Especificação OpenChain

Versão 1.1

Índice

Aviso Legal / Disclaimer

Esta é uma tradução oficial do projeto OpenChain, traduzida do texto original inglês. No caso de duvidas entre a tradução e a versão em inglês, o texto em inglês terá precedência.

This is an official translation from the OpenChain Project. It has been translated from the original English text. In the event there is confusion between a translation and the English version, The English text shall take precedence.

Translators

- Bill Weinberg – Open Source Sense

Reviewers

- Gianna Cardinale – Open Source Sense
- Gianfranco Cardinale – Alquimia Moderna

1) Introdução

A iniciativa Openchain começou em 2013 quando um grupo de praticantes FOSS observou duas tendências emergentes: 1) Similaridades significantes de processo entre organizações com programas maduros de conformidade às obrigações de FOSS; e 2) Ainda permanecer um grande número de organizações trocando softwares com programas menos desenvolvidos. A segunda observação resultou numa falta de confiança na consistência e na qualidade dos artefatos de conformidade sendo trocados. Como consequência, a cada nível da cadeia de abastecimento, organizações jusantes precisavam refazer os serviços de conformidade FOSS (e.g., às obrigações de uma licença) já feitos por outras organizações montantes.

Um comitê se organizou para considerar a criação de uma especificação standard que i) Facilitaria a troca de informação de conformidade FOSS de maior qualidade e consistência através da indústria; e ii) Diminuiria os altos custos ligados a software de fonte livre resultante da necessidade de refazer os serviços de conformidade. Este comitê evoluiu a um grupo de trabalho, e em abril de 2016, se organizou formalmente como um projeto colaborativo da Linux Foundation.

A visão e a missão da iniciativa são as seguintes:

- Visão: uma cadeia de abastecimento de software entrega informações de conformidade confiáveis e consistentes sobre o software free/livre (FOSS).
- Missão: estabelecer requisitos para realizar o gerenciamento efetivo de FOSS para participantes na cadeia de abastecimento de software, assim que os requisitos e os matérias associadas se desenvolvem numa maneira colaborativa e aberta por representantes da cadeia de abastecimento de software, a comunidade FOSS, e a academia.

De acordo com a Visão e a Missão, esta especificação define um conjunto de requisitos, que sendo cumpridos, aumentariam a probabilidade que um programa de conformidade FOSS realize um nível suficiente de qualidade, consistência e plenitude; mesmo que um programa satisfaça todos os requisitos da especificação, isto não garante conformidade plena. Os requisitos representam um nível básico (mínimo) de requisitos para um programa a ser julgado em conformidade a OpenChain. A especificação tem como foco as qualidades do programa do "quê" e do "porquê" versus as considerações de "como" e "quando". Este foco assegura um nível prático de flexibilidade que habilita diferentes organizações a customizar os próprios processos e diretrizes para que se adaptem aos seus objetivos.

A Secção 2 introduz a definição da terminologia-chave que se usa ao longo da especificação. A Secção 3 apresenta os requisitos da especificação onde cada requisito inclui uma lista mínima de um Artefato de Verificação. Estes artefatos são obrigatórios e representam as provas da satisfação dos requisitos para um programa de conformidade FOSS a acomodar os requisitos da versão 1.1 da especificação OpenChain. Artefatos de verificação não devem ser abertos ao escrutínio público, com a opção de fornecê-los sobre um acordo de não divulgação ou em

resposta particular da organização OpenChain para validar a conformidade à própria especificação OpenChain.

2) Definições

Artefatos de Verificação – provas obrigatórias de que um requisito está satisfeito.

Contato FOSS – uma pessoa designada que recebe inquéritos sobre assuntos FOSS de fora da sua própria organização.

Em conformidade com OpenChain – um programa de conformidade que satisfaz todos os requisitos desta especificação.

FOSS (software de fonte livre e software livre) – software sujeito a uma ou mais licenças que satisfazem a Definição de Software de Fonte Libre publicada pela Open Source Inititive (OpenSource.org) ou a Definição de Free Software publicada pela Free Software Foundation ou licenças similares**.**

Funcionários de software – empregados ou contratantes que definem, contribuem, ou são responsáveis pela preparação do Software Fornecido.

Licenças Identificadas – uma lista de licenças FOSS identificadas como o resultado de um método apropriado de identificar tais licenças.

Software Fornecido – o software que uma organização entrega a terceiros (e.g., outras organizações ou outras pessoas físicas).

SPDX (format de troca de informações de pacotes de software) – formato estandardizado criado pelo grupo de trabalho SPDX da Linux Foundation para trocar informações de copyright e licenciamento para pacotes de software. Possui uma descrição da especificação SPDX no endereço www.spdx.org.

3) Requisitos

G1: Conheça a suas responsabilidades FOSS

1.1 Existe uma diretriz por escrito que governa a conformidade à licença FOSS da distribuição de Software Fornecida. A diretriz deve ser comunicada internamente.

Verificação

☐ 1.1.1 Existe uma diretriz documentada

☐ 1.1.2 Um procedimento documentado existe que informa os Funcionários de Software da existência de uma diretriz FOSS (e.g., via treinamento, num wiki interno, ou por outros meios de comunicação).

Raciocínio:

Garantia de que os funcionários de software foram informados sobre a existência de uma diretriz de FOSS. Apesar da ausência de requisitos sobre a matéria que deve ser incluída na diretriz, outras secções desse documento podem impor requisitos na diretriz.

1.2 Treinamento obrigatório para todos os funcionários de software assim que

- O treinamento, no mínimo, inclui os seguintes tópicos:
  - A diretriz FOSS e onde/como localizar uma cópia dela
  - Os conceitos básicos da lei de propriedade intelectual que pertencem a FOSS e licenciamento de software livre
  - Os conceitos de licenciamento FOSS (incluindo os conceitos de licenças permissivas e as licenças “copyleft”)
  - Os modelos de licenciamento de projetos FOSS
  - As responsabilidades dos funcionários de software que pertencem a conformidade FOSS especificamente, e a diretriz FOSS em geral, e
  - O processo para identificar, documentar e rastrear componentes de tipo FOSS que fazem parte do software fornecido.
- Os funcionários de software devem ter completado o treinamento FOSS nos últimos 24 meses (para serem considerados atualizados). Pode-se utilizar um exame para permitir que os funcionários de software satisfaçam o treinamento requisitado.

Verificação

- ☐ 1.2.1 Materiais de treinamento FOSS que tratam dos assuntos acima mencionados (e.g., apresentações, aulas on-line e outros materiais)
- ☐ 1.2.2 Um método para rastrear a conclusão do treinamento de todos os funcionários de software
- ☐ 1.2.3 Um mínimo de 85% dos funcionários de software atualizados, usando a definição acima

Raciocínio

Assegurar-se que os funcionários de software tenham recentemente comparecido a um treinamento FOSS tratando de assuntos relevantes a FOSS. Há a intenção de garantir a inclusão de material a um nível básico, porém um treinamento típico provavelmente seria mais compreensivo que o requisito desta especificação.

1.3 Existe um processo para a revisão das licenças identificadas para determinar as obrigações, restrições e direitos concedidos por cada licença.

Verificação

- ☐ 1.3.1 Um procedimento documentado para rever e documentar as obrigações, restrições e direitos concedidos por cada licença identificada que governa o Fornecedor de Software.

Raciocínio:

Para assegurar que um processo existe para rever e identificar as obrigações, acompanhando cada licença para os vários casos de uso.

G2: Atribuir Responsabilidade para Efetuar Conformidade

2.1 Identificar a pessoa responsável para receber inquéritos sobre FOSS (“Contato FOSS”)

- Identificar a pessoa ou as pessoas responsáveis
- O Contato FOSS deve responder aos inquéritos sobre conformidade, de forma apropriada, e
- Identificar, publicamente, os meios de alcançar o Contato FOSS

Verificação

☐ 2.1.1 O Contato FOSS está publicamente identificado (e.g., via um endereço de correio eletrônico visível ou via o diretório Open Compliance da Linux Foundation)

☐ 2.1.2 Existe um procedimento interno atribuindo reponsabilidade de receber inquéritos sobre a conformidade FOSS

Raciocínio:

Assegurar que existe um meio razoável para terceiros de contatar a organização com inquéritos sobre conformidade FOSS e que essa responsabilidade está atribuída efetivamente.

2.2 Identificar Funções do Processo de Conformidade FOSS Interna

- Atribuir responsabilidades individuais para gerenciar a conformidade interna FOSS. O Gerente de Conformidade e o Contato FOSS podem ser a mesma pessoa
- Garantir que existam recursos de apoio a atividades de gerenciamento de FOSS
- Alocar tempo para o desempenho das funções
- Fazer com que um orçamento comercialmente razoável esteja disponível
- Atribuir responsabilidades para desenvolver e manter as diretrizes e os processos de conformidade
- Garantir que perícia jurídica esteja acessível às pessoas responsáveis para as funções de conformidade (recursos internos ou externos), e
- Ter certeza de que exista um processo para a resolução de questões sobre a conformidade FOSS

Verificação

☐ 2.1.1 Identificação de nomes de pessoas, grupos ou funções de conformidade FOSS.

☐ 2.2.2 Identificação de fontes de perícia disponíveis às pessoas (internas ou externas) responsáveis para a conformidade FOSS.

☐ 2.2.3 Existência de um procedimento documentado que atribua responsabilidades internas para conformidade FOSS.

☐ 2.2.4 Existência de um procedimento documentado para a revisão e a remediação de casos fora de conformidade

Raciocínio:

Para assegurar que as responsabilidades FOSS estejam efetivamente atribuídas.

G3: Rever e Aprovar Conteúdo FOSS

3.1 Existe um processo para a criação e o gerenciamento da lista de materiais (BoM) de componentes FOSS, que detalha cada componente e sua licença dentro de uma entrega de Software Fornecido.

Verificação

☐ 3.1.1 Existência de um procedimento documentado para rastrear e arquivar as informações sobre a coleção de componentes FOSS do qual uma entrega de Software Fornecida é composta.

☐ 3.1.2 Existência de registros para cada entrega de Software Fornecido que demonstre que o procedimento documentado está corretamente seguido.

Raciocínio:

Assegurar-se que exista um processo para a criação e o gerenciamento de uma lista de matérias (BoM) usada para construir o Software Fornecido. Necessita-se uma lista de materiais (BoM) que apoie a revisão sistemática dos termos de licença de cada componente para que se compreendam as obrigações e as restrições aplicadas à distribuição do Software Fornecido.

3.2 O programa de gerenciamento de FOSS deve ser capaz de lidar com casos de uso comuns de licenças FOSS encontrados por Funcionários de Software para o Software Fornecido, que podem incluir os casos seguintes. Nota-se que a lista não é exaustiva e que nem todos os casos de uso se aplicam:

- distribuído em forma binária
- distribuído como código fonte
- integrado com outros componentes FOSS podendo assim desencadear obrigações “copyleft”
- contendo FOSS modificado
- contendo FOSS e/ou outro software licenciado sob uma outra licença incompatível que interage com outros componentes do Software Fornecido; e/ou
- contendo FOSS com requisitos de atribuição

Verificação

☐ 3.2.1 Foi implementado um procedimento que lida com os casos de uso comuns de FOSS para os componentes FOSS em cada entrega de Software.

Raciocínio:

Para assegurar que o programa de conformidade é suficientemente robusto para lidar com os casos de uso mais comuns de uma organização, e que existe um procedimento para apoiar esta atividade onde ele é seguido.

G4: Entrega Documentação e Artefatos de Conteúdo FOSS

4.1 Prepare o conjunto de artefatos que represente a produção do programa de gerenciamento de FOSS para cada entrega de Software Fornecido. Este conjunto se refere a 'Os Artefatos de Conformidade', podendo incluir (mas não limitado a) um ou mais dos seguintes itens: código fonte, noticias de atribuição, notícias de copyright, cópias de licenças, notificações de modificação de código, ofertas por escrito, documentos SPDX, e assim por diante.

Verificação

☐ 4.1.1 Existência de um procedimento documentado que assegure que os Artefatos de Conformidades estão preparados e distribuídos com a entrega do Software Fornecido como exigido pelas licenças identificadas.

☐ 4.1.2 Cópias dos Artefatos de Conformidade estão arquivadas e facilmente acessíveis, e o arquivo existirá enquanto existe o Software Fornecido, ou no mínimo, pelo tempo em que o Software Fornecido esteja disponível ou por um período exigido pela licença, o que for de maior duração.

Raciocínio:

Para assegurar que a coleção completa de Artefatos de Conformidade acompanhe o Software Fornecido, como exigido pelas Licenças Identificadas que dirige o Software Fornecido, juntamente com outros relatórios emitidos como parte do processo da revisão FOSS.

G5: Entender a Interação com a Comunidade FOSS

5.1 Existência de diretrizes escritas que dirijam contribuições aos projetos FOSS pela organização. Estas diretrizes devem ser comunicadas internamente.

Verificação

- ☐ 5.1.1 Existência de diretrizes escritas de contribuição aos projetos FOSS
- ☐ 5.1.2 Existência de um procedimento que informe a todos os Funcionários de Software da existência de diretrizes (e.g., via treinamento, wikis internos, ou outros meios práticos de comunicação)

Raciocínio:

Assegurar-se de que uma organização tenha dado consideração razoável ao desenvolvimento de diretrizes com respeito às contribuições públicas a FOSS. Tais diretrizes de contribuição FOSS podem fazer parte de uma diretriz integral, ou existir como uma diretriz independente. Numa situação onde nenhuma contribuição é permitida, uma diretriz deverá também existir para clarificar esta proibição.

5.2 Se uma organização permite contribuições aos projetos FOSS, deve-se existir um processo que implemente a diretriz delineada na Seção 5.1 acima.

Verificação

- ☐ 5.2.1 Desde que a diretriz de contribuição FOSS permita contribuições, deve-se existir um procedimento documentado que as controle

Raciocínio

Assegurar-se que uma organização tenha um processo documentado que determine como se façam contribuições publicamente aos projetos FOSS. Deve existir uma diretriz que proíba tais contribuições, se for o caso de existir tal proibição, entende-se que nenhuma diretriz existiria, mas que este requisito mesmo assim estaria satisfeito.

G6: Certificar Aderência aos Requisitos OpenChain

6.1 Para conferir a certificação OpenChain a uma organização, a organização deve afirmar que possui um programa de gerenciamento FOSS em conformidade aos critérios descritos nesta Especificação versão 1.1.

Verificação

☐ 6.1.1 A organização afirma possuir um programa de gerenciamento FOSS, em conformidade a todos os requisitos desta Especificação OpenChain versão 1.1.

Raciocínio

Assegurar que se uma organização declara possuir um programa de gerenciamento FOSS que se conforme a OpenChain, que tal programa preencha realmente todos os requisitos da especificação. Atender meramente a uma porção destes requisitos não seria considerado suficiente para ganhar a certificação OpenChain.

6.2 Conformidade com esta versão da especificação durará 18 meses da data da validação de conformidade. Os requisitos da validação de conformidade se encontram no site do Project OpenChain.

Verificação

☐ 6.2.1 A organização afirma que um programa de gerenciamento FOSS existe e que este atende todos os requisitos da Especificação OpenChain versão 1.1 durante os últimos 18 meses desde a validação de conformidade.

Raciocínio

É essencial que uma organização se mantenha atualizada se deseja afirmar a conformidade ao longo do tempo. Este requisito assegura que os processos de suporte e controles não se degradem se a organização deseja continuar a afirmar a conformidade à especificação ao longo do tempo.

Apêndice I: Traduções em Outros Idiomas

Para facilitar a adoção global, nós damos boas-vindas aos empenhos de tradução da especificação em várias línguas. Considerando que o OpenChain funciona como um projeto aberto, as traduções surgem da vontade de quem contribui com tempo e perícia para traduzir este documento sob a licença CC-BY-4.0 e sob a diretriz de tradução do projeto. Os detalhes desta diretriz, juntamente com as traduções disponíveis, se encontram no site do Projeto OpenChain na página de especificação.