



Política de Segurança da Informação

Resumo

Estabelece os conceitos, critérios e diretrizes do Grupo Paulista para minimizar possíveis ameaças na segurança da informação.

Sumário

1. Objetivo	2
2. Público-alvo	2
3. Diretrizes Gerais	2
4. Conceitos e regras básicas de Segurança da Informação	2
4.1. Intervenientes da Segurança da Informação e responsabilidades	2
4.2. Ativos de Informação	3
4.3. Princípios da Segurança da Informação	4
4.4. Ciclo de vida da Informação	4
4.5. Incidentes de Segurança da Informação	4
5. Sistema de Gestão da Segurança da Informação	4
5.1. Classificação da Informação	4
5.2. Controles Internos de Segurança da Informação	5
5.3. Avaliação contínua do Sistema de Gerenciamento de Segurança da Informação	6
5.4. Programa de conscientização sobre a Segurança da Informação	6
6. Referência Cruzada com Outros Normativos Internos	6
7. Alinhamento com Órgãos Reguladores e Legislações	6
8. Informações de Controle	7



Política de Segurança da Informação

1. Objetivo

Formalizar os conceitos e as diretrizes da Segurança da Informação do Grupo Paulista (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.

2. Público-alvo

Administradores, gestores, colaboradores, prestadores de serviços, estagiários e usuários externos das informações pertencentes/custodiados ao/pelo PAULISTA.

3. Diretrizes Gerais

- a) Deve ser assegurado pelo PAULISTA que esta Política, normas complementares e as responsabilidades quanto à Segurança da Informação estejam amplamente divulgadas aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com o Grupo 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 recursos 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, 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 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 5.1**).
- d) O PAULISTA é o 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 (RTIC's), portanto, deve proibir 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 PAULISTA pode inspecionar quaisquer RTICs (v. item 4.2.a) que porventura interajam com seus ambientes, lógicos ou físicos e/ou suas informações, incluindo aqueles de propriedade de terceiros, quando autorizada a sua entrada nas instalações do PAULISTA, independentemente da interação com seus ambientes e informações.
- f) O PAULISTA deve manter a segurança da rede e de sistemas 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 digitais;
- g) O Compliance Corporativo é o responsável por definir, zelar e garantir a aderência do PAULISTA às diretrizes de Segurança da Informação;
- h) As ocorrências que podem ser consideradas violações desta Política de Segurança da Informação devem ser avaliadas pelo Compliance Corporativo e, constatado como um incidente (**v. item 4.5**), dependendo de sua gravidade, deve ser encaminhado para o Comitê de GRC e TI para deliberação quanto ao curso de ação a ser tomado.
- i) As situações não previstas nesta política serão arbitradas pela Presidência e Diretoria Geral Administrativa, com assessoria do Departamento de Compliance Corporativo.

4. Conceitos e regras básicas de Segurança da Informação

4.1. 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 que possui a responsabilidade de classificar a informação quanto a 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 PAULISTA.

Política de Segurança da Informação

- b) **Custodiante da Informação:** indicado pelo Proprietário da Informação, é o colaborador, unidade organizacional ou fornecedor contratado responsável pela guarda, proteção e defesa das informações produzidas, adquiridas ou custodiadas pelo PAULISTA e deve observar os critérios e controles definidos no tratamento e classificação da informação.
- c) **Usuário da Informação:** é pessoa, unidade organizacional, entidade ou recurso computacional (por exemplo, programas computacionais ou dispositivos) que está autorizado a acessar e fazer uso da informação.
- d) **Gestor da Segurança da Informação:** o Departamento de Compliance Corporativo é a área responsável pelo Sistema de Gestão da Segurança da Informação (v. **item 5**).

Os gestores, colaboradores, prestadores de serviços e estagiários devem aderir aos termos e condições desta Política de Segurança da Informação, formalizado pelo **Termo de Adesão à Política de Segurança da Informação (GRC-11/A1 – versão impressa)** ou pela plataforma de Educação Corporativa **Paulista E-Learning (GRC-11/A – versão eletrônica)**.

4.2. Ativos de Informação

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005, “A **informação** é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, conseqüentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente”.

Assim, para efeitos desta Política de Segurança da Informação, são considerados os seguintes Ativos de Informação:

- a. Recursos de Tecnologia da Informação e de Comunicação (**RTICs**), que contemplam, no mínimo:
 - Estações de trabalho
 - Sistema de telefonia
 - Sistemas de comunicação de dados (e-mail, ftp)
 - Acessos à Internet
 - Serviços de rede local (wireless e repositórios de dados)
 - “Data center”
 - Sistemas aplicativos de processamento de dados
 - Dispositivos de computação móvel (celulares, notebooks e tablets)
 - Softwares, que englobam também pacotes aplicativos, extensões e complementos
- b. Informações pertencentes ou relacionadas aos clientes
- c. Informações relacionadas ao PAULISTA
- d. Estratégias e decisões da alta administração
- e. Informações contábeis do PAULISTA
- f. Processos e metodologias internos do PAULISTA
- g. Marcas, logotipos e nomes relacionados aos negócios conduzidos pelo PAULISTA
- h. Sistema de Instrumentos Normativos Internos do PAULISTA
- i. Informações disponibilizadas na Intranet do PAULISTA

Os Ativos de Informação são de propriedade e direito de uso exclusivo do PAULISTA e devem ser empregadas unicamente para fins profissionais, limitado às atribuições de cargo e/ou função desempenhadas pelo colaborador, que deve cumpri-las dentro do padrão de conduta ética estabelecida pelo 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 PAULISTA deve controlar o acesso físico e lógico aos seus RTICs, considerando a mitigação do risco de conflito de interesses. Também deve orientar sobre uso de credenciais e coibir o compartilhamento. 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.

Política de Segurança da Informação

4.3. Princípios da Segurança da Informação

- **Confidencialidade:** garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos (sistemas e ferramentas do pacote Office, como por exemplo Excel) sem autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.
- **Integridade:** garantir que a informação não tenha sido alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna. Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada.
- **Disponibilidade:** permite que a informação seja utilizada quando necessário, portanto, esteja ao alcance de seus usuários e destinatários e possa ser acessada no momento em que for necessário utilizá-la.

4.4. 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), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

4.5. 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 4.3**.

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.
- Compartilhamentos de login e senhas

5. Sistema de Gestão da Segurança da Informação

O Sistema de Gestão da Segurança da Informação (SGSI) é um conjunto de disciplinas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a Segurança da Informação.

Esse sistema abrange as esferas da Tecnologia (controles de segurança em ativos tecnológicos e o uso seguro da tecnologia), Processos, Ambientes (acessos físicos e proteção ao ambiente de trabalho) e Pessoas (conscientização de pessoas no tratamento e uso seguro das informações).

A gestão da segurança da informação é um processo contínuo, que envolve as atividades descritas a seguir.

5.1. Classificação da Informação

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

Política de Segurança da Informação

O acesso, divulgação e tratamento de documento (físico ou digitalizado), dado ou informação do 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.

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:

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.

O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem da empresa.

b) Restrita

São informações específicas para uso interno, com circulação exclusiva e irrestrita dentro da empresa. Estas informações podem estar disponíveis a todas os colaboradores e prestadores de serviços e devem ser utilizadas somente para as atividades do PAULISTA.

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

c) Pública

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

A confidencialidade da informação não é vital para a empresa, no entanto, há a necessidade de cuidados em relação a sua integridade e alçada de gestão.

5.2. Controles Internos de Segurança da Informação

5.2.1. Controles internos dos RTICs

Devem ser implementados controles internos efetivos para proteção dos RTICs do PAULISTA, garantindo a sua confidencialidade, integridade e disponibilidade. (v. **SCI-11 – Controle de Segurança da Informação**)

5.2.2. Tratamento de Incidentes de Segurança da Informação

Os incidentes de Segurança da Informação (v. **item 4.5**) devem ser identificados e registrados para acompanhamento dos planos de ação e análise das vulnerabilidades da instituição. (v. **SCI-03 – Procedimentos de Gerenciamento do Risco Operacional**)

a) Comunicação de Incidentes:

Os intervenientes (v. **Item 4.1**) devem comunicar imediatamente os casos de incidentes ao Gestor do Sistema de Segurança da Informação.

b) Tentativa de Burla:

A mera tentativa de burla às diretrizes e controles estabelecidos pelo PAULISTA, quando constatada, deve ser tratada como uma violação.

5.2.3. Monitoramento das atividades dos intervenientes

O PAULISTA deve comunicar aos intervenientes (v. **item 4.1**) sobre o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, seus RTICs, além de seus ambientes, físicos e lógicos, para verificação da eficácia dos controles implantados e proteção de seu patrimônio e reputação, mantendo os acessos gravados e passíveis de monitoração, portanto, não há expectativas de privacidade em sua utilização.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre os ambientes de produção, homologação e teste.

Política de Segurança da Informação

5.2.4. Continuidade do Negócio e Contingência dos RTICs

O Instrumento Normativo Interno **GRC-12 Política da Continuidade do Negócio** contém as diretrizes que devem orientar os processos e planejamento estratégico do PAULISTA na disponibilidade e continuidade de seus processos críticos.

5.3. Avaliação contínua do Sistema de Gerenciamento de Segurança da Informação

O PAULISTA deve possuir e manter um programa de revisão/atualização visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente.

O PAULISTA deve prover auditorias periódicas que visam certificar o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

5.4. Programa de conscientização sobre a Segurança da Informação

O PAULISTA deve implementar um programa conscientização sobre a importância da Segurança da Informação voltada aos administradores, gestores, colaboradores e estagiários.

6. 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-03 – Procedimentos de Gerenciamento do Risco Operacional

SCI-11 – Controles Internos para Segurança da Informação

7. Alinhamento com Órgãos Reguladores e Legislações

Resolução CMN 2554/1998: Dispõe sobre a implantação e implementação de sistema de controles internos.

Resolução CMN 3380/2006: Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional.

Resolução BACEN 4.474/2016: Procedimentos para a produção e a gestão de documentos digitalizados relativos às operações e às transações realizadas.

Resolução BACEN 4.557/2017: Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.

Instrução CVM 505/2011: Estabelece normas e procedimentos a serem observados nas operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários.

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.

Lei Complementar nº. 105 10/01/2001: Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

Art. 5º, inciso X e XII da Constituição Federal.



Política de Segurança da Informação

8. Informações de Controle

Vigência: até 11.set.2018

Registro das alterações (últimos dois anos):

Versão	Item alterado	Descrição resumida da alteração	Motivo	Dt. Publicação
05	Todo documento	Revisão geral	Aprimoramento	23.mai.2016
	4.1	Possibilidade de formalizar o Termo de Adesão pela plataforma de e-Learning.	Implementação da plataforma de e-Learning.	
06	3 4.2 5.1 7	Adequação de Texto	Alinhamento às Resoluções BACEN 4.474/2016 e 4.557/2017.	11.set.2017

Responsáveis pelo Instrumento Normativo:

Etapa	Responsável	Contato / Ramal	Unid.Organizacional
Elaboração	Rodrigo Duarte	rodrigo.duarte@bancopaulista.com.br	Compliance Corporativo
Revisão	Nelson Heleno	nelson.heleno@bancopaulista.com.br	Compliance Corporativo
	Eduardo Kuniyoshi	eduardo.kuniyoshi@bancopaulista.com.br	Compliance Corporativo
	Gerson Brito	gerson.brito@bancopaulista.com.br	Diretoria Geral Administrativa
Aprovação	Comitê GRC		Comitê GRC

Comitê GRC