

Modelo de Política de Desenvolvimento Seguro de Aplicações (Softwares)

1ª Edição | 2025

Sumário

Sobre o Modelo de Política.....	3
Política de Desenvolvimento Seguro de Aplicações (Softwares).....	4
1. Objetivo	4
2. Abrangência	4
3. Glossário	4
4. Diretrizes e Regras	5
5. Responsabilidades	9
6. Penalidades ou Consequências	9
7. Referências	10
8. Disposições finais.....	11
9. Histórico de Versões	11

Sobre o Modelo de Política

Este Modelo de Política para Desenvolvimento Seguro de Aplicações (Softwares) é resultado do trabalho conjunto da ANBIMA – Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais com participantes de mercado reunidos no Grupo Consultivo de Cibersegurança e consultoria técnica da PwC – PricewaterhouseCoopers. Trata-se de um material de apoio complementar ao Guia Técnico de Orientações para Desenvolvimento Seguro de Aplicações (Softwares)¹. O Modelo visa apoiar as organizações atuantes nos mercados financeiro e de capitais a implementar políticas e controles internos voltados ao desenvolvimento seguro de aplicações em conformidade com as orientações e recomendações do Guia Técnico.

O conteúdo deste documento não é vinculante para quaisquer organizações, associadas ou não à ANBIMA, e não se caracteriza, de nenhum modo, como elemento da autorregulação da Associação. O presente material se caracteriza, tão somente, como de apoio, e, sob nenhuma hipótese, vincula as organizações e a ANBIMA a futuras discussões sobre o tema que forem tratadas no âmbito da autorregulação.

O conteúdo deste documento também não deve ser interpretado de forma a contrariar, mitigar ou se opor a nenhum normativo da legislação, regulação² e autorregulação³ aplicáveis às organizações participantes dos mercados financeiro e de capitais, limitando-se, tão somente, a apoiar o mercado na melhor consecução de suas atividades.



Para se aprofundar nos tópicos relacionados à segurança da informação e cibernética, consulte nossa página especial, acessando o QR CODE ao lado.



¹ ANBIMA. Orientações para o Desenvolvimento Seguro de Aplicações (Softwares) (2025). Disponível em:

<https://www.anbima.com.br/data/files/B7/75/47/EE/9003A910C8D0A1A9BA2BA2A8/Orientacoes_Desenvolvimento_Seguro_de_Aplicacoes.pdf>

BRASIL. Resolução CVM Nº 35/2021. Disponível em:

<<https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol035consolid.pdf>>.

² BRASIL. Resolução CMN Nº 4.893/2021. Disponível em:

<<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893>>.

BRASIL. Resolução CVM Nº 35/2021. Disponível em:

<<https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol035consolid.pdf>>.

³ ANBIMA. Regras e Procedimentos de Deveres Básicos. Disponível em:

<https://www.anbima.com.br/data/files/1E/42/14/73/BB3EF810B99A0EF8B82BA2A8/Regras%20e%20Procedimentos%20de%20Deveres%20Basico%20vigente%20a%20partir%20de%2003.06.24_.pdf>.

Política de Desenvolvimento Seguro de Aplicações (Softwares)

1. Objetivo

Definir regras e diretrizes para a implementação de um processo de Desenvolvimento Seguro na organização, com o objetivo de garantir que exista um ciclo de desenvolvimento de sistemas adequado para as realidades de Segurança da Informação e Cibernética, bem como para o cumprimento das normas e regulamentações internas e externas pertinentes ao tema.

2. Abrangência

Esta política se aplica a toda a organização, desde que não exista norma ou procedimento mais específico que regulamente o tema disposto neste documento.

Aplica-se a todos os colaboradores, terceiros e parceiros envolvidos em atividades de desenvolvimento, manutenção e implantação de softwares e sistemas para a organização.

3. Glossário

- **Ambientes de Desenvolvimento:** referem-se aos diferentes contextos e configurações em que o software é projetado, codificado, testado e preparado para implantação em produção. Geralmente existem em três grandes etapas, desenvolvimento, testes / qualidade e produção.
- **Bibliotecas:** coleções de componentes de software reutilizáveis ou rotinas que podem ser utilizadas por programas diferentes.
- **CI/CD (Integração Contínua e Entrega Contínua / Deploy Contínuo):** Conjunto de práticas e processos que automatizam a integração de código desenvolvido por diferentes membros da equipe (Integração Contínua), a construção, teste e validação automatizada do software, e a entrega ou implantação rápida, frequente e segura das mudanças em ambientes de produção ou homologação (Entrega/Deploy Contínuo). O CI/CD visa aumentar a eficiência, reduzir erros humanos, garantir qualidade e acelerar o ciclo de desenvolvimento e entrega de software.
- **Ciclo de Vida do Software:** etapas de planejamento, codificação, teste, implantação e manutenção.
- **Dados Pessoais:** são quaisquer informações que possam identificar uma pessoa natural, seja diretamente (nome, CPF, etc.) ou indiretamente (endereço IP, histórico de compras, etc.).

- **Desenvolvimento Seguro:** práticas que buscam integrar a segurança em todas as etapas do ciclo de vida do software.
- **DAST (Teste de segurança dinâmica de aplicações):** prática de segurança cibernética que se concentra na análise das aplicações em execução para identificar vulnerabilidades de segurança em tempo real.
- **SAST (Teste de segurança de aplicações estáticas):** prática de segurança cibernética que envolve a análise do código-fonte ou do código compilado de uma aplicação, sem executar o programa.
- **SCA (Análise de composição de software):** processo que permite às organizações identificar e gerenciar componentes de software de terceiros em suas aplicações, através da avaliação de segurança e conformidade de bibliotecas, frameworks e pacotes usados em sistemas.
- **Pentest:** técnica de segurança cibernética que envolve a simulação de ataques a sistemas, aplicações ou redes com o objetivo de identificar vulnerabilidades e falhas de segurança antes que possam ser exploradas por atacantes mal-intencionados.
- **Privilegio:** conjunto de permissões e direitos de acesso concedidos a um usuário ou sistema dentro de uma rede ou aplicação.
- **Vulnerabilidade:** fraqueza em um sistema que pode ser explorada por agentes maliciosos.

4. Diretrizes e Regras

Os subtópicos abaixo podem ser direcionados ou remetidos a diferentes áreas ou responsáveis, de acordo com a estrutura da organização. Dessa forma, a adoção e aplicabilidade dos itens pode ser feita de forma integral ou fracionada, realizando as devidas adaptações conforme coerente.

4.1. Governança e Cultura de Segurança

- Incorporar os princípios de proteção da informação de forma estruturada e alinhada aos objetivos estratégicos da organização.
- Tratar a segurança como valor organizacional e requisito essencial de qualidade no desenvolvimento de software.
- Formalizar, comunicar amplamente e revisar periodicamente as diretrizes de desenvolvimento seguro.
- Compartilhar a responsabilidade pela segurança entre todas as áreas envolvidas no ciclo de vida do software, promovendo atuação colaborativa e integrada.
- Estabelecer mecanismos de supervisão, auditoria e melhoria contínua das práticas de segurança adotadas.
- Garantir a conformidade do desenvolvimento seguro com políticas, normas internas e regulamentações externas aplicáveis.

- Referenciar obrigatoriamente a Política de Segurança da Informação, o Guia Técnico de Desenvolvimento Seguro e os requisitos regulatórios e normativos vigentes.
- Estabelecer mecanismos de monitoramento e auditoria periódica para avaliar a conformidade e eficácia das práticas de segurança.
- Revisar regularmente as diretrizes considerando mudanças no ambiente regulatório, tecnológico e organizacional, visando à melhoria contínua.

4.2. Modelo e Ciclo de Vida de Desenvolvimento Seguro (SSDLC)

- Adotar o modelo Secure Software Development Life Cycle (SSDLC) em todas as fases do software - planejamento, design, implementação, testes, entrega e manutenção.
- Orientar a implementação do SSDLC conforme o framework NIST SSDF v1.1, contemplando:
 - Preparação da Organização (PO);
 - Proteção do Software (PS);
 - Produção de Software Bem Protegido (PW);
 - Resposta a Vulnerabilidades (RV).
- Adaptar as práticas de segurança às realidades organizacionais e aos riscos relevantes, incluindo as categorias do OWASP Top 10.
- Incorporar continuamente a segurança em todas as fases do ciclo de vida, identificando e mitigando riscos desde o início.
- Avaliar riscos e definir requisitos de segurança alinhados ao negócio durante o planejamento.
- Incorporar princípios de arquitetura segura e controles de autenticação, autorização e criptografia durante o design.
- Adotar práticas de codificação segura, validação de entradas, tratamento de erros e uso de ferramentas de análise estática durante a implementação.
- Realizar testes de segurança automatizados e manuais, incluindo análises dinâmicas, fuzzing e pentests.
- Garantir controles de segurança eficazes antes da entrega, validando riscos residuais e planejando rollback seguro.
- Monitorar vulnerabilidades, aplicar correções ágeis e manter atualizações constantes durante a manutenção.

4.3. Práticas de Codificação Segura

- Promover práticas de codificação segura para prevenir vulnerabilidades desde a origem do código.
- Validar e sanitizar todas as entradas de dados, tratando-as como potencialmente maliciosas.
- Implementar mecanismos robustos de autenticação, como autenticação multifator (MFA), e práticas seguras de gerenciamento de sessões.

- Prevenir injeções e comandos maliciosos por meio de consultas parametrizadas e separação entre dados e comandos.
- Tratar erros de forma segura, evitando exposição de informações sensíveis e centralizando o monitoramento de exceções.
- Proteger dados sensíveis com criptografia adequada em repouso e trânsito, utilizando algoritmos reconhecidos.
- Aplicar princípios de segurança por design, como menor privilégio e separação de responsabilidades.

4.4. Controle de Acesso e Segurança nos Ambientes de Desenvolvimento

- Controlar rigorosamente o acesso a ambientes e ferramentas de desenvolvimento, seguindo o princípio do menor privilégio.
- Segregar ambientes de desenvolvimento, homologação e produção, mantendo controles independentes e restrições adequadas.
- Evitar o uso de contas genéricas, assegurando identificação individual e rastreabilidade das ações.
- Gerenciar credenciais e segredos de forma segura, utilizando cofres de segredo, com rotação periódica e monitoramento.
- Aplicar políticas de acesso condicional e autenticação forte, como MFA para acessos privilegiados.
- Realizar auditorias e revisões periódicas de acessos, revogando permissões obsoletas imediatamente.

4.5. Análises e Testes de Segurança

- Integrar análises de segurança contínuas durante todo o ciclo de desenvolvimento, contemplando SAST, DAST, IAST, SCA, testes manuais e pentests.
- Registrar, classificar e tratar vulnerabilidades conforme sua criticidade, validando correções antes da liberação.
- Documentar e armazenar evidências das análises para garantir rastreabilidade e conformidade.
- Retroalimentar o processo de desenvolvimento com os resultados das análises para aprimoramento contínuo.

4.6. Proteção dos Pipelines CI/CD

- Proteger pipelines de CI/CD, incorporando controles de segurança automáticos em build, teste e deploy.
- Isolar e monitorar ambientes de execução de pipelines, restringindo acesso a identidades autorizadas.
- Prevenir execução de código malicioso ou não autorizado durante automação, controlando alterações em scripts e configurações.

- Assinar digitalmente e armazenar artefatos em repositórios seguros, garantindo autenticidade e rastreabilidade.

4.7. Gestão de Dependências e Componentes de Terceiros

- Avaliar rigorosamente a segurança de bibliotecas, frameworks, APIs e componentes de terceiros antes da adoção.
- Manter inventário atualizado (ex.: SBOM) de todas as dependências utilizadas no desenvolvimento.
- Monitorar continuamente vulnerabilidades conhecidas em componentes usados, utilizando fontes confiáveis e ferramentas automatizadas.
- Atualizar ou substituir componentes vulneráveis com validação de compatibilidade antes da liberação em produção.

4.8. Gestão de Vulnerabilidades

- Instituir processo contínuo e ágil para identificar, priorizar e corrigir vulnerabilidades, baseado em critérios técnicos e de impacto.
- Comunicar de forma clara e transparente as atualizações de segurança relevantes.

4.9. Segurança na Entrega e Operação

- Configurar ambientes de produção com hardening e políticas restritivas de acesso.
- Implementar monitoramento e detecção de anomalias em tempo real nos ambientes produtivos.
- Manter planos de contingência e procedimentos seguros de rollback validados.
- Aplicar patches e atualizações via processo controlado, com testes prévios e documentação.

4.10. Diretrizes Específicas por Tipo de Aplicação

- Mitigar riscos específicos conforme o tipo de aplicação, adotando práticas específicas para:
 - Aplicações Web (autenticação forte, validação e sanitização de entradas, criptografia, monitoramento);
 - APIs (controle granular de acesso, rate limiting, proteção de tokens, inventário e versionamento);
 - Aplicações Mobile (armazenamento seguro, evitar hardcoding, TLS, ofuscação);
 - Aplicações com Modelos de Linguagem (separação de instruções, monitoramento, validação da origem, restrição de uso).

4.11. Capacitação e Ferramentas de Apoio

- Incentivar o uso de ferramentas especializadas para identificar, mitigar e monitorar riscos em todo o ciclo de desenvolvimento.
- Atualizar e capacitar equipes continuamente para fortalecer a cultura de desenvolvimento seguro.

5. Responsabilidades

a) Segurança da Informação

1. Elaborar, revisar e atualizar esta política sempre que necessário.
2. Avaliar as solicitações de mudança para assegurar que todos os devidos testes de segurança foram realizados.
3. Auxiliar a tecnologia da informação no processo de concepção de sistemas seguros.

b) Tecnologia da Informação

1. Gerenciar ativos de software.
2. Informar todos os usuários sobre suas responsabilidades no uso de quaisquer ativos que lhes sejam atribuídos.
3. Estabelecer o ciclo de segurança para o desenvolvimento de software, inclusive terceirizado.
4. Solicitar e realizar os testes de segurança aplicáveis para a devida etapa de desenvolvimento de sistemas.

c) Equipe de desenvolvimento

1. Cumprir e fazer cumprir as regras dessa política.

6. Penalidades ou Consequências

O não cumprimento desta política pode resultar em ações disciplinares, incluindo advertências, treinamento obrigatório, suspensão de atividades e, em casos graves, desligamento, conforme regulamento interno.

7. Referências

- NIST (National Institute of Standards and Technology) ⁴;
- OWASP (Open Web Application Security Project) ⁵;
- Lei Nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) ⁶;
- Resoluções CVM Nº 35/2021 ⁷, CMN Nº 4.893/2021 ⁸, BCB Nº 498/2025, CD/ANPD nº 2/2022 ⁹ e CD/ANPD nº 15/2024 ¹⁰;
- Normas ISO/IEC 9001 ¹¹, ISO/IEC 19249 ¹², ISO/IEC 27001 ¹³ e 27034 ¹⁴;
- Regras e Procedimentos internos de Deveres Básicos ¹⁵;
- Guia de Cibersegurança ¹⁶;
- Guia Técnico – Orientações para Contratação de Terceiros e Nuvem ¹⁷; e
- Guia Técnico – Orientações para Desenvolvimento Seguro de Aplicações (Softwares) ¹⁸.

⁴ NIST. Secure Software Development Framework (SSDF) v1.1 (2022). Disponível em:

<https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=959767>

⁵ OWASP. OWASP Secure Coding Practices (2010). Disponível em: <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/assets/docs/OWASP_SCP_Quick_Reference_Guide_v21.pdf>

⁶ BRASIL. Lei Nº 13.709/2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

⁷ BRASIL. Resolução CVM Nº 35/2021. Disponível em:

<<https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol035consolid.pdf>>.

⁸ BRASIL. Resolução CMN Nº 4.893/2021. Disponível em:

<<https://www.bcb.gov.br/estabilidadefinanceira/exibnormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893>>

⁹ BRASIL. Resolução CD/ANPD nº 2/2022. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022>.

¹⁰ BRASIL. Resolução CD/ANPD nº 15/2024. Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>>.

¹¹ ISO. Quality management systems — Requirements (2015). Disponível em: <<https://www.iso.org/standard/62085.html>>

¹² ISO. Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications (2017). Disponível em: <<https://www.iso.org/standard/64140.html>>

¹³ ISO. Information security, cybersecurity and privacy protection — Information security management systems — Requirements (2022). Disponível em: <<https://www.iso.org/standard/27001>>

¹⁴ ISO. Information technology — Security techniques — Application security (2011). Disponível em: <<https://www.iso.org/standard/44378.html>>

¹⁵ ANBIMA. Regras e Procedimentos de Deveres Básicos. Disponível em:

<https://www.anbima.com.br/data/files/1E/42/14/73/BB3EF810B99A0EF8B82BA2A8/Regras%20e%20Procedimentos%20de%20Deveres%20Basico%20vigente%20a%20partir%20de%2003.06.24_.pdf>.

¹⁶ ANBIMA. Guia de Cibersegurança (3ª Edição, 2021). Disponível em:

<<https://www.anbima.com.br/data/files/34/B3/04/8F/D96F971013C70F976B2BA2A8/Guia%20de%20Ciberseguranca%20ANBIMA.pdf>>.

¹⁷ ANBIMA. Orientações para Contratação de Terceiros e Nuvem (2022). Disponível em:

<<https://www.anbima.com.br/data/files/85/60/2A/F9/3B8C4810272519486B2BA2A8/Guia%20para%20Contratacao%20de%20Terceiros%20e%20Nuvem.pdf>>.

¹⁸ ANBIMA. Orientações para o Desenvolvimento Seguro de Aplicações (Softwares) (2025). Disponível em:

<https://www.anbima.com.br/data/files/B7/75/47/EE/9003A910C8D0A1A9BA2BA2A8/Orientacoes_Desenvolvimento_Seguro_de_Aplicacoes.pdf>

8. Disposições finais

- Data de Vigência: [inserir data]
- Esta política deverá ser revisada anualmente ou sempre que necessário para adequação às mudanças tecnológicas e regulatórias.

9. Histórico de Versões

Versão:	Data:	Motivo:	Elaborado por:	Aprovador por: