Especificaciones para la Conformidad con OpenChain

Versión 2.1

Estas Especificaciones son funcionalmente idénticas a:

- **La Especificación de Conformidad OpenChain 1.1**
- **ISO/IEC PRF 5230**

Para obtener más información: www.openchainproject.org

Contenidos

Introducción

Este documento define los requisitos más importantes de un programa de cumplimiento de licencias de código abierto de calidad. El objetivo es proporcionar un punto de referencia que genere confianza entre las organizaciones que intercambian soluciones de software compuestas por software de código abierto. La conformidad con las especificaciones proporciona la garantía de que un programa ha sido diseñado para producir los artefactos de cumplimiento requeridos (es decir, avisos legales, código abierto, etc.) para cada solución de software. El presente documento se centra en los aspectos como el «qué» y el «por qué» de un programa, más que en el «cómo» y el «cuándo». De este modo se garantiza la flexibilidad para que organizaciones de distinto tamaño en distintos mercados puedan elegir el contenido de las políticas y procesos específicos que se ajusten a su tamaño, a sus objetivos y a su ámbito. Por ejemplo, un programa conforme a OpenChain puede dirigirse a una sola línea de productos o a toda la organización.

Esta introducción proporciona el contexto para todos los usuarios potenciales. En la cláusula 2 se definen los términos clave utilizados a lo largo de este documento. La cláusula 3 define los requisitos que un programa debe satisfacer para lograr la conformidad con estas especificaciones. Un requisito consiste en uno o más materiales de verificación (por ejemplo, registros) que deben ser producidos para satisfacer el requisito. No se requiere que los materiales de verificación se hagan públicos, aunque una organización puede decidir proporcionarlos a otras organizaciones, etc., posiblemente bajo un Acuerdo de Confidencialidad (ADC)

El presente documento ha sido desarrollado como una iniciativa abierta gracias a la información recibida de más de 200 contribuyentes. Se puede obtener información sobre su evolución histórica revisando la lista de correo de las Especificaciones y las preguntas más frecuentes (FAQ).

Tecnología de la información — Especificaciones de OpenChain

1 Ámbito

En este documento se especifican los requisitos fundamentales de un programa para el cumplimiento de las licencias de código abierto de calidad, a fin de proporcionar un punto de referencia que fomente la confianza entre las organizaciones que intercambian soluciones de software de código abierto.

2 Términos y definiciones

En este documento se aplican los siguientes términos y definiciones.

2.1
Artefactos de cumplimiento:
Son una colección de artefactos que representan el resultado de un programa de cumplimiento y acompañan al software suministrado.

Nota: La colección puede incluir (pero no se limita) a uno o más de los siguientes elementos: avisos de atribución, código fuente, scripts de construcción e instalación, copia de licencias, avisos de derechos de autor, notificaciones de modificación, ofertas escritas, lista de materiales de componentes del código abierto y documentos del SPDX.

2.2
Licencias identificadas:
Es un conjunto de licencias de software de código abierto identificadas como resultado de seguir un método apropiado de identificación de los componentes de código abierto de los que se compone el software suministrado.

2.3
Conformidad con OpenChain:
Es un programa que satisface todos los requisitos de este documento.

2.4
Código abierto:
Es un tipo de software sujeto a una o más licencias que cumplen con la definición de código abierto publicada por la *Open Source Iniciative* (véase opensource.org/osd) o la definición de software libre publicada por la *Free Software Foundation* (véase gnu.org/philosophy/free-sw.html) o una licencia similar.

2.5
Programa:
Es el conjunto de políticas, procesos y personal que comprende las actividades de cumplimiento de las licencias de código abierto de una organización.

2.6
Participantes del programa
Es cualquier empleado o contratista de la organización que defina, contribuya o tenga la responsabilidad de preparar el software suministrado.

Nota: Dependiendo de la organización, esto puede incluir (pero no se limita) a desarrolladores de software, ingenieros responsables del «reléase», ingenieros de calidad, a personas de gestión del marketing y al personal de gestión del producto.

2.7
SPDX o *Software Package Data Exchange* (Intercambio de Datos sobre Paquetes de Software):
Es el formato estándar creado por el Grupo de Trabajo SPDX de la Fundación Linux para el intercambio de la lista de materiales de un determinado paquete de software, incluyendo la información asociada a la licencia y a los derechos de autor (véase spdx.org)

2.8
Software suministrado:
Es el software que una organización distribuye a terceros (por ejemplo, a otras organizaciones o individuos).

2.9
Materiales de verificación:
Son los materiales que demuestran que se cumple un determinado requisito de las especificaciones.

La Organización Internacional de Normalización (ISO, por sus siglas en inglés) y la Comisión Eléctrica Internacional (CEI) mantienen bases de datos terminológicas para su uso en la normalización en las siguientes direcciones:

- ISO Plataforma de navegación online: disponible en https://www.iso.org/obp/ui

- Electropedia CEI: disponible en http://www.electropedia.org/

3 Requisitos

3.1 Fundación del programa

3.1.1 Política

Se debe contar con una política escrita de código abierto que rija el cumplimiento de la licencia de código abierto del software suministrado. Esta política debe ser comunicada internamente.

Material(es) de verificación:

- 3.1.1.1 Una política escrita sobre el código abierto.
- 3.1.1.2 Un procedimiento escrito que haga que los participantes del programa conozcan la existencia de la política de código abierto (por ejemplo, a través de formación, de un wiki interno u otro método práctico de comunicación).

Razón fundamental:

Asegurar que se toman las medidas necesarias para crear, registrar y hacer que los participantes en el programa conozcan la existencia de una política de código abierto. Aunque aquí no se especifiquen los requisitos sobre lo que debe incluirse en esa política, otras secciones pueden imponer requisitos sobre la política.

3.1.2 Competencia

La organización deberá:

- Identificar las funciones y correspondientes responsabilidades de las funciones que afectan al rendimiento y eficacia del programa;
- Determinar la competencia necesaria de los participantes en el programa que cumplen cada función;
- Asegurarse de que los participantes en el programa sean competentes sobre la base de una educación, formación y experiencia apropiadas;
- Cuando proceda, tomar medidas para adquirir la competencia necesaria; y
- Conservar la información documentada apropiada como prueba de esa competencia.

Material(es) de verificación:

- 3.1.2.1 Una lista escrita en la que se describan las funciones con las correspondientes responsabilidades para los diferentes participantes en el programa.
- 3.1.2.2 Un documento que identifique las competencias para cada función.
- 3.1.2.3 Pruebas escritas sobre la competencia evaluada para cada participante del programa.

Razón fundamental:

Asegurarse de que los participantes en el programa han obtenido un nivel de competencia suficiente para desempeñar sus respectivas funciones y responsabilidades.

3.1.3 Concienciación

La organización debe asegurarse de que los participantes en el programa estén al tanto de:

- La política de código abierto;
- Los objetivos relevantes del código abierto;
- Su contribución a la eficacia del programa; y
- Las implicaciones de no seguir los requisitos del Programa.

Material(es) de verificación:

- 3.1.3.1 Pruebas escritas sobre la concienciación evaluada de los participantes en el programa, que deben incluir los objetivos del programa, la contribución de cada persona dentro del programa y las implicaciones de no cumplir el programa.

Razón fundamental:

Asegurarse de que los participantes en el programa han obtenido un nivel de concienciación suficiente para sus respectivas funciones y responsabilidades.

3.1.4 Alcance del programa

Diferentes programas pueden estar regidos por diferentes niveles de alcance. Por ejemplo, un programa podría regir una sola línea de productos, un departamento o una organización entera. El alcance debe ser declarado para cada programa.

Material(es) de verificación:

- 3.1.4.1 Una declaración escrita que defina claramente el alcance y los límites del programa.

Razón fundamental:

Proporcionar la flexibilidad de construir un programa que se adapte mejor al alcance de las necesidades de una organización. Algunas organizaciones podrían optar por mantener un programa para una línea de productos específica, mientras que otras podrían implementar un programa para regir el software suministrado de toda la organización.

3.1.5 Obligaciones de la licencia

Se deberá contar con un proceso de revisión de las licencias identificadas para determinar las obligaciones, restricciones y derechos otorgados por cada licencia.

Material(es) de verificación:

- 3.1.5.1 Un procedimiento escrito para revisar y documentar las obligaciones, restricciones y derechos otorgados por cada licencia identificada.

Razón fundamental:

Garantizar que existe un proceso de revisión e identificación de las obligaciones de licencia para cada licencia identificada, para los diversos casos de utilización que una organización pueda encontrar (como se define en el §3.3.2).

3.2 Tareas relevantes definidas y apoyadas

3.2.1 Acceso

Mantener un proceso para poder responder eficazmente a las consultas externas de código abierto. Identificar públicamente un medio por el cual un tercero pueda hacer una investigación sobre el cumplimiento del código abierto.

Material(es) de verificación:

- 3.2.1.1 Método públicamente visible que permite a cualquier tercero hacer una consulta sobre el cumplimiento de la licencia de código abierto (por ejemplo, a través de una dirección de correo electrónico de contacto publicada, o a través del *Linux Foundation's Open Compliance Directory*).
- 3.2.1.2 Un procedimiento documentado interno para responder a las consultas sobre el cumplimiento de la licencia de código abierto de terceros.

Razón fundamental:

Garantizar que haya una forma razonable para que terceros se pongan en contacto con la organización en relación con las investigaciones sobre el cumplimiento del código abierto y que la organización esté preparada para responder eficazmente.

3.2.2 Recursos efectivos

Identificación y tarea(s) del programa de recursos:

- Asignar la responsabilidad de asegurar la ejecución exitosa de las tareas del programa.
- Garantizar que las tareas del programa tienen suficientes recursos:
  - Se ha asignado tiempo para realizar las tareas; y
  - Se han asignado fondos adecuados.
- Habilitar un proceso para revisar y actualizar la política y las tareas de apoyo;
- Informar sobre conocimientos jurídicos relativos al cumplimiento de las licencias de código abierto para que estén a disposición de quienes puedan necesitar esa orientación; y

- Habilitar un proceso para la resolución de los problemas de cumplimiento de las licencias de código abierto.

Material(es) de verificación:

- 3.2.2.1 Documento con el nombre de las personas, grupo o función o funciones en el programa identificado.
- 3.2.2.2 Las funciones del programa identificado han sido debidamente dotadas de personal y se han proporcionado los fondos adecuados.
- 3.2.2.3 Identificación de los conocimientos jurídicos disponibles para abordar los asuntos relacionados con el cumplimiento de la licencia de código abierto que podrían ser internos o externos.
- 3.2.2.4 Un procedimiento escrito que asigne responsabilidades internas para el cumplimiento del código abierto.
- 3.2.2.5 Un procedimiento documentado para gestionar la revisión y solución de los casos de incumplimiento.

Razón fundamental:

Garantizar: i) que las responsabilidades de los programas reciben un apoyo y unos recursos eficaces y ii) que las políticas y los procesos de apoyo se actualicen periódicamente para dar cabida a los cambios en las mejores prácticas de cumplimiento del código abierto.

3.3 Revisión y aprobación del contenido de código abierto

3.3.1 Lista de materiales

Se deberá contar con un proceso para crear y gestionar una lista de materiales que incluya cada componente de código abierto (y sus licencias identificadas) del que se compone el software suministrado.

Material(es) de verificación:

- 3.3.1.1 Un procedimiento escrito para identificar, rastrear, revisar, aprobar y archivar la información sobre la colección de componentes de código abierto de la que forma parte el software suministrado.
- 3.3.1.2 Registros de componentes de código abierto para el software suministrado que demuestren que se ha seguido correctamente el procedimiento que hay escrito.

Razón fundamental:

Garantizar que existe un proceso para crear y gestionar una lista de materiales de componentes del código abierto utilizados para construir el software suministrado. Se necesita una lista de materiales para apoyar la revisión y aprobación sistemáticas de los términos de la licencia de cada componente para comprender las obligaciones y restricciones que se aplican a la distribución del software suministrado.

3.3.2 Cumplimiento de la licencia

El programa deberá ser capaz de gestionar los casos de uso de licencias de código abierto comunes que encuentren los participantes en el programa para el software suministrado, entre los que pueden figurar los siguientes casos de utilización (obsérvese que la lista no es exhaustiva ni puede aplicarse a todos los casos de utilización):

- Distribuido en forma binaria;

- Distribuido en forma de fuente;
- Integrado con otro código abierto de tal manera que desencadena en obligaciones de licencia adicionales;
- Contiene código abierto modificado;
- Contiene software de código abierto u otro software bajo una licencia incompatible que interactúa con otros componentes dentro del software suministrado; y/o
- Contiene código abierto con requisitos de atribución.

Material(es) de verificación:

- 3.3.2.1 Un procedimiento escrito para gestionar los casos de uso de la licencia de código abierto común para los componentes de código abierto del software suministrado.

Razón fundamental:

Asegurarse de que el programa sea lo suficientemente robusto como para gestionar los casos de uso de licencias de código abierto comunes de una organización. Que exista un procedimiento para apoyar esta actividad y que se siga el procedimiento.

3.4 Creación y entrega de artefactos de cumplimiento

3.4.1 Artefactos de cumplimiento

Se deberá contar con un proceso para crear el conjunto de artefactos de cumplimiento para el software suministrado.

Material(es) de verificación:

- 3.4.1.1 Un procedimiento escrito que describa el proceso de preparación y distribución de los artefactos de cumplimiento con el software suministrado, según lo requerido por las licencias identificadas.
- 3.4.1.2 Un procedimiento escrito para archivar copias de los artefactos de cumplimiento del software suministrado, cuando se prevea que el archivo va a existir durante un período de tiempo[1] razonable desde la última oferta del software suministrado; o según lo requieran las licencias identificadas (el que dure más en el tiempo). Se debe contar con registros que demuestran que el procedimiento se ha seguido correctamente.

Razón fundamental:

Garantizar que se hayan realizado esfuerzos comerciales razonables en la preparación de los artefactos de cumplimiento que acompañan al software suministrado, según lo requieran las licencias identificadas.

3.5 Comprender los compromisos de la comunidad de código abierto

3.5.1 Contribuciones

Si una organización considera la realización de contribuciones a proyectos de código abierto, entonces:

- se deberá contar con una política escrita que rija las contribuciones a los proyectos de código abierto;
- la política deberá comunicarse internamente; y
- se deberá contar con un procedimiento que aplique esa política.

[1]*Determinado por dominio, jurisdicción legal y/o contratos con el cliente*

Material(es) de verificación:

Si una organización permite las contribuciones a los proyectos de código abierto, entonces se deberá contar con:

- 3.5.1.1 Una política escrita de contribución de código abierto;
- 3.5.1.2 Un procedimiento escrito que rija las contribuciones de código abierto; y
- 3.5.1.3 Un procedimiento escrito que haga que todos los participantes en el programa conozcan la existencia de la política de contribución de código abierto (por ejemplo, a través de formación, un wiki interno u otro método de comunicación práctica).

Razón fundamental:

Cuando una organización permite contribuciones de código abierto, la intención es que la organización haya considerado razonablemente la posibilidad de elaborar y aplicar una política de contribuciones. La política de contribuciones de código abierto puede formar parte de la política general de código abierto o ser una política propia independiente.

3.6 Adhesión a los requisitos de las especificaciones

3.6.1 Conformidad

Para que un programa se considere conforme a OpenChain, la organización deberá afirmar que el programa satisface los requisitos presentados en este documento.

Material(es) de verificación:

- 3.6.1.1 Un documento que afirme que el programa especificado en el §3.1.4 satisface todos los requisitos de este documento.

Razón fundamental:

Asegurar que, si una organización declara que tiene un programa que es conforme a OpenChain, dicho programa ha cumplido todos los requisitos de este documento. El mero cumplimiento de un subconjunto de estos requisitos no se considera suficiente.

3.6.2 Duración

Un programa que sea conforme a OpenChain con esta versión de las especificaciones durará 18 meses desde la fecha en que se obtuvo la validación de la conformidad. El procedimiento de registro de la validación de conformidad se puede encontrar en el sitio web del proyecto OpenChain.

Material(es) de verificación:

- 3.6.2.1 Un documento en el que se afirme que el programa cumple todos los requisitos del presente documento, sin haber transcurrido 18 meses desde la obtención de la validación de la conformidad.

Razón fundamental:

Si una organización desea afirmar su conformidad a lo largo del tiempo, es importante que el programa se mantenga al día con las especificaciones. Si una organización continúa afirmando la conformidad del programa a lo largo del tiempo, este requisito asegura que los procesos y controles de apoyo al programa no se erosionan.

Anexo A
(informativo)

Traducciones de estas especificaciones

Con el fin de facilitar la adopción mundial, se acogen con gran satisfacción los esfuerzos por traducir las especificaciones en diferentes idiomas. Dado que OpenChain funciona como un proyecto de código abierto, las traducciones son preparadas por aquellos que están dispuestos a contribuir con su tiempo y experiencia para realizar las traducciones. Las traducciones son i) ofrecidas bajo los términos de la licencia CC-BY-4.0 y ii) consistentes con la política de traducción del proyecto. Los detalles de la política y las traducciones disponibles se pueden encontrar en el proyecto wiki de OpenChain.