Departamento de Seguridad Nacional

Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA)

Instrucciones del formulario de certificación de desarrollo de software seguro

---

Lea todas las instrucciones antes de completar este formulario

---

Declaración de la Ley de Privacidad

[NOTA: *Esta Declaración de la Ley de Privacidad es exclusiva del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés). Todas las agencias que utilicen este formulario común deberán proporcionar una Declaración de la Ley de Privacidad exclusiva de la agencia cuando soliciten utilizarlo. Cada agencia que utilice este formulario común deberá proporcionar Declaraciones de la Ley de Privacidad que se ajusten a los procedimientos y requisitos aplicables de su agencia*].

Autoridad: El párrafo 3554 del Título 44 del Código de los Estados Unidos (USC, por sus siglas en inglés), la Orden Ejecutiva (EO, por sus siglas en inglés) 14028, "Mejora de la ciberseguridad de la nación", y el Memorando M-22-18 de la Oficina de Administración y Presupuesto (OMB, por sus siglas en inglés), "Mejora de la seguridad de la cadena de suministro de software mediante prácticas seguras de desarrollo de software", según la modificación del Memorando M-23-16 de la OMB, "Actualización del Memorando M-22-18, Mejora de la seguridad de la cadena de suministro de software mediante prácticas seguras de desarrollo de software", autorizan la recopilación de esta información.

Objetivo: El propósito de este formulario es brindarle al Gobierno federal garantías de que el software que utilizan las agencias se desarrolla de manera segura.

Contexto: Esta información puede divulgarse según lo permitido de forma general en virtud de la Orden Ejecutiva 14028, Mejora de la ciberseguridad de la nación (EO 14028), y el Memorando M-22-18, "Mejora de la seguridad de la cadena de suministro de software mediante prácticas seguras de desarrollo de software" (M-22-18), en su versión modificada. Este formulario recopila información de contacto de los empleados del proveedor que realizan la certificación. Para el DHS, la información puede divulgarse según sea necesario y autorizado por los usos de rutina publicados en el DHS/ALL-002 Sistema de listas de correo y otras listas del Departamento de Seguridad Nacional (DHS), 25 de noviembre de 2008, 73 FR 71659.

Si no se proporciona la información solicitada, es posible que la agencia deje de utilizar el software en cuestión. Proporcionar intencionalmente información falsa o engañosa puede constituir una violación del párrafo 1001 del Título 18 del USC, un estatuto penal.

¿Cuál es el propósito de completar este formulario?

La Ley Federal de Modernización de la Seguridad de la Información de 2014 (FISMA, por sus siglas en inglés) exige que cada agencia federal proporcione protecciones de seguridad tanto para la "información recopilada o mantenida por una agencia o en su nombre" como para los "sistemas de información utilizados u operados por una agencia o por un contratista de una agencia u otra organización en nombre de una agencia". La FISMA y otras disposiciones de la ley federal autorizan al director de la Oficina de Administración y Presupuesto (OMB) a promulgar estándares de seguridad de la información para sistemas de seguridad de la información, incluso para garantizar el cumplimiento de los estándares promulgados por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés).

La Orden Ejecutiva 14028, "Mejora de la ciberseguridad de la nación" (EO 14028), enfatiza la importancia de proteger el software utilizado por el Gobierno federal para realizar sus funciones críticas. Para promover este objetivo, la EO 14028 exigió al NIST que emitiera una guía para "identificar prácticas que mejoren la seguridad de la cadena de suministro de software".[1] El Marco de desarrollo de software seguro (SSDF, por sus siglas en inglés) del NIST (SP 800-218)[2] y la Guía de seguridad de la cadena de suministro de software del NIST[3] (estos dos documentos, en conjunto, se denominarán en lo sucesivo "Guía del NIST") incluyen un conjunto de prácticas que crean las bases para el desarrollo de software seguro.

La EO 14028 requiere además que el director de la OMB tome las medidas adecuadas para garantizar que las agencias federales cumplan con la Guía del NIST. Para ello, el 14 de septiembre de 2022, la OMB emitió el Memorando M-22-18, "Mejora de la seguridad de la cadena de suministro de software mediante prácticas seguras de desarrollo de software" (M-22-18). Dicho memorando se actualizó el 9 de junio de 2023 mediante el Memorando M-23-16 de la OMB, "Actualización del Memorando M-22-18, Mejora de la seguridad de la cadena de suministro de software mediante prácticas seguras de desarrollo de software" (M-23-16). El M-22-18, según la modificación del M-23-16, establece que una agencia federal puede usar el software sujeto a los requisitos del M-22-18 solo si el productor de ese software ha certificado primero el cumplimiento de las prácticas seguras de desarrollo de software especificadas por el Gobierno federal y extraídas del SSDF.

Este formulario de autocertificación identifica los requisitos mínimos de desarrollo de software seguro que un productor de software debe cumplir, y certificar que cumple, antes de que las agencias federales puedan utilizar el software sujeto a los requisitos del M-22-18 y el M-23-16. Los productores de software utilizan este formulario para certificar que el software que producen se desarrolla de conformidad con prácticas seguras de desarrollo de software específicas.

[1] Executive Order on Improving the Nation's Cybersecurity (E.O. 14028), Section 4(e).
[2] Disponible en https://csrc.nist.gov/Projects/ssdf
[3] Disponible en https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidanceunder-EO-14028-section-4e.pdf

El software requiere autocertificación si se cumple alguna de las siguientes condiciones:

1. El software se desarrolló después del 14 de septiembre de 2022.
2. El software se desarrolló antes del 14 de septiembre de 2022, pero se modificó con cambios importantes de versión (p. ej., usar un esquema de control de versiones semántico de Major.Minor.Patch, el número de versión del software pasa de 2.5 a 3.0) después del 14 de septiembre de 2022.
3. El productor realiza cambios continuos en el código del software (como es el caso de los productos de software como servicio u otros productos que utilizan la entrega o la implementación continua).

Los productos y componentes de software en las siguientes categorías no están dentro del alcance del M-22-18, según la modificación del M-23-16, y no requieren una autocertificación:

1. Software desarrollado por agencias federales.
2. Software de código abierto obtenido libre y directamente por una agencia federal.
3. Componentes patentados y de código abierto de terceros que se incorporan al producto final de software utilizado por la agencia.
4. Software que se obtiene gratuitamente y está disponible de forma pública.

Los productores de software que utilizan componentes de terceros en su software deben certificar que han tomado medidas específicas, detalladas en la "Sección III: Certificación y firma" del formulario común, para minimizar los riesgos de depender de dichos componentes en sus productos.

Se pueden proporcionar instrucciones específicas de la agencia al productor de software fuera de este formulario común. La conformidad con los requisitos específicos de la agencia se puede incluir con este formulario como un anexo. Las agencias son responsables de cumplir con los requisitos de la Ley de Reducción de Trámites aplicables a las adiciones específicas de la agencia.

Si un productor de software no puede enviar el formulario en línea, puede enviar una versión en PDF del formulario por correo electrónico a la agencia respectiva:
Instrucciones del formulario en línea:

☐ Seleccionar la dirección de localizador uniforme de recursos (URL, por sus siglas en inglés) proporcionada: https://softwaresecurity.cisa.gov

O BIEN

Instrucciones del PDF local:

☐ Guardar el formulario completado como PDF usando la siguiente convención de nomenclatura:
Productor de software: nombre del productor de software que fabricó o compiló el producto de software
Nombre del producto: nombre completo del producto de software
Versión: número de versión del producto de software
Fecha de certificación: fecha en que se certificó el producto de software:

p. ej.: [Productor de software]_[Producto]_[Versión]_[Fecha de certificación] →Acme_SecuritySuite_4.6.2.1_20230124
Las agencias individuales proporcionarán sus respectivas direcciones de correo electrónico.

Completar el formulario

Información del productor de software
Proporcione una descripción del software e información sobre su productor. El productor de software debe completar correctamente todos los campos del formulario de certificación. No se aceptarán formularios incompletos.

El formulario debe contener la firma del director ejecutivo (CEO, por sus siglas en inglés) del productor de software o de su persona designada, quien debe ser un empleado del productor de software y tener la autoridad para vincular a la empresa. Con su firma, esa persona certifica que el software en cuestión se desarrolla de conformidad con las prácticas seguras de desarrollo de software delineadas en este formulario. El software puede ser utilizado por una agencia federal, de conformidad con los requisitos del M-22-18, según la modificación del M-23-16, una vez que la agencia haya recibido una copia debidamente firmada del formulario de certificación.

El productor de software puede optar por demostrar la conformidad con los requisitos mínimos presentando una evaluación de un tercero que documente dicha conformidad. La evaluación de terceros debe ser realizada por una organización evaluadora externa (3PAO, por sus siglas en inglés) que haya sido certificada por el Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP, por sus siglas en inglés) o aprobada por escrito por un funcionario de la agencia correspondiente. La 3PAO debe utilizar la Guía del NIST relevante que incluya todos los elementos descritos en este formulario como parte de la referencia de evaluación. Para confiar en una evaluación externa, el productor de software debe marcar la casilla correspondiente en la Sección III y adjuntar la evaluación al formulario. En este caso, no es necesario que el productor firme el formulario. La agencia deberá tomar las medidas adecuadas para garantizar que la evaluación no sea publicada, ni por el proveedor ni por la propia agencia.

Información adicional:
En el caso de que una agencia no pueda obtener una autocertificación completada por parte del productor de software, aún puede decidir utilizar el software del productor si este identifica las prácticas que no puede certificar, documenta las que tiene implementadas para mitigar los riesgos asociados y presenta un plan de acciones e hitos (POA&M, por sus siglas en inglés) a la agencia. Cuando no se proporciona una certificación, según las pautas de la OMB, las agencias son responsables de solicitar a la OMB una extensión o una exención para el uso continuo.

Este formulario común de autocertificación cumple con los requisitos mínimos establecidos por la OMB en el M-22-18, según la modificación del M-23-16.

El formulario de certificación, el contexto y las instrucciones están sujetos a cambios y pueden modificarse.

Formulario de certificación de desarrollo de software seguro

Versión 1.0

Sección I

☐ **Certificación nueva** ☐ **Certificación después de una extensión o exención**
☐ **Certificación revisada**

Tipo de certificación: ☐ Para toda la empresa ☐ Producto individual ☐ Múltiples productos o versiones específicas de productos (proporcione la lista completa)

Si esta certificación es para un producto individual o varios productos, proporcione el nombre del software, el número de versión y la fecha de lanzamiento o publicación a la que se aplica esta certificación. Se pueden adjuntar páginas adicionales a esta certificación si se necesitan más líneas:

Nombre del producto	Número de versión[4] (si corresponde)	Fecha de lanzamiento o publicación (si corresponde)

Para el software especificado anteriormente, este formulario no cubre el software ni ningún componente de ese software que se encuentre en las siguientes categorías:

1. Software desarrollado por agencias federales.
2. Software de código abierto obtenido libre y directamente por una agencia federal.
3. Componentes patentados y de código abierto de terceros que se incorporan al producto final de software utilizado por la agencia.
4. Software que se obtiene gratuitamente y está disponible de forma pública.

Nota: Al firmar esta certificación, los productores de software certifican que cumplen con las prácticas seguras de desarrollo de software descritas en la Sección III para el código desarrollado por el productor.

[4] Las certificaciones son vinculantes para las versiones futuras del producto de software designado, a menos y hasta que el productor de software notifique a las agencias a las que envió previamente el formulario que sus prácticas de desarrollo ya no se ajustan a los elementos requeridos especificados en la certificación.

Sección II

1. Información del productor de software
Nombre de la empresa: _____
Dirección: _____
Ciudad: _____
Estado o provincia: _____
Código postal: _____
País: _____
Sitio web de la empresa: _____

2. Contacto principal para este documento e información relacionada (puede ser una persona, una función o un grupo):
Nombre: _____
Cargo: _____
Dirección: _____
Número de teléfono: _____
Dirección de correo electrónico (puede ser un alias o una lista de distribución): _____

Sección III

Certificación y firma

En nombre de la empresa mencionada anteriormente, certifico que, a mi leal saber y entender, [productor de software] actualmente hace un uso consistente de las siguientes prácticas, derivadas del Marco de desarrollo de software seguro (SSDF),[5] al desarrollar el software identificado en la Sección I:

1) El software se desarrolla y se compila en entornos seguros. Esos entornos están protegidos, como mínimo, mediante las siguientes acciones:

    a) Separar y proteger cada entorno involucrado en el desarrollo y la compilación de software.

    b) Registrar, monitorear y auditar periódicamente las relaciones de confianza utilizadas para la autorización y el acceso:

        i) a cualquier entorno de desarrollo y compilación de software;

        ii) entre componentes dentro de cada entorno.

    c) Hacer cumplir la autenticación multifactor y el acceso condicional en todos los entornos relevantes para el desarrollo y la compilación de software de una manera que minimice el riesgo de seguridad.

[5] El SSDF son estándares y prácticas recomendadas establecidos por el Instituto Nacional de Estándares y Tecnología (NIST) en la Publicación especial (SP, por sus siglas en inglés) 800-218 del NIST.

d) Adoptar medidas consistentes y razonables para documentar y minimizar el uso o la inclusión de productos de software que creen riesgos indebidos en los entornos utilizados para desarrollar y compilar software.

e) Cifrar datos confidenciales, como credenciales, en la medida de lo posible y en función del riesgo.

f) Implementar prácticas defensivas de ciberseguridad, incluido el monitoreo continuo de operaciones y alertas, y, según sea necesario, responder a incidentes cibernéticos sospechados y confirmados.

2) El productor de software hace un esfuerzo de buena fe para mantener cadenas de suministro de código fuente confiables mediante el empleo de herramientas automatizadas o de procesos comparables para abordar la seguridad del código interno y de los componentes de terceros, y para gestionar las vulnerabilidades relacionadas.

3) El productor de software mantiene la procedencia del código interno y de los componentes de terceros incorporados al software en la mayor medida posible.

4) El productor de software emplea herramientas automatizadas o procesos comparables que buscan vulnerabilidades de seguridad. Además:
   a) El productor de software opera estos procesos de forma continua y antes del lanzamiento del producto, de la versión o de la actualización.
   b) El productor de software tiene una política o un proceso para abordar las vulnerabilidades de seguridad descubiertas antes del lanzamiento del producto.
   c) El productor de software opera un programa de divulgación de vulnerabilidades y acepta, revisa y aborda las vulnerabilidades de software divulgadas de manera oportuna y de acuerdo con los plazos especificados en el programa de divulgación de vulnerabilidades o las políticas aplicables.

☐ Además, certifico que el productor de software notificará a cualquier agencia a la que haya enviado este formulario si deja de hacer un uso consistente de las prácticas identificadas anteriormente en el desarrollo del software.

Firma del CEO o de su persona designada con autoridad para vincular a la empresa

_____

Fecha (AAAA-MM-DD): _____
Nombre: _____
Cargo: _____

O BIEN

☐ Una organización evaluadora externa (3PAO) certificada por el FedRAMP u otra 3PAO aprobada por escrito por un funcionario de la agencia correspondiente ha evaluado nuestro cumplimiento de todos los elementos de este formulario. La 3PAO utilizó la Guía del NIST

relevante que incluye todos los elementos descritos en este formulario como la referencia de evaluación. Se adjunta la evaluación.

ARCHIVOS ADJUNTOS:

- **[Título del objeto/anexo]:** [Descripción del objeto/anexo]

Declaración de carga

La carga de presentación de informes públicos para completar esta recopilación de información se estima en **3 horas y 20 minutos** por respuesta, incluido el tiempo para revisar las instrucciones, buscar fuentes de datos, recopilar y mantener los datos necesarios, y completar y revisar la recopilación de información. Una agencia no puede realizar ni patrocinar, y una persona no está obligada a responder, una recopilación de información, a menos que muestre un número de control de la OMB y una fecha de vencimiento actualmente válidos. El número de control de la OMB asignado a esta recopilación es 1670-0052, el cual vence el 03/31/2027. Envíe comentarios sobre esta estimación de carga o cualquier otro aspecto de esta recopilación de información, incluidas las sugerencias para reducir esta carga, a la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) del DHS al correo electrónico **CSCRM@cisa.dhs.gov.** ATTN: PRA 1670-0052 Secure Software Self-Attestation Common Form.

APÉNDICE
REFERENCIAS

Referencias mínimas de certificación:
Los requisitos mínimos dentro del Formulario de certificación de software seguro abordan los requisitos establecidos en la subsección (4)(e) de la EO 14028. Se proporciona una asignación a prácticas y tareas específicas del SSDF a modo de referencia.

Requisitos de certificación	**Subsección de la EO 14028 relacionada**		**Prácticas y tareas del SSDF relacionadas**
1) El software se desarrolla y se compila en entornos seguros. Esos entornos están protegidos, como mínimo, mediante las siguientes acciones:	4e(i)		[Ver las siguientes filas]
a) Separar y proteger cada entorno involucrado en el desarrollo y la compilación de software.	4e(i)(A)		PO.5.1
b) Registrar, monitorear y auditar periódicamente las relaciones de confianza utilizadas para la autorización y el acceso: i) a cualquier entorno de desarrollo y compilación de software; ii) entre componentes dentro de cada entorno.	4e(i)(B)		PO.5.1
c) Hacer cumplir la autenticación multifactor y el acceso condicional en todos los entornos relevantes para el desarrollo y la compilación de software de una manera que minimice el riesgo de seguridad.	4e(i)(C)		PO.5.1, PO.5.2
d) Adoptar medidas consistentes y razonables para documentar y minimizar el uso o la inclusión de productos de software que creen riesgos indebidos en los entornos utilizados para desarrollar y compilar software.	4e(i)(D)		PO.5.1

e) Cifrar datos confidenciales, como credenciales, en la medida de lo posible y en función del riesgo.	4e(i)(E)		PO.5.2
f) Implementar prácticas defensivas de ciberseguridad, incluido el monitoreo continuo de operaciones y alertas, y, según sea necesario, responder a incidentes cibernéticos sospechados y confirmados.	4e(i)(F)		PO.3.2, PO.3.3, PO.5.1, PO.5.2
2) El productor de software hace un esfuerzo de buena fe para mantener cadenas de suministro de código fuente confiables mediante el empleo de herramientas automatizadas o de procesos comparables para abordar la seguridad del código interno y de los componentes de terceros, y para gestionar las vulnerabilidades relacionadas.	4e(iii)		PO.1.1, PO.3.1, PO.3.2, PO.5.1, PO.5.2, PS.1.1, PS.2.1, PS.3.1, PW.4.1, PW.4.4, PW.7.1, PW.8.1, RV.1.1
3) El productor de software mantiene la procedencia del código interno y de los componentes de terceros incorporados al software en la mayor medida posible.	4e(vi)		PO.1.3, PO.3.2, PO.5.1, PO.5.2, PS.3.1, PS.3.2, PW.4.1, PW.4.4, RV.1.1, RV.1.2
4) El productor de software empleó herramientas automatizadas o procesos comparables que buscan vulnerabilidades de seguridad. Además: a) El productor de software opera estos procesos de forma continua y antes del lanzamiento del producto, de la versión o de la actualización. b) El productor de software tiene una política o un proceso para abordar las vulnerabilidades de seguridad descubiertas antes del lanzamiento del producto. c) El productor de software opera un programa de divulgación de vulnerabilidades y acepta, revisa y aborda las vulnerabilidades de software divulgadas de manera oportuna y de acuerdo con los plazos especificados en el programa de divulgación de vulnerabilidades o las políticas aplicables.	4e(iv)		PO.4.1, PO.4.2, PS.1.1, PW.2.1, PW.4.4, PW.5.1, PW.6.1, PW.6.2, PW.7.1, PW.7.2, PW.8.2, PW.9.1, PW.9.2, RV.1.1, RV.1.2, RV.1.3, RV.2.1, RV.2.2, RV.3.3