DI-1TP-00134-B

DIRETRIZ DE SEGURANÇA PARA APLICAÇÕES

Órgão aprovador: TP/DFIN/GRE/SI	Data da aprovação: 09/11/2026
Órgão gestor: TP/DFIN/GRE/SI	Status: Ativo
Aprovado por: CLAUDIA DILLAN FRAGOSO	Código de Classificação:

SUMÁRIO

1. OBJETIVO 2
2. APLICAÇÃO E ABRANGÊNCIA 2
3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES 2
3.1. Documentos de referência 2
3.2. Documentos complementares 2
4. DEFINIÇÕES 2
5. AUTORIDADE E RESPONSABILIDADE 2
6. DESCRIÇÃO 3
7. REGISTROS 4
8. ANEXOS 5

A impressão deste documento torna a cópia não-controlada

1. OBJETIVO

Estabelecer orientações, regras e requisitos mínimos, definindo controles de segurança da informação e boas práticas aplicáveis ao ciclo de vida de aplicações desenvolvidas, contratadas ou adquiridas.

2. APLICAÇÃO E ABRANGÊNCIA

Aplica-se à força de trabalho e terceiros envolvidos no ciclo de vida das aplicações. Abrange as aplicações desenvolvidas por equipe própria ou terceirizada, bem como as aplicações contratadas ou adquiridas, destinadas ao uso interno ou externo.

3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

3.1. Documentos de referência

PL-0TP-00021 - Política de Segurança da Informação

DI-1TP-00059 - Diretriz de Segurança da Informação

DI-0TP-00036 - Diretriz de Classificação da Informação

DI-1TP-00120 - Diretriz para Criptografia, Anonimização e Pseudonimização de Dados

PP-3TP-00003 - Gerir Identidades e Acessos

PL-0TP-00019 - Código de Conduta Ética

DI-0TP-00029 - Diretriz de Proteção de Dados Pessoais e Privacidade

PE-1TP-00374 - Elaborar Aviso de Privacidade

PE-0TP-00488 - Requisitos de Segurança para Utilização de Computação em Nuvem

PP-2TP-00178 - Ciclo de Vida de Gestão de Acervo de Aplicações

PP-1TP-00176-0 - Gestão de Mudança

A impressão deste documento torna a cópia não-controlada

3.2. Documentos complementares

ABNT NBR ISO/IEC 27002:2022

BSIMM – Building Security In Maturity Model

OWASP Software Assurance Maturity Model (SAMM) version 2

OWASP Top 10 Web Application Security Risks

CWE Top 25 Most Dangerous Software Weaknesses

OWASP Top 10 Non-Human Identities Risks

OWASP API Security Top 10

NIST - Secure Software Development Framework (SSDF)

4. DEFINIÇÕES

Análise de segurança de imagens de contêiner: Varredura de imagens de contêiner para a identificação de vulnerabilidades, componentes inseguros e configurações inadequadas.

Ciclo de Vida de Desenvolvimento: abrange todas as fases desde a concepção até a entrega e manutenção de um produto de software. Inclui planejamento, levantamento de requisitos, codificação, testes, implantação e manutenção.

CID: Confidencialidade, Integridade e Disponibilidade

DAST: Análise dinâmica de aplicação (Dynamic Application Security Testing)

Esteira de Desenvolvimento: abrange os fluxos de atividades, ferramentas e processos, em parte automatizados, que apoiam as etapas do ciclo de vida do desenvolvimento de software.

LINDDUN: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, Non-compliance. Metodologia de modelagem de ameaças voltada à identificação de riscos à privacidade.

PASTA: Process for Attack Simulation and Threat Analysis. Metodologia de modelagem de ameaças baseada em análise de risco e simulação de ataques.

A impressão deste documento torna a cópia não-controlada

Pipeline de CI/CD (Continuous Integration / Continuous Delivery; Integração Contínua / Entrega Contínua): Conjunto de processos automatizados, integrados à esteira de desenvolvimento, que viabilizam, de forma contínua, a construção (*build*), integração, testes, validação, entrega e implantação (*deploy*) de aplicações.

SAST: Análise estática de código (Static Application Security Testing)

SCA: Análise de componentes de software (Software Composition Analysis)

Segredo: Informações sensíveis utilizadas por sistemas que possam habilitar acesso, configuração, ativação ou operação, cuja confidencialidade deve ser mantida e cujo acesso, cópia ou reprodução devem ser controlados; incluem, sem limitação: senhas, tokens, chaves (de acesso, de licença ou criptográficas), certificados digitais e demais credenciais técnicas, incluindo connection strings.

STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege. Metodologia de modelagem de ameaças baseada em categorias clássicas de ataques.

5. AUTORIDADE E RESPONSABILIDADE

Tabela 1 - Atribuições

Quem	O quê
Equipe de Desenvolvimento	∗Responsável por compreender e aplicar esta diretriz e os padrões técnicos complementares no trabalho diário, projetar sistemas que incorporem princípios de segurança desde a concepção (Security by Design) e integrar ferramentas e processos de segurança automatizados à esteira de desenvolvimento.
Equipe de Segurança da Informação (SI)	∗Responsável por manter esta diretriz, prestar orientações, realizar testes de segurança e aprovar exceções. Contato: si@transpetro.com.br.
Gestores de Produto/Projeto	∗ Responsáveis por alocar tempo e recursos para a implementação dos requisitos de segurança.

A impressão deste documento torna a cópia não-controlada

6. DESCRIÇÃO

6.1. Disposições gerais

Na fase de planejamento do desenvolvimento, os requisitos de segurança devem ser definidos, tendo como base os requisitos da aplicação, garantindo a integração de requisitos de segurança ao desenvolvimento desde o início, reduzindo riscos e retrabalho nas etapas posteriores.

Exemplos de requisitos de Segurança da Aplicação:

- *Os dados pessoais do processo de cadastro devem ser transferidos e armazenados de forma segura;*
- *As credenciais do usuário devem ser armazenadas de modo a impedir acesso não autorizado, mesmo em caso de vazamento;*
- *O sistema deve mitigar tentativas de adivinhação de senha e automação de abuso no processo de autenticação.*

Critérios de aceitação:

- Existência de lista de requisitos de segurança de alto nível por funcionalidade/fluxo com justificativa CID;
- Registro de casos de mau uso com objetivos de proteção associados;
- Rastreabilidade dos requisitos nos artefatos do projeto e revisão quando houver alterações relevantes nos requisitos funcionais.

Os requisitos de segurança da informação para o software devem ser estabelecidos com base em uma abordagem orientada a riscos. Quando aplicável às características, à arquitetura e à criticidade do projeto, essa abordagem deve ser apoiada pela utilização de metodologia formal de modelagem de ameaças, como STRIDE, PASTA, LINDDUN ou metodologia equivalente. A não utilização de metodologia formal deve ser justificada e registrada, sem prejuízo da identificação, da definição e do registro dos requisitos de segurança aplicáveis.Esses requisitos devem ser formalmente documentados, comunicados às partes interessadas e revisados periodicamente, acompanhando a evolução tecnológica, alterações nos processos organizacionais e modelos de negócio, bem como a identificação de novas ameaças, vulnerabilidades e obrigações regulatórias.

Para aplicações web, o OWASP *Application Security Verification Standard (ASVS)* deve ser considerado como um catálogo padronizado de requisitos de segurança organizados em várias categorias e critérios para a verificação da segurança de aplicações.

Para atender aos requisitos de segurança definidos na fase de planejamento do software, os controles devem ser implementados preferencialmente por meio da

A impressão deste documento torna a cópia não-controlada

reutilização de componentes de software previamente validados e confiáveis.

Quando a reutilização não for viável, recomenda-se que os controles sejam desenvolvidos seguindo boas práticas e, sempre que aplicável, estruturados como componentes de software registrados em repositório de controle de versão corporativo, assegurando sua manutenção, rastreabilidade e reutilização futura. A verificação dos requisitos de segurança da informação deve ocorrer ao longo de todo o ciclo de desenvolvimento, garantindo que esses requisitos sejam atualizados, documentados e implementados sempre que houver alterações.

6.2 Requisitos de segurança da informação

6.2.1. Inventário

Quaisquer aplicações em desenvolvimento devem ser devidamente cadastradas na ferramenta corporativa de inventário e gestão de ativos pelo seu respectivo líder técnico, conforme o padrão vigente sobre ciclo de vida e gestão de acervo de aplicações.

6.2.2. Requisitos de autenticação de autorização de acessos

Todos os acessos e autorizações ao sistema devem, desde a concepção, seguir os princípios do menor privilégio, da necessidade de conhecer e da necessidade de uso.

Todo o acesso deve ser autenticado por contas individuais e quaisquer exceções devem ser justificadas e registradas. Cada conta deve estar vinculada a um único usuário e as exceções deverão ser justificadas e registradas.

O histórico de autenticação do sistema deve registrar, no mínimo, a conta utilizada, a data e a hora do acesso, devendo ser retido por um período previamente definido, em conformidade com os requisitos não funcionais do sistema, as normas da Companhia e a legislação aplicável.

Credenciais locais padrão devem ser desabilitadas. Se as desabilitar não for possível, a senha padrão deve ser substituída por uma de complexidade alta, conforme melhores práticas e normas estabelecidas da Companhia.

A autenticação de contas de usuários internos ou externos à Companhia, deve utilizar soluções corporativas padronizadas de gestão de identidade e acesso, e, preferencialmente, através do sistema de *Single Sign On* (SSO) da Companhia.

Deve-se evitar o uso de bases locais da aplicação para armazenamento de credenciais. Quando necessário, seguir as melhores práticas referentes à complexidade e à criptografia de senhas.

A impressão deste documento torna a cópia não-controlada

Quando for necessário utilizar mecanismos locais de autenticação, devem ser observados os requisitos corporativos padronizados para credenciais de usuários, especialmente no que se refere às senhas de acesso.

Sempre que tecnicamente viável, segredos devem ser armazenados e disponibilizados por solução corporativa de gestão de segredos (cofre de senhas), incluindo aqueles consumidos por pipelines, scripts de build, aplicações, serviços, automações e variáveis de ambiente injetadas em tempo de execução.

As credenciais de contas com acessos privilegiados utilizadas por um sistema para acessar qualquer ativo de TIC (como aplicações, servidores, serviços, bancos de dados etc.) devem ser obrigatoriamente armazenadas em solução corporativa de cofre de senhas, garantindo criptografia e controle de acesso.

A autenticação de contas de usuários individuais deve possibilitar a exigência de múltiplo fator de autenticação (MFA), considerando pelo menos dois fatores, sempre que o acesso ao sistema ocorrer de forma lógica ou física fora do ambiente da rede corporativa integrada.

Sessões de contas de usuários individuais autenticados em sistemas web devem expirar automaticamente após um período entre 15 e 30 minutos de inatividade do usuário, ou de acordo com os requisitos não funcionais do sistema. Referência da OWASP sobre gerenciamento de sessão para aplicações web: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html.

As contas utilizadas pelo sistema para acessar outros recursos, como bancos de dados, armazenamento e outros, devem ser de uso exclusivo do próprio sistema e seguir o princípio de menor privilégio.

As contas de usuários individuais (que não sejam contas aquelas utilizadas pelo sistema) não devem, em regra, possuir acesso direto para consulta ou escrita no banco de dados e exceções devem ser justificadas e registradas (por exemplo, administradores do banco de dados). Qualquer necessidade de acesso ao banco de dados do ambiente de produção seja para leitura ou escrita, deve ser previamente aprovada pelo gestor responsável pela aplicação.

A aplicação idealmente deve oferecer mecanismos para possibilitar a concessão de privilégios ou perfis de acesso a contas de usuários mediante a aprovação de gestor hierárquico do solicitante. O atendimento a esta orientação poderá ocorrer alternativamente por meio de uma API segura para concessão e revogação de acessos, permitindo integração com sistemas corporativos de gestão de identidade (IAM), garantindo automação e rastreabilidade.

A aplicação idealmente deverá oferecer mecanismos para possibilitar a revogação imediata de privilégios ou perfis de acesso associados às contas de

A impressão deste documento torna a cópia não-controlada

usuários individuais quando a pessoa vinculada à conta for desligada da organização ou mudar de área na estrutura organizacional. O atendimento a esta orientação deve ocorrer de forma automática por meio de uma API segura, permitindo integração com sistemas corporativos de gestão de identidade (IAM).

Tokens utilizados por APIs devem possuir tempo de expiração definido, prever expiração por inatividade e exigir a emissão de novo token por autenticação ou processo autorizado equivalente quando expirarem, devendo também ser possível a sua revogação imediata.

O histórico de autorizações para concessão de privilégios e perfis de acesso às contas de usuários deve ser registrado, indicando, no mínimo, a conta que recebeu o privilégio, o responsável pela autorização ou revogação, a data e a hora do evento. Esse histórico deve ser retido por um período predefinido, conforme requisitos não funcionais do sistema e normas de conformidade da Companhia.

O histórico de concessão e revogação de privilégios e perfis de acesso às contas de usuários deve ser registrado, indicando no mínimo a conta que recebeu ou teve o privilégio revogado, o responsável pela autorização ou revogação, e a data e a hora do evento. Esse histórico deve ser retido por um período predefinido, conforme requisitos não funcionais do sistema e normas de conformidade da Companhia.

Os acessos temporários a aplicações, dados ou ambientes tecnológicos para fins de auditoria ou avaliação técnica devem ser solicitados e autorizados por meio do processo de solicitação de acesso existente em ferramenta de registro e controle de mudanças (ex.: sistema de ITSM). O pedido deve identificar a auditoria, o escopo, as permissões necessárias e o período de validade, priorizando-se o acesso somente para leitura. A concessão e a revogação do acesso devem ser registradas.

Quando o teste puder alterar configurações, degradar o desempenho, interromper serviços ou afetar o ambiente tecnológico, também deve ser observado o processo corporativo de Gestão de Mudanças.

6.2.3. Requisitos para o registro de histórico de eventos

O histórico de eventos (log ou trilha de auditoria) deve identificar minimamente a conta do usuário, o evento realizado e a data e hora do evento, garantindo que o horário do sistema esteja correto e configurado para o fuso horário oficial de Brasília (GMT-3). Esse histórico deve ser armazenado de forma segura, para garantir sua integridade e mantido por tempo predefinido conforme requisitos não funcionais do sistema e normas de conformidade da Companhia.

6.2.4. Requisitos de segurança, privacidade e proteção de dados

A impressão deste documento torna a cópia não-controlada

Os relatórios gerados pelo sistema e que sejam exportáveis devem estar visualmente ou textualmente rotulados conforme o grau de sigilo das informações neles contidas.

Os relatórios gerados pelo sistema e utilizados como subsídio para a execução de controles de negócio, especialmente no âmbito da certificação pela Lei Sarbanes-Oxley dos Estados Unidos (SOx), devem ser verificados e validados por gestor responsável pelas informações de forma a demonstrar a integridade e precisão dos dados, incluindo a especificação e o registro dos filtros aplicados, bem como a descrição detalhada do processo de geração, incluindo o passo a passo adotado, de forma a garantir rastreabilidade e integridade das informações.

Dados classificados como confidenciais, devem ser armazenados utilizando criptografia robusta, empregando algoritmos e padrões reconhecidos, e as chaves criptográficas devem ser gerenciadas de forma segura, nunca armazenadas junto aos dados. As exceções devem ser justificadas e controles compensatórios devem ser estabelecidos.

Dados classificados como confidenciais, incluindo credenciais de acesso, devem ser transmitidos utilizando protocolos criptográficos, inclusive dentro da rede interna corporativa, independentemente de a outra ponta ser um usuário final ou um ativo de TIC. As exceções devem ser justificadas e controles compensatórios devem ser estabelecidos.

O sistema deve armazenar apenas as informações indispensáveis para seu funcionamento e não deve exibir dados desnecessários ao usuário. Dados pessoais e informações sujeitas a requisitos de confidencialidade não devem ser exibidos sem a adoção prévia de mecanismos de mascaramento dinâmico de dados.

O sistema não deve obter informações desnecessárias nas transações com outros sistemas, nem disponibilizar em suas interfaces informações que não sejam indispensáveis ao correto funcionamento.

O tratamento de dados pessoais nos sistemas deve ser legítimo, em conformidade com os requisitos e as normas internas da Companhia e com a legislação aplicável.

A coleta de dados pessoais em formulários de cadastro do sistema, o uso de cookies de rastreamento e as requisições de consentimento do usuário, quando necessários, devem incluir aviso de privacidade claro e acessível, informando a finalidade da coleta, a base legal, direitos do titular e a política de retenção e descarte.

A impressão deste documento torna a cópia não-controlada

Os dados de entrada provenientes de fontes externas ao sistema, seja essa fonte um usuário final, outro sistema ou repositórios externos de informação, devem ser verificados para garantir que são válidos e coerentes com o tipo de dado esperado.

A validação de dados deve ocorrer no lado da aplicação. Como um exemplo, em campos de texto, deve-se garantir que apenas os caracteres permitidos sejam processados, que um tamanho máximo de caracteres ou bytes seja definido conforme a necessidade do campo. Para outros tipos de campos, devem ser aplicadas regras específicas de validação, como formato, intervalo de valores e limites de tamanho, conforme a finalidade do dado.

6.2.5. Requisitos de tratamento de erros

As mensagens de erro da aplicação ou sistema mostrados na interface de usuário final devem receber tratamento apropriado para que informações internas da aplicação não sejam disponibilizadas sem necessidade, como por exemplo, versão do sistema operacional, tipo do banco de dados, nome de tabelas e campos, formato de campos, trechos de código etc.

6.3 Requisitos de segurança cibernética

Os sistemas web devem estar protegidos por Web Application Firewall (WAF), com logs obrigatoriamente encaminhados para o SIEM, quando se enquadrarem em, pelo menos, uma das seguintes categorias:

- Aplicações acessíveis através da Internet, direta ou indiretamente. Nos casos de exposição indireta (ex.: via Proxy Reverso, Gateway de Aplicação, *Load Balancer*), o WAF deve ser aplicado no ponto de exposição.
- O WAF deve implementar mecanismos de proteção contra diferentes tipos de ataques cibernéticos a aplicações web, especialmente aqueles listados no OWASP Top 10. No mínimo, deve aplicar as regras do OWASP *Core Rule Set* (OWASP CRS).

As aplicações devem ser submetidas às análises de segurança (SAST, SCA, análise de segurança de imagens de contêiner ou DAST) quando se enquadrarem em, pelo menos, uma das seguintes categorias:

- Aplicações acessíveis através da Internet, direta ou indiretamente.
- Manipularem ou processarem informações confidenciais ou secretas;
- Estiverem no escopo da Lei Sarbanes-Oxley dos EUA (SOx);
- Tratarem e processarem dados pessoais sensíveis, conforme definido pela Lei Geral de Proteção de Dados (LGPD).

Quanto a aplicabilidade das análises de segurança:

A impressão deste documento torna a cópia não-controlada

- A análise estática de código (SAST) e a análise de composição de software (SCA) são aplicáveis quando o código-fonte da aplicação estiver disponível;
- A análise de segurança de imagens de contêiner deverá sempre ser aplicada quando a aplicação utilizar contêineres;
- A análise dinâmica de aplicação (DAST) será aplicada para aplicações web, serviços web, APIs e *endpoint*s http(s) expostos à Internet.

No caso de uso de ferramentas ou bibliotecas externas como, por exemplo, as de terceiros e as *open source*, deve-se garantir que elas sejam inventariadas em repositório de controle de versão corporativo e sempre atualizadas para a última versão ou a recomendada pelo fornecedor/fabricante.

As vulnerabilidades classificadas como críticas, altas e médias, identificadas por meio das análises de segurança aplicáveis, tais como SAST, SCA, análise de segurança de imagens de contêiner e DAST, devem ser corrigidas obrigatoriamente antes de a aplicação entrar em produção ou imediatamente caso descobertas após a entrada em produção. Em casos excepcionais, a correção deve ocorrer tempestivamente, mediante negociação com a área de Segurança da Informação, sendo a SI responsável pelo aval final.

Os *pipelines* de CI/CD das aplicações devem implantar portões de segurança (*security gates*) que realizem bloqueio automático da construção (*build*) e da implantação (*deploy*) de aplicações que apresentem falhas de segurança classificadas como críticas, altas e médias, identificadas por meio das análises de segurança aplicáveis, conforme priorização de aplicações definida pela SI em conjunto com a TI.

Em condições de emergência ou de exceção, os portões de segurança podem ser desativados se, e somente se, houver negociação com a SI, conduzida pela SI e com seu aval final.

Sempre que operacionalmente viável, a conexão ao banco de dados do ambiente de produção deve ser restrita exclusivamente aos endereços dos servidores de aplicação que necessitam acessar os dados. Essa restrição deve ser implementada por meio de Listas de Controle de Acesso (ACL), regras de firewall ou configuração de grupos de segurança na infraestrutura, seja *on-premises* ou em nuvem.

É proibido permitir acesso irrestrito ou genérico ao banco de dados, mesmo dentro da rede corporativa.

Deve-se verificar se os requisitos funcionais de segurança e de qualidade de código do sistema foram atendidos antes da implantação. Essa verificação deve ocorrer por meio de testes funcionais automatizados e análise estática do código.

A impressão deste documento torna a cópia não-controlada

Sempre que possível, utilizar ferramenta corporativa para análise de qualidade de código, garantindo conformidade com padrões internos de desenvolvimento seguro, detecção de vulnerabilidades e más práticas de codificação, e a geração de relatórios para auditoria e rastreabilidade.

Além das aplicações tradicionais e do tipo web, os requisitos desta seção devem ser aplicados, sempre que tecnicamente viável, aos seguintes tipos de solução: Aplicativos móveis (Android, iOS e outros); Produtos de prateleira adquiridos pela organização; Aplicações e serviços em nuvem (SaaS, PaaS, IaaS); Produtos e aplicações customizadas desenvolvidos internamente ou por terceiros; Aplicações geradas por plataformas *low-code* ou *no-code*; Aplicações, transações e sistemas da plataforma SAP ou equivalentes. Quando houver limitações técnicas ou contratuais que impeçam a aplicação integral das diretrizes, deve-se adotar medidas compensatórias aprovadas pela área de Segurança da Informação (SI).

6.3.1 Requisitos para software desenvolvido externamente

Devem ser estabelecidos acordos de confidencialidade com todo e qualquer time terceirizado de desenvolvimento que venha a ter acesso a: dados sensíveis ou confidenciais, código-fonte da aplicação, arquitetura ou outras informações técnicas críticas.

O desenvolvimento e a manutenção de software devem se realizar em conformidade às normas, aos padrões e às diretrizes de segurança da informação da Transpetro, garantindo aderência às políticas corporativas, à legislação e às regulamentações aplicáveis, de forma contínua, durante todo o ciclo de vida do software.

Antes da liberação de recursos de infraestrutura de produção, o time de desenvolvimento terceirizado de software deve apresentar evidências técnicas registradas que demonstrem: o atendimento aos controles aplicáveis desta Diretriz, incluindo os controles relacionados à segurança da informação e, quando aplicável, os controles de privacidade e proteção de dados; a realização das análises de segurança previstas sobre os artefatos entregues, tais como: SAST, SCA, análise de segurança de imagens de contêiner e DAST; o tratamento de quaisquer componentes não autorizados, inseguros ou potencialmente maliciosos identificados nessas análises; e a correção das vulnerabilidades classificadas como críticas, altas e médias identificadas.

Todo o código-fonte e demais artefatos relacionados, produzidos no decorrer do desenvolvimento de aplicações ou sistemas por time terceirizado devem ser mantidos em repositório de controle de versão corporativo, com controle de acesso baseado em identidade seguindo o principio do privilégio mínimo, controle de versão com rastreabilidade de alterações e registro de auditoria das operações críticas.

A impressão deste documento torna a cópia não-controlada

O time de desenvolvimento terceirizado deve disponibilizar, por meio do repositório de controle de versão corporativo, arquivo SBOM (*Software Bill of Materials*) atualizado, contendo todos os componentes, bibliotecas e dependências utilizadas, as versões exatas de cada item e a origem e fornecedor, indicando se é *open source* ou proprietário. O SBOM deve ser atualizado a cada release ou sempre que houver inclusão ou atualização de dependências.

Todas as aplicações ou sistemas desenvolvidos por equipes terceirizadas devem passar por análises de segurança antes da implantação, sendo estas: análise estática de segurança (SAST), quando houver código-fonte disponível; análise de composição de software (SCA), sempre que a aplicação utilizar componentes externos; análise dinâmica de segurança (DAST), quando tecnicamente viável; e análise de segurança de imagens de contêiner, quando aplicável. Todas essas análises devem seguir os mesmos critérios aplicados às aplicações desenvolvidas internamente.

Os resultados dessas análises devem ser compartilhados com os desenvolvedores responsáveis pelo software em questão para que as vulnerabilidades identificadas sejam corrigidas.
O fornecedor deve corrigir as vulnerabilidades classificadas como críticas, altas e médias, identificadas por meio das análises de segurança aplicáveis, tais como SAST, SCA, análise de segurança de imagens de contêiner e DAST, antes da entrada da aplicação em ambiente de produção ou imediatamente quando descobertas após sua entrada nesse ambiente.

Os casos de fornecedores que não consigam corrigir as vulnerabilidades apontadas pelas análises de segurança devem ser: registrados formalmente pela área de segurança para fins de auditoria, considerados como critério negativo em futuras renegociações contratuais ou novas contratações.

Devem ser observados acordos de licenciamento, propriedade dos códigos e direitos de propriedade intelectual, incluindo aqueles relacionados a componentes, bibliotecas, dependências de software, conteúdos ou demais artefatos de terceiros utilizados na solução, de forma clara e documentada, garantindo alinhamento com os interesses da Transpetro quanto à aquisição da titularidade completa do sistema (código-fonte, documentação e direitos) ou direito de uso conforme instrumento aplicável.

No caso de aquisição da titularidade do sistema pela Transpetro, devem ser previstas condições para a transferência do conhecimento do sistema, incluindo a documentação completa, em especial, o código-fonte comentado, memorial descritivo, especificações funcionais internas, diagramas, fluxogramas e outros dados técnicos necessários à absorção da tecnologia.

A impressão deste documento torna a cópia não-controlada

A empresa contratada deve adotar frameworks de desenvolvimento seguro reconhecidos internacionalmente, conforme recomendações da OWASP ou do NIST (ex: OWASP SAMM ou NIST SSDF) como forma de comprovar o seu nível de maturidade em segurança de aplicações. Caso a empresa não possua documentação comprobatória, a Transpetro poderá exigir, a qualquer tempo (inclusive de forma periódica) durante a vigência do contrato, resultado das análises estática de segurança de aplicações (SAST), da análise de composição de software (SCA), da análise dinâmica de segurança (DAST) no caso de aplicações Web, e da análise de segurança de imagens de contêiner (se for utilizado).

Os instrumentos contratuais aplicáveis devem exigir a adoção de práticas seguras de projeto, arquitetura, codificação, testes e aceite da solução, em conformidade com esta Diretriz e com os requisitos de segurança definidos para o projeto.

O time de desenvolvimento terceirizado deve adotar metodologia formal de modelagem de ameaças quando sua utilização for aplicável às características, à arquitetura e à criticidade do projeto. A não utilização de metodologia formal deve ser justificada e registrada, sem prejuízo da identificação, da definição e do registro dos requisitos de segurança aplicáveis ao projeto.

Quando realizada, a modelagem de ameaças deve orientar a identificação de ameaças, cenários de ataque relevantes, controles de segurança requeridos, riscos identificados e decisões de tratamento. Seus resultados devem ser considerados na definição e no atendimento dos requisitos de segurança e mantidos como artefatos no repositório de controle de versão corporativo.

Os ambientes, ferramentas e processos utilizados pelo fornecedor para desenvolvimento, teste, compilação, armazenamento e entrega dos artefatos devem observar requisitos de segurança desta Diretriz, incluindo segregação entre ambientes, controle de acesso, rastreabilidade de alterações, proteção dos artefatos, restrição ao uso de dados sensíveis e prevenção de acesso não autorizado ao ambiente de produção.

Antes da implantação, as soluções, aplicações ou sistemas desenvolvidos por equipe terceirizada devem passar por teste de aceitação cabíveis, com evidências registradas quanto ao atendimento dos requisitos funcionais, não funcionais, de segurança, qualidade e precisão definidos para o projeto.

Devem ser previstas, no instrumento contratual correspondente, disposições para a custódia do código-fonte da solução, aplicação ou sistema contratado, de forma a possibilitar sua continuidade, manutenção ou sustentação em caso de falha, descontinuidade ou indisponibilidade da empresa contratada.

A impressão deste documento torna a cópia não-controlada

Deve ser previsto, no instrumento contratual correspondente, o direito da Transpetro de auditar ou solicitar evidências dos processos, controles e práticas de desenvolvimento seguro adotados pelo fornecedor, a fim de verificar a conformidade com os requisitos desta Diretriz.

Os requisitos descritos nessa seção devem estar previstos no instrumento contratual correspondente, conforme descrito no **Anexo B - Requisitos para Contratação de Software**.

6.3.2. Requisitos sobre o ciclo de vida de aquisição, desenvolvimento e manutenção de aplicações

6.3.2.1. Identificar, especificar, aprovar e manter atualizados todos os requisitos do sistema (incluindo Segurança da Informação), com rastreabilidade aos cenários de uso.

Na contratação ou aquisição de aplicações, os requisitos de segurança da informação aplicáveis devem ser definidos antes da seleção da solução e considerados durante sua avaliação e contratação.

Esses requisitos devem ser definidos com base nas características da aplicação, nas informações tratadas e nos riscos associados, utilizando como apoio o **Anexo B - Requisitos para Contratação de Software**.

6.3.2.2. Para soluções SaaS, é obrigatório seguir os requisitos de Segurança da Informação definidos no padrão PE-0TP-00488 - Requisitos de Segurança para Utilização de Computação em Nuvem e anexo contratual, garantindo conformidade as políticas corporativas e normas aplicáveis. É terminantemente proibido contratar ou manter serviços SaaS que não atendam aos controles exigidos, incluindo, mas não se limitando a: proteção de dados sensíveis conforme legislação vigente, gestão de identidade e acesso com autenticação forte, criptografia em trânsito e em repouso, monitoramento e resposta a incidentes, conformidade com padrões reconhecidos (ex: ISO 27001 e SOC 2). A responsabilidade pela verificação de conformidade é contínua, podendo ser auditada a qualquer momento durante a vigência do contrato.

6.3.2.3. Registrar na documentação de requisitos qualquer controle de segurança não implementado, com justificativa, e encaminhar para parecer da área de Segurança da Informação.

6.3.2.4. Manter todo código-fonte, scripts, configurações e demais artefatos de aquisição, desenvolvimento e manutenção obrigatoriamente em repositório de controle de versão corporativo integrado a um *pipeline* de CI/CD, com controle de acesso baseado em identidade e seguindo o principio do privilégio mínimo, garantindo rastreabilidade, histórico de alterações, auditoria e controles através de portões de segurança, sendo vedado o armazenamento em repositórios não

A impressão deste documento torna a cópia não-controlada

corporativos ou ambientes locais não controlados. As versões aprovadas para implantação em produção devem ser identificadas, documentadas e versionadas como linhas de base, mantendo-se o registro da linha de base anteriormente implantada para fins de rastreabilidade, comparação e reversão.

6.3.2.5. Verificar e testar previamente todo novo desenvolvimento ou mudança (corretiva/evolutiva) conforme os requisitos especificados, incluindo os de segurança.

6.3.2.6. Qualquer criação ou alteração de requisitos deve ser validada e homologada pelo gestor responsável pela aplicação.

6.3.2.7. Software de prateleira ou aplicações adquiridas devem ser homologadas pelas áreas responsáveis, com o aval da área de Segurança da Informação e, quando aplicável, também da área de Arquitetura Empresarial. A homologação deve verificar o atendimento aos requisitos de segurança definidos durante a avaliação e a contratação da solução.

6.3.2.8. Verificação e testes devem ser realizados por pessoa diferente da que desenvolveu o código.

6.3.2.9. Realizar testes, incluindo os de segurança, em ambiente não produtivo e o mais próximo possível do ambiente de produção, garantindo a representatividade e a confiabilidade dos resultados. O responsável pela aplicação deve avaliar e disponibilizar ambiente e dados de teste de forma segura, utilizando dados de teste anonimizados ou pseudonimizados, preferencialmente efetuando a minimização de dados por meio do fornecimento de um subconjunto dos dados ou, quando suficiente, apenas do esquema lógico do banco de dados, evitando a exposição de informações sensíveis. Eventuais exceções devem ser submetidas à aprovação formal da SI.

6.3.2.10. Segregar o ambiente de produção (aplicação e dados) dos ambientes de teste, desenvolvimento, homologação, treinamento etc.

6.3.2.11. Ambientes que não sejam de produção não devem ser expostos diretamente na Internet.

6.3.2.12. Compiladores, editores e demais ferramentas/utensílios de desenvolvimento não devem acessar produção; exceções somente com autorização do gestor.

6.3.2.13. Não copiar dados confidenciais de produção para outros ambientes sem anonimização ou pseudonimização, ou controles de segurança equivalentes aos de produção, observando a minimização de dados.

A impressão deste documento torna a cópia não-controlada

6.3.2.14. Implementar segregação de funções para impedir que uma única pessoa desenvolva, teste, homologue e implante em produção sem a participação de pelo menos outra pessoa.

6.3.2.15. Seguir os padrões corporativos de retenção, recuperação e redundância de dados em lógicos e físicos.

6.3.2.16. Manter plano de recuperação de desastres (físicos e cibernéticos) alinhado à análise de impacto no negócio.

6.3.2.17. A lista de verificação proposta no **Anexo A - Lista de Verificação de Controles** pode ser usada como um guia, mas não representa o conjunto exaustivo de controles considerados obrigatórios e deve ser utilizada como parte dos instrumentos de verificação de aderência a controles mínimos previstos nessa diretriz.

6.3.3. Diretrizes para segurança de APIs REST

Para o desenvolvimento seguro de APIs REST, é obrigatório seguir as diretrizes de segurança definidas pela OWASP. Resumidamente, as orientações são:

1. Mantenha tudo simples.
2. Sempre use HTTPS.
3. Use hash de senha com salt.
4. Nunca exponha informações nas URLs.
5. Considere utilizar OAuth.
6. Considere adicionar timestamp na solicitação.
7. Valide todos os parâmetros de entrada.

Os detalhes são discutidos no link de referência, que deve ser lido e seguido com atenção:
https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html
Para avaliar e testar APIs REST, a referência OWASP é:
https://cheatsheetseries.owasp.org/cheatsheets/REST_Assessment_Cheat_Sheet.html.

7. REGISTROS

Não Aplicável

8. ANEXOS

Anexo A – Lista de Verificação de Controles

Anexo B – Requisitos para Contratação de Software

A impressão deste documento torna a cópia não-controlada

RESUMO DE REVISÕES	
REV.	**DESCRIÇÃO E/OU ITENS ATINGIDOS**
0	Emissão inicial
A	Revisão textual; Inclusão do item 6.3.2.11. Revisão do item 6.3.1; Alteração do item 6.3.2.7. **Antes:** Aplicações adquiridas devem ser homologadas pelas áreas responsáveis e, quando aplicável, pelas áreas de arquitetura tecnológica e de segurança da informação. **Depois:** 6.3.2.7. Software de prateleira ou aplicações adquiridas devem ser homologadas pelas áreas responsáveis, com o aval da área de Segurança da Informação e, quando aplicável, pela área de Arquitetura Empresarial. Alteração do item 6.3.2.4. **antes:** Manter todos os artefatos de aquisição, desenvolvimento e manutenção em repositório de gerenciamento de configuração. Identificar e rotular linhas de base antes de implantar mudanças em produção. **Por**: Manter todo código-fonte, scripts, configurações e demais artefatos de aquisição, desenvolvimento e manutenção obrigatoriamente em repositório de controle de versão corporativo integrado a um pipeline de CI/CD, com controle de acesso baseado em identidade e seguindo o princípio do privilégio mínimo, garantindo rastreabilidade, histórico de alterações, auditoria e controles através de portões de segurança, sendo vedado o armazenamento em repositórios não corporativos ou ambientes locais não controlados. As versões aprovadas para implantação em produção devem ser identificadas, documentadas e versionadas como linhas de base, mantendo-se o registro da linha de base anteriormente implantada para fins de rastreabilidade, comparação e reversão;
B	Revisão textual; Revisão nos Anexos A e B. Alteração do item 1: **Antes**: Estabelecer orientações, regras, e requisitos mínimos, definindo controles de segurança da informação e melhores práticas para a melhoria da segurança em todo o ciclo de desenvolvimento de software. **Depois:** Estabelecer orientações, regras e requisitos mínimos, definindo controles de segurança da informação e boas práticas aplicáveis ao ciclo de vida de aplicações desenvolvidas, contratadas ou adquiridas. Alteração item 2:**Antes**: Aplica-se a toda a força de trabalho de empregados próprios e terceiros envolvidos no ciclo de vida de desenvolvimento de software. Aplica-se a todo o software desenvolvido por equipe própria ou terceirizada, seja para uso interno ou externo. **Depois:** Aplica-se à força de trabalho e terceiros envolvidos no ciclo de vida das aplicações. Abrange as aplicações desenvolvidas por equipe própria ou terceirizada, bem como as aplicações contratadas ou adquiridas, destinadas ao uso interno ou externo. Alteração do item 6.1: **Antes:** Os requisitos de segurança da informação para o software devem ser estabelecidos com base em uma abordagem orientada a riscos, apoiada pela utilização de metodologias formais de modelagem de ameaças, como STRIDE, PASTA e LINDDUN, ou metodologias similares, considerando ameaças que possam comprometer a confidencialidade, integridade, disponibilidade e autenticidade. **Depois:** Os requisitos de segurança da informação para o software devem ser estabelecidos com base em uma abordagem orientada a riscos. Quando aplicável às características, à arquitetura e à criticidade do projeto, essa abordagem deve ser apoiada pela utilização de metodologia formal de modelagem de ameaças, como STRIDE, PASTA, LINDDUN ou metodologia equivalente. A não utilização de metodologia formal deve ser justificada e registrada, sem prejuízo da identificação, da definição e do registro dos requisitos de segurança aplicáveis. Inclusão de texto no item 6.2.2: Os acessos temporários a aplicações, dados ou ambientes tecnológicos para fins de auditoria ou avaliação técnica devem ser solicitados e autorizados por meio do processo de solicitação de acesso existente na ferramenta de registro e controle de mudanças (ex.: sistema de ITSM). O pedido

A impressão deste documento torna a cópia não-controlada

	deve identificar a auditoria, o escopo, as permissões necessárias e o período de validade, priorizando-se o acesso somente para leitura. A concessão e a revogação do acesso devem ser registradas. Quando o teste puder alterar configurações, degradar o desempenho, interromper serviços ou afetar o ambiente tecnológico, também deve ser observado o processo corporativo de Gestão de Mudanças. Alteração do item 6.3.1: **Antes:** O time de desenvolvimento terceirizado deve adotar, para cada projeto, uma metodologia formal de modelagem de ameaças, tais como STRIDE, PASTA, LINDDUN ou equivalente. A metodologia formal de modelagem de ameaças adotada deve orientar a identificação de ameaças, cenários de ataque relevantes, controles de segurança requeridos, riscos identificados e decisões de tratamento, devendo seus resultados ser considerados na atividade de definição de requisitos de segurança e no atendimento destes requisitos. Os resultados obtidos a partir de modelagem de ameaças devem ser registrados como artefatos no repositório de controle de versão corporativo. **Depois:** O time de desenvolvimento terceirizado deve adotar metodologia formal de modelagem de ameaças quando sua utilização for aplicável às características, à arquitetura e à criticidade do projeto. A não utilização de metodologia formal deve ser justificada e registrada, sem prejuízo da identificação, da definição e do registro dos requisitos de segurança aplicáveis ao projeto. Quando realizada, a modelagem de ameaças deve orientar a identificação de ameaças, cenários de ataque relevantes, controles de segurança requeridos, riscos identificados e decisões de tratamento. Seus resultados devem ser considerados na definição e no atendimento dos requisitos de segurança e mantidos como artefatos no repositório de controle de versão corporativo. Inclusão no item 6.3.2.1.: Na contratação ou aquisição de aplicações, os requisitos de segurança da informação aplicáveis devem ser definidos antes da seleção da solução e considerados durante sua avaliação e contratação. Esses requisitos devem ser definidos com base nas características da aplicação, nas informações tratadas e nos riscos associados, utilizando como apoio o Anexo B - Requisitos para Contratação de Software. Inclusão no item 6.3.2.7.: A homologação deve verificar o atendimento aos requisitos de segurança definidos durante a avaliação e a contratação da solução.

A impressão deste documento torna a cópia não-controlada