# Propósito

A Norma de Desenvolvimento Seguro **NOR-SGSI-013** complementa a Política de Segurança da Informação e Política de Proteção de Dados, definindo as diretrizes para o processo de desenvolvimento seguro de softwares e produtos durante todo o seu ciclo de vida.

# Escopo

Esta norma é aplicável ao escopo definido na Política de Segurança da Informação e na Política de Proteção de Dados.

# Glossário

* **Arquitetura de software:** Elemento da engenharia de software, utilizado para definir os componentes de software.
* **SAST:** Static Application Security Testing (Teste de segurança estático em aplicação), consiste no uso de ferramenta para análise do código-fonte em busca de vulnerabilidades.
* **API:** Application Programming Interface (Interface de programa de aplicação) são usadas para integrar novas aplicações com sistemas de software existentes.

# Diretrizes

O desenvolvimento seguro de softwares é fundamental para assegurar que os dados e informações processados pelos softwares sejam protegidos contra ameaças de Segurança da Informação e atendam aos requisitos de privacidade que forem pertinentes. As seguintes diretrizes devem ser observadas:

## Abordagem de segurança na arquitetura de software

1. Durante o desenvolvimento ou a manutenção de software, é crucial conduzir análises da arquitetura em relação às necessidades do sistema. Essa avaliação deve abranger a identificação dos requisitos de segurança e privacidade, com os resultados registrados.
2. É recomendável envolver pessoas ou empresas externas com expertise em segurança ou privacidade para apoiar essas análises, garantindo uma abordagem abrangente e especializada.
3. Riscos e ameaças existentes para a arquitetura do software devem ser mapeados e monitorados periodicamente, conforme os requisitos da **NOR-SGSI-002**;
4. Os desenvolvedores devem ser conscientizados sobre este processo de análise dos requisitos de segurança e privacidade de softwares;

## Processo de desenvolvimento, sustentação e manutenção de software

1. Os desenvolvedores devem possuir conhecimentos comprovados em práticas de desenvolvimento seguro e quando não o tiverem, ações devem ser tomadas para que seja adquirido. É importante que ocorra uma reciclagem periódica destes conhecimentos, através da realização de um novo treinamento ou de repetição de um treinamento realizado anteriormente.
2. Convém que seja desenvolvido internamente um guia contendo as diretrizes de codificação segura para as linguagens de programação que forem utilizadas;
3. Deve ser estabelecido entre os desenvolvedores a padronização de:
4. Ambiente e ferramentas de desenvolvimento a serem utilizadas;
5. Linguagens e uso de frameworks;
6. Uso de bibliotecas e componentes open-source ou de terceiros;
7. Uso recomendável de ferramenta SAST no pipeline de desenvolvimento.
8. Deve ser estabelecido processo para a mudança dos ambientes e a alteração deve estar restrita a pessoas autorizadas;
9. É recomendável que a documentação do software seja estabelecida e atualizada conforme o processo de sustentação e manutenção;
10. Convém que as permissões de acesso e alteração da documentação do software sejam restritas as pessoas autorizadas;
11. Convém que seja definido o responsável por comunicações oficiais sobre o software.

## Testes e Homologação de software

1. Os ambientes de desenvolvimento, teste e produção de softwares devem ser segregados e possuírem as mesmas características, incluindo as de segurança;
2. Mediante a criação de novas funcionalidades de software, a análise estabelecida para a arquitetura deve ser realizada, para a identificação de novos riscos e necessidades de segurança e privacidade;
3. Dados e informações utilizados em ambientes de desenvolvimento e testes devem ser fictícios;
4. Não convém que sejam feitos testes de software diretamente no ambiente de produção, salvo em situações avaliadas previamente, validadas como seguras e autorizadas formalmente;
5. Novos softwares e atualizações devem ser homologados pelas partes interessadas e validados formalmente antes da implementação no ambiente de produção;
6. É parte integral do processo de desenvolvimento a validação de segurança do software, através da realização de Pentests, conforme os requisitos da **NOR-SGSI-007**.
7. A correção de vulnerabilidades identificadas em software deve obedecer aos requisitos estabelecidos na **NOR-SGSI-007**.

## Desenvolvimento terceirizado

1. O responsável pelo desenvolvimento terceirizado de software deverá apresentar estrutura mínima para o seu desenvolvimento seguro, como:
2. Comprovar capacitação da equipe em codificação segura;
3. Utilizar ferramenta SAST ou similar dentro do pipeline de desenvolvimento;
4. Estabelecer processo ou requisitos de segurança utilizados para o desenvolvimento seguro de softwares.
5. Deve ser definido junto ao terceiro, em um acordo formal, todos os critérios, responsabilidades e requisitos associados a:
6. Propriedade intelectual do código;
7. Segurança da informação;
8. Privacidade e proteção de dados.

## API

1. Toda API que participe de processo de compartilhamento de dados, antes de ser contratada para ser parte integrante de qualquer sistema, deve estar de acordo com todos os termos do **CONTRATO DE COMPARTILHAMENTO DE DADOS POR MEIO DE API;**
2. As API’s contratadas devem ser submetidas a verificações antes de implementadas nos sistemas;
3. Após a verificação positiva da API e a implementação dela no sistema, deve passar por testes em ambiente controlado, seguindo as orientações do item 4.3 desta norma;
4. Convém que as API’s possuam controle de tráfego e criptografia para buscar garantir maior assertividade na segurança das informações.

# Papéis e Responsabilidades

## DIRETORIA DE TECNOLOGIA

1. Assegurar a condução periódica das análises de arquitetura de software;
2. Envolver outras partes na análise de arquitetura de software;
3. Estabelecer processos e atividades para cumprir requisitos de segurança da informação para o desenvolvimento seguro de software, com a validação da área de Infraestrutura e Segurança da Informação;
4. Assegurar que os ambientes utilizados possuam a padronização necessária;
5. Manter e utilizar ferramentas de segurança de código;
6. Criar e atualizar a documentação do software, quando aplicável;
7. Estabelecer a padronização de elementos de segurança no processo de desenvolvimento;
8. Assegurar que seja realizada a correção de vulnerabilidades, conforme a **NOR-SGSI-007**.

## ÁREA DE INFRAESTUTURA E SEGURANÇA DA INFORMAÇÃO

1. Validar os processos e atividades estabelecidos para cumprir requisitos de segurança da informação para o desenvolvimento seguro de software estabelecidos pela Diretoria de Tecnologia

## COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Participar das análises de arquitetura de software;
2. Apoiar a análise dos requisitos de segurança da informação e privacidade dos softwares.

# Gestão de versões

A revisão, aprovação e alteração desta norma segue os requisitos estabelecidos na Política de Segurança da Informação e Política de Proteção de Dados.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 09/10/2023 | CSIP | Criação da política |
| 0.2 | 22/02/2024 | Nowcy | Atualização dos tópicos 3. 4.3 e 4.5 |
| 0.3 | 23/02/2024 | CSIP | Ajustes e validação |
| 0.4 | 09/07/2024 | CSIP | Revisão e ajustes |