POLÍTICA DE DESENVOLVIMENTO DE SOFTWARE TERCEIRIZADO
Versão 1

Última atualização: 27/03/2025
Classificação: Público

Acesso ao código-fonte

O controle de acesso ao código-fonte visa a salvaguarda da propriedade intelectual da organização e a integridade das informações nele contidas.

O acesso ao código-fonte de quaisquer sistemas corporativos desenvolvidos por terceiros em favor exclusivo da CATTALINI, é limitado somente aos desenvolvedores indicados pela Coordenação de Sistemas, divididos no escopo de atuação de cada tipo de força de trabalho que possua atividades correlatas ao desenvolvimento de sistemas, conforme abaixo:

Sistemas geridos por força de trabalho terceirizada:

As atividades de desenvolvimento de softwares realizadas por fornecedores seguem rigorosamente o disposto na presente política, considerando ainda boas práticas para desenvolvimento seguro de software.

Os contratos de desenvolvimento terceirizado estabelecem regulamentação clara acerca da propriedade intelectual produzida e conformidade legislatória de privacidade, os prazos para fornecimento do código-fonte em sua integralidade quando findado o acordo e o requisito de não retenção de quaisquer informações da CATTALINI após o encerramento do acordo, bem como, prover meios para que a CATTALINI realize auditorias de conformidade dessa cláusula.

A PDS deve constar como anexo nos contratos de fornecedores de desenvolvimento de software que operem processos que manipulem informação.

Sistemas geridos pelas equipes internas:

Os sistemas geridos pelas equipes internas da CATTALINI seguem os padrões de acesso ao código-fonte onde para quaisquer liberações de acesso, o princípio do "privilégio mínimo" requer que os privilégios de acesso ao código-fonte sejam concedidos de forma a permitir somente o acesso às partes do código necessárias para a execução de tarefas específicas.

Em todo o ambiente de desenvolvimento, existem métodos de autenticação seguros para garantir a identidade dos usuários que acessam o código-fonte com rastreamento por logs que detalha:

- Quem acessou o código;
- Quando acessou o código;
- O que foi acessado;
- As alterações realizadas.

É requerido que o acesso aos códigos-fonte seja realizado por meio de autenticação segura que deve ser integrada a um serviço de diretório com protocolo LDAP ou algum protocolo criptografado.

Todos os código-fonte de sistemas da CATTALINI (mesmo aqueles geridos com o uso de desenvolvimento terceirizado) são gerenciados por meio de sistema centralizado de colaboração e desenvolvimento de código que permita o rastreamento das alterações conforme versionamento do produto.

As não-conformidades de acesso ao código-fonte devem ser reportadas pelos contatos publicados nos termos da POL-SGSI-007-Política de Segurança da Informação.

CICLO DE VIDA DE DESENVOLVIMENTO

O desenvolvimento de todos os softwares utilizados em favor da CATTALINI deve seguir o ciclo de desenvolvimento seguro de software abrangendo todas as fases do ciclo de vida, incluindo concepção, especificação, design, codificação, testes, implementação, manutenção e descontinuação. Cada fase requer a implementação de práticas de segurança específicas.

A trilha do ciclo de Desenvolvimento Seguro de sistemas em favor da CATTALINI será realizada conforme o disposto no PG-TI-013-Gestão de Mudanças de TI (GMUD), bem como, todas as etapas descritas abaixo devem ter evidência no Plano de Mudança citado na GMUD.

ETAPA 1 - Concepção:

Antes de iniciar qualquer projeto de desenvolvimento de software, deve-se conduzir uma análise inicial de riscos para identificar ameaças e vulnerabilidades potenciais. Deve ser considerada a possibilidade de acesso SSO dos usuários, criptografia de dados e mascaramento para dados pessoais, incluindo anonimização e pseudo-anonimização.

ETAPA 2 - Especificação:

Os requisitos de segurança devem ser documentados e integrados aos requisitos funcionais e técnicos dentro dos registros de Plano de Mudança previstos pela GMUD.

ETAPA 3 - Design:

Seguir os princípios de arquitetura e engenharia de sistemas seguros para agregar resiliência contra ameaças cibernéticas:

Segregação de dados: separação em linha de código do tratamento de dados públicos e código de tratamento de dados com acesso restrito.

Defesa em profundidade: combinação de várias camadas de proteção, como firewalls, detecção de intrusões, criptografia e monitoramento contínuo, visando o aumento da resiliência da aplicação, tornando-a mais difícil de ser comprometida.

Controle de acesso: garantia de que somente usuários autorizados tenham permissão para acessar determinadas partes da aplicação ou dados.

Segregação de função: garantia de separação de funções conflitantes entre si nos diferentes processos da organização;

ETAPA 4 - Codificação:

A codificação de software por desenvolvimento interno ou por desenvolvimento terceirizado deverá, obrigatoriamente valer-se de uma das técnicas abaixo para garantir qualidade e segurança do sistema:

Revisão de código por pares: processo em que um desenvolvedor revisa o código escrito por outro desenvolvedor antes que ele seja integrado ao projeto. Isso é feito para identificar e corrigir potenciais problemas, vulnerabilidades ou erros no código.

Uso de ferramentas de análise estática: são programas de software projetados para examinar o código-fonte em busca de possíveis problemas, vulnerabilidades e não conformidades com padrões.

ETAPA 5 - Testes de segurança em desenvolvimento e aceitação:

Testes de segurança devem ser realizados durante a fase de testes, podendo ser testes de penetração, avaliações de vulnerabilidades e testes automatizados.

Os testes de segurança realizados nos componentes do pacote de implantação devem ser devidamente registrados, bem como, as não conformidades com os requisitos de segurança devem ser identificadas, registradas e tratadas.

Nenhum componente do pacote de implantação dos softwares aplicados em produção pode ser aprovado para produção sem que um teste relativo à sua segurança tenha sido realizado de forma bem-sucedida.

ETAPA 6 - Implementação:

A implementação deve ser trilhada considerando todos os requisitos de segurança do ambiente de produção e backup, possibilitando planos de rollback, considerando o disposto no processo da GMUD.

ETAPA 7 - Manutenção:

Durante o desenvolvimento de novas funcionalidades ou projetos que alterem funcionalidades em andamento, os desenvolvedores deverão manter evidências acerca de falhas de segurança que eventualmente venham a encontrar no código da aplicação. Tais falhas potencialmente exploráveis deverão ser tratadas e receber maior prioridade em detrimento a outras atividades previstas, reduzindo a possibilidade que um sistema entre em produção com vulnerabilidades. As atividades de correção de segurança em projetos que estão em andamento deverão ser registradas em sistema gerencial de acompanhamento de tarefas utilizado para gestão do projeto, tal como as tarefas para desenvolvimento de novas funcionalidades.

A Cattalini poderá solicitar a realização de testes de vulnerabilidades do software a qualquer momento.

ETAPA 8 - Descontinuação:

Quando uma aplicação é retirada, as informações sensíveis devem ser adequadamente protegidas por meio de backup em fita ou por qualquer outro dispositivo, que garanta seu armazenamento pelo período que for necessário à Cattalini e em cumprimento de leis e regulamentos vigentes.

CODIFICAÇÃO SEGURA

A CATTALINI espera dos desenvolvedores de software terceirizados o uso de todas as práticas previstas na presente PDS, quando aplicável, visando não haver incorrência de incidentes de segurança causados por exploração de defeitos ou *bugs* em seus sistemas internos.

As equipes de desenvolvimento terceirizadas atuam em ambiente compartilhado de homologação, onde os analistas internos atuam como validadores do resultado obtido pelo recurso externo, considerando a segurança da aplicação na aprovação do pacote de implantação para produção como um dos fatores de aprovação de versão.

Por padrão, todos os desenvolvedores de softwares à serviço da CATTALINI estão proibidos de adotar práticas reconhecidamente inseguras em seu Design,

não se limitando : à uso de senhas como texto puro no código-fonte, uso de amostras de código-fonte não aprovadas (mesmo quando comentadas) em produção e o uso de serviços integrados baseados na WEB que não utilizem autenticação (acesso anônimo).

SEPARAÇÃO DE AMBIENTES DE TESTE, DESENVOLVIMENTO E PRODUÇÃO

A separação de ambientes deve ser estrita, com cada ambiente sendo claramente distinto e possuindo infraestruturas, configurações e dados separados. O acesso aos ambientes de desenvolvimento, teste e produção é estritamente monitorado por meio de logs de acesso e sua liberação é realizada seguindo o princípio de necessidade e menor privilégio.

O ambiente de desenvolvimento é exclusivamente destinado à criação e testes de novas funcionalidades. Neste ambiente, apenas os desenvolvedores e equipe de testes têm acesso, e é expressamente proibido desenvolver ou manipular informações em linha de código direto nos ambientes de teste e produção.

O ambiente de teste é reservado para a avaliação de novas funcionalidades, correções e atualizações. Todos os pacotes aplicados em ambiente produção deverão obrigatoriamente ter sido homologados neste ambiente.

O ambiente de produção é reservado para a execução de sistemas em produção e para atender aos usuários finais.

Dados classificados como confidenciais para a PSI não devem ser utilizados nos ambientes de teste ou desenvolvimento. Quando dados de produção são necessários para testes, eles devem ser anonimizados ou mascarados para proteger a privacidade e a segurança em conformidade com a PSI e Política de Privacidade e Proteção de Dados Pessoais.

Os registros de acesso aos servidores destinados aos acessos nos ambientes de teste, desenvolvimento e produção são mantidos conforme para avaliação em auditoria caso necessário. Além disso, planos de backup e recuperação são mantidos para os ambientes de produção, com testes regulares para garantir a integridade dos dados periodicamente. Para os ambientes de desenvolvimento on premisses, a Cattalini é responsável pelo backup, em caso de ambiente de desenvolvimento SAAS, a responsabilidade é do fornecedor.

AUDITORIA DA POLÍTICA DE DESENVOLVIMENTO DE SOFTWARE

Como forma de garantir o cumprimento integral da PDS por desenvolvedores internos e externos ou provedores de software e sistemas da CATTALINI, o dono da política poderá realizar ou contratar auditorias técnicas de forma programada.

Os seguintes requisitos serão observados:

- Verificação dos direitos de acesso de desenvolvedores internos à CATTALINI, registrando os direitos que não estiverem em conformidade com a necessidade da organização e o princípio do “privilégio mínimo”, bem como, as funções e responsabilidades dos usuários;
- O cumprimento por parte dos fornecedores de serviços de desenvolvimento de sistemas acerca dos termos previstos em contrato e na PDS;
- Verificação da realização dos backups dos ambientes teste e desenvolvimento;
- Avaliação de erros ou suspeitas de falhas de segurança nos logs das aplicações.

Caso seja evidenciado Não Conformidade será registrada para tratativa do fornecedor com SLA definido para correção.