Política de Segurança da Informação e Segurança Cibernética

Última atualização: Agosto de 2025

Classificação da Informação: Pública

GLOSSÁRIO

I. Bacen ou BCB: é o Banco Central do Brasil;
II. *Backup:* é ação de copiar dados de um sistema ou ambiente de produção para um ambiente paralelo com o objetivo de permitir a recuperação dos dados;
III. Nuvem (*Cloud*): é o fornecimento de recursos externos de tecnologia que possibilita o armazenamento, processamento e troca de informações. Os dados inseridos na Nuvem são acessíveis a dispositivos conectados à internet que tenham usuário e senha válidos;
IV. Plano de Ação e de Resposta a Incidentes ou Plano de Gestão de Incidentes (PGI): é o plano que tem como objetivo assegurar que a **sim;paul Investimentos** implemente as ações para adequar suas estruturas organizacional e operacional aos princípios, diretrizes, procedimentos e controles relacionados à esta Política e seus documentos correlatos;
V. Programa de Segurança da Informação ou PSI: é o conjunto de princípios, diretrizes, regras, procedimentos e controles estabelecidos pela **sim;paul Investimentos** para assegurar a confidencialidade, a integridade e a disponibilidade das informações de sua propriedade ou que estejam sob sua custódia;
VI. Segurança Cibernética: é o conjunto de medidas e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, rede de computadores e/ou dispositivos pessoais com o objetivo de prevenir danos, roubos, intrusão ou destruição de informações através de ataques cibernéticos; e,
VII. Segurança da Informação: é o conjunto de medidas e tecnologias empregadas na preservação das propriedades das informações, tais como a confidencialidade, disponibilidade e integridade.

1. DO OBJETO

Esta Política estabelece os princípios, diretrizes e responsabilidades adotados pela **sim;paul Investimentos** com o objetivo de garantir a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela instituição.

As disposições aqui previstas são compatíveis com o porte, o perfil de risco, o modelo de negócio, a natureza das operações, a complexidade dos produtos e serviços oferecidos, bem como com a criticidade e a sensibilidade dos dados e das informações sob responsabilidade da **sim;paul Investimentos**.

2. DA ABRANGÊNCIA

O presente documento aplica-se aos Colaboradores da sim;paul e aos Parceiros contratados para desempenhar atividades relacionadas ao objeto desta Política.

3. DOS PAPÉIS E RESPONSABILIDADES

3.1. Diretoria Executiva

I. Aprovar esta Política e o Plano de Gestão de Incidentes;
II. Acompanhar o resultado do Relatório de Efetividade e do Plano de Gestão de Incidentes e as ações designadas para correção e saneamento, se aplicável;
III. Comprometer-se continuamente com a melhoria do Programa de Segurança da Informação; e,
IV. Deliberar sobre eventuais isenções e exceções a esta Política.

3.2. Diretor de TI

I. Implementar e gerir o Programa de Segurança da Informação;
II. Designar responsabilidades e funções para a área de TI;
III. Elaborar e revisar esta Política e o Plano de Gestão de Incidentes anualmente e submeter para aprovação da Diretoria Executiva;
V. Elaborar Relatório de Efetividade do Plano de Gestão de Incidentes anualmente e apresentar para a Diretoria Executiva até o dia 31 de março do ano seguinte ao da data-base;
VI. Assegurar que esta Política seja divulgada aos Colaboradores e aos Parceiros mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações;
VII. Divulgar no site da instituição resumo contendo as linhas gerais desta Política;
VIII. Assegurar que esta Política, assim como seus documentos correlatos estejam em conformidade com a regulamentação;

IX. Manter contato com os reguladores, nos casos previstos nesta Política e na regulamentação;
X. Promover programas de conscientização, educação e treinamento que abordem os temas que integram o Programa de Segurança da Informação; e
XI. Elaborar e manter atualizado o inventário de ativos da instituição.

3.3. Área de TI

I. Implementar procedimentos e controles para reduzir a vulnerabilidade da instituição a incidentes;
II. Implementar controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis, devendo abranger:
    a. A autenticação e criptografia dos dados e informações;
    b. A prevenção e detecção de intrusão;
    c. A prevenção de vazamento de informações;
    d. A realização periódica de testes e varreduras para detecção de vulnerabilidades;
    e. A proteção contra softwares maliciosos;
    f. O estabelecimento de mecanismos de rastreabilidade;
    g. Os controles de acesso e de segmentação da rede de computadores; e,
    h. A manutenção de cópias de segurança dos dados e das informações;
III. Implementar procedimentos e controles para o registro, análise da causa e análise dos impactos de incidentes relevantes para as atividades da instituição;
IV. Elaborar cenários de incidentes considerados nos testes de continuidade de negócios;
V. Implementar procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por Parceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição, devendo contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição;
VI. Classificar os dados e as informações quanto à relevância sob a ótica de segurança da informação;
VII. Definir parâmetros a serem utilizados na avaliação da relevância dos incidentes;
VIII. Definir os mecanismos para disseminar a cultura de Segurança da Informação e Segurança Cibernética na instituição; e,
IX. Definir as iniciativas para compartilhamento de informações sobre os incidentes relevantes com as instituições autorizadas pelo Bacen, nos termos da regulamentação.

3.4. Área Jurídica

I. Assegurar que haja cláusula de confidencialidade nos contratos de prestação de serviços que impliquem no acesso ou manuseio de informações confidenciais; e,
II. Assegurar que os contratos de prestação de serviços de processamento e armazenamento de dados e de computação em Nuvem contenham as cláusulas obrigatórias previstas na Resolução BCB 85/21.

3.5. Gestores de Equipe

I. Solicitar para a área de TI liberação de acesso para seus Colaboradores; e,
II. Informar à área de TI em tempo hábil as demissões e eventuais movimentações dos Colaboradores que integram sua equipe.

3.6. Auditoria Interna

I. Realizar trabalhos de auditoria para determinar o grau de cumprimento e efetividade desta Política e do Programa de Gestão de Incidentes.

3.7. Área de Compliance

I. Aprovar e validar a Matriz de segregação de acessos aos sistemas; e
II. Assegurar que a elaboração, aprovação, execução, monitoramento e testes referentes ao Programa de Segurança da Informação da **sim;paul Investimentos** sejam de maneira a preservar a independência das funções envolvidas e a prevenir potenciais conflitos de interesse, garantindo a adequada segregação de responsabilidades conforme as melhores práticas de governança corporativa.

3.8. Área de Gestão de Riscos e Controles

I. Assegurar que as políticas integrantes da estrutura de gerenciamento de riscos da **sim;paul Investimentos** contemplem, no âmbito da continuidade de negócios, o tratamento dos incidentes relevantes de que trata esta Política e seus documentos correlatos, em conformidade com as exigências regulamentares aplicáveis;
II. Assegurar que as políticas, estratégias e estruturas de gerenciamento de riscos previstas na regulamentação incluam, de forma expressa, os critérios de decisão sobre terceirização de serviços, abrangendo a contratação de serviços relevantes de processamento e armazenamento de dados, bem como de computação em nuvem, no país ou no exterior.

3.9. Colaboradores, Parceiros e Clientes

Todos que integram a instituição e sua cadeia de valor são responsáveis pela Segurança da Informação e pela Segurança Cibernética. Cabe aos Colaboradores, Parceiros e Clientes, no limite de suas atribuições e responsabilidades:

I. Preservar os ativos da instituição e zelar pela proteção adequada das informações e sistemas a que tenham acesso;
II. Assegurar o sigilo, a confidencialidade, a privacidade e a integridade das informações a que tiver acesso;
III. Armazenar e proteger adequadamente documentos impressos e/ou arquivos eletrônicos que contenham informações confidenciais e restritas;
IV. Responder pela guarda e proteção de todos os equipamentos disponibilizados pela instituição para o desempenho de suas funções;
V. Bloquear o computador e/ou notebook ao se ausentar de seu local de trabalho, mesmo quando estiver trabalhando remotamente;
VI. Zelar, proteger e manter em local seguro suas senhas de acesso, respondendo pelo uso exclusivo e intransferível;
VII. Certificar-se, ao identificar mensagem com título ou anexo suspeito, que não se trata de vírus ou *softwares* maliciosos;
VIII. Informar ao Diretor de TI qualquer incidente de segurança da informação e segurança cibernética que tenha conhecimento; e,
IX. Informar ao Diretor de TI e ao Diretor de Compliance os descumprimentos ao Programa de Segurança da Informação que tiver conhecimento, podendo também acionar o canal de denúncias.

4. DA GESTÃO DO PROGRAMA DE SEGURANÇA DA INFORMAÇÃO (GSI)

Com o objetivo de implementar as diretrizes acima e adequar as estruturas organizacional e operacional, a **sim;paul Investimentos** estruturou um Programa de Segurança da Informação com base nas diretrizes da NBR ISO / IEC 27002 e o dividiu em 3 (três) macroprocessos: (i) controles organizacionais, (ii) controles de pessoas e, (iii) controles tecnológicos.

4.1. DOS CONTROLES ORGANIZACIONAIS

4.1.1. Políticas

Os documentos que integram o Programa de Segurança da Informação são: (i) esta Política de Segurança da Informação e Segurança Cibernética, (ii) Plano de Ação e de Resposta a Incidentes ou Plano de Gestão de Incidentes (PGI), (iii) Manuais de Segurança da Informação e Segurança Cibernética, (iv) Política de Privacidade, e (v) Inventário de Ativos.

4.1.2. Plano de ação e de Resposta a Incidentes

O Plano de Ação, Gestão e Resposta a Incidentes, formalizado em documento específico, estabelece os procedimentos a serem adotados pela **sim;paul Investimentos** para o registro, a análise de causas e impactos e o controle dos efeitos decorrentes de incidentes relevantes que possam afetar as atividades da instituição.

4.1.3. Classificação de informações

Compete à área de Compliance classificar as informações, dados e ativos relevantes da **sim;paul Investimentos**, em conformidade com a legislação e a regulamentação aplicáveis, bem como definir e divulgar aos colaboradores os critérios de classificação a serem adotados. Também é responsabilidade da área orientar sobre a forma adequada de rotulagem dessas informações, incluindo a utilização de cabeçalhos e rodapés em documentos, títulos de e-mails e demais meios de registro e comunicação.

4.1.4. Inventário de informações

Cabe à área de TI identificar as informações, dados e ativos da instituição sob a ótica de Segurança da Informação e Segurança Cibernética, bem como elaborar e manter atualizado um inventário que contenha a relação completa desses elementos.

4.1.5. Diligências na contratação de terceiros com acesso a informações

Todas as contratações de Parceiros são precedidas de análises e diligências nos termos estabelecidos pelo Manual de KYP. O nível de diligência aplicado será compatível com a classificação de risco da atividade, observada a AIR. Todas as diligências são documentadas e arquivadas pelo prazo exigido pela regulamentação.

4.1.6. Serviços de processamento e armazenamento em Nuvem

Para a contratação de serviços de processamento e armazenamento de dados, bem como de computação em nuvem, no país ou no exterior, a **sim;paul Investimentos** realizará diligência adicional específica. Essa diligência deverá contemplar todos os requisitos estabelecidos nesta Política, independentemente da classificação de risco atribuída na Avaliação Interna de Riscos (AIR) ou da análise de risco da empresa contratada, de modo a verificar se o potencial parceiro atende, no mínimo, aos critérios abaixo:

I. Práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e,
II. Capacidade de assegurar: (i) o cumprimento da legislação e da Regulamentação em vigor; (ii) o acesso da instituição aos dados e às informações a serem processados ou armazenados; (iii) a confidencialidade, a integridade, a disponibilidade e a

recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço; (iv) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado, caso aplicável; (v) o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados; (vi) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados; (vii) a identificação e a segregação dos dados dos Clientes e dos usuários finais da instituição por meio de controles físicos ou lógicos e (viii) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos Clientes e dos usuários finais da instituição.

4.1.7. Contrato de prestação de serviços

Os contratos que envolvam processamento, armazenamento de dados e computação em nuvem devem conter, obrigatoriamente, as cláusulas específicas previstas na Resolução BCB nº 85/2021. Compete à área Jurídica da **sim;paul Investimentos** assegurar que tais contratos estejam em conformidade com a regulamentação vigente, bem como promover a atualização das cláusulas sempre que necessário.

4.1.8. Comunicação ao Bacen

Na hipótese de contratação de serviços relevantes de processamento, armazenamento de dados ou computação em nuvem, o Diretor de TI da **sim;paul Investimentos** deverá comunicar o Banco Central do Brasil no prazo máximo de 10 (dez) dias contados da formalização contratual. Havendo alterações contratuais que impliquem modificação das informações anteriormente reportadas, nova comunicação deverá ser realizada no mesmo prazo. A comunicação deve conter, no mínimo, as seguintes informações:

I. A denominação da empresa contratada;
II. Os serviços relevantes contratados; e
III. A indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, conforme consta na Resolução BCB 85/21.

4.2. DO CONTROLE DE PESSOAS

O fator humano constitui um dos elementos mais relevantes a serem considerados no Programa de Segurança da Informação. Determinadas funções exercidas por colaboradores apresentam maior nível de risco em razão do acesso a informações sensíveis

da instituição, o que pode potencializar a ocorrência ou a facilitação de ataques cibernéticos, vazamentos de dados e outras práticas ilícitas. Diante disso, a **sim;paul Investimentos** estabeleceu processos e controles específicos voltados à mitigação desses riscos, conforme descrito a seguir.

4.2.1. Conheça seu colaborador (KYE)

Todas as contratações de Colaboradores são precedidas de análises e diligências nos termos estabelecidos no Manual de KYE. O nível de diligência aplicado será compatível com a classificação de risco da atividade, observada a AIR da **sim;paul Investimentos**. Todas as diligências são documentadas e arquivadas pelo prazo exigido pela regulamentação.

4.2.2. Termos e condições de contratação

Os contratos de trabalho celebrados com os Colaboradores da **sim;paul Investimentos** contêm cláusulas específicas de confidencialidade e não divulgação, que estabelecem a responsabilização por ações ou omissões decorrentes de eventual descumprimento. De forma exemplificativa, tais cláusulas podem dispor sobre: a obrigação de o colaborador ou parceiro proteger as informações confidenciais a que tiver acesso durante a vigência da relação contratual, por prazo determinado estabelecido pela instituição ou até que as informações se tornem públicas; as medidas de segurança a serem observadas no tratamento, acesso ou armazenamento de informações fora das instalações da instituição, especialmente em regime de trabalho remoto; os procedimentos para devolução ou destruição das informações ao término do contrato; as providências cabíveis em caso de rescisão; e as medidas a serem adotadas diante de situações de não conformidade, em especial com relação às disposições de confidencialidade.

4.2.3. Trabalho remoto

Os colaboradores da **sim;paul Investimentos** podem desempenhar suas atividades, parcial ou integralmente, em regime de teletrabalho. Nessas situações, o desempenho das atividades ocorrerá em ambiente remoto, com suporte da área de TI para garantir a infraestrutura necessária ao adequado funcionamento dos sistemas e recursos corporativos. O acesso remoto será realizado por meio de **VPN** (*Virtual Private Network*), de forma a assegurar a confidencialidade, integridade e disponibilidade das informações.

4.2.4. Conscientização, educação e treinamento em segurança da informação

A **sim;paul Investimentos** possui um Programa de Capacitação e Treinamento para Colaboradores que engloba a conscientização e treinamentos sobre o Programa de Segurança da Informação da instituição. A área de TI, em conjunto com a área de

Compliance, planeja os treinamentos, cursos e demais programas de conscientização de acordo com os papéis e responsabilidade dos Colaboradores, atribuindo, ao cabo, avaliações para testar as lições aprendidas.

4.2.5. Uso de e-mail corporativo

Os treinamentos de conscientização e capacitação incluem diretrizes sobre a utilização do e-mail corporativo, considerado um dos principais meios de comunicação da **sim;paul Investimentos** e que deve ser empregado exclusivamente para o exercício das funções profissionais.

O Colaborador assume compromisso formal com a instituição ao reconhecer que o endereço de e-mail corporativo disponibilizado é de sua inteira responsabilidade. Nesse sentido, cabe ao profissional, entre outras obrigações:

I. Zelar pelas mensagens enviadas pelo e-mail corporativo, uma vez que elas podem ser equiparadas a documentos de caráter oficial da instituição;
II. Atentar-se ao nível de sigilo da informação contida nas mensagens;
III. Zelar pelo conteúdo das mensagens recebidas ou enviadas, sendo vedado criar, copiar ou encaminhar mensagens ou imagens que:
    a. Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
    b. Menosprezem, depreciem ou incitem o preconceito a classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, deficiência física, entre outros;
    c. Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
    d. Defendam ou possibilitem a realização de atividades ilegais; e,
    e. Possam prejudicar a imagem da **sim;paul Investimentos**.
IV. Abster-se de utilizar e-mail corporativo para emitir opinião pessoal, salvo se autorizado pela **sim;paul Investimentos**.

4.2.6. Uso da internet

Também integram os treinamentos de conscientização e capacitação as diretrizes relativas à utilização da internet, com o objetivo de dar transparência aos colaboradores quanto às restrições aplicadas. Nesses treinamentos, a **sim;paul Investimentos** esclarece os sites bloqueados pela instituição, incluindo, mas não se limitando, àqueles que:

I. Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes;

II. Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
III. Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física; e,
IV. Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuam *links* suspeitos.

4.3. DO CONTROLE TECNOLÓGICO

Com o objetivo de prevenir, proteger, mitigar e reduzir vulnerabilidades e incidentes, a **sim;paul Investimentos** adota, incluindo, mas não se limitando, às seguintes medidas:

I. Autenticação e criptografia dos dados e informações;
II. Prevenção, detecção e bloqueio de intrusão;
III. Prevenção de vazamento de informações;
IV. Realização periódica de testes e varreduras para detecção de vulnerabilidades;
V. Proteção contra softwares maliciosos;
VI. Estabelecimento de mecanismos de rastreabilidade;
VII. Controle de acessos;
VIII. Segmentação da rede de computadores; e,
IX. *Backup* e manutenção das informações.

5. DO MONITORAMENTO

Com o objetivo de assegurar a efetividade do Programa de Segurança da Informação, a área de TI deve realizar, em periodicidade definida pela instituição ou pela regulamentação aplicável, o monitoramento contínuo das diretrizes, procedimentos e controles previstos nesta Política e em seus documentos correlatos. Esse monitoramento deve abranger, entre outros aspectos, a verificação de conformidade dos acessos, a aderência aos processos de tratamento de incidentes, a análise da eficácia dos controles técnicos e operacionais e a avaliação de eventuais vulnerabilidades identificadas.

Todos os monitoramentos devem ser devidamente formalizados e documentados, contemplando, quando aplicável, a descrição das falhas detectadas, as recomendações de melhorias e o respectivo Plano de Ação para saneamento, com indicação de responsáveis e prazos. Os resultados poderão ser consolidados em relatórios específicos ou incorporados ao Relatório Anual de Efetividade do Programa de Segurança da Informação, de forma a subsidiar a Diretoria Executiva no processo de tomada de decisão e no acompanhamento da evolução da maturidade em segurança da informação e cibersegurança.

6. DA AVALIAÇÃO DE EFETIVIDADE DO PROGRAMA DE SI

6.1. Teste de efetividade

O Diretor de TI deve assegurar a realização, ao menos uma vez ao ano, de testes nos procedimentos e controles previstos no Programa de Segurança da Informação (PSI) e na regulamentação aplicável, com o objetivo de avaliar sua conformidade e efetividade. Esses testes devem ser conduzidos por área ou profissional independente da área de TI, como Controles Internos, Auditoria Interna ou consultoria especializada, de modo a garantir imparcialidade e isenção nos resultados.

6.2. Relatório de efetividade

A área ou profissional responsável pela execução dos testes deve consolidar os resultados em um Relatório Anual de Efetividade do Programa de Segurança da Informação, abordando, no mínimo, os requisitos previstos na Resolução BCB 85/21, incluindo a descrição dos testes realizados, as falhas identificadas, os planos de ação propostos e a avaliação da maturidade do programa.

O Relatório de Efetividade deve ser formalmente apresentado à Diretoria Executiva da **sim;paul Investimentos** até o dia 31 de março do ano subsequente à data-base, para ciência, deliberação e acompanhamento das medidas corretivas e de melhoria contínua.

7. DAS DISPOSIÇÕES FINAIS

Esta Política será divulgada aos Colaboradores e aos Parceiros da **sim;paul Investimentos** mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações acessadas.

Adicionalmente, a **sim;paul Investimentos** poderá divulgar em seu site na internet resumo contendo as linhas gerais desta Política de modo a dar transparência aos Clientes, Parceiros, reguladores e a todas as partes interessas, dos princípios e diretrizes que regem o Programa de Segurança da Informação da instituição.

As diretrizes, regras e processos descritos nesta Política entram em vigor a partir da data de sua aprovação e publicação oficial pela organização. Todas as áreas e colaboradores devem cumpri-las integralmente, observando seus papéis e responsabilidades.

Esta Política e os demais documentos que integram o PSI serão formalizados e arquivados, no mínimo, pelo prazo de 5 (cinco) anos.

Dúvidas ou esclarecimentos sobre a aplicação desta Política devem ser encaminhadas para a área de PLD/FTP através do e-mail controlesinternos@simpaul.com.br

8. DO CONTROLE DE VERSÕES

Código do Documento: POL-TI-001		**Classificação:** Pública
Elaborado por: Área de TI		
Revisado por: Diretor de TI		
Aprovado por: Diretoria Executiva		
Data	**Versão**	**Sumário**
02/09/2025	1.0	Estabelecer princípios e diretrizes para segurança da informação e segurança cibernética da sim;paul.