




POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CÓDIGO: PLT-SI-001	VERSÃO: 1.2
APROVAÇÃO:  335D4089F26B4EB...	DATA: Jun/20

Sumário

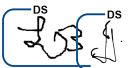
1. OBJETIVO	4
2. DEFINIÇÕES	4
3. ABRANGÊNCIA	4
4. DIRETRIZES	4
4.1 Segurança da Informação	5
4.2 Gestão de Vulnerabilidades	5
4.3 Definição e Implementação das Regras de Segurança	5
4.4 Treinamento e Conscientização	6
4.5 Classificação da Informação	6
4.6 Uso da Informação	7
4.7 Reporte de Irregularidades	7
4.8 Acesso aos Recursos e Ativos de Informação	7
4.9 Monitoramento e Controle	8
4.10 Direitos de propriedade intelectual e uso de softwares proprietários	8
4.11 Proteção dos Perímetros	9
4.12 Casos Omissos	9
4.13 Segurança Cibernética	9
4.14 Demandas e projetos	9
4.15 PCI-DSS	9
5 PAPÉIS E RESPONSABILIDADES	11
5.1 Diretoria	11
5.2 Área de Segurança da Informação	11
5.3 Gestores	12
5.4 Colaboradores	13
6 BASE REGULATÓRIA / LEGISLAÇÃO APLICÁVEL	13
7 REGULAMENTAÇÃO INTERNA RELACIONADA	14
8 SANÇÕES E PUNIÇÕES	14
8.1 Disposições Gerais	14
9 GESTÃO DA POLÍTICA	15
9.1 Elaboração, revisão e aprovação	15



10 REVISÕES.....15

10.1 Periodicidade de Revisões 15

10.2 Histórico de Revisões..... 15





1. OBJETIVO

O presente documento tem por objetivo padronizar e disciplinar regras e diretrizes relativas à Segurança da Informação, de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes para a melhor utilização dos recursos disponíveis e entrega de valor para o cliente.

2. DEFINIÇÕES

- **Segurança da informação:** é a proteção da informação contra diversos tipos de ameaças que visa garantir a continuidade do negócio, minimizar o risco à organização e prover oportunidades de negócio. É obtida a partir da implementação de controles adequados para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.
- **Usuários:** o usuário é quem irá usufruir do serviço prestado. Para esta Política, considera-se usuários os colaboradores, diretores, menores aprendizes, estagiários e terceiros que acessam qualquer tipo de informação para realizar as suas atividades profissionais na/para a Phi.

3. ABRANGÊNCIA

A presente política se aplica a todos os colaboradores, diretores, menores aprendizes, estagiários e terceiros que possuam vínculo, ainda que transitório, coma a Phi.

4. DIRETRIZES

Toda informação ou sistema de informações possui um determinado valor. Sendo assim, pode ser considerado como um ativo da Phi. Este ativo, como todos os outros, deve ser protegido de forma adequada. Um sistema de segurança visa proteger as informações contra um grande número de ameaças internas e externas. Esta proteção pretende garantir a continuidade do negócio minimizando os possíveis prejuízos e maximizando as oportunidades.

Um sistema de Segurança da Informação tem como objetivo:

- **Confidencialidade:** Garantir que as informações são acessadas apenas por aqueles expressamente autorizados;
- **Integridade:** Preservar a Integridade da Informação. Garantir que todas as informações estão íntegras e precisas durante todo o ciclo: Criação, Processamento e Destruição;

- **Disponibilidade:** Garantir que os usuários, quando devidamente autorizados, tenham acesso às informações sempre que necessitarem.

As informações apresentam-se de formas diferentes, podendo ser impressa ou manuscrita em papel, armazenada física ou eletronicamente, remetida pelo correio ou transmitida por meios eletrônicos, mostrados em projeções de imagens ou falada.

A rotina operacional indica que não bastam medidas restritivas somente aos acessos externos, pois ocorre o risco de quebra da segurança da informação também por ameaças internas. A visão integrada do risco é fundamental para que se busque o desenvolvimento e a continuidade dos negócios, capacitando a infraestrutura para operacionalizar seus processos sob risco controlado.

Neste contexto, a Política de Segurança da Informação estabelece o direcionamento estratégico para a proteção efetiva das informações da Phi e possui as seguintes diretrizes especificadas nos subitens abaixo.

4.1 Segurança da Informação

- 4.1.1 A Segurança da Informação deve ser desenvolvida de forma integrada, unindo ações para a gestão inteligente dos ativos humanos, físicos e da infraestrutura tecnológica da informação em todos os ambientes corporativos.

4.2 Gestão de Vulnerabilidades

- 4.2.1 A gestão de vulnerabilidades visa garantir a confidencialidade, integridade e disponibilidade das informações através de processos de avaliação de vulnerabilidades, identificando possíveis ameaças em que a Phi possa estar exposta, buscando a implementação de controles de segurança adequados, frente aos custos, tecnologia e objetivos de negócio.

4.3 Definição e Implementação das Regras de Segurança

- 4.3.1 As definições das presentes diretrizes devem ser revisadas e atualizadas periodicamente, baseada nos diagnósticos e avaliações de segurança realizados no ambiente da Phi;
- 4.3.2 No que tange à implementação das regras, a área de Segurança da Informação é responsável por definir as regras e colocar em prática nas diversas áreas da Phi e respectivos parceiros.
- 4.3.3 Todo projeto desenvolvido na Phi, independentemente do produto ou serviço fim, deverá considerar e assegurar desde a sua concepção, a segurança e privacidade de dados como característica fundamental;

4.4 Treinamento e Conscientização

- 4.4.1 A Phi promove capacitações e ações de treinamento e conscientização aos colaboradores para devida ciência e concordância com as responsabilidades no cumprimento da Política de Segurança da Informação, suas Normas e Procedimentos. Além disso, promove treinamentos institucionais e comunicações de atualização, contemplando informações relevantes sobre o tema.

4.5 Classificação da Informação

- 4.5.1 A área de Segurança da Informação tem por objetivo definir os critérios de classificação dos ativos de informação contra acesso, divulgação, alteração e/ou destruição não autorizados, conforme critérios de tratamento, armazenamento e descarte. A informação pode ser classificada conforme os critérios abaixo:

a) **Confidencial**

É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da empresa. São protegidas, por exemplo, por criptografia.

b) **Restrita**

É o nível médio de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores. Podem ser protegidas, por exemplo, restringindo o acesso à uma pasta ou diretório da rede.

c) **Uso interno**

Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

d) **Pública**

São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público. No entanto, sempre cabe lembrar dos outros dois pilares: a disponibilidade e a integridade.

4.6 Uso da Informação

- 4.6.1 As informações armazenadas, processadas e ou geradas pelos sistemas da Phi ou sob sua responsabilidade não devem ser divulgadas ou compartilhadas. As informações devem ser usadas exclusivamente para atividades de negócio da Phi respeitando as normas e definições aplicadas no ambiente;
- 4.6.2 A Phi disponibiliza a seus colaboradores um local para o armazenamento e compartilhamento seguro de informações (OneDrive, SharePoint), desaconselhando totalmente a utilização de outros formatos de compartilhamento ou armazenamento de informações (HDs externos, pendrives, Google Drive, e-mail particular, WhatsApp, Dropbox etc.) que não os oficiais.

4.7 Reporte de Irregularidades

- 4.7.1 O descumprimento de controles estabelecidos pela Política de Segurança da Informação e os demais documentos que a compõem deve ser comunicado a área de Segurança da Informação, assim como qualquer incidente ou atividade suspeita, relacionados ao uso de informações de propriedade ou sob a responsabilidade da Phi. O contato deve ser realizado através do canal seginfo@somosphi.com.

4.8 Acesso aos Recursos e Ativos de Informação

- 4.8.1 O cumprimento das regras previstas na presente Política deve garantir que todos os acessos aos recursos de processamento de informação sejam devidamente autenticados e autorizados, utilizem uma identificação pessoal e intransferível, sejam compatíveis com a função e destinados somente às finalidades da Phi. As máquinas serão bloqueadas após um período de inatividade com objetivo de minimizar risco de acesso indevidos no caso do colaborador não realizar o bloqueio ao se ausentar do equipamento.
- 4.8.2 Cada colaborador deverá possuir acessos estritamente necessários para desempenhar suas atividades. Ao ser desligado da organização, todos os acessos atrelados ao usuário do colaborador deverão ser revogados imediatamente.
- 4.8.3 Todo sistema deverá ser desenvolvido/implementado tendo como base o princípio da segregação de funções, evitando o acúmulo de funções por parte de um mesmo usuário, assegurando a legitimidade das operações, diminuindo a chance de ocorrências de fraudes e erros, e mitigando o risco de acessos não autorizados ou indevidos;

- 4.8.4 Acessos VPN (*Virtual Private Network*) serão concedidos unicamente e exclusivamente aos colaboradores que necessitem do acesso para desempenho das suas atividades. O acesso deverá ser único e aprovado pelo gestor imediato. Além disto, todo acesso remoto possui desconexão automático depois de muito tempo de atividade ou um período especificado de inatividade.

4.9 Monitoramento e Controle

- 4.9.1 No intuito de assegurar o efetivo cumprimento da Política de Segurança, a Phi se reserva o direito de monitorar, inspecionar ou auditar o acesso e o uso das informações de sua propriedade ou sob sua guarda. Esse exame pode acontecer com ou sem o consentimento, presença ou conhecimento dos usuários envolvidos.

4.10 Direitos de propriedade intelectual e uso de softwares proprietários

- 4.10.1 A fim de garantir a conformidade relacionada aos direitos de propriedade intelectual, bem como o uso de produtos de software proprietários, nenhum usuário deverá utilizar sob hipótese alguma quaisquer tipos de softwares (programa, aplicativo, aplicação, utilitário, plugin, app etc.) sem que o mesmo esteja devidamente licenciado para a finalidade ao qual foi adquirido;
- 4.10.2 Toda a qualquer aquisição de software (programa, aplicativo, aplicação, utilitário, plugin, app etc.) deverá obrigatoriamente ser realizada somente junto a fontes (fornecedores, distribuidores, representantes etc.) legítimas e confiáveis;
- 4.10.3 Nenhum usuário deverá realizar a instalação de softwares proprietário (programa, aplicativo, aplicação, utilitário, plugin, app etc.), sem que o mesmo tenha sido devidamente licenciado e homologado pela área responsável;
- 4.10.4 Nenhuma modificação que descaracterize a originalidade de um software proprietário deverá ser realizada sem que exista a devida autorização formal do proprietário.
- 4.10.5 Todo o colaborador fica sujeito a respeitar as normas que regem o direito à propriedade intelectual, como, mas não se limitando as regras de propriedade industrial e direitos autorais e demais normas que protejam de qualquer forma a propriedade intelectual.
- 4.10.6 Deverão ser respeitados ainda, normas, regras e diretrizes dos órgão regulamentares que tratem sobre a propriedade intelectual, como, mas não se limitando ao INPI (Instituto Nacional de Propriedade Industrial).

4.11 Proteção dos Perímetros

- 4.11.1 A área de Segurança da Informação busca garantir que haja controles para prevenir acesso físico não autorizado, danos e interferências nas instalações que abrigam ou armazenam ativos de propriedade da Phi.

4.12 Casos Omissos

- 4.12.1 Antes de efetuar um acesso, armazenamento, transmissão, destruição ou qualquer outra atividade envolvendo sistemas ou informações da Phi, o usuário deve consultar a Política de Segurança da Informação e demais Normas associadas para certificar-se de que a atividade é permitida. A execução de qualquer atividade envolvendo ativos de informação da Phi, não claramente definidos na presente Política e/ou em seus respectivos complementos, deve ser precedida de uma consulta a área de Segurança da Informação.

4.13 Segurança Cibernética

- 4.13.1 Os procedimentos e os controles da segurança cibernética são implementados de modo a abranger a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

4.14 Demandas e projetos

- 4.14.1 As demandas e projetos de negócio, serviços de retaguarda ou tecnologia devem estar em conformidade com as diretrizes, processos e arquitetura corporativa de segurança da informação. As demandas e projetos devem ser submetidos aos checklists de Segurança da Informação aplicado pela área de Segurança da Informação, garantindo a sua aderência às melhores práticas e normativas de segurança.

4.15 PCI-DSS

O *Payment Card Industry Data Security Standards* é a norma que prevê a proteção da privacidade e confidencialidade de dados de cartões de crédito. Toda organização que transmita, processe ou armazene dados de cartão deve estar em conformidade com o PCI-DSS.

a) Certificação

A companhia é auditada com base nos requisitos level 1 do PCI-DSS, sendo este o mais rigoroso controle de conformidade. A empresa deve renovar sua certificação anualmente, com bases nos 12 requisitos da norma. A auditoria deve ser realizada por uma companhia QSA (*Qualified Security Assessor*).

b) Manutenção

É de responsabilidade do time de segurança da informação as atividades de manutenções do PCI-DSS, sejam atividades recorrentes tais como: Análise de vulnerabilidades, atualização de patches de segurança, gestão de mudanças etc., bem como novas demandas relacionadas ao ambiente de PCI-DSS.

c) Monitoramento

Deve-se haver um monitoramento proativo das atividades de manutenção do PCI-DSS, de forma que atividades recorrentes sejam executadas nos períodos pré-estabelecidos e que nenhuma atividade seja executada sem o devido controle e aprovação, de forma que possa afetar a conformidade do ambiente com as normas do PCI-DSS.

É de responsabilidade também do time de segurança da informação o monitoramento do ambiente do CDE, através de sistemas de monitoramento e capazes de gerar alertas, a fim de identificar prontamente qualquer incidente relacionado ao ambiente.

Da mesma forma, todos os acessos a ambientes que refletem dados de cartão de crédito são monitorados, de forma que todo e qualquer acesso ao CDE seja possível identificar e rastrear.

d) Divulgação

Deve ser de conhecimento de toda a companhia o processo de certificação e manutenção da certificação, bem como suas responsabilidades para com a certificação. As informações devem ser divulgadas ao menos uma vez por ano para todos os colaboradores da companhia.

e) Atualização

A Política de Segurança deve ser revisada com a periodicidade de 1 (um) ano. A decisão de revisar a Política de Segurança pode ser tomada com base em critérios próprios ou a partir de um dos seguintes acontecimentos:

- Incidentes de segurança considerados significativos;
- Pontos identificados por auditorias e/ou testes de aderência periódicos;
- Vulnerabilidades encontradas em uma análise de risco;
- Alteração ou publicação de legislação aplicável à segurança de dados;
- Mudanças na estrutura técnica ou organizacional da Phi.

5 PAPÉIS E RESPONSABILIDADES

5.1 Diretoria

- 5.1.1 Aprovar, em nível estratégico, a Política de Segurança da Informação, através de Reunião de Diretoria precedida da avaliação e recomendação;
- 5.1.2 Cumprir e fazer cumprir o estabelecido nesta Política;
- 5.1.3 Garantir aderência e cumprimento dos controles de segurança da informação estabelecidos pelas Normas e Política de Segurança da Informação;
- 5.1.4 Aplicar as sanções previstas àqueles que deliberadamente violarem as determinações de controles desta Política de Segurança da Informação, suas Normas e Instruções, mediante orientação.

5.2 Área de Segurança da Informação

- 5.2.1 Efetuar a gestão e o direcionamento das ações de Segurança da Informação da Phi.
- 5.2.2 Definir a Política de Segurança da Informação, suas Normas e demais Procedimentos/Instruções;
- 5.2.3 Definição e da implementação das normas de segurança lógica e física, das instalações, equipamentos, sistemas e dados, bem como das normas gerais de acesso e proteção aos equipamentos, programas e arquivos de dados, visando garantir a integridade, qualidade e continuidade dos serviços prestados pela área;
- 5.2.4 Preservar a integridade dos dados e das informações sob sua responsabilidade;
- 5.2.5 Zelar pela eficácia dos controles de Segurança da Informação utilizados e informar aos gestores e demais interessados acerca dos riscos associados;
- 5.2.6 Configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação.
- 5.2.7 Gerar e manter trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;

- 5.2.8 Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para a Phi;
- 5.2.9 Assegurar, nas movimentações internas dos ativos de TI, que as informações de determinado usuário não sejam removidas de forma irreversível antes de disponibilizar o ativo para outro usuário;
- 5.2.10 Planejar e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas internas da organização;
- 5.2.11 Assegurar que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Phi ou em fase de mudança de ambiente de desenvolvimento, teste, homologação ou produção de sistemas;
- 5.2.12 Garantir adequado monitoramento e análise de alertas de segurança da informação, direcionando as ações necessárias para as equipes/áreas apropriadas;
- 5.2.13 Desenvolver e disseminar ações de conscientização em Segurança da Informação para todos os colaboradores e parceiros da Phi;
- 5.2.14 Analisar o resultado de auditorias relacionadas à segurança da informação e medir a eficácia dos controles estabelecidos pela Política de Segurança da Informação da Phi;
- 5.2.15 Emitir pareceres relacionados a análises de vulnerabilidades, avaliação de riscos e incidentes de segurança da informação a toda a Phi;
- 5.2.16 Manter o programa de certificação PCI-DSS.

5.3 Gestores

- 5.3.1 Cumprir e fazer cumprir o estabelecido nesta Política;
- 5.3.2 Transmitir aos seus subordinados as disposições constantes deste documento a fim de que o mesmo tenha ampla divulgação no ambiente de trabalho;
- 5.3.3 Garantir aderência e cumprimento dos controles de segurança da informação estabelecidos pelas Normas e Política de Segurança da Informação;
- 5.3.4 Garantir que as inconformidades ocorridas em suas áreas sejam identificadas e reportadas, e que sejam adotadas as medidas corretivas apropriadas, conforme controles estabelecidos pelas Normas e Instruções de segurança da informação;

- 5.3.5 Garantir que seus subordinados recebem os acessos estritamente necessários para desempenhar suas atividades;
- 5.3.6 Proteger os ativos de sua área (físico e lógico), de acordo com os critérios de classificação das informações definidos pela Phi;
- 5.3.7 Garantir que todos os seus subordinados tenham pleno conhecimento e cumpram a Política de Segurança da Informação.

5.4 Colaboradores

- 5.4.1 Cumprir o estabelecido na Política de Segurança da Informação, reportando ao seu gestor qualquer irregularidade verificada;
- 5.4.2 Indenizar todo prejuízo e/ou dano que vier a causar a Phi em decorrência da não obediência às diretrizes estabelecidas na Política de Segurança da Informação, bem como demais Normas e Procedimentos associados;
- 5.4.3 Parceiros externos, por sua vez, também devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes;
- 5.4.4 Seguir as orientações fornecidas pelas áreas competentes em relação ao uso dos recursos computacionais e informacionais da Phi.
- 5.4.5 Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da Phi;
- 5.4.6 Manter-se atualizado em relação a esta política e às normas e procedimentos relacionados, buscando informação junto a Área de Segurança da Informação sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações.

6 BASE REGULATÓRIA / LEGISLAÇÃO APLICÁVEL

- Lei Federal 12.965, de 23 de abril de 2014;
- Lei 13.709, de 14 de agosto de 2018;
- Circular BCB 3.909, de 16 de agosto de 2018;
- Payment Card Industry Data Security Standard (PCI-DSS);
- ISO/IEC 27001;
- ISO/IEC 27002.
- ISO/IEC 27002.
- Lei Nº 9.279, de 14 de maio de 1996
- Lei Nº 9.610, de 19 de maio de 1998



7 REGULAMENTAÇÃO INTERNA RELACIONADA

- Diretrizes do Manual de Conduta Phi – Na Dúvida Não Tenha Dúvida

8 SANÇÕES E PUNIÇÕES

8.1 Disposições Gerais

- 8.1.1 O descumprimento aos termos desta Política pode ser objeto de medidas disciplinares e/ou consequências legais e regulatórias;
- 8.1.2 A aplicação de sanções e/ou medidas disciplinares deverá ser realizada tendo como base a gravidade da infração cometida e o impacto por ela causado;
- 8.1.3 No caso de infrações cometidas por terceiros e/ou prestadores de serviços as sanções e/ou medidas disciplinares deverão ser aplicadas conforme definido e previsto em contrato;
- 8.1.4 Em caso de violações que caracterizem atividades ilegais, que causem dano de imagem e/ou financeiro, o transgressor deverá ser devidamente identificado, podendo ser responsabilizado, respondendo judicialmente e financeiramente;
- 8.1.5 Para segregação de assuntos inerentes ao tema, bem como para detalhamento da atividade, podem ser elaborados regulamentação interna complementar, à qual será mencionada no item 6. Regulamentação Interna Associada.
- 8.1.6 A Phi, embora não seja instituição regulada pelo Banco Central do Brasil, em razão da natureza dos produtos e serviços ofertados, adota como boa prática, de forma análoga, a regulamentação pertinente ao tema, emitida pela referida autarquia.



9 GESTÃO DA POLÍTICA

9.1 Elaboração, revisão e aprovação

9.1.1 A **PLT-SI-001 - Política de Segurança da Informação** deverá ser aprovada e validada pela direção da Phi.

DocuSigned by:


555D4089F26B4EB
José Renato Silveira Hopf – Diretor
Presidente

10 REVISÕES

10.1 Periodicidade de Revisões

10.1.1 Esta Política será atualizada com a periodicidade de 1 (um) ano, salvo se houver especificidade regulatória/legal, ou alterações na atividade/processo que ensejem alterações.

10.2 Histórico de Revisões

Data	Responsável	Ação
23/07/2019	Anderson Camargo	Criação
14/05/2020	Anderson Camargo	Revisão
07/04/2021	Diego Souza	Revisão
14/04/2021	Diego Souza	Atualização estrutura do documento
22/06/2022	Diego Souza	Atualização