

<b>softplan</b>		Título <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – R.I.</b>				Código <b>POL_113</b>
Unidade de Negócio	Área responsável	Classificação	Aprovação	Revisada em	Vigência	Versão
<b>UC</b>	<b>SI</b>	<b>Pública</b>	<b>COSEG &amp; ESG</b>	<b>19/03/2024</b>	<b>Indeterminada</b>	<b>1.0</b>

## MENSAGEM DO CEO SOBRE SEGURANÇA DA INFORMAÇÃO NA GRUPO SOFTPLAN



“Somos uma das maiores empresas de software do Brasil e essa posição nos traz grandes responsabilidades pela segurança dos nossos sistemas, produtos e informações. Esse cuidado deve se refletir em ações diárias, garantindo nosso compromisso com todos os clientes, colaboradores e sócios. A Segurança da Informação tem se tornado cada vez mais importante, principalmente em empresas de tecnologia. Por isso, eu quero compartilhar com vocês a minha visão e como cada um pode contribuir para que nosso ambiente de trabalho se torne cada vez mais seguro”

A cada dia, com o crescimento das nossas operações, participamos direta ou indiretamente da instrumentalização das informações de clientes e de consumidores finais de nossos sistemas. Muitas vezes, essas informações incluem dados sensíveis que envolvem importantes setores da sociedade, como Justiça, Gestão Pública e Indústria da Construção Civil, além de outros adjacentes a esses. Dedicar nossos melhores esforços na segurança dessas informações deve ser parte da nossa busca diária por excelência.

Também é natural que novos regulamentos entrem em vigor para reforçar a importância da proteção de dados e informações, como por exemplo, na área de privacidade de dados, com a LGPD — Lei Geral de Proteção de Dados. Esse processo exige que as empresas implementem medidas protetivas e é responsabilidade de todos os colaboradores estarem atentos ao impacto dessas mudanças em suas atividades.

Estamos crescendo: Temos grandes objetivos estratégicos para os próximos anos, mantendo o crescimento orgânico e consistente das nossas operações atuais e acelerando nossos processos de M&A. Avançaremos muito rápido nos mercados privados rumo a construção de uma plataforma Multi-SaaS e para manter esse ritmo precisamos acompanhar as tecnologias que avançam a passos largos.

O mesmo tempo em que crescemos, as ameaças cibernéticas se tornam cada vez mais sofisticadas. E isso pode diretamente impactar nossa capacidade de entregar nossos serviços aos clientes e consumidores. Portanto, para uma empresa como a nossa, que pretende crescer com boas margens, ganhar mercado incorporando novas tecnologias e soluções e estar preparada, se necessário para um IPO, segurança da informação passa a ser pauta de primeira importância em todos os níveis da companhia.

Nós, colaboradores, somos o Grupo Softplan e temos o compromisso de buscar o melhor que estiver ao nosso alcance para que as informações e sistemas utilizados por nossos clientes estejam seguros e íntegros. É por isso que conto com todos para garantir e incorporar ações coletivas e individuais orientadas à proteção das tecnologias e segurança das informações em nossas atividades diárias.

<b>softplan</b>		Título <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – R.I.</b>				Código <b>POL_113</b>
Unidade de Negócio	Área responsável	Classificação	Aprovação	Revisada em	Vigência	Versão
<b>UC</b>	<b>SI</b>	<b>Pública</b>	<b>COSEG &amp; ESG</b>	<b>19/03/2024</b>	<b>Indeterminada</b>	<b>1.0</b>

## 1. OBJETIVO

- 1.1. A presente Política tem como objetivo dar diretrizes do modelo de governança de segurança da informação no Grupo Softplan e deve ser utilizada como base para todas as políticas, diretrizes e processos relacionados à segurança da informação.

## 2. APLICAÇÃO E ABRANGÊNCIA

- 2.1. A presente política aplica-se a todos os colaboradores do Grupo Softplan, suas subsidiárias integrais, e suas controladas de forma direta ou indireta que exercem atividade no Brasil e no exterior.
- 2.2. Aplica-se a todos os colaboradores, (inclusive aprendizes, estagiários, Diretores, Membros do Conselho e Membros dos Comitês) de qualquer nível hierárquico, (os “Softplayers”); Prestadores de serviço, Terceiros; Consultores e trabalhadores temporários; Todos os usuários autorizados a acessar/administrar os sistemas internos da Grupo Softplan.

## 3. DEFINIÇÕES:

- 3.1. **Ativos de informação:** Tudo o que armazena, trafega, manipula ou processo informações
- 3.2. **Risco Residual:** É o nível de risco após ter levado em consideração as ações de mitigação
- 3.3. **Informações confidenciais, restritas ou internas:** Conforme descrito na POL\_091 Política de Classificação da Informação
- 3.4. **RoadMap: Mapa de planejamento de ações**
- 3.5. **Grupo Softplan:** Para fins dessa política significa Softplan S.A.
- 3.6. **Colaboradores:** Empregados CLT.
- 3.7. **Subsidiária integral:** Empresa cuja totalidade das ações (100%) é pertencente ao Grupo Softplan, sendo por ela controlada.
- 3.8. **Controlada:** Empresa cuja maioria das ações (mais que 50%) é pertencente ao Grupo Softplan, sendo por ele controlada.

## 4. DIRETRIZES GERAIS

- 4.1. Todos os colaboradores, prestadores de serviços, terceiros, consultores, trabalhadores temporários, não se limitando a estes, que venham a realizar serviços para a Grupo Softplan devem observar, cumprir e fazer cumprir os termos e condições desta Política, preservar e garantir a confidencialidade das informações, zelar pela integridade e disponibilidade dos ativos da Softplan, e estar em conformidade com regulamentações de cada segmento de negócio da Softplan.
- 4.2. Principais objetivos do Grupo Softplan relacionados à Segurança da Informação:
  - 4.2.1. Assegurar a disponibilidade e continuidade dos sistemas informacionais do Grupo Softplan;
  - 4.2.2. Proteger os ativos de ameaças internas e externas;
  - 4.2.3. Evitar o roubo de informações confidenciais, restritas ou internas do Grupo Softplan;
  - 4.2.4. Estar em conformidade com leis e regulamentações;
  - 4.2.5. Proteger o Grupo Softplan e seus clientes de possíveis fraudes internas ou externas

## 5. EXCEÇÕES

- 5.1. Para se adequar a realidade do Grupo Softplan e seus diferentes segmentos de negócio, exceções podem ser aprovadas mediante a avaliação do COSEG - Comitê Executivo de Segurança da Informação da Softplan, através da aplicação do Formulário de Aceitação de Riscos de Segurança da Informação [FARSI].

<b>softplan</b>		Título <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – R.I.</b>				Código <b>POL_113</b>
Unidade de Negócio	Área responsável	Classificação	Aprovação	Revisada em	Vigência	Versão
<b>UC</b>	<b>SI</b>	<b>Pública</b>	<b>COSEG &amp; ESG</b>	<b>19/03/2024</b>	<b>Indeterminada</b>	<b>1.0</b>

## 6. DIVULGAÇÃO

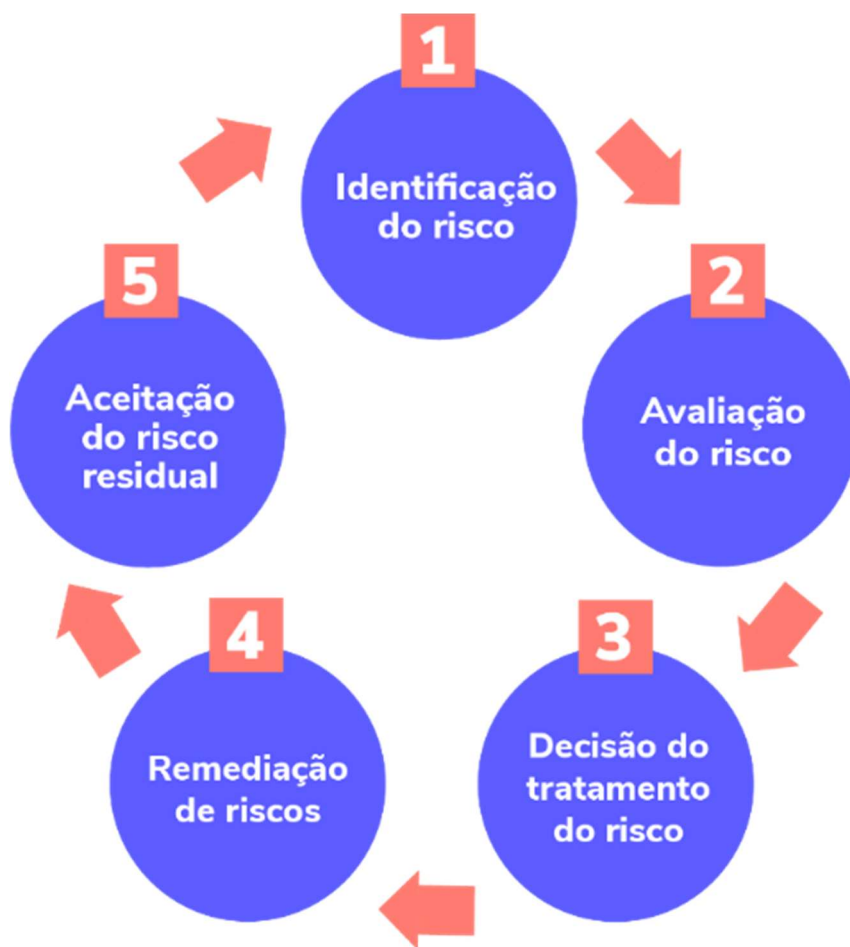
6.1. Este documento está classificado como “Pública”.

## 7. GESTÃO DE RISCOS DE SEGURANÇA

7.1. Segurança da informação está estruturada com base na ISO 27001:2022, que é regida pela avaliação de riscos e melhoria contínua.

7.2. Esta política segue os seguintes princípios:

- 7.2.1. Segurança é regida pela avaliação de riscos;
- 7.2.2. Cem por cento de riscos mitigados não é algo que pode ser atingido;
- 7.2.3. Proteções devem ser implementadas avaliando a criticidade dos ativos de informação;
- 7.2.4. Segurança deve trabalhar com um facilitador ao negócio.



<b>softplan</b>		Título <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – R.I.</b>				Código <b>POL_113</b>
Unidade de Negócio	Área responsável	Classificação	Aprovação	Revisada em	Vigência	Versão
<b>UC</b>	<b>SI</b>	<b>Pública</b>	<b>COSEG &amp; ESG</b>	<b>19/03/2024</b>	<b>Indeterminada</b>	<b>1.0</b>

- 7.2.5. **Identificação do risco:** Uma revisão baseada na PPSI - Política de Princípios de Segurança da Informação deve ser conduzida anualmente, visando a identificação de riscos e maturidade de segurança, bem como a cada nova implementação, atualização e/ou mudança nos sistemas da Grupo Softplan;
- 7.2.6. **Avaliação de risco:** Os riscos de segurança da informação devem ser avaliados e analisados pela área de segurança da informação. Quando necessário, a área de segurança da informação pode envolver de outras partes para auxiliar na análise;
- 7.2.7. **Decisão do tratamento do risco:** Os riscos, bem como o tratamento deles, devem ser apresentados pela área de segurança da informação aos executivos e comitês responsáveis, a fim de deliberar como serão tratados;
- 7.2.8. **Remediação de riscos:** Planos de ação devem ser elaborados pelas áreas apropriadas e sua evolução deve ser apresentada a área de segurança da informação periodicamente;
- 7.2.9. **Aceitação do risco residual:** Os riscos residuais, devem ser apresentados pela área de segurança da informação aos executivos e comitês responsáveis, a fim de deliberar como serão tratados.

## 8. GOVERNANÇA E ORGANIZAÇÃO

### 8.1. Funções e responsabilidades de segurança da informação:

#### 8.1.1. Área de segurança da informação:

- 8.1.1.1. Gerir os riscos estratégicos e táticos ligados à segurança da informação;
- 8.1.1.2. Coordenar e liderar COSEG - Comitê Executivo de Segurança da Informação;
- 8.1.1.3. Propor o RoadMap anual para segurança da informação;
- 8.1.1.4. Garantir o andamento do RoadMap e elaborar os reports do mesmo para o COMEX (Comitê Executivo) e Conselho de Administração;
- 8.1.1.5. Coordenar eventuais “comitês de crise” ligados à segurança da informação;

#### 8.1.2. COSEG – Comitê Executivo de Segurança da Informação

- 8.1.2.1. Direcionar como a estratégia de segurança da informação está sendo implementada e monitorar a evolução dos processos mitigatórios de riscos;
- 8.1.2.2. Arbitrar em questões de grande importância de segurança da informação.
- 8.1.2.3. Garantir que a estratégia da unidade esteja de acordo com as políticas e processos de segurança da informação, bem como alinhada ao RoadMap de segurança da informação.

#### 8.1.3. CTO Corporativo e das Unidades

- 8.1.3.1. Garantir que as áreas funcionalmente subordinadas, tanto nas unidades de negócios quando no corporativo estejam implementando as ações de segurança da informação conforme RoadMap.

#### 8.1.4. DPO

- 8.1.4.1. Assegurar que as diretrizes de proteção de dados e privacidade estejam alinhadas com a estratégia de segurança da informação, bem como trabalhando em conjunto nos casos de eventos/incidentes de segurança da informação que impactem a privacidade.

<b>softplan</b>		Título <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – R.I.</b>				Código <b>POL_113</b>
Unidade de Negócio	Área responsável	Classificação	Aprovação	Revisada em	Vigência	Versão
<b>UC</b>	<b>SI</b>	<b>Pública</b>	<b>COSEG &amp; ESG</b>	<b>19/03/2024</b>	<b>Indeterminada</b>	<b>1.0</b>

#### 8.1.5. TI Corporativa

- 8.1.5.1. Garantir que as melhores práticas, políticas, processos e procedimentos de segurança sejam implementados e seguidos. Implementar e sugerir soluções de segurança da informação. Envolver e manter segurança da informação informada sobre projetos ou processos, para que ela realiza as avaliações necessárias
- 8.1.5.2. Garantir o funcionamento das soluções para proteção dos ativos de TI da unidade corporativa.

#### 8.1.1. Área de Gente e Cultura

- 8.1.1.1. Garantir que o processo de contratação envolva os requisitos de segurança da Informação.
- 8.1.1.2. Garantir que a POL\_054\_Política de Segurança para Colaboradores seja assinada em conjunto com o Contrato. Garantir que segurança da informação faça parte dos processos de *onboarding*, bem como qualquer outro processo corporativo que vise a conscientização dos colaboradores em segurança da informação.

#### 8.1.2. Auditoria interna, Riscos & Compliance

- 8.1.2.1. Garantir que a Softplan esteja em conformidade com as práticas e políticas de segurança da informação, bem como regulamentações, através de mecanismos internos de controle e acompanhamento. Adicionalmente, a auditoria interna verifica anualmente a aderência dos processos e controles internos aos normativos e relata de forma sistemática e tempestivamente, os resultados no tocante aos riscos/gaps corporativos à Diretoria, Comitê de Auditoria Interna e ao Conselho de Administração.

### 9. PRINCIPIOS DE SEGURANÇA DE SISTEMAS E INFORMAÇÃO

- 9.1. Todos os princípios serão definidos na PPSI - Política de Princípios de Segurança da Informação e estão alinhados com a estrutura da ISO 27002:2022.

TEMA	DESCRIÇÃO
<b>Controles pessoais</b>	Composto por oito controles relacionados às proteções dos usuários
<b>Controles físicos</b>	Composto por quatorze controles relacionados à proteção física dos ambientes
<b>Controle tecnológicos</b>	Composto por trinta e quatro controles relacionados às proteções tecnológicas e as tecnologias de proteção
<b>Controles organizacionais</b>	Composto por trinta e sete controles que não se classificam nos temas acima

<b>softplan</b>		Título <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – R.I.</b>				Código <b>POL_113</b>
Unidade de Negócio	Área responsável	Classificação	Aprovação	Revisada em	Vigência	Versão
<b>UC</b>	<b>SI</b>	<b>Pública</b>	<b>COSEG &amp; ESG</b>	<b>19/03/2024</b>	<b>Indeterminada</b>	<b>1.0</b>

## 10. DÚVIDAS

- 10.1. Em caso de dúvidas a respeito desta Política, entrar em contato pelo e-mail: [seginfo@softplan.com.br](mailto:seginfo@softplan.com.br).

## 11. SANÇÕES APLICÁVEIS

- 11.1. Violações aos termos desta Política e demais normativos internos, serão devidamente apuradas pelo respectivo Comitê, e, caso comprovadas, serão aplicadas as medidas disciplinares e legais cabíveis, em consonância com a POL\_006 Política de Consequências;
- 11.2. As sanções para violações praticadas pelos colaboradores incluem advertência, suspensão, demissão e acionamento judicial, a depender da gravidade, da mesma forma que para os terceiros que atuam em nome das empresas do Grupo Softplan, as penalidades estabelecidas em contrato podem ser executadas, sem prejuízo de reparação do dano causado.

## 12. REFERÊNCIAS

- 12.1. Código de Conduta Grupo Softplan
- 12.2. POL\_002\_Política Anticorrupção
- 12.3. POL\_013\_Política de Elaboração e Publicação de Documentos Normativos.
- 12.4. POL\_006\_Política de Consequências.
- 12.5. POL\_014\_Política de Alçadas
- 12.6. POL\_054\_Política de Segurança para Colaboradores
- 12.7. POL\_055\_Política de Segurança Grupo Softplan
- 12.8. POL\_056\_Política de Princípios de Segurança da Informação
- 12.9. POL\_058\_Política de Desenvolvimento Seguro
- 12.10. POL\_059\_Diretriz de Princípios para Projetar Sistemas Seguros
- 12.11. POL\_060\_Política de Gestão de Incidente de Segurança da Informação
- 12.12. POL\_061\_Diretriz de Segurança do Gerenciamento de Projetos
- 12.13. POL\_069\_Política de Segurança para Uso de Dispositivos Pessoais
- 12.14. POL\_070\_Política de Segurança para Trabalho Remoto
- 12.15. POL\_091\_Política de Classificação da Informação – PCI
- 12.16. POL\_099\_Política de Continuidade de Negócios
- 12.17. Formulário de Aceitação de Riscos de Segurança da Informação [FARSI]

## 13. CONTROLE E REVISÃO DO DOCUMENTO

Versão	Elaboração	Revisão	Aprovação	Data	Modificação	Motivo
1.0	- Daniel Mizga da Silva (Head de Segurança da Informação)	CTO Corporativo CTOs das Unidades CFO Corporativo TI Corporativa Auditoria interna, Compliance & Risco Jurídico Corporativo Time de ESG	COSEG Comitê Executivo de Segurança da Informação + Time de ESG	19/03/24	N/A	Elaboração da Política de segurança da informação para atendimento ao requisito de ESG, para relação com investidores