças e vulnerabilidades.

b. Governança da Gestão de Risco: Diz respeito à efetividade da gestão de riscos realizada pelo Banco Paulista no que tange às ameaças identificadas.

c. Dados e Informações: Isso abrange as Informações Confidenciais, que englobam dados relativos a investidores, clientes, Colaboradores e ao próprio Banco Paulista, além de informações sobre as operações realizadas.

d. Processos e Controles: Aqui se enquadram os processos e controles internos que integram a rotina das diversas áreas de negócio do Banco Paulista.

Não obstante, conforme o Guia de Cibersegurança divulgado pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA"), destacam-se abaixo os principais ataques cibernéticos que o Banco Paulista poderá enfrentar, sem prejuízo dos incidentes do item 4.8. abaixo:

a. Malware – softwares desenvolvidos para corromper computadores e redes (por exemplo: Vírus, Cavalo de Troia, Spyware e Ransomware);

b. Engenharia social – métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);

c. Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

d. Invasões (advanced persistent threats): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

7. Ações de Prevenção e Proteção

O Banco Paulista desenvolveu e estabeleceu um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados, ou seja, que busca impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles internos adequados e robustos.

Objeto	Conduta
Controlar o acesso adequado aos ativos do Banco Paulista	Os colaboradores apenas irão conseguir realizar o acesso as suas ferramentas de trabalho através de desktop ou notebook, o qual deverá conter uma senha pessoal e intransferível.
Definição de Senhas	Os Colaboradores deverão trocar as suas senhas a cada 30 dias. Nesse sentido, os Colaboradores receberão uma notificação quando o prazo para esta ação estiver se aproximando. É possível ter exceções para os casos onde há limitações técnicas declaradas pelos fabricantes dos sistemas.
Limitação de Acesso aos Colaboradores	Cada Colaborador, quando de sua entrada no Banco Paulista, receberá uma permissão específica para entrar nas pastas e diretórios de rede aplicáveis à sua atividade. Caso seja necessário acessar um documento e/ou pasta que não possua permissão, deverá solicitar o acesso ao Departamento de Segurança da Informação através de formulário específico.
Ativos da Banco Paulista	Os ativos tecnológicos do Banco Paulista estão instalados em um ambiente fechado em que apenas Colaboradores autorizados estão autorizados para entrar.
Restrição de acesso físico às áreas com informações críticas/sensíveis	Para que os colaboradores possam acessar o ambiente físico da Banco Paulista pela primeira vez, será necessário realizarem de forma prévia um acesso, em que serão coletadas as suas informações pessoais e disponibilizado um acesso através de biometria. Para as demais entradas no espaço físico do Banco Paulista, será suficiente apenas a aproximação do crachá ou leitura biométrica.
Backup	A Banco Paulista conta atualmente com um backup diário, em que todas as informações são replicadas para a nuvem ou para o Site de Contingência.
Firewall	Hardwares impedem acessos não autorizados e protegem contra invasões maliciosas.

	O Departamento de Segurança da Informação e Segurança Cibernética define o uso adequado dos firewalls, garantindo a segurança do perímetro da rede.
Proteção contra Malware	Softwares antivírus atualizados detectam, previnem e eliminam programas maliciosos (vírus, worms, spyware) nos dispositivos do Banco Paulista. Varreduras constantes identificam e removem qualquer programa que obtenha acesso indevido à rede.

8. Proteção e privacidade da informação de identificação pessoal

O Banco Paulista realiza tratamento de dados pautado na boa-fé, com finalidade específica e fundamentação legal, mantendo controles aderentes a criticidade dos dados e riscos associados.

Bases Legais para Tratamento

O Banco Paulista realizará o tratamento dos dados pessoais observando rigorosamente as hipóteses estabelecidas na Lei, incluindo o expresso consentimento do titular, contratos firmados, procedimentos preliminares contratuais e interesses legítimos.

Os interesses abarcam o cumprimento das legislações, normas bancárias, bem como normas reguladoras, o exercício regular de direito em processo judicial, administrativo ou arbitral, proporcionar a realização e gestão do negócio, incluindo emissão de relatórios, estatísticas e afins dos serviços prestados, gerenciamento de transações bancárias, análise do negócio visando a sua otimização, prover o relacionamento com os clientes, além de estabelecer meios para indicar oportunidades econômicas.

- **Tratamento de Dados Pessoais**

As informações coletadas dos titulares são as mínimas necessárias para cumprimento da sua finalidade, sendo acessadas e utilizadas por pessoal devidamente autorizado e qualificado.

- **Tratamento de Dados Pessoais Sensíveis**

Dados pessoais sensíveis somente serão coletados em situações quando forem indispensáveis para o cumprimento de obrigação legal ou regulatória, ou consecução dos serviços prestados. Os consentimentos devem ser fornecidos de forma específica e destacada pelo titular. Em nenhuma hipótese dados pessoais sensíveis serão utilizados com a finalidade de legítimo interesse e proteção ao crédito.

- **Dados Pessoais de Crianças e Adolescentes**

O tratamento de dados pessoais de crianças e adolescentes ocorrerá obrigatoriamente mediante consentimento específico e em destaque dado por um dos pais ou pelo responsável legal. O consentimento deve ser realizado mediante apresentação de documentação que comprove que a concessão foi realmente dada pelo responsável.

Relacionamento com Terceiros

O Banco Paulista poderá compartilhar, observando o princípio da boa-fé, de maneira consistente e de acordo com os propósitos para os quais foram coletados, os dados pessoais nas seguintes situações e nos limites exigidos e autorizados pela lei:

I. Quando necessário e/ou apropriado à prestação de serviço, incluindo à fornecedores e parceiros;
II. Com empresas do grupo, visando otimizar a prestação de serviço;
III. Para finalidades administrativas (planejamento, execução de contratos, pesquisa e outros);
IV. Em decorrência de obrigação legal, determinação de autoridade competente ou decisão judicial.

9. Desenvolvimento Seguro de Aplicações e Sistemas

Esta norma se aplica aos colaboradores e prestadores de serviços (terceirizados) que exerçam funções profissionais técnicas de desenvolvimento e manutenção de sistemas de propriedade do Banco Paulista em qualquer local em que estejam atuando. Não é admitida a alegação de desconhecimento ou não concordância com esta ou com qualquer outra norma de segurança da informação para se justificar qualquer forma de não cumprimento.

- **Trilhas de Auditoria e Controle**

Todo sistema crítico do Banco Paulista, suportado por ambientes e recursos corporativos de TI da instituição, deve ter a possibilidade de registro de logs ou “trilhas de auditoria”.

Toda atividade crítica do Banco Paulista, operacional e/ou técnica, inclusive acesso remoto de usuários e colaboradores, que dependa de ambiente e recurso de TI corporativo da instituição deve ter registro em log arquivado.

Procedimentos operacionais devem assegurar que as informações contidas nos arquivos de logs dos servidores de sistemas e aplicativos estejam disponíveis no momento em que forem necessárias.

- **Ambiente de Desenvolvimento/Testes, Homologação e Produção**

Dados e informações do ambiente de produção de TI do Banco Paulista não devem ser utilizados no desenvolvimento ou teste de sistemas, programas ou aplicativos. Critério permanece caso necessário deve ser disponibilizado massa de testes criada com base em dados reais.

Para segregação e integridade das informações deve ser viabilizado ambientes distintos para desenvolvimento/teste, homologação e produção. No mínimo é obrigatória a existência de ambientes distintos: desenvolvimento/testes e produção.

- **Criptografia de Dados**

Toda informação que seja considerada crítica para o Banco Paulista, pelos gestores de tais informações, e que requeira proteção e sigilo, conforme estabelecido no normativo de Classificação da Informação deve ser avaliada para que seja aplicada criptografia adequada ou qualquer outra forma de recurso que garanta sua confidencialidade, integridade e disponibilidade.

- **Banco de Dados**

Os bancos de dados de desenvolvimento/teste, de homologação e de produção devem ser segregados fisicamente e logicamente.

Os sistemas de desenvolvimento e de sistemas de produção devem, sempre que possível, ser executados em ambientes diferentes.

Os analistas desenvolvedores somente devem acessar as bases de dados no ambiente de desenvolvimento.
Excepcionalmente, poderá receber autorização temporária e controlada para acesso ao ambiente de produção, se comprovada a necessidade pelo gestor da informação e pelo gestor do analista, e aprovada pela área de Segurança da Informação.

10. Segurança física e do ambiente

O Banco Paulista possui normativo que fornece orientações para o controle de acesso físico de colaboradores e prestadores de serviços nos ambientes críticos e Data Centers do Banco Paulista (**SOP-63 - Controle de Acesso Físico às dependências do Banco Paulista**).

11. Backup

Os recursos de tecnologia, "software" e "hardwares", utilizados deverão estar devidamente autorizados, homologados e/ou serem de propriedade do Paulista.

Os contratos com as empresas desenvolvedoras e/ou fornecedoras deverão ser analisados quanto aos riscos ás informações da empresa e deverão possuir cláusulas de confidencialidade, bem como de responsabilidades no cumprimento das medidas de segurança e da continuidade dos negócios do Paulista.

Tais contratos devem, ainda, conter a descrição completa de suas funções, atribuições, obrigações, permissões e cláusulas de penalização no caso de descumprimento ou performance aquém do estabelecido.

O Banco Paulista possui regras básicas para o Backup seguro (**SOP-30 - Gestão de Tecnologia da Informação**).

12. Monitoramento e Testes

O Departamento de Segurança da Informação realiza, sob demanda, o monitoramento por amostragem do acesso dos Colaboradores a:

- Sites, blogs, fotologs, webmails; e
- E-mails enviados e recebidos.

O Departamento de Segurança da Informação também por amostragem, verifica as informações de acesso a:

- Desktops, pastas e sistemas utilizados.

O objetivo é garantir que os colaboradores tenham o privilégio mínimo necessário para a execução das atividades.

13. Arquivamento de Informações

Os colaboradores do Banco Paulista assumem a responsabilidade de manter arquivados, pelo período legal aplicável, todos os dados, documentos e extratos que se mostrarem necessários para o pleno atendimento de auditorias ou investigações.

14. Responsabilidade

As questões de segurança de informação e segurança cibernética, deverão ser endereçadas ao Diretor de Segurança da Informação e Segurança Cibernética (Resolução CMN 4.893 de 26/2/2021).

15. Referência Cruzada com Outros Normativos Internos

GRC-11/A – Termo de Adesão à Política de Segurança da Informação (versão eletrônica)

GRC-11/A1 – Termo de Adesão à Política de Segurança da Informação (versão impressa)

GRC-12 – Política de Continuidade do Negócio

SCI-11 – Controles Internos para Segurança da Informação

GRC-27 - Política de Privacidade

GRC-27 / A - Procedimento de Resposta a Incidente de Segurança envolvendo Dados Pessoais

GRC-28 - Política de Governança de Proteção de Dados Pessoais

GRC-29 - Política de Privacidade de Colaboradores

SOP-63 - Controle de Acesso Físico às dependências

SOP-30 - Gestão de Tecnologia da Informação

16. Alinhamento com Órgãos Reguladores e Legislações

Lei Complementar nº. 105/2001: Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

Constituição Federal, art. 5º, inciso X e XII

Resolução CMN 4.474/2016: Dispõe sobre a digitalização e a gestão de documentos digitalizados relativos às operações e às transações realizadas pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil, bem como sobre o procedimento de descarte das matrizes físicas dos documentos digitalizados e armazenados eletronicamente.

Resolução CMN 4.557/2017: Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

Resolução CMN 4.745/2019: Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.

Resolução CMN 4.194/2024: Altera as Resoluções ns. 4.553, de 30 de janeiro de 2017; 4.557, de 23 de fevereiro de 2017; e 4.606, de 19 de outubro de 2017; e as Resoluções CMN ns. 4.945, de 15 de setembro de 2021; 4.955, de 21 de outubro de 2021; e 4.958, de 21 de outubro de 2021, para excluir de seus escopos de aplicação as sociedades corretoras de títulos e valores mobiliários, as sociedades distribuidoras de títulos e valores mobiliários e as sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.

ABNT NBR ISO/IEC 27001: Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos

ABNT NBR ISO/IEC 27002: Estabelece as melhores práticas de segurança da informação.

Resolução CMN 4.893/2021: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Regras e Procedimentos de Deveres Básicos ANBIMA: Dispõe sobre as regras de Selos ANBIMA e as regras estruturais, quais sejam: (a) ambientes de controles; (b) segregação de atividades; (c) privacidade/proteção de dados pessoais; (d) plano de continuidade de negócios; (e) segurança da informação e (f) segurança cibernética.

Resolução da CVM nº 21/2021: Dispõe sobre o exercício profissional de administração de carteiras de valores mobiliários.

17. Informações de Controle

Vigência: até dois anos após a publicação desta versão.

Registro das alterações (últimos dois anos):

Versão	Item alterado	Descrição resumida da alteração	Motivo	Dt. Publicação
11	Todo o documento	Exclusão da SOCOPA Exclusão do Conselho de Administração	Atualização	03.fev.2021
12	Todo o documento	Reavaliação das Resoluções de referência; Referencias cruzadas com outros normativos internos.	Alinhamento à Resolução CMN n° 4.893; Atualização; Mudança organizacional.	13.jul.2023
13	Todo o documento	Adequação procedimentos CVM.	Alinhamento a Resolução CVM 21/2021.	19.set.2024
14	Todo o documento	Aprimoramento	Atualização	14. abr.2025

Responsáveis pelo Instrumento Normativo:

Etapa	Responsável	Contato	Unidade Organizacional
Elaboração	Talita Carvalho	talita.carvalho@bancopaulista.com.br	Segurança da Informação
Revisão	Marcos Palmieri	marcos.palmieri@bancopaulista.com.br	TI – Infraestrutura e SGSI
	Alexandre Barros	alexandre.barros@bancopaulista.com.br	Riscos
	Nelson Geraldo	nelson.geraldo@bancopaulista.com.br	Compliance e PLD
	Edson Abreu	edson.abreu@bancopaulista.com.br	Compliance e PLD
Aprovação	Rui Luis Fernandes	rui.fernandes@bancopaulista.com.br	Diretoria Administrativa e de Crédito
	Marcelo Guimarães	marcelo.guimaraes@bancopaulista.com.br	Diretoria Institucional e de Compliance