OPENCHAIN

Especificación de Conformidad OpenChain

Versión 1.1

Contenidos

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.

Introducción

La iniciativa OpenChain comenzó en el 2013 cuando un grupo de profesionales especialistas en materia de la cadena de suministro de software de código abierto (*Open Source Software*, OSS) identificó dos patrones emergentes: 1) existían similitudes significativas en los procesos de las organizaciones con programas maduros de conformidad en materia de OSS; y 2) existen un gran número de organizaciones, intercambiando software, que tienen programas de conformidad menos desarrollados. Esto crea a una falta de confianza en la coherencia y la calidad de los "artefactos de conformidad" que acompañan el software que se intercambia. Como consecuencia de ello, en cada nivel de la cadena de suministro, las organizaciones situadas en la parte final de la cadena (*downstream*) frecuentemente repiten el trabajo de conformidad ya realizado por otras organizaciones en el inicio de la cadena (*upstream*).

Se creó un grupo de estudio para considerar si podría establecerse una especificación general para un programa de conformidad estándar que: i) incremente la calidad y consistencia en la información respecto al conformidad de OSS compartida en toda la industria; y ii) disminuya los altos costos de transacción asociados con el OSS que resultan de la repetición del trabajo de conformidad. El grupo de estudio se transformó en un grupo de trabajo, y en abril del 2016, se organizó formalmente como un proyecto de colaboración de la Linux Foundation.

La Visión y Misión de la Iniciativa OpenChain son las siguientes:

- **Visión**: Una cadena de suministro de software donde el software libre / de código abierto (FOSS) se entrega con información de conformidad confiable y consistente.

- **Misión**: Establecer los requisitos para lograr una gestión eficaz de software libre / de código abierto (FOSS) para los participantes de la cadena de suministro de software, de tal forma que los requisitos y los elementos asociados con ellos se desarrollen de manera conjunta y abierta por los miembros de la cadena de suministro de software, de la comunidad OSS y de la comunidad académica.

De acuerdo con su Visión y Misión, esta especificación define un conjunto de requisitos que, si se cumplen, incrementan significativamente la probabilidad de que un programa de conformidad para OSS alcance un nivel adecuado de calidad, consistencia e integridad (aunque se debe tener en cuenta que un programa que satisfaga todos los requisitos de la especificación no garantiza la conformidad total). Estos requisitos representan un conjunto de requisitos básicos (un nivel mínimo) que un programa debe satisfacer para ser considerado "*OpenChain Conforming*". La especificación se centra en las características del "qué" y del "por qué" de un programa de conformidad, y no en las del "cómo" y del "cuándo". Esto asegura un nivel práctico de flexibilidad que permite a las organizaciones adaptar sus políticas y procesos para que se ajusten mejor a sus objetivos.

La Sección 2 presenta las definiciones de los términos más importantes utilizados a lo largo de esta especificación. La Sección 3 presenta los diferentes requisitos de la especificación, cada uno con una lista de uno o más Artefactos de Verificación. Éstos representan la evidencia que debe existir para que un determinado requisito se considere satisfecho. Si se cumplen todos los requisitos para un programa dado, éste se consideraría en conformidad con OpenChain (*OpenChain Conforming*), de acuerdo con la versión 1.1 de la especificación. Los Artefactos de Verificación no están destinados a ser públicos, pero

podrían proporcionarse bajo Acuerdo de Confidencialidad (NDA) o previa solicitud privada a la organización OpenChain para validar esta conformidad.

Definiciones

FOSS (software libre y de código abierto) - software sujeto a una o más licencias que cumplan con la definición de código abierto publicada por la *Open Source Initiative* (OpenSource.org) o la Definición de Software Libre (publicada por la *Free Software Foundation*) o una licencia similar.

Contacto FOSS - una persona de la organización designada para servir de contacto para entidades externas sobre consultas respecto al FOSS creado o utilizado en la organización.

Licencias Identificadas – un conjunto de licencias que se ha identificado son utilizadas en la organización.

"*OpenChain Conforming*" - un programa que satisface todos los requisitos de esta especificación.

Personal de Software - cualquier empleado o contratista que defina, contribuya o tenga la responsabilidad de preparar el Software Suministrado. Según cada organización, puede incluir (pero no está limitado a) los desarrolladores del software, los ingenieros responsables del "*release*", los ingenieros de calidad, el personal de marketing de producto y/o de gestión de producto.

SPDX o ***Software Package Data Exchange*** (**Intercambio de Datos sobre Paquetes de Software)** - el estándar creado por el Grupo de Trabajo SPDX que define un formato para intercambiar información sobre las licencias y los derechos de autor referentes a un paquete específico de software. La descripción de la especificación SPDX se encuentra en www.spdx.org.

Software Suministrado: el software que una organización entrega a terceros (otras organizaciones o individuos).

Artefactos de Verificación – Documentos que deben existir para que un determinado requisito *de esta especificación* se considere satisfecho.

Requisitos

G1: Conozca sus responsabilidades con respecto al FOSS

1.1. Debe existir una política escrita sobre FOSS que rige la conformidad con las licencias FOSS en la distribución de Software Suministrada. Esta política debe ser comunicada internamente.

Artefacto/s de Verificación:

- ☐ Existe una política documentada sobre FOSS.
- ☐ Existe un procedimiento documentado que informa a todo el Personal de Software sobre la existencia de la política FOSS (por ejemplo, a través de la capacitación, un wiki interno u otro método práctico de comunicación).

Razón fundamental:
Asegurar que se tomaron las medidas necesarias para crear, registrar e informar al Personal de Software de la política FOSS. Aunque no se especifiquen aquí requisitos sobre lo que debe incluirse en esta política, otros requisitos en otras secciones pueden hacerlo.

1.2 Debe existir capacitación obligatoria sobre FOSS para todo el Personal de Software; esta capacitación debe cumplir los siguientes requisitos:

- **Debe cubrir, por lo menos, los siguientes temas:**
  - **La política FOSS de la organización y dónde encontrar una copia de ella;**
  - **Los fundamentos del derecho de propiedad intelectual relacionados con el FOSS y las licencias libres;**
  - **Los conceptos relevantes del régimen de licenciamiento FOSS (incluyendo los conceptos de licencias permisivas y copyleft);**
  - **Los modelos de licenciamiento de proyectos FOSS;**
  - **Las funciones y responsabilidades del Personal de Software relacionadas específicamente con el conformidad FOSS y la política FOSS en general; y**
  - **El proceso de identificación, registro y / o seguimiento de componentes FOSS contenidos en el Software Suministrado.**
- **El Personal de Software debe haber completado esta capacitación en los últimos 24 meses (para ser considerado "al día"). Se puede utilizar una examen para demostrar que el Personal de Software cumple con los requisitos de formación.**

Artefacto/s de Verificación:

- ☐ 1.2.1 Existen materiales para la formación sobre FOSS que abarcan los temas indicados (por ejemplo, presentaciones, cursos en línea u otros materiales de capacitación).
- ☐ 1.2.2 Método para dar seguimiento a la capacitación de todo el Personal de Software.
- ☐ 1.2.3 Al menos el 85% del Personal de Software debe estar "al día" (según la definición de la sección anterior).

Razón fundamental:
Asegurarse de que el Personal de Software haya sido recientemente capacitado sobre FOSS y que se cubran un conjunto básico de temas relevantes relacionados con el FOSS. La intención es

asegurarse que esta capacitación cubra un conjunto básico de temas, aunque se espera que un programa de capacitación típico probablemente será más completo de lo que se requiere aquí.

1.3 Existe un proceso para revisar las Licencias Identificadas para determinar las obligaciones, restricciones y derechos otorgados por cada licencia.

Artefacto/s de Verificación:

- ☐ 1.3.1 Existe un procedimiento documentado para revisar y documentar las obligaciones, restricciones y derechos otorgados por cada Licencia Identificada que rige el Software Suministrado.

Razón fundamental:
Asegurar que exista un proceso para revisar e identificar las obligaciones de licencia para cada Licencia Identificada para los diversos casos de uso.

G2: Assign Responsibility for Achieving Compliance

2.1 Identificar el rol del Contacto FOSS ("Contacto FOSS").

- **Designar la/s persona/s responsable/s de recibir consultas externas sobre FOSS;**
- **Asegurarse que el Contacto FOSS haga un esfuerzo comercialmente razonable para responder a las consultas sobre conformidad FOSS, según corresponda; e**
- **Identificar públicamente los medios para contactar con el Contacto FOSS mediante comunicación electrónica.**

Artefacto/s de Verificación:

- ☐ 2.1.1 El rol de Contacto FOSS debe ser públicamente identificado (por ejemplo, a través de una dirección de correo electrónico pública, o en el *Open Directory* de la Fundación Linux).
- ☐ 2.1.2 Existe un proceso interno documentado que determina el proceso para recibir consultas de conformidad FOSS.

Razón fundamental:
Asegurarse de que haya un método razonable para que terceros puedan ponerse en contacto con la organización para realizar consultas sobre la conformidad *FOSS* de la organización y que esta responsabilidad se haya asignado efectivamente.

2.2 Identificar el/los rol/es interno/s para las verificaciones de conformidad FOSS.

- **Designar la/s persona/s responsable/s de la gestión de las verificaciones de conformidad internas del FOSS. El responsable de conformidad FOSS y el Contacto FOSS pueden ser la misma persona.**
- **Asegurarse que la actividad de gestión del conformidad FOSS tenga recursos suficientes:**
  - **Se ha sido asignado el tiempo necesario para desempeñar el rol; y**
  - **Se ha asignado un presupuesto comercialmente razonable.**
- **Atribuir responsabilidades para desarrollar y mantener la política y los procesos de conformidad FOSS;**
- **Asegurarse que el responsable de las verificaciones de conformidad FOSS tenga acceso a personas con experiencia jurídica relacionada con las verificaciones de conformidad FOSS (por ejemplo, a un experto jurídico interno o externo); y**
- **Asegurarse que exista un camino de escalamiento para la resolución de problemas de conformidad FOSS.**

Artefacto/s de Verificación:

- ☐ 2.2.1 Identificación interna del nombre de las personas, grupos o funciones responsables del conformidad FOSS.
- ☐ 2.2.2 Identificación de la fuente de conocimientos jurídicos accesibles para los responsables de conformidad FOSS (fuente interna o externa).
- ☐ 2.2.3 Existencia de un procedimiento documentado que asigna responsabilidades internas para el conformidad FOSS.
- ☐ 2.2.4 Existencia de un procedimiento documentado para gestionar la revisión y solución de casos no conformes.

Razón fundamental:

Asegurarse que determinadas responsabilidades respecto al FOSS hayan sido atribuidas de manera efectiva.

G3: Revisar y aprobar los Contenidos FOSS

3.1 Existe un proceso para crear y gestionar una lista de todos los componentes FOSS (y sus respectivas Licencias Identificadas) que son parte del Software Suministrado.

Artefacto/s de Verificación:

- ☐ 3.1.1 Existe un proceso documentado para identificar, rastrear (*trace*) y archivar una lista de componentes FOSS (y sus Licencias Identificadas) que constituyen el Software Suministrado.
- ☐ 3.1.2 Existen registros para cada *release* de Software Suministrado que demuestren que se siguió correctamente el procedimiento documentado.

Razón fundamental:
Asegurarse que exista un proceso para crear y gestionar una "lista de materiales" de los componentes FOSS usados para construir el Software Suministrado. Este listado debe existir para permitir la revisión sistemática de los términos de la licencia de cada componente, para entender sus respectivas obligaciones y restricciones de distribución aplicables al Software Suministrado.

3.2 El programa de FOSS debe ser capaz de gestionar casos comunes de uso de FOSS encontrados por el Personal del Software para el Software Suministrado, que pueden incluir los siguientes casos de uso (tenga en cuenta que la lista no es exhaustiva ni que serán aplicables todos los casos de uso):

- **Distribuidos en forma binaria;**
- **Distribuidos en forma de código fuente;**
- **Integrado con otros componentes FOSS de tal manera que pueda desencadenar obligaciones copyleft;**
- **Contiene FOSS modificado;**
- **Contiene FOSS u otro tipo de software bajo una licencia incompatible cuando interactúa con otros componentes dentro del Software Suministrado; y/o**
- **Contiene FOSS con requisitos de atribución.**

Artefacto/s de Verificación:

- ☐ 3.2.1 Se ha implementado un procedimiento capaz de gestionar los casos comunes de uso de FOSS encontrados por Personal de Software en el Software Suministrado.

Razón fundamental:
Asegurarse que el programa de gestión de FOSS sea lo suficientemente robusto como para gestionar los casos comunes de uso de FOSS de una organización. Que exista un proceso para apoyar esta actividad y que se siga ese proceso.

G4: Entrega de documentación de contenido FOSS y artefactos

4.1 Preparar el conjunto de documentos que representa los resultados del programa de revisión FOSS para cada distribución (*release*) de Software Suministrado. Este conjunto se denomina "Artefactos de conformidad" que podría incluir (pero no se limita a) lo siguiente: el código fuente, los avisos de atribución, los avisos de derechos de autor, una copia de las licencias, notificaciones sobre modificaciones, ofertas escritas, documentos SPDX y similares.

Artefacto/s de Verificación:

- ☐ 4.1.1 Existe un procedimiento documentado que asegura que los Artefactos de conformidad se preparan y se distribuyen con el Software Suministrado en la manera requerida por las Licencias Identificadas.
- ☐ 4.1.2 Se archivan copias de los Artefactos de conformidad del Software Suministrado, que pueden ser recuperadas fácilmente, y se establece un plan para que estas copias existan por lo menos mientras el Software Suministrado esté ofrecido o por el tiempo requerido por las Licencias Identificadas (lo que sea más largo).

Razón fundamental:
Asegurase que el conjunto completo de Artefactos de conformidad acompañe al Software Suministrado en la manera requerida por las Licencias Identificadas que rigen el Software Suministrado, junto con otros informes creados durante el proceso de revisión FOSS.

G5: Entender el compromiso con la comunidad FOSS

5.1 Existe una política escrita que rige las contribuciones a los proyectos FOSS por parte de la organización. La política debe ser comunicada internamente.

Artefacto/s de Verificación:

- ☐ 5.1.1 Existe una política documentada sobre las contribuciones a proyectos FOSS;
- ☐ 5.1.2 Existe un procedimiento documentado que informe a todo el Personal de Software de la existencia de la política sobre contribuciones FOSS (por ejemplo, a través de la formación, un wiki interno u otro método de comunicación práctica).

Razón fundamental:
Asegurarse que la organización haya considerado razonablemente el desarrollo de una política con respecto a la contribución pública a proyectos FOSS. La política sobre contribuciones a proyectos FOSS puede ser parte de la política general de FOSS de la organización o ser una política independiente. En el caso de prohibir totalmente las contribuciones a FOSS, debe existir una política que establezca de manera clara esta posición.

5.2 Si la organización permite contribuciones a proyectos FOSS, entonces debe existir un proceso que implemente la política de contribuciones FOSS descrita en la Sección 5.1.

Artefacto/s de Verificación:

- ☐ 5.2.1 Siempre que la política sobre contribuciones FOSS permita contribuciones, debe existir un procedimiento documentado que describa el proceso de contribuciones a proyectos FOSS.

Razón fundamental:
Asegurarse que la organización tenga un proceso documentado para saber cómo la organización contribuye públicamente a proyectos FOSS. Puede existir una política que prohíba las contribuciones FOSS en absoluto. En este caso se entiende que no puede existir ningún proceso, lo cual cumplirá este requisito.

G6: Certificar el cumplimiento de los requisitos de OpenChain

6.1 Para que una organización sea certificada Conforme con OpenChain, debe afirmar que tiene un programa FOSS que cumple con los criterios descritos en esta Especificación OpenChain versión 1.1.

Artefacto/s de Verificación:

- ☐ 6.1.1 La organización afirma que existe un programa que cumpla con todos los requisitos de esta Especificación OpenChain versión 1.1.

Razón fundamental:
Asegurarse que, si la organización declara que tiene un programa que es *OpenChain Conforming*, dicho programa cumple con todos los requisitos de esta especificación. La mera satisfacción de un subconjunto de estos requisitos no se consideraría suficiente para justificar que un programa sea certificado conforme con OpenChain.

6.2 La conformidad con esta versión de la especificación durará 18 meses a partir de la fecha en que la conformidad fue validada. Los requisitos de validación de conformidad pueden encontrarse en el sitio web del proyecto OpenChain.

Artefacto/s de Verificación:

- ☐ 6.2.1 La organización afirma que existe un programa de conformidad FOSS que cumple con todos los requisitos de esta Especificación OpenChain versión 1.1 en los últimos 18 meses de lograr la conformidad.

Razón fundamental:
Es importante que la organización se mantenga al día con la especificación si desea afirmar la conformidad pasado el plazo de vigencia. Este requisito asegura que los procesos y controles de soporte del programa no se erosionen si la organización quiere seguir afirmando la conformidad con especificación después del plazo de 18 meses.

Apéndice I: Traducciones de este documento

Para facilitar la adopción global (de esta especificación) agradecemos los esfuerzos para traducir la especificación en varios idiomas. Dado que OpenChain funciona como un proyecto de código abierto, las traducciones son impulsadas por aquellos que están dispuestos a aportar su tiempo y experiencia para realizar traducciones bajo los términos de la licencia CC-BY 4.0 y la política de traducción del proyecto. Los detalles de la política y las traducciones disponibles se pueden encontrar en la página web de especificaciones del proyecto OpenChain.