TLP:CLEAR


## CAMBIAR EL EQUILIBRO DEL

# RIESGO DE LA CIBERSEGURIDAD:

PRINCIPIOS Y ENFOQUES PARA UN SOFTWARE SEGURO DESDE EL DISEÑO

TLP:CLEAR




Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Federal Office for Information Security

Communications Security Establishment
**Canadian Centre for Cyber Security**

Centre de la sécurité des télécommunications
**Centre canadien pour la cybersécurité**


National Cyber Security Centre
*Ministry of Justice and Security*










# Índice

# DESCRIPCIÓN GENERAL: VULNERABLE DESDE EL DISEÑO

La tecnología está integrada en casi todas las facetas de la vida diaria, ya que los sistemas orientados a Internet nos conectan cada vez más con sistemas críticos que impactan directamente en nuestra prosperidad económica, nuestros medios de vida e incluso en nuestra salud, desde la gestión de la identidad personal hasta la atención médica. Un ejemplo de la desventaja de tales comodidades son las vulneraciones de seguridad cibernética a nivel mundial que provocan que los hospitales cancelen cirugías y deriven la atención a los pacientes. La tecnología insegura y las vulnerabilidades en los sistemas críticos pueden provocar intrusiones cibernéticas maliciosas, lo que genera posibles riesgos para la seguridad[1].

Como resultado, es crucial que los fabricantes de software hagan que los puntos focales de los procesos de diseño y desarrollo de productos sean seguros desde el diseño y seguros por defecto. Algunos proveedores han logrado grandes avances y han impulsado la industria en materia de garantía de software, mientras que otros continúan rezagados. Las organizaciones autoras alientan encarecidamente a todos los fabricantes de tecnología a crear sus productos basándose en la reducción de la carga de la ciberseguridad sobre los clientes, lo que incluye evitar que tengan que realizar monitoreos constantes, actualizaciones de rutina y control de daños en sus sistemas para mitigar las intrusiones cibernéticas. También instamos a los fabricantes de software a que desarrollen sus productos de una manera que facilite la automatización de la configuración, el monitoreo y las actualizaciones de rutina. Se anima a los fabricantes a asumir la responsabilidad de mejorar los resultados de seguridad de sus clientes. Históricamente, los fabricantes de software han recurrido a la corrección de las vulnerabilidades encontradas después de la implementación de los productos por parte de los clientes, y esto ha obligado a los clientes a aplicar esos parches por su cuenta. Simplemente incorporando prácticas de seguridad desde el diseño romperemos el círculo vicioso de crear y aplicar parches constantemente. **Nota:** el término “seguro desde el diseño” abarca tanto la seguridad desde el diseño como la seguridad por defecto.

Para lograr este alto estándar de seguridad de software, las organizaciones autoras alientan a los fabricantes a priorizar la integración de la seguridad del producto como un requisito previo crítico para las características y la velocidad de comercialización. Con el tiempo, los equipos de ingeniería podrán establecer un nuevo ritmo estable en el que la seguridad esté realmente integrada y requiera menos esfuerzo para mantenerla.

Como reflejo de esta perspectiva, la Unión Europea refuerza la importancia de la seguridad de los productos en la Ley de Resiliencia Cibernética, que enfatiza que los fabricantes deben implementar seguridad durante todo el ciclo de vida de un producto para evitar que los fabricantes introduzcan productos vulnerables en el mercado.

Para crear un futuro en el que la tecnología y los productos asociados sean más seguros para los clientes, las organizaciones autoras instan a los fabricantes a renovar sus programas de diseño y

[1] Las organizaciones autoras reconocen que el término “seguridad” tiene múltiples significados según el contexto. A los efectos de esta guía, “seguridad” se referirá a elevar los estándares de seguridad tecnológica para proteger a los clientes de actividades cibernéticas maliciosas.

desarrollo para permitir únicamente el envío de productos seguros desde el diseño y por defecto. Mucho antes del desarrollo, los productos que son seguros desde el diseño se conceptualizan con la seguridad de los clientes como un objetivo comercial central, no solo una característica técnica. Los productos seguros desde el diseño comienzan con ese objetivo antes de que comience el desarrollo. Los productos existentes pueden evolucionar hasta llegar a ser seguros desde el diseño a lo largo de múltiples iteraciones. Los productos seguros por defecto son aquellos productos "listos para usar" y que requieren pocos o ningún cambio de configuración para un uso seguro y tienen funciones de seguridad disponibles sin costo adicional. Juntas, estas dos filosofías trasladan gran parte de la carga de mantener la seguridad a los fabricantes y reducen las posibilidades de que los clientes sean víctimas de incidentes de seguridad resultantes de configuraciones erróneas, aplicaciones de parches insuficientemente rápidas por parte de los clientes o muchos otros problemas comunes.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (Cybersecurity and Infrastructure Security Agency, CISA), la Agencia de Seguridad Nacional (National Security Agency, NSA), la Oficina Federal de Investigaciones (Federal Bureau of Investigation, FBI) y los siguientes socios internacionales[2] brindan las recomendaciones en esta guía como una hoja de ruta para que los fabricantes de software garanticen la seguridad de sus productos:

- Centro Australiano de Seguridad Cibernética (Australian Cyber Security Centre, ACSC)
- Centro Canadiense de Seguridad Cibernética (Canadian Centre for Cyber Security, CCCS)
- Centro Nacional de Seguridad Cibernética del Reino Unido (United Kingdom's National Cyber Security Centre, NCSC-UK)
- Oficina Federal de Seguridad de la Información (BSI) de Alemania
- Centro Nacional de Seguridad Cibernética de los Países Bajos (NCSC-NL)
- Centro Nacional de Seguridad Cibernética de Noruega (NCSC-NO)
- Equipo de respuesta a emergencias informáticas de Nueva Zelanda (Computer Emergency Response Team New Zealand, CERT NZ) y Centro Nacional de Seguridad Cibernética de Nueva Zelanda (New Zealand's National Cyber Security Centre, NCSC-NZ)
- Agencia de Seguridad & Internet de Corea (KISA)
- Dirección Nacional de Cibernética de Israel (INCD)
- Centro Nacional de Preparación para Incidentes y Estrategia de Ciberseguridad (NISC) de Japón y Centro de Coordinación del Equipo de Respuesta a Emergencias Informáticas de Japón (JPCERT/CC)
- OAS/CICTE Red de Equipos Gubernamentales de Respuesta a Incidentes Cibernéticos (CSIRT) de las Américas
- Agencia de Seguridad Cibernética de Singapur (CSA)
- Agencia Nacional de Seguridad Cibernética y de la Información de la República Checa (NÚKIB)

Las organizaciones autoras reconocen las contribuciones de muchos socios del sector privado para promover la seguridad desde el diseño y la seguridad por defecto. Este producto tiene como objetivo promover una conversación internacional sobre prioridades, inversiones y decisiones clave necesarias para lograr un futuro donde la tecnología sea segura y resistente desde el diseño y por defecto. Con ese fin, las organizaciones autoras buscan comentarios sobre este producto de las partes interesadas y tienen la intención de convocar una serie de sesiones de escucha para perfeccionar, especificar y avanzar en nuestra orientación para lograr nuestros objetivos comunes.

Para obtener más información sobre la importancia de la seguridad de los productos, consulte el artículo de CISA, El costo de la tecnología insegura y qué podemos hacer al respecto.

[2] En adelante denominadas "organizaciones autoras".

# NOVEDADES

La publicación inicial de este informe generó una importante cantidad de conversaciones dentro de la industria del software. Las noticias diarias sobre organizaciones e individuos comprometidos resaltan la necesidad de una mayor conversación sobre cómo abordar los problemas crónicos y sistémicos en los productos de software.

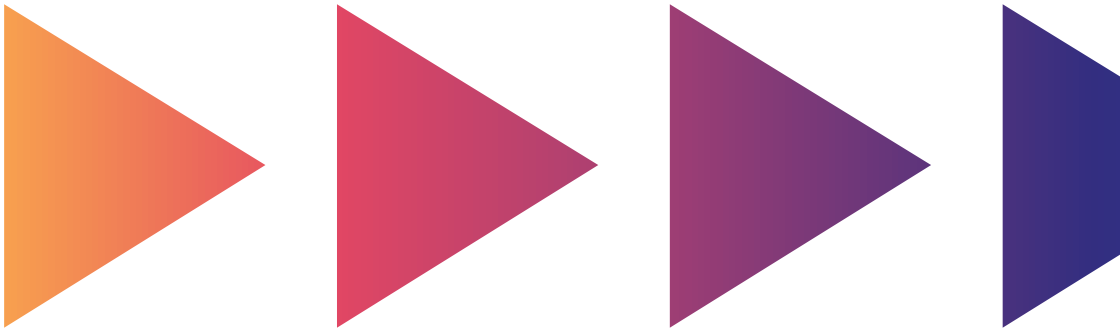
Después del lanzamiento en abril de 2023, las organizaciones autoras (en adelante denominadas "nosotros" y "nuestro") recibieron comentarios certeros de cientos de personas, empresas y asociaciones comerciales. La solicitud más común en los comentarios fue la de proporcionar más detalles sobre los tres principios que se aplican tanto a los fabricantes de software como a sus clientes. En este documento, ampliamos el informe original y abordamos otros temas como el tamaño del fabricante y del cliente, la madurez del cliente y el alcance de los principios.

El software está en todas partes y ningún informe podrá cubrir adecuadamente toda la gama de sistemas de software, el desarrollo de productos de software, la implementación y el mantenimiento del cliente y la integración con otros sistemas. Como orientación, que no se corresponda claramente con un entorno en particular, esperamos escuchar de la comunidad cómo las prácticas descritas en este documento condujeron a mejoras de seguridad particulares.

Este informe también se aplica a los fabricantes de sistemas y modelos de software de inteligencia artificial (artificial intelligence, AI). Si bien pueden diferir de las formas tradicionales de software, las prácticas de seguridad fundamentales aún se aplican a los sistemas y modelos de AI. Es posible que algunas prácticas de seguridad desde el diseño necesiten modificaciones para tener en cuenta consideraciones específicas de la AI, pero los tres principios generales de seguridad por diseño se aplican a todos los sistemas de AI.

Reconocemos que transformar un ciclo de vida de desarrollo de software (software development lifecycle, SDLC) para alinearlo con estos principios de "seguro desde el diseño" no es una tarea sencilla y puede llevar tiempo. Además, los fabricantes de software más pequeños pueden tener dificultades para implementar muchas de estas sugerencias. Creemos que la industria del software necesita hacer que las herramientas y los procedimientos que hacen que los productos sean más seguros estén ampliamente disponibles. A medida que más personas y organizaciones centran su atención en las mejoras de seguridad del software, creemos que hay espacio para innovaciones que reducirán la brecha entre los fabricantes de software más grandes y más pequeños, en beneficio de todos los clientes.

Esta actualización del informe original de seguridad desde el diseño es parte de nuestro compromiso de construir asociaciones con las muchas comunidades de partes interesadas interconectadas que sustentan nuestro ecosistema tecnológico. Es el resultado de la retroalimentación de muchas partes de ese ecosistema, y continuaremos escuchando y aprendiendo a partir de las diferentes perspectivas. Si bien hay muchos desafíos por delante, somos increíblemente optimistas a medida que aprendemos más sobre personas y organizaciones que ya han adoptado una filosofía de diseño seguro, a menudo con éxito.



# CÓMO UTILIZAR ESTE DOCUMENTO

Instamos a los fabricantes de software a que cumplan los principios contenidos en este documento. Los fabricantes de software pueden demostrar su compromiso documentando públicamente las acciones que han tomado, de acuerdo con los pasos que se enumeran a continuación. Alentamos a los fabricantes de software a encontrar tácticas que cumplan con el espíritu de estos principios y a crear artefactos que convenzan, incluso a clientes actual y posiblemente escépticos, de que están incorporando la filosofía de seguridad desde el diseño.

Además de las acciones que deben tomar los fabricantes de software, los clientes también pueden aprovechar este documento. Las empresas que compran software deben hacer preguntas difíciles a sus proveedores, inspirándose en los ejemplos de cumplimiento de los principios enumerados en este documento. Al hacerlo, los clientes pueden ayudar a orientar al mercado hacia productos que sean más seguros desde el diseño. Un ejemplo de preguntas que los clientes pueden hacer a los proveedores se proporciona en la Guía de CISA para adquisiciones de tecnología para K-12.

Alentamos a los clientes empresariales a incorporar estas prácticas en los procesos de adquisiciones, evaluaciones de diligencia debida de proveedores, decisiones de aceptación de riesgos empresariales y otras medidas tomadas al evaluar proveedores. Los clientes también deben presionar a sus proveedores para que documenten públicamente las acciones de seguridad desde el diseño que realiza cada proveedor. En conjunto, esto puede crear una fuerte señal de demanda de seguridad, que puede alentar y permitir a los fabricantes de software tomar medidas hacia una mayor seguridad. En otras palabras, así como buscamos crear una filosofía generalizada de seguridad desde el diseño entre los fabricantes de software, necesitamos crear una cultura de “seguridad por demanda” con sus clientes.

# Seguridad desde el diseño

"Seguro desde el diseño" significa que los productos tecnológicos se construyen de manera que protejan razonablemente contra ciberataques maliciosos que logran acceder a dispositivos, datos e infraestructura conectada. Los fabricantes de software deben realizar una evaluación de riesgos para identificar y enumerar las amenazas cibernéticas prevalentes de los sistemas críticos y luego incluir protecciones en los modelos de productos que tengan en cuenta el panorama en evolución de las amenazas cibernéticas.

También se recomiendan prácticas seguras de desarrollo de tecnología de la información (information technology, IT) y múltiples capas de defensa, conocidas como defensa en profundidad, para evitar que actores malintencionados comprometan los sistemas u obtengan acceso no autorizado a datos confidenciales. Las organizaciones autoras recomiendan además que los fabricantes utilicen un modelo de amenazas personalizado durante la etapa de desarrollo del producto para abordar todas las amenazas potenciales a un sistema y tener en cuenta el proceso de implementación de cada sistema.

Las organizaciones autoras instan a los fabricantes a adoptar un enfoque de seguridad integral para sus productos y plataformas. El desarrollo seguro desde el diseño requiere la inversión estratégica de recursos dedicados por parte de los fabricantes de software en cada capa del proceso de diseño y desarrollo del producto que no se pueden "integrar" más adelante. Se requiere un fuerte liderazgo por parte de los principales ejecutivos del fabricante para hacer de la seguridad una prioridad empresarial, no solo una característica técnica. Esta colaboración entre líderes empresariales y equipos técnicos se extiende desde las etapas preliminares de diseño y desarrollo hasta la implementación y el mantenimiento una vez que el producto está en manos del cliente. Se alienta a los fabricantes a hacer concesiones e inversiones difíciles, incluidas aquellas que serán "invisibles" para los clientes (por ejemplo, migrar a lenguajes de programación que eliminen vulnerabilidades generalizadas). Deberían priorizar las características, los mecanismos y la implementación de herramientas que protejan a los clientes en lugar de las características del producto que parecen atractivas, pero amplían la superficie de ataque.

No existe una solución única para poner fin a la amenaza persistente de los actores cibernéticos maliciosos que explotan las vulnerabilidades tecnológicas, y los productos que son "seguros desde el diseño" seguirán sufriendo vulnerabilidades; sin embargo, un gran conjunto de vulnerabilidades se debe a un subconjunto relativamente pequeño de causas fundamentales. Los fabricantes deben desarrollar hojas de ruta escritas para alinear sus carteras de productos existentes con prácticas de diseño más seguras, asegurándose de desviarse solo en situaciones excepcionales.

Las organizaciones autoras reconocen que apropiarse de los resultados de seguridad para los clientes y garantizar este nivel de seguridad del cliente puede aumentar los costos de desarrollo. Sin embargo, invertir en prácticas seguras desde el diseño mientras se desarrollan productos tecnológicos innovadores y se mantienen los existentes puede mejorar sustancialmente la postura de seguridad de los clientes y reducir la probabilidad de compromiso. Los principios de seguridad desde el diseño no solo fortalecen la postura de seguridad para los clientes y la reputación de la marca para los desarrolladores, sino que la práctica también reduce los costos de mantenimiento y parches para los fabricantes a largo plazo.

La sección Recomendaciones para fabricantes de software que se enumera a continuación proporciona una lista de prácticas y políticas de desarrollo de productos que los fabricantes deben considerar.

# Seguro por defecto

"Seguro por defecto" significa que los productos son resistentes a las técnicas de explotación predominantes desde el primer momento y sin cargo adicional. Estos productos protegen contra las amenazas y vulnerabilidades más frecuentes sin que los usuarios finales tengan que tomar medidas adicionales para protegerse. Los productos seguros por defecto están diseñados para que los clientes sean plenamente conscientes de que cuando se desvían de los valores predeterminados seguros, aumentan la probabilidad de ataques, a menos que implementen controles compensatorios adicionales. La seguridad por defecto es una forma de seguridad desde el diseño.

- Una configuración segura debe ser la base predeterminada. Los productos seguros por defecto habilitan automáticamente los controles de seguridad más importantes necesarios para proteger a las empresas de actores cibernéticos maliciosos, además de brindar la capacidad de usar y configurar controles de seguridad adicionales sin costo adicional.
- La complejidad de la configuración de seguridad no debería ser un problema para el cliente. El personal de IT de la organización con frecuencia está sobrecargado con responsabilidades operativas y de seguridad, lo que resulta en un tiempo limitado para comprender e implementar las implicaciones de seguridad y las mitigaciones necesarias para una postura sólida de ciberseguridad. Los fabricantes pueden ayudar a sus clientes optimizando la configuración segura de sus productos (asegurando la "ruta predeterminada"), garantizando que sus productos se fabriquen, distribuyan y utilicen de forma segura de acuerdo con los estándares "seguros por defecto".

Los fabricantes de productos que son "seguros por defecto" no cobran más por implementar configuraciones de seguridad adicionales. En cambio, las incluyen en el producto base, como se incluyen los cinturones de seguridad en todos los automóviles nuevos.

***La seguridad no debe ser una opción de lujo, sino que debe considerarse un derecho que los clientes reciben sin negociar ni pagar más.***

## RECOMENDACIONES PARA FABRICANTES DE SOFTWARE

Esta guía conjunta proporciona recomendaciones a los fabricantes para desarrollar una hoja de ruta escrita para implementar y garantizar la seguridad de IT. Las organizaciones autoras recomiendan que los fabricantes de software implementen las estrategias descritas en las secciones siguientes para apropiarse de los resultados de seguridad de sus clientes a través de principios de seguridad desde el diseño y por defecto.

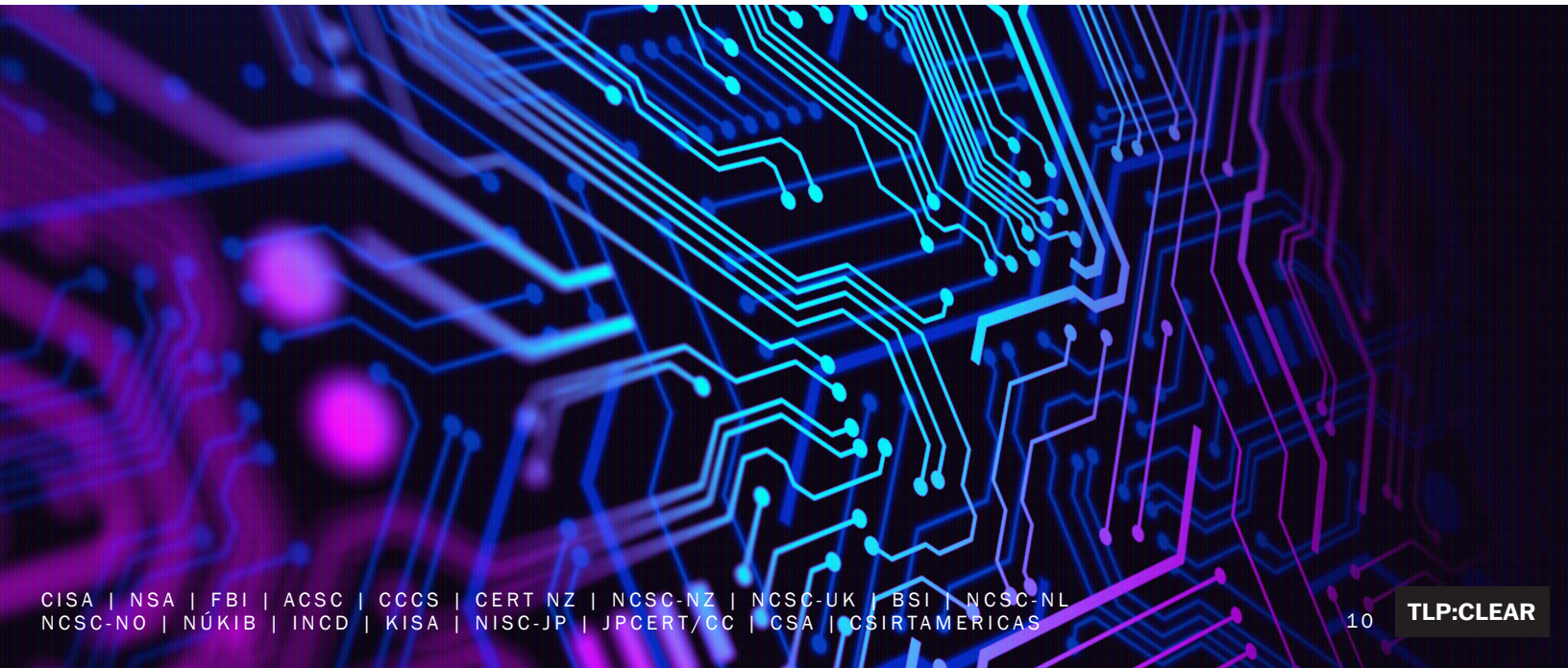
# PRINCIPIOS DE SEGURIDAD PARA PRODUCTOS DE SOFTWARE

Se anima a los fabricantes de software a adoptar un enfoque estratégico que priorice la seguridad del software. Las organizaciones autoras desarrollaron los siguientes tres principios básicos para guiar a los fabricantes de software a la hora de incorporar la seguridad del software en sus procesos de diseño antes del desarrollo, la configuración y el envío de sus productos.

1. **Asumir los resultados del cliente en materia de seguridad** y desarrollar productos en consecuencia. La carga de la seguridad no debe recaer únicamente en el cliente.

2. **Adoptar métodos radicales de transparencia y rendición de cuentas.** Los fabricantes de software deben enorgullecerse de ofrecer productos seguros, además de diferenciarse del resto de la comunidad de fabricantes en función de su capacidad para hacerlo. Esto puede incluir compartir información que aprenden de las implementaciones de sus clientes, como la adopción de mecanismos de autenticación sólidos de forma predeterminada. También incluye un fuerte compromiso para garantizar que los asesoramientos de vulnerabilidad y los registros de exposiciones y vulnerabilidades comunes (common vulnerability and exposure, CVE) asociados sean completos y precisos. Sin embargo, se debe tener cuidado con la tentación de considerar los CVE como una métrica negativa, ya que dichos números también son una señal de una comunidad saludable de análisis y pruebas de código.

3. **Construir estructura organizacional y liderazgo para lograr estos objetivos.** Si bien la experiencia técnica en la materia es fundamental para la seguridad del producto, los ejecutivos sénior son los principales tomadores de decisiones para implementar cambios en una organización. Los ejecutivos deben priorizar la seguridad como un elemento crítico del desarrollo de productos en toda la organización y en asociación con los clientes.



Para habilitar estos tres principios, los fabricantes deberían considerar varias tácticas operativas para hacer evolucionar sus procesos de desarrollo.

Convoque reuniones de rutina con el liderazgo ejecutivo de la empresa para impulsar la importancia de la seguridad desde el diseño y la seguridad por defecto dentro de la organización. Se deben establecer políticas y procedimientos para recompensar a los equipos de producción que desarrollen productos que cumplan con estos principios, lo que podría incluir premios por implementar prácticas sobresalientes de seguridad de software o incentivos para escalar puestos y criterios de promoción.

Opere en torno a la importancia de la seguridad del software para el éxito empresarial. Por ejemplo, considere asignar un "líder de seguridad de software" o un "equipo de seguridad de software" que defienda las prácticas comerciales y de IT que vinculen directamente los estándares de seguridad del software y la responsabilidad del fabricante. Los fabricantes deben asegurarse de contar con programas sólidos e independientes de evaluación y evaluación de la seguridad de sus productos.

Utilice un modelo de amenazas personalizado durante la asignación y el desarrollo de recursos para priorizar las características más críticas y de alto impacto. Los modelos de amenazas consideran el caso de uso específico de un producto y permiten a los equipos de desarrollo fortalecer los productos. Finalmente, los líderes sénior deben responsabilizar a los equipos por la entrega de productos seguros como elemento clave de la excelencia y la calidad del producto.

Como parte de la actualización de octubre de 2023 de esta guía, estos tres principios se amplían a través de las siguientes explicaciones, demostraciones y evidencia.

# **PRINCIPIO 1:** Asumir los resultados del cliente en materia de seguridad

### EXPLICACIÓN

Las prácticas recomendadas modernas dictan que los fabricantes de software deben invertir en esfuerzos de seguridad de productos que incluyan **el refuerzo de las aplicaciones, las características de las aplicaciones** y **la configuración predeterminada de las aplicaciones.**

Los fabricantes de software deben implementar **el refuerzo de las aplicaciones** mediante el uso de procesos y tecnologías que aumenten el costo para un actor malintencionado que desee comprometerlas. Los protocolos y procedimientos de refuerzo de aplicaciones ayudan a los productos a resistir ataques de actores maliciosos inteligentes. Términos como refuerzo, seguridad del producto y resiliencia están estrechamente relacionados con la calidad del producto. La idea es que la seguridad debe estar "integrada" y no "añadida". [1] Al integrar la seguridad, los fabricantes de software no solo pueden aumentar la seguridad de sus clientes sino también la calidad de sus productos. Las tácticas de ejemplo incluyen garantizar que lo que el usuario ingrese pueda validarse y limpiarse, y que no se ingrese directamente en el código (es decir, mediante el uso de consultas parametrizadas en su lugar), mediante un lenguaje de programación seguro para la memoria, con una gestión rigurosa del ciclo de vida del desarrollo de software (SDLC) y una gestión de claves criptográfica con respaldo de hardware.

Las aplicaciones deben ser compatibles con **características de las aplicaciones** relacionadas con la ciberseguridad. A veces denominadas "capacidades", estas características amplían la funcionalidad de un producto o servicio de manera que ayudan a mantener o aumentar la postura de seguridad de un cliente. Las características de ejemplo relacionadas con la seguridad incluyen la compatibilidad con la seguridad de la capa de

transporte (transport layer security, TLS) para todas las conexiones de red, la compatibilidad con el inicio de sesión único (single sign on, SSO), la compatibilidad con la autenticación multifactor (multifactor authentication, MFA), el registro de auditoría de eventos de seguridad, el control de acceso basado en roles (role-based access control, RBAC) y el control de acceso basado en atributos (attribute-based access control, ABAC).

Algunas de estas características del producto son configurables, lo que permite a los clientes integrar más fácilmente el producto en sus entornos y flujos de trabajo existentes. Esas configuraciones significan que las aplicaciones deben tener **configuraciones predeterminadas** establecidas hasta que los clientes las configuren. Esas configuraciones predeterminadas deben establecerse de forma segura "listas para usar" para que los clientes gasten menos recursos para hacer que su conjunto de productos tecnológicos sea más seguro.

Cada uno de estos elementos (refuerzo de la aplicación, características de seguridad de la aplicación y configuración predeterminada de la aplicación) desempeña un papel en la seguridad de la aplicación y en la postura de seguridad resultante del cliente. Los fabricantes de software deberían pensar en cada uno de estos elementos y cómo se relacionan entre sí. Los fabricantes deberían pensar en algo más que en inversiones para incorporar estos elementos a sus productos. Los fabricantes deberían ir un paso más allá y considerar cómo esos elementos cambian la postura de seguridad de sus clientes en el mundo real, para bien o para mal.

Los fabricantes deberían responsabilizarse de los resultados de seguridad de sus clientes en lugar de medirse únicamente por sus esfuerzos e inversiones. La responsabilidad debería recaer en los fabricantes, donde existe la mayor probabilidad de reducir las posibilidades de compromiso.

Lamentablemente, hoy en día este no es el caso. Demasiados fabricantes imponen la carga de la seguridad al cliente en lugar de invertir en **un refuerzo integral de las aplicaciones.** Por ejemplo, cuando el fabricante coloca un parche sobre una vulnerabilidad, a menudo vemos vulnerabilidades similares expuestas porque abordaron el síntoma en lugar de la causa raíz de ese defecto. El producto podría implementar diferentes medidas de mitigación en varias partes del código base para la misma clase de vulnerabilidad. Como ejemplo, después de que el fabricante solucionó una vulnerabilidad de limpieza de datos de entrada, los investigadores o atacantes encontraron rutas de código que no se beneficiaron de la limpieza mejorada de los datos de entrada. El fabricante aplicó las correcciones una a la vez, en lugar de unificar el código base para eliminar esa clase de vulnerabilidad en toda la aplicación.

**Las características de la aplicación** pueden generar tanto beneficios como riesgos para los clientes. Las funciones que permiten puntos de integración con muchos sistemas y versiones externos pueden aumentar considerablemente el valor de un producto. Y, sin embargo, admitir funciones sin un plan para el final de la vida útil del producto, como un protocolo de red, puede dejar a los clientes vulnerables si no comprenden las implicaciones del uso continuo de esa función. Por ejemplo, algunos productos continúan utilizando protocolos de red que tienen sus orígenes en las décadas de 1990 o 2000 y que ahora se sabe que no son seguros. Existen numerosos factores que pueden ralentizar la rapidez con la que los clientes actualizan e implementan medidas de seguridad modernas. Es posible que utilicen productos que se integran con el resto de la red de la organización, pero carecen de medidas de seguridad modernas, lo que impide que el equipo de IT se modernice. Aun así, los fabricantes de software pueden tener en cuenta estos patrones en su proceso de planificación para alentar a los clientes a mantenerse actualizados.

**La configuración predeterminada de la aplicación** es un área adicional de posible riesgo para los clientes. Los fabricantes suelen elegir ciertas configuraciones predeterminadas, lo que facilita a los clientes el uso de las funciones de la aplicación que desean. La desventaja es que esta práctica aumenta la superficie de ataque para los clientes que tal vez no necesiten ciertas funciones y protocolos habilitados de forma predeterminada. Además, muchos controles de seguridad están desactivados de forma predeterminada o requieren que los clientes se tomen un tiempo para configurar sus ajustes para aumentar la seguridad. El modelado explícito de amenazas es una táctica que puede ayudar a informar la decisión sobre qué funciones deben activarse de forma predeterminada o qué configuraciones son necesarias para ser seguras de forma predeterminada. Otra táctica es investigar formas de hacer que las funciones sean más visibles para el administrador.

Algunos fabricantes envían productos con valores predeterminados que pueden generar riesgos para algunos o todos sus clientes. En lugar de establecer valores predeterminados más seguros, a menudo optan por producir una **guía de refuerzo** que los clientes deben implementar por su propia cuenta. Las guías de refuerzo sufren varios problemas comunes. Algunas guías de refuerzo son difíciles de encontrar y no cuentan con el soporte adecuado. Otras son complejas de implementar y en ocasiones requieren desarrollo de software para escribir un módulo de extensión. Aun así, otros suponen que el lector tiene una amplia experiencia en ciberseguridad para comprender las formas en que diversas configuraciones cambian la superficie de ataque. Los usuarios que no comprenden completamente las formas en que trabajan los atacantes pueden no implementar adecuadamente las instrucciones de la guía de refuerzo, especialmente si las instrucciones no aclaran las ventajas y desventajas. Además, no todas las guías de refuerzo están escritas por ingenieros que estén íntimamente familiarizados con las tácticas y la economía de los atacantes, lo que les lleva a crear guías de refuerzo que son ineficaces incluso si se implementan fielmente. Millones de clientes asumen la responsabilidad de reforzar múltiples instancias de software o sistemas, a menudo en entornos con recursos limitados. Depender de las guías de refuerzo simplemente no es un modelo escalable.

La configuración de una aplicación debe evaluarse continuamente, ya sea que sea la predeterminada o la haya establecido el cliente, en comparación con la comprensión actual del fabricante sobre el panorama de amenazas. Las aplicaciones deben realizarse con indicadores claros sobre los posibles riesgos que pueden resultar de esos entornos y deben dar a conocer esos indicadores. Así como un automóvil moderno tiene un indicador sobre los cinturones de seguridad y expresa ese indicador haciendo sonar una alerta si alguien intenta conducir sin abrocharse el cinturón, el software debería expresar indicadores sobre el estado de seguridad de un sistema. Si una aplicación está configurada para no requerir MFA para las cuentas de administrador, los administradores deberían recibir recordatorios periódicos de que ellos y toda su organización están en peligro si no configuran una MFA. Además, si una aplicación está configurada para admitir protocolos más antiguos, que ahora se sabe que implementan criptografía débil, se les debe aclarar periódicamente a los administradores que la organización está en peligro y proporcionar recursos para resolver la situación. Instamos a los fabricantes a implementar recordatorios de rutina integrados en el producto, en lugar de depender de que los administradores tengan el tiempo, la experiencia y la conciencia para interpretar las guías de refuerzo. Claramente existen oportunidades para que la innovación equilibre las consideraciones de seguridad y uso.

Cada uno de los elementos anteriores crea una situación insostenible en la que los clientes necesitan investigar, financiar, comprar, dotar de personal, implementar y monitorear **productos de seguridad** adicionales para reducir la posibilidad de vulneración. Las organizaciones pequeñas y medianas (small and medium-sized organization, SMO) generalmente no pueden facilitar estas opciones. Se enfrentan a una escasez de experiencia, financiación y tiempo, lo que pone presión sobre el ancho de banda y el funcionamiento y convierte a la seguridad a una menor prioridad y, en conjunto, exacerba el riesgo colectivo. Por el contrario, las inversiones en seguridad de los relativamente pocos fabricantes podrán escalarse. Una frase común que resume el problema es que la industria del software necesita productos más seguros, no más productos de seguridad. Los fabricantes de software deberían liderar esa transformación.

***La industria del software necesita productos más seguros, no más productos de seguridad. Los fabricantes de software deberían liderar esa transformación.***

Hoy en día, a veces leemos comentarios de fabricantes que explican que un cliente se vio vulnerado por no habilitar una característica de seguridad en particular o por no seguir una guía de refuerzo específica. En cambio, después de una vulneración, los fabricantes deben explicar si una característica de seguridad particular o una guía de refuerzo específica habría evitado dicha vulneración y considerar convertirla en una característica predeterminada sin costo alguno. En aquellos casos en los que el producto en sí no se haya reforzado lo suficiente durante las fases de diseño e implementación, el fabricante debe explicar cómo está trabajando para eliminar esa clase de vulnerabilidad de sus líneas de productos.

Los fabricantes de software tienen la responsabilidad de garantizar que sus productos se diseñen y desarrollen teniendo la seguridad como máxima prioridad. Para ello, deberían **medir objetivamente los resultados** de sus esfuerzos sobre el terreno. Hacemos un llamado a los fabricantes no solo a centrarse en sus esfuerzos internos, sino también a medir objetivamente e informar periódicamente los resultados y la efectividad de los esfuerzos y las configuraciones de seguridad de un producto, y a construir un circuito de retroalimentación que cree cambios en el SDLC que conduzcan a mejoras mensurables en seguridad del cliente y a productos más seguros. Los informes deben incluir datos anónimos que la comunidad académica y de investigación de seguridad pueda utilizar para rastrear tendencias de alto nivel y medir el progreso en todo el ecosistema.

## DEMOSTRACIÓN DE ESTE PRINCIPIO

Los fabricantes de software y los servicios en línea deberían encontrar formas de demostrar éxitos en la implementación de este principio. Deberían tratar de proporcionar evidencia en forma de artefactos para que los examinen personas externas. Ningún artefacto por sí solo demostrará que un fabricante está implementando un programa sólido de seguridad desde el diseño, pero al proporcionar varios artefactos, demostrarían el compromiso del fabricante con el desarrollo de productos seguros. Este enfoque tiene el espíritu de “acciones antes que palabras”.

Para demostrar este principio, los fabricantes de software deberían considerar pasos como los de la siguiente lista. Las organizaciones autoras reconocen que pocos fabricantes de software podrán implementar inmediatamente estas prácticas y producir los artefactos correspondientes al comienzo del traspaso a la seguridad desde el diseño. Además, los fabricantes de software deberán priorizar esta lista según cómo los clientes implementen el producto en el campo para lograr los mayores beneficios de seguridad.

# PRÁCTICAS DE SEGURIDAD POR DEFECTO

1. **Eliminar las contraseñas predeterminadas.** Las contraseñas predeterminadas siguen siendo la causa de muchos ataques cada año. Comprometerse a eliminar este problema crónico negará el fácil acceso a los atacantes. De manera similar, los fabricantes deben considerar qué prácticas de contraseñas deben implementarse, como la longitud mínima de la contraseña y no permitir contraseñas descifradas anteriormente.
2. **Realizar pruebas de campo.** A medida que la tecnología continúa evolucionando y volviéndose más compleja, es cada vez más importante que los fabricantes de software realicen pruebas de usuario centradas en la seguridad para comprender la situación de seguridad de sus productos en acción. De manera similar a la manera en que la investigación de usuarios informa los requisitos de desarrollo de software, los fabricantes de software también deben realizar investigaciones de usuarios centradas en la seguridad para comprender dónde la experiencia de seguridad del usuario (UX) se queda corta. Al observar cómo los clientes implementan y utilizan sus productos en entornos del mundo real, los fabricantes de software pueden obtener información valiosa sobre el uso y la eficacia de sus funciones y controles de seguridad. Estos conocimientos pueden ayudar a identificar áreas de mejora y perfeccionar sus productos para satisfacer mejor las necesidades de seguridad de los clientes. Por ejemplo, las pruebas de campo pueden sugerir cambios en el flujo de UX, los valores predeterminados, las alertas y el monitoreo. Las pruebas de campo también pueden mostrar dónde las mejoras pasadas hechas en l diseño del producto reducen la velocidad de los parches de seguridad, reducen los errores de configuración y minimizan la superficie de ataque.

### Los fabricantes deben considerar lo siguiente:

- ¿Los clientes implementan correctamente la guía de refuerzo?
- ¿Las funciones de seguridad existentes del producto funcionan como se espera en el campo?
- ¿Esas características realmente resisten los ataques del mundo real?
- ¿Qué características reducirían mejor la probabilidad de vulneraciones?

*Nota: para obtener una visión más profunda de estos elementos, es posible que los fabricantes de software deseen asociarse con los clientes para realizar ejercicios de situaciones de la vida real para ver cómo el producto resiste los ataques. Estas pruebas de campo pueden realizarse en el sitio físico del cliente, virtualmente o mediante telemetría desde la aplicación, de manera que se preserve la privacidad.*

3. **Reducir el tamaño de la guía de refuerzo.** Los fabricantes pueden mejorar las posturas de seguridad de los clientes simplificando o incluso eliminando las guías de refuerzo de productos y centrándose en las medidas de seguridad más críticas que los clientes deben priorizar al implementar sus productos. En lugar de abrumar a los clientes con una larga lista de medidas de seguridad, los fabricantes deben identificar los principales riesgos de seguridad a los que son susceptibles sus productos y proporcionar una orientación clara y concisa sobre cómo mitigar estos riesgos. Además, los fabricantes deben proporcionarles a los clientes herramientas y automatización que simplifiquen el proceso de implementación de controles de seguridad, como líneas de comandos que puedan implementarse fácilmente en su entorno. Además, estas herramientas deberían poder verificar y mostrar claramente los cambios realizados desde la línea de base original. Al simplificar las guías de refuerzo y brindar a los clientes herramientas y automatización fáciles de usar, los fabricantes pueden reducir la carga de sus clientes y ayudar a garantizar que sus productos se implementen de manera segura. Una táctica sería considerar implementar el principio de Pareto para reducir el número de pasos para los casos de uso comunes (el 80%), y luego proporcionar orientación contextual y herramientas para escenarios menos comunes (el 20%). De esta manera, los fabricantes

de software harán que las cosas simples sean simples y las difíciles, posibles. Las pruebas de campo serán una herramienta poderosa para medir cuánto tiempo les lleva a los clientes descubrir, comprender e implementar guías de refuerzo. Los fabricantes deberían considerar cómo el producto podría impulsar a los administradores a tomar medidas dentro del propio producto en lugar de depender de ellos para implementar tareas de una guía de refuerzo.

4. **Desalentar activamente el uso de funciones heredadas que no sean seguras.** Priorizar la seguridad a través de rutas de actualización claras sobre la compatibilidad con versiones anteriores. Realizar publicaciones de blog que muestren la adopción de funciones y protocolos más seguros, y desaprobar funciones inseguras mediante anuncios, posiblemente desde el propio producto. Un número significativo de clientes ha demostrado que no mantendrán sus sistemas actualizados con redes modernas, identidad y otras características de seguridad críticas. En algunos casos, los clientes temen que la funcionalidad existente se rompa con una actualización. Al realizar las actualizaciones de la manera más fluida posible, es probable que los clientes actualicen y obtengan correcciones de seguridad con mayor frecuencia y rapidez. Los fabricantes de software deberían impulsar agresivamente a los clientes a seguir rutas de actualización que reduzcan el riesgo para el cliente.

5. **Implementar alertas que llamen la atención.** De manera similar a las alarmas de aviso de los cinturones de seguridad en los automóviles, que hacen ruido continuamente cuando los cinturones de seguridad no están abrochados, los fabricantes deben implementar alertas oportunas y repetidas cuando los usuarios o administradores se encuentren en estados verdaderamente inseguros, y así advertir a los administradores que están utilizando protocolos obsoletos en sus entornos y sugerir rutas de actualización. Implementar alertas oportunas y repetidas cuando los usuarios o administradores, o la configuración de la aplicación, se encuentren en un estado inseguro. Aclarar el modo inseguro a los administradores con regularidad. Una característica adicional podría requerir que un superadministrador reconozca la falta de MFA en su cuenta cada vez que inicie sesión, o incluso deshabilite ciertas funciones clave hasta que habilite MFA. Hay margen para innovar para lograr estos objetivos sin generar fatiga de alerta.

6. **Crear plantillas de configuración seguras.** Estas plantillas pueden preestablecer ciertas configuraciones en configuraciones seguras según el apetito de riesgo de una organización. Si bien podría ser demasiado simplista tener plantillas de seguridad de riesgo bajo/medio/alto, ese ejemplo ilustra cuántas configuraciones podrían actualizarse para gestionar el riesgo para la organización. Las plantillas pueden estar respaldadas por guías de refuerzo sobre los riesgos que el fabricante ha identificado.

# PRÁCTICAS SEGURAS DE DESARROLLO DE PRODUCTOS

1. **Conformidad del documento con un marco de SDLC seguro.** Los marcos de SDLC seguros proporcionan objetivos y ejemplos de personas, procesos y tecnologías. Considere publicar una descripción detallada de qué controles del marco de SDLC seguro se han implementado y describa cualquier control alternativo que se haya utilizado. Dentro de EE. UU., considere utilizar el marco de desarrollo de software seguro (SSDF) del NIST. Si bien no es una lista de verificación, el SSDF "describe un conjunto de prácticas sólidas y fundamentales para el desarrollo de software seguro".

2. **Documentar los objetivos de rendimiento de ciberseguridad (CPG) o conformidad equivalente.** Cuando una organización certifica que cumple con el estándar SSDF del NIST, está afirmando que su SDLC se basa en las mejores prácticas bien entendidas. Sin embargo, no les basta con tener un SDLC sólido. También necesitan proteger sus propios entornos empresariales y de desarrollo de actores maliciosos que intentarían manipular las propiedades de seguridad del producto mientras aún está en desarrollo. Esta no es una clase teórica de ataque, sino uno que se ha llevado a cabo con efectos adversos para los clientes y, por extensión, para la seguridad nacional. Las organizaciones deben considerar publicar detalles sobre el cumplimiento de la organización con las CPG de CISA, el marco de ciberseguridad (CSF) del NIST u otros marcos de programas de ciberseguridad.

3. **Gestión de vulnerabilidades.** Algunos fabricantes tienen un programa de gestión de vulnerabilidades que se centra en colocar parches sobre las vulnerabilidades descubiertas interna o externamente, y poco más. Los programas más maduros incorporan análisis exhaustivos basados en datos de las vulnerabilidades y sus causas fundamentales, tomando medidas para eliminar sistemáticamente clases enteras de vulnerabilidades[3]. Implementan programas formales en torno al establecimiento de la planificación de la calidad, el control de la calidad, la mejora de la calidad y la medición de la calidad. Consideran que la gestión de defectos es una cuestión de negocios, no simplemente una cuestión de seguridad. Estos programas no son diferentes en algunos aspectos de los programas de calidad y seguridad de otras industrias.

4. **Uso responsable del software de código abierto.** Cuando se utilice software de código abierto, sea responsable de examinar los paquetes de código abierto, fomentar las contribuciones de código a las dependencias y ayudar a sostener el desarrollo y mantenimiento de componentes críticos. Como referencia, el Ministerio de Economía, Comercio e Industria (METI) de Japón ha publicado una "Colección de ejemplos de casos de uso sobre métodos de gestión para utilizar OSS y garantizar su seguridad".

5. **Proporcionar valores predeterminados seguros para los desarrolladores.** Haga que la ruta predeterminada durante el desarrollo de software sea segura proporcionando componentes básicos seguros para los desarrolladores. Por ejemplo, dada la prevalencia de vulnerabilidades de inyección SQL que causan daños en el mundo real, asegúrese de que los desarrolladores utilicen una biblioteca bien mantenida para evitar ese tipo de vulnerabilidad. También conocida como "caminos pavimentados" o "caminos bien iluminados", esta práctica garantiza velocidad y seguridad y reduce el error humano.

6. **Fomentar una fuerza laboral de desarrolladores de software que comprenda la seguridad.** Asegúrese de que sus desarrolladores de software comprendan la seguridad capacitándolos sobre las mejores prácticas de codificación segura. Además, ayude a transformar la fuerza laboral en general actualizando las prácticas de contratación para evaluar el conocimiento de seguridad y trabajando con universidades, colegios comunitarios, campamentos de entrenamiento y otros educadores para integrar la seguridad en los planes de estudio de ciencias de la computación y desarrollo de software.

[3] NIST SSDF, PO 1.2, ejemplo 2: "Defina políticas que especifiquen los requisitos de seguridad para el software de la organización y verifique el cumplimiento en puntos clave del SDLC (por ejemplo, clases de fallas de software verificadas por puertas, respuestas a vulnerabilidades descubiertas en el software presentado)".

7. **Prueba de la integración de la gestión de eventos de incidentes de seguridad (security incident event management, SIEM) y la orquestación, automatización y respuesta de seguridad (orchestration, automation, and response, SOAR).** Además de realizar pruebas de campo, trabaje en conjunto con proveedores SIEM y SOAR populares junto con clientes selectos para comprender cómo los equipos de respuesta a incidentes utilizan los registros para investigar incidentes de seguridad reales o sospechados. Pocos desarrolladores de software tienen experiencia en responder a un incidente y pueden crear entradas de registro que no ayuden a los respondedores tanto como esperarían. Al trabajar con tecnologías SIEM y SOAR y profesionales reales de respuesta a incidentes, el equipo de desarrollo puede crear registros que cuenten la historia correcta y completa, ahorrando tiempo y reduciendo la incertidumbre durante un incidente.
8. **Alinearse con Zero Trust Architecture (ZTA).** Alinear las guías de implementación de productos con, por ejemplo, los modelos NIST ZTA y el modelo CISA Zero Trust Maturity. Aliente a los clientes a incorporar estos principios en sus entornos.

# PRÁCTICAS EMPRESARIALES PRO-SEGURIDAD

1. **Proporcionar un registro sin cargo adicional.** Los servicios en la nube deben comprometerse a generar y almacenar registros relacionados con la seguridad sin costo adicional. Los productos locales también deberían generar registros relacionados con la seguridad sin costo adicional. Además, el producto debe registrar los eventos de seguridad de forma predeterminada, ya que es posible que muchos clientes no comprendan su valor hasta después de un incidente. Estas tácticas pueden requerir una revisión exhaustiva de qué eventos de seguridad deben registrarse para brindar conciencia sobre el estado de la ciberseguridad, cómo un cliente puede configurar el registro, durante qué período de tiempo se conservan los registros, cómo se protegen la integridad y el almacenamiento de los registros y cómo se pueden analizar los registros. En algunos casos, la revisión puede sugerir la necesidad de refactorizar la arquitectura de administración de registros de la aplicación para ayudar a que sea viable y a un costo que funcione para el fabricante. Trabajar con expertos en respuesta a incidentes (incident response, IR) puede aumentar las posibilidades de que los registros sean útiles para los investigadores en el campo. Consulte la sección sobre SIEM.

2. **Eliminar impuestos ocultos.** Publique un compromiso de no cobrar nunca por funciones o integraciones de seguridad o privacidad. Por ejemplo, dentro del ámbito más amplio de la gestión de identidades y accesos (identity and access management, IAM), existen servicios denominados servicios de inicio de sesión único (SSO). Algunos fabricantes cobran más por conectar su sistema a un servicio SSO (a veces denominado proveedor de identidad). Este "impuesto SSO" significa que una buena gestión de identidades y accesos está fuera del alcance de muchas SMO, lo que les impide lograr una postura de seguridad sólida. Algunos servicios cobran más para habilitar MFA para los usuarios. **La seguridad no debe valorarse como un bien de lujo, sino considerarse un derecho del cliente.** Algunos fabricantes han argumentado que pocos clientes solicitan estas funciones y su mantenimiento cuesta más. Estos argumentos ignoran el hecho de que pocos clientes llamarán para quejarse o negociar, que no todos los clientes entienden realmente cuáles son los beneficios de estas características y que mantener todas las características cuesta algo. Sin embargo, no vemos que muchos fabricantes cobren más por la disponibilidad o la integridad de los datos. Los costos para respaldar esos atributos clave están integrados en el precio que pagan todos los clientes, al igual que los costos para incluir cinturones de seguridad, columnas de dirección plegables y bolsas de aire que salvan vidas en accidentes.

3. **Adoptar estándares abiertos.** Implemente estándares abiertos, especialmente en torno a protocolos de identidad y redes comunes. Evite protocolos propietarios cuando haya estándares abiertos disponibles.

4. **Proporcionar herramientas de actualización.** Muchos clientes se muestran reacios a adoptar la última versión del producto, incluida la implementación de funciones más nuevas y seguras, como conexiones de red seguras. Los fabricantes de software pueden aumentar la adopción de nuevas actualizaciones por parte de los clientes proporcionando herramientas para ayudar a reducir la incertidumbre y el riesgo. Ofrezca licencias gratuitas para que los clientes prueben actualizaciones y parches en un entorno de prueba como una forma de motivarlos.

# **PRINCIPIO 2:** Adoptar métodos radicales de transparencia y rendición de cuentas

**EXPLICACIÓN**

Los fabricantes de software deben enorgullecerse de ofrecer productos seguros, además de diferenciarse del resto de la comunidad de fabricantes en función de su capacidad para hacerlo.

Abordemos una preocupación común sobre la transparencia. Cuando los usuarios analizan la transparencia radical, existe una tendencia a que la conversación se estanque en la preocupación de que están proporcionando una "hoja de ruta para los atacantes". Sin embargo, la evidencia abrumadora es que a los atacantes les va bien sin tales hojas de ruta, y esas preocupaciones deberían pasar a un segundo plano frente a la transparencia que beneficia a los clientes directos, a los clientes indirectos, a las cadenas de suministro y a toda la industria del software.

La transparencia ayuda a la industria a establecer convenciones; en otras palabras, cómo es lo "bueno". Ayuda a que esas convenciones cambien con el tiempo en respuesta a las necesidades de los clientes, los cambios en las tácticas o la economía de los actores de amenazas o la evolución de la tecnología. La transparencia ayuda a los fabricantes con menos recursos a aprender de aquellos con recursos más maduros y capaces. Las conversaciones sobre el intercambio de información deberían ir más allá de los indicadores de amenazas en tiempo real, para incluir los elementos siguientes.

La transparencia obliga a que las decisiones sobre seguridad se tomen en las primeras etapas del proceso de desarrollo y a que sean una actividad continua de los líderes empresariales, así como de los ingenieros y profesionales de la seguridad. La transparencia genera responsabilidad en el producto.

Una nota sobre la elección del adjetivo “radical” frente a “transparencia”. Hoy en día, es poco común que los fabricantes de software publiquen información detallada sobre cómo desarrollan y mantienen el software y cómo maduran sus programas utilizando datos a lo largo del tiempo. En la industria del software, pocos fabricantes ofrecen visitas guiadas sobre cómo diseñan su software. Hay pocas oportunidades para que los fabricantes de software vean cómo organizaciones pares estructuran sus programas SDLC y cómo esos programas resisten en los entornos de los clientes contra atacantes reales. La industria colectiva se beneficiaría de un mayor intercambio de información sobre temas como estrategias para medir el costo de los defectos de seguridad y eliminar clases de vulnerabilidad. Como resultado de estas prácticas comunes, cada fabricante de software debe aprender cómo abordar la seguridad del producto por su cuenta. Quizás al no imponer un impuesto de lujo a las características de seguridad, la seguridad y la protección se conviertan en un centro de costos en lugar de un centro de ganancias, y las empresas se beneficiarían al aligerar la carga a través de la colaboración y la transparencia.

Queremos centrarnos en las tácticas que acelerarán materialmente la evolución de la industria del software. Ya no podemos darnos el lujo de realizar mejoras incrementales y oportunistas. Si queremos superar colectivamente las amenazas que plantean los adversarios inteligentes y adaptables, debemos adoptar niveles de transparencia que hoy resultarán incómodos, pero que impulsarán a la industria hacia adelante. Hoy en día hay fabricantes que incorporan algunos de estos principios de seguridad desde el diseño. Como dijo William Gibson, “el futuro ya está aquí, sólo que no está distribuido de manera muy equitativa”. **La transparencia radical ayudará a distribuir esa información y beneficiará a los defensores más que a nuestros adversarios.**

La transparencia puede hacer más que ayudar a las organizaciones pares a madurar sus SDLC. Los posibles clientes e inversores pueden obtener más información sobre las inversiones y las compensaciones que han realizado los fabricantes, y la postura de seguridad que esas inversiones han creado para los clientes. Los fabricantes que adopten una transparencia radical brindarán a los clientes información para ayudarlos a tomar decisiones de compra no sólo sobre el precio y las características, sino también sobre la seguridad.

Por mucho que las organizaciones trabajen para proteger su cadena de suministro y su SDLC, los procesos de construcción de las empresas se han visto comprometidos en el pasado reciente. Adoptar una transparencia radical debería llevar a la divulgación pública del ataque, así como de las mejoras que realizó la empresa para prevenir y detectar futuros ataques. Esa forma de compartir información ayudará a otras organizaciones a aprender sin tener que correr la misma suerte.

## DEMOSTRACIÓN DE ESTE PRINCIPIO

Para demostrar este principio, los fabricantes de software deberían seguir pasos como los siguientes:

# PRÁCTICAS DE SEGURIDAD POR DEFECTO

1. **Publicar estadísticas y tendencias agregadas relevantes para la seguridad.** Los temas de ejemplo incluyen la adopción de MFA por parte de clientes y administradores y el uso de protocolos heredados inseguros.
2. **Publicar estadísticas de parches.** Ofrezca detalles sobre qué porcentaje de clientes tienen la última versión del producto y qué está haciendo para que las actualizaciones sean más fáciles y confiables.
3. **Publicar datos sobre privilegios no utilizados.** Publique información agregada sobre permisos excesivos en su base de clientes, así como los empujones y otros cambios en el producto que está realizando para reducir las superficies de ataque de los clientes. Es probable que estos privilegios no utilizados sean buenos candidatos para alertas de administrador, como las alarmas de aviso de cinturón de seguridad.

# PRÁCTICAS SEGURAS DE DESARROLLO DE PRODUCTOS

1. **Establecer controles de seguridad internos.** Muchas empresas han visto los beneficios de trasladar sus datos a proveedores de nube. Ahora esos proveedores de nube se convierten en el objetivo de los atacantes. Los proveedores de software como servicio (Software as a Service, SaaS) deben publicar estadísticas de sus controles internos. Por ejemplo, los proveedores de SaaS deberían publicar estadísticas sobre su implementación interna de MFA resistente al phishing, como la autenticación rápida en línea (Fast Identity Online, FIDO). Idealmente, deberían poder decir que ningún miembro del personal puede acceder a datos de clientes u otros datos confidenciales sin autenticarse a través de MFA resistente al phishing.

2. **Publicar modelos de amenazas de alto nivel.** Los productos seguros desde el diseño comienzan con modelos de amenazas escritos que describen qué intentan proteger los creadores y de quién. Los modelos de amenazas efectivos se basan en la forma en que ocurren las intrusiones en la naturaleza y deben cubrir tanto los entornos empresariales como de desarrollo, así como la forma en que los fabricantes de software pretenden que se utilice en los entornos de los clientes.

3. **Publicar autocertificaciones SDLC seguras y detalladas.** Los fabricantes que siguen NIST SSDF u otros marcos similares están trabajando activamente para lograr un ciclo de vida de desarrollo de software maduro. La publicación de una autocertificación de qué controles ha implementado el fabricante y para qué productos demostraría un compromiso de adherirse a estas mejores prácticas y proporcionaría un mayor nivel de confianza a sus clientes. Otros esquemas de certificación incluyen la Metodología de la Cadena de Suministro Cibernético de Israel, por ejemplo.

4. **Adoptar la transparencia sobre la vulnerabilidad.** Publicar un compromiso que garantice que las vulnerabilidades identificadas del producto se publiquen como entradas CVE que sean correctas y completas. Esto es especialmente cierto para el campo de enumeración de debilidades comunes que identifica la causa raíz de las vulnerabilidades. Cuanto más correcta y completa sea la base de datos pública CVE, más podrá la industria rastrear cómo los productos se están volviendo más seguros y qué clases de vulnerabilidades son más frecuentes. Sin embargo, se debe tener cuidado con la tentación de considerar los CVE como una métrica negativa, ya que dichos números también son una señal de una comunidad saludable de análisis y pruebas de código. A medida que los fabricantes implementan una filosofía de diseño seguro, es posible que al principio su recuento de CVE sin procesar aumente debido a un descubrimiento y corrección más completos de las vulnerabilidades en el código existente. Los fabricantes deben publicar análisis de vulnerabilidades pasadas, incluidos los patrones y medidas que se tomaron para abordar toda la clase de vulnerabilidades. Por ejemplo, si un gran porcentaje de los CVE de una empresa estuvieran relacionados con secuencias de comandos entre sitios (cross-site scripting, XSS), documentar el análisis de la causa raíz, la respuesta (como el cambio a marcos de plantillas web que eviten XSS) y los resultados indicarían a los clientes que no serán víctimas de una clase de vulnerabilidad para la cual se han entendido medidas de mitigación durante décadas.

5. **Publicar listas de materiales de software (SBOM).** Los fabricantes deberían tener el control de sus cadenas de suministro. Las organizaciones deben crear y mantener listas de materiales de software (Publish Software Bills of Materials, SBOM) [2] para cada producto, solicitar datos a sus proveedores y poner los SBOM a disposición de los clientes y usuarios intermedios. Esto ayudará a demostrar su diligencia a la hora de comprender los componentes que utilizan en la creación de sus productos, su capacidad para responder a riesgos recientemente identificados y puede ayudar a los clientes a comprender cómo responder si uno de los módulos de la cadena de suministro tiene una vulnerabilidad recién descubierta. Como referencia, el Ministerio de Economía, Comercio e Industria (METI) de Japón ha

publicado la "Guía de introducción de la lista de materiales de software (SBOM) para la gestión de software". La transparencia debe extenderse al firmware de los dispositivos integrados y a los datos y modelos utilizados en AI/aprendizaje automático (machine learning, ML). Más allá de ayudar en las decisiones de compra y las capacidades operativas, los SBOM desempeñan un papel importante en la infraestructura para detectar y responder a ataques maliciosos a la cadena de suministro.

6. **Publicar una política de divulgación de vulnerabilidades.** Publicar una política de divulgación de vulnerabilidades que (1) autorice las pruebas con todos los productos ofrecidos por el fabricante y las condiciones para esas pruebas, (2) proporcione un puerto seguro legal para las acciones realizadas de manera consistente con la política y (3) permita la divulgación pública de vulnerabilidades después de una establecer cronograma. Los fabricantes deben realizar análisis de la causa raíz de las vulnerabilidades descubiertas y, en la mayor medida posible, tomar medidas para eliminar clases enteras de vulnerabilidad. Consulte la Plantilla de política de divulgación de vulnerabilidades de CISA para obtener un idioma de referencia.

# PRÁCTICAS EMPRESARIALES PRO-SEGURIDAD

1. **Nombrar públicamente a un patrocinador ejecutivo sénior seguro desde el diseño.** En muchas organizaciones, la seguridad (al igual que la calidad) se delega a equipos técnicos que tienen una capacidad limitada para realizar cambios estructurales para mejorar drásticamente la seguridad de los productos. Nombrar públicamente a un alto ejecutivo empresarial para supervisar el programa de seguridad por diseño transformará la seguridad de los productos en una preocupación empresarial de alto nivel.

2. **Publicar una hoja de ruta segura desde el diseño.** Los fabricantes deben documentar los cambios realizados en su SDLC para mejorar la seguridad del cliente, incluidos detalles sobre los informes de pruebas de campo, las acciones tomadas para eliminar clases enteras de vulnerabilidad y otros elementos enumerados en los demás principios. Como en el caso de los esfuerzos de mejora de la calidad, los programas de mejora de la seguridad tienen distintas fases de planificación, control y mejora. Con el espíritu de mostrar en lugar de contar, la publicación de la hoja de ruta y los detalles detrás de estas fases generará confianza en que los productos son seguros desde el diseño. Después de lograr avances significativos, los fabricantes pueden detallarlos en informes de transparencia. Hacerlo no solo demuestra un compromiso con los principios de seguridad desde el diseño, sino que también puede inspirar a otros a adoptar programas similares al mostrar una prueba de existencia.

3. **Publicar una hoja de ruta para la seguridad de la memoria.** Los fabricantes pueden tomar medidas para eliminar una de las mayores clases de vulnerabilidad migrando productos existentes y creando nuevos productos utilizando lenguajes seguros para la memoria. Si bien esto puede no ser posible en todos los casos, los fabricantes pueden considerar desarrollar contenedores de aplicaciones en lenguajes seguros para la memoria en lugar de reescribir aplicaciones completas. Esto también puede incluir cómo los fabricantes actualizan la contratación, la capacitación, la revisión de códigos y otros procesos internos, así como las formas en que ayudan a la comunidad de código abierto a hacer lo mismo.

4. **Publicar resultados.** Al actualizar su SDLC para incorporar una filosofía de seguridad desde el diseño, las organizaciones encontrarán victorias rápidas, victorias que requieren más recursos y algunos contratiempos inesperados. Al presentar sus éxitos y obstáculos internos, toda la industria puede aprender de los resultados.

# PRINCIPIO 3: Liderar desde arriba

**EXPLICACIÓN**

Si bien la filosofía general se denomina “seguro desde el diseño”, los incentivos para la seguridad del cliente comienzan mucho antes de la fase de diseño del producto. Comienzan con metas comerciales y objetivos implícitos y explícitos y resultados deseados. Sólo cuando los líderes sénior hagan de la seguridad una prioridad empresarial, creando incentivos internos y fomentando una cultura generalizada para hacer de la seguridad un requisito de diseño, lograrán los mejores resultados.

Si bien la experiencia técnica en la materia es fundamental para la seguridad del producto, no es una cuestión que pueda dejarse exclusivamente en manos del personal técnico. Es una prioridad empresarial que debe empezar desde arriba.

Algunas personas se han preguntado si un fabricante de software adopta los dos primeros principios y produce artefactos significativos, ¿es necesario el tercer principio? La forma en que una empresa establece su visión, misión, valores y cultura afectará el producto, y esos elementos tienen un gran componente en la cima. Vemos esto en otras industrias que han logrado mejoras espectaculares en seguridad y calidad. El destacado experto en calidad, J.M. Juran escribió:

> ***Lograr el liderazgo en calidad requiere que los altos directivos se hagan cargo personalmente de la gestión de la calidad. En las empresas que lograron un liderazgo de calidad, los altos directivos guiaron personalmente la iniciativa. No conozco ninguna excepción. [3]***

**Creemos que la seguridad es una subcategoría de la calidad del producto.** Cuando la seguridad y la calidad se conviertan en imperativos comerciales, en lugar de funciones técnicas dejadas únicamente al personal técnico, las organizaciones podrán responder a las necesidades de seguridad de sus clientes de manera más rápida y eficiente. Además, invertir los recursos necesarios para garantizar que la seguridad del software sea una prioridad empresarial central desde el principio reducirá los costos a largo plazo de abordar los defectos del software y, a su vez, reducirá los riesgos de seguridad nacional.

De la misma manera que los equipos de liderazgo han implementado programas de responsabilidad social corporativa (corporate social responsibility, CSR), existe una creciente conciencia de que los directorios corporativos, incluidos los de los fabricantes de software, deberían asumir un papel más activo en la orientación de los programas de ciberseguridad. El término ciberresponsabilidad corporativa (corporate cyber responsibility, CCR) se utiliza a veces para describir esta idea emergente.

# DEMOSTRACIÓN DE ESTE PRINCIPIO

Para demostrar este principio, los fabricantes de software deberían seguir pasos como los siguientes:

1. **Incluir detalles de un programa seguro desde el diseño en los informes financieros corporativos.** Si el fabricante es una empresa que cotiza en bolsa, agregue una sección en cada informe anual dedicada a los esfuerzos de seguridad mediante el diseño. Es común que los informes financieros anuales de los automóviles incluyan secciones sobre la seguridad del conductor y de los pasajeros, incluida información sobre comités de calidad y seguridad centralizados y distribuidos. Detallar el programa de seguridad desde el diseño en un informe financiero demostrará que la organización está vinculando la seguridad del cliente y los resultados financieros corporativos y no simplemente adoptando un término en materiales de comercialización porque está de moda.
2. **Proporcionar informes periódicos a su junta directiva.** Los informes del director de seguridad de la información (chief information security officer, CISO) a las juntas corporativas generalmente incluyen información sobre programas de seguridad actuales y planificados, amenazas, incidentes de seguridad sospechosos y confirmados, y otras actualizaciones centradas en la postura de seguridad y la salud de la empresa. Además de recibir información sobre la postura de seguridad de la empresa, las juntas directivas deben solicitar información sobre la seguridad del producto y el impacto que tiene en la seguridad del cliente. Las juntas directivas no deben recurrir únicamente al CISO, sino principalmente a otros miembros de la dirección de la empresa para reducir el riesgo del cliente.
3. **Empoderar al ejecutivo de la seguridad desde el diseño.** Existe una diferencia significativa entre una organización donde los equipos técnicos cuentan con la "compra ejecutiva" y aquellas donde los líderes empresariales administran personalmente el proceso de mejora de la seguridad del cliente utilizando procesos comerciales estándar. El término "compra ejecutiva" implica que alguien tenía que vender la idea de un programa de seguridad del cliente en lugar de que fuera un objetivo comercial de alto nivel. Este ejecutivo debe estar capacitado para influir en las inversiones en productos para lograr resultados de seguridad para el cliente.
4. **Crear incentivos internos significativos.** Sin dejar de ser consciente de no crear incentivos perversos, alinee los sistemas de recompensas para mejorar la seguridad del cliente y que coincida con otros comportamientos y resultados valiosos. Desde el ejecutivo de seguridad por diseño hasta la gestión de productos, el desarrollo de software, el soporte, las ventas, el departamento legal y otras organizaciones, combine los incentivos de seguridad del cliente con la contratación, los ascensos, los salarios, las bonificaciones, las opciones sobre acciones y otros procesos comunes en el funcionamiento del negocio. Por ejemplo, al establecer criterios para promocionar a los desarrolladores de software, incluya consideraciones para mejorar la seguridad del producto junto con otros criterios como el tiempo de actividad, el rendimiento y las mejoras de funciones.
5. **Crear un consejo seguro desde el diseño.** En algunas industrias, es común que las organizaciones creen un consejo de calidad central e incorporen representantes de calidad en divisiones o unidades de negocios clave. Al incluir miembros centralizados y distribuidos, estos grupos trabajan para mejorar la calidad, en comparación con objetivos de alto nivel mientras reciben telemetría desde lo más profundo de la organización. De manera similar, un consejo de seguridad desde el diseño mejoraría la seguridad frente a los objetivos de seguridad desde el diseño en toda la organización.
6. **Crear y evolucionar consejos de clientes.** Muchos fabricantes de software tienen consejos de clientes compuestos por clientes de diferentes regiones, industrias y tamaños. Estos consejos pueden proporcionar una gran cantidad de información sobre los éxitos de los clientes y los desafíos en la implementación de los productos de la empresa. Estructure la agenda del consejo con temas dedicados a la seguridad del cliente, incluso si actualmente no es una prioridad para los participantes. Considere dónde informa el consejo de clientes y cómo recurrir a los participantes para obtener información sobre la seguridad del producto tal como se implementa. Por ejemplo, ¿el consejo tiene un sesgo con fines de comercialización y ventas, o hacia la gestión de productos? El ejecutivo de seguridad desde el diseño debería ayudar a dirigir estas interacciones con los clientes y debería vincularlas con otros elementos de este documento, como los estudios de campo.

# TÁCTICAS DE SEGURIDAD DESDE EL DISEÑO

El Marco de desarrollo de software seguro (SSDF), también conocido como SP 800-218 del Instituto Nacional de Estándares y Tecnología (NIST), es un conjunto central de prácticas de desarrollo de software seguro de alto nivel que se pueden integrar en cada etapa del ciclo de vida del desarrollo de software (SDLC). Seguir estas prácticas puede ayudar a los productores de software a ser más eficaces a la hora de encontrar y eliminar vulnerabilidades en el software presentado, mitigar el impacto potencial de la explotación de vulnerabilidades y abordar las causas fundamentales de las vulnerabilidades para evitar que se repitan en el futuro.

Las organizaciones autoras fomentan el uso de tácticas seguras desde el diseño, incluidos principios que hacen referencia a las prácticas SSDF. Los fabricantes de software deben desarrollar una hoja de ruta escrita para adoptar prácticas de desarrollo de software más seguras desde el diseño en toda su cartera. La siguiente es una lista ilustrativa no exhaustiva de las mejores prácticas de la hoja de ruta:

- **Lenguajes de programación seguros para la memoria (SSDF PW.6.1).** Priorice el uso de lenguajes seguros para la memoria siempre que sea posible. Las organizaciones autoras reconocen que las mitigaciones específicas de la memoria pueden ser tácticas útiles a corto plazo para las bases de código heredadas. Ejemplos incluyen mejoras de lenguaje C/C++, mitigaciones de hardware, aleatorización del diseño del espacio de direcciones (ASLR), integridad del flujo de control (CFI) y fuzzing. Sin embargo, existe un consenso cada vez mayor de que la adopción de lenguajes de programación seguros para la memoria puede eliminar esta clase de defecto, y los fabricantes de software deberían explorar formas de adoptarlos. Algunos ejemplos de lenguajes modernos seguros para la memoria incluyen C#, Óxido, Ruby, Java, Go y Swift. Lea la hoja de información de seguridad de la memoria de la NSA para obtener más información.
- **Base de hardware segura.** Incorpore características arquitectónicas que permitan una protección de memoria detallada, como las descritas en las Instrucciones RISC mejoradas de hardware de capacidad (CHERI) que pueden ampliar las arquitecturas de conjunto de instrucciones (ISA) de hardware convencional, así como otras características como módulos de plataforma confiable y módulos de seguridad de hardware. Para obtener más información, visite la página web CHERI de la Universidad de Cambridge.
- **Componentes de software seguros (SSDF PW 4.1).** Adquiera y mantenga componentes de software bien protegidos (por ejemplo, bibliotecas de software, módulos, middleware, marcos) de desarrolladores externos, de código abierto y comerciales verificados para garantizar una seguridad sólida en los productos de software de consumo.
- **Marcos de plantillas web (SSDF PW.5.1).** Utilice marcos de plantillas web que implementen el escape automático de la entrada del usuario para evitar ataques web como secuencias de comandos entre sitios.
- **Consultas parametrizadas (SSDF PW 5.1).** Utilice consultas parametrizadas en lugar de incluir entradas del usuario en las consultas para evitar ataques de inyección SQL.
- **Pruebas de seguridad de aplicaciones estáticas y dinámicas.** (SAST/DAST) (SSDF PW.7.2, PW.8.2). Utilice estas herramientas para analizar el código fuente del producto y el comportamiento de las aplicaciones para detectar prácticas propensas a errores. Estas herramientas cubren problemas que van desde la gestión inadecuada de la memoria hasta la construcción de consultas de bases de datos propensas a errores (por ejemplo, entradas de usuario sin escape que conducen a una inyección de SQL). Las herramientas SAST y DAST se pueden incorporar a los procesos de desarrollo y ejecutarse automáticamente como parte del desarrollo de software. SAST y DAST deben complementar otros tipos de pruebas, como pruebas unitarias y pruebas de integración, para garantizar que los productos cumplan con los requisitos de seguridad esperados. Cuando se identifican problemas, los fabricantes deben realizar un análisis de la causa raíz para abordar las vulnerabilidades de manera sistémica.

- **Revisión de código** (SSDF PW.7.1, PW.7.2). Esfuércese por garantizar que el código enviado a los productos pase por técnicas de control de calidad, como la revisión por pares de otros desarrolladores o la "siembra de errores".
- **Lista de materiales de software (SBOM)** (SSDF PS.3.2, PW.4.1). Incorpore la creación de SBOM[4] para brindar visibilidad del conjunto de software que incluye los productos.
- **Programas de divulgación de vulnerabilidades** (SSDF RV.1.3). Establezca programas de divulgación de vulnerabilidades que permitan a los investigadores de seguridad informar sobre vulnerabilidades y recibir protección legal al hacerlo. Como parte de esto, los proveedores deben establecer procesos para determinar las causas fundamentales de las vulnerabilidades descubiertas. Dichos procesos deben incluir la determinación de si la adopción de alguna de las prácticas seguras desde el diseño en este documento (u otras prácticas similares) habría evitado la introducción de la vulnerabilidad.
- **Completitud CVE.** Asegúrese de que los CVE publicados incluyan la causa raíz o la enumeración de debilidades comunes (CWE) para permitir el análisis de las fallas de diseño de seguridad del software en toda la industria. Si bien garantizar que cada CVE sea correcto y completo puede llevar más tiempo, permite a entidades dispares detectar tendencias de la industria que benefician a todos los fabricantes y clientes. Para obtener más información sobre la gestión de vulnerabilidades, consulte la guía de Categorización de vulnerabilidades específicas de las partes interesadas (SSVC) de CISA.
- **Defensa en profundidad.** Diseñe la infraestructura de modo que el compromiso de un único control de seguridad no resulte en el compromiso de todo el sistema. Por ejemplo, garantizar que los privilegios de usuario se proporcionen de manera estricta y que se empleen listas de control de acceso puede reducir el impacto de una cuenta comprometida. Además, las técnicas de zona de pruebas de software pueden poner en cuarentena una vulnerabilidad para limitar el riesgo de una aplicación completa.
- **Satisfacer los objetivos de rendimiento en ciberseguridad (CPG).** Diseñe productos que cumplan con las prácticas básicas de seguridad. Los Objetivos de desempeño en ciberseguridad de CISA describen medidas básicas y fundamentales de ciberseguridad que las organizaciones deben implementar. Además, para conocer más formas de fortalecer la postura de su organización, consulte el Marco de evaluación cibernética del NCSC-Reino Unido, que comparte similitudes con las CPG de CISA. Si un fabricante no cumple con las CPG, como no exigir MFA resistente al phishing para todos los empleados, entonces no se puede considerar que ofrezca productos seguros por diseño.

Las organizaciones autoras reconocen que estos cambios son cambios significativos en la postura de una organización. Como tal, se debe priorizar su introducción en función de un modelado de amenazas personalizado, la criticidad, la complejidad y el impacto comercial. Estas prácticas pueden introducirse para software nuevo y ampliarse gradualmente para cubrir casos de uso y productos adicionales. En algunos casos, la criticidad y la postura de riesgo de un determinado producto pueden ameritar un cronograma acelerado para adoptar estas prácticas. En otros, las prácticas pueden introducirse en un código base heredado y corregirse con el tiempo.

[4] Algunas de las organizaciones autoras están explorando enfoques alternativos para obtener garantías de seguridad en toda la cadena de suministro de software.

# TÁCTICAS DE SEGURIDAD POR DEFECTO

Además de adoptar prácticas de desarrollo seguras por diseño, las organizaciones autoras recomiendan que los fabricantes de software den prioridad a las configuraciones seguras por defecto en sus productos. Estos deberían esforzarse por actualizar los productos para que se ajusten a estas prácticas a medida que se actualizan. Por ejemplo:

- **Eliminar las contraseñas predeterminadas.** Los productos no deben venir con contraseñas predeterminadas que se compartan universalmente. Para eliminar las contraseñas predeterminadas, las organizaciones autoras recomiendan que los productos requieran que los administradores establezcan una contraseña segura durante la instalación y configuración o que el producto se envíe con una contraseña segura única para cada dispositivo.

- **Exigir autenticación multifactor (MFA) para usuarios privilegiados.** Observamos que muchas implementaciones empresariales son administradas por administradores que no han protegido sus cuentas con MFA. Dado que los administradores son objetivos de alto valor, los productos deberían hacer que MFA opte por no participar en lugar de optar por participar. Además, el sistema debería solicitar periódicamente al administrador que se inscriba en MFA hasta que lo haya habilitado correctamente en su cuenta. El NCSC de los Países Bajos tiene una guía paralela a la de CISA; visite su hoja informativa sobre autenticación para adultos para obtener más información.

- **Inicio de sesión único (SSO).** Las aplicaciones de IT deben implementar soporte de inicio de sesión único a través de estándares abiertos modernos. Los ejemplos incluyen Security Assertion Markup Language (SAML) u OpenID Connect (OIDC). Esta capacidad debería estar disponible de forma predeterminada sin costo adicional.

- **Registro seguro.** Proporcione registros de auditoría de alta calidad a los clientes sin costo adicional ni configuración adicional. Los registros de auditoría son cruciales para detectar y escalar posibles incidentes de seguridad. También son cruciales durante la investigación de un incidente de seguridad sospechoso o confirmado. Considere las mejores prácticas, como proporcionar una integración sencilla con sistemas de gestión de eventos e información de seguridad (SIEM) con acceso a la interfaz de programación de aplicaciones (API) que utiliza hora universal coordinada (UTC), formato de zona horaria estándar y técnicas de documentación sólidas.

- **Perfil de autorización de software.** Los proveedores de software deben proporcionar recomendaciones sobre roles de perfil autorizados y su caso de uso designado. Los fabricantes deben incluir una advertencia visible que notifique a los clientes sobre un mayor riesgo si se desvían de la autorización del perfil recomendado. Por ejemplo, los médicos pueden ver todos los registros de los pacientes, pero un programador médico tiene acceso limitado a cierta información necesaria para programar citas.

- **Seguridad orientada al futuro frente a la compatibilidad con versiones anteriores.** Con demasiada frecuencia, se incluyen funciones heredadas compatibles con versiones anteriores en los productos, y a menudo se habilitan, a pesar de causar riesgos para la seguridad del producto. Priorice la seguridad sobre la compatibilidad con versiones anteriores, lo que permitirá a los equipos de seguridad eliminar funciones inseguras incluso si eso significa provocar cambios importantes.

- **Buscar la guía de refuerzo y reducirla.** Reduzca el tamaño de las "guías de refuerzo" que se incluyen con los productos y esfuércese por garantizar que el tamaño se reduzca con el tiempo a medida que se lanzan nuevas versiones del software. Integre componentes de la "guía de refuerzo" como configuración predeterminada del producto. Las organizaciones autoras

reconocen que las guías de refuerzo abreviadas son el resultado de una asociación continua con los clientes existentes e incluyen esfuerzos de muchos equipos de productos, incluida la experiencia del usuario (UX).

- **Considerar las consecuencias de la configuración de seguridad en la experiencia del usuario.** Cada nueva configuración aumenta la carga cognitiva de los usuarios finales y debe evaluarse junto con el beneficio empresarial que deriva. Idealmente, no debería existir una configuración; en cambio, la configuración más segura debería integrarse en el producto de forma predeterminada. Cuando es necesaria la configuración, la opción predeterminada debe ser ampliamente segura contra amenazas comunes.

Las organizaciones autoras reconocen que estos cambios pueden tener efectos operativos en la forma en que se emplea el software. Por lo tanto, la opinión de los clientes es fundamental para equilibrar las consideraciones operativas y de seguridad. Creemos que desarrollar hojas de ruta escritas y apoyo ejecutivo que prioricen estas ideas en los productos más críticos de una organización es el primer paso para avanzar hacia prácticas de desarrollo de software seguras. Si bien la opinión de los clientes es importante, hemos observado casos importantes en los que los clientes no han querido o no han podido adoptar estándares mejorados, a menudo protocolos de red. Es importante que los fabricantes creen incentivos significativos para que los clientes se mantengan actualizados y no les permitan permanecer vulnerables indefinidamente.

# GUÍAS DE REFUERZO FRENTE A LAS DE FLEXIBILIZACIÓN

Las guías de refuerzo pueden resultar de la falta de controles de seguridad del producto integrados en la arquitectura de un producto desde el inicio del desarrollo. En consecuencia, las guías de refuerzo también pueden ser una hoja de ruta para que los adversarios identifiquen y exploten características inseguras. Es común que muchas organizaciones desconozcan las guías de refuerzo, por lo que dejan los ajustes de configuración de sus dispositivos en una postura insegura. Un modelo invertido conocido como guía de alivio debería reemplazar dichas guías de refuerzo y explicar qué cambios deben realizar los usuarios y al mismo tiempo enumerar los riesgos de seguridad resultantes. Estas guías deben estar escritas por profesionales de la seguridad que puedan explicar las ventajas y desventajas en un lenguaje claro para aumentar las posibilidades de que se apliquen correctamente.

En lugar de desarrollar guías de refuerzo que enumeren métodos para proteger los productos, las organizaciones autoras recomiendan que los fabricantes de software adopten un enfoque seguro por defecto y proporcionen "guías de flexibilización". Estas guías explican el riesgo empresarial de las decisiones en un lenguaje sencillo y comprensible y pueden aumentar la conciencia organizacional sobre los riesgos de intrusiones cibernéticas maliciosas. Los ejecutivos sénior de los clientes deben determinar las compensaciones en materia de seguridad, equilibrando la seguridad con otros requisitos comerciales.

# RECOMENDACIONES PARA CLIENTES

Las organizaciones autoras recomiendan que las organizaciones responsabilicen a los fabricantes de software proveedores de los resultados de seguridad de sus productos. Como parte de esto, las organizaciones autoras recomiendan que los ejecutivos prioricen la importancia de comprar productos seguros desde el diseño y seguros por defecto. Esto puede manifestarse mediante el establecimiento de políticas que exijan que los departamentos de IT evalúen la seguridad del software antes de comprarlo, y que también empoderen a los departamentos de IT para que retrocedan si es necesario. Los departamentos de IT deben estar facultados para desarrollar criterios de compra que enfaticen la importancia de las prácticas seguras por diseño y seguras por defecto (tanto las descritas en este documento como otras desarrolladas por la organización). Además, los departamentos de IT deben contar con el apoyo de la dirección ejecutiva a la hora de hacer cumplir estos criterios en las decisiones de compra. Las decisiones organizacionales para aceptar los riesgos asociados con productos tecnológicos específicos deben documentarse formalmente, aprobarse por un alto ejecutivo comercial y presentarse periódicamente a la junta directiva.

Los servicios clave de IT empresarial que respaldan la postura de seguridad de la organización, como la red empresarial, la gestión de acceso e identidad empresarial, y las operaciones de seguridad y capacidades de respuesta, deben verse como funciones comerciales críticas que se financian para alinearse con su importancia para el éxito de la misión de la organización. Las organizaciones deben desarrollar un plan para actualizar estas capacidades para aprovechar los fabricantes que adoptan prácticas seguras desde el diseño y seguras por defecto.

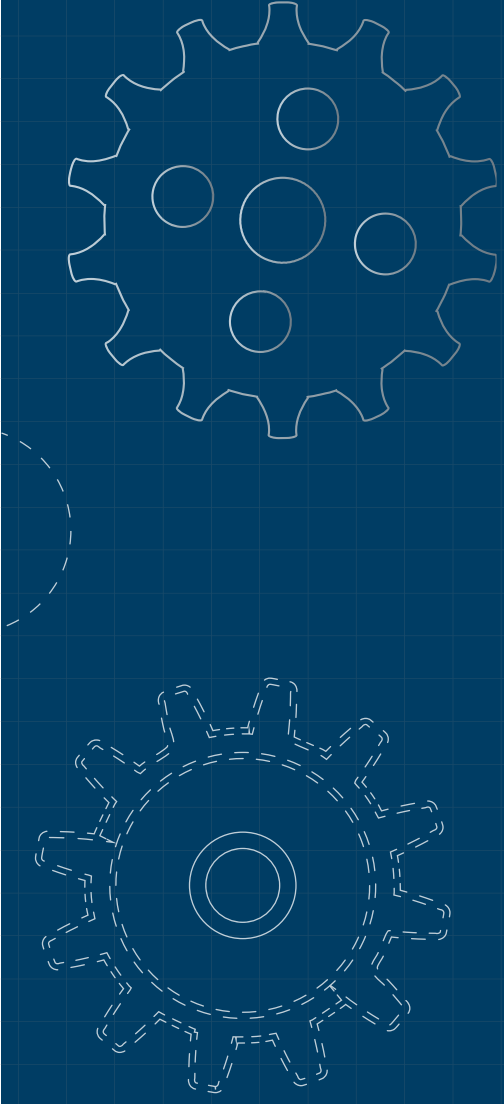
Siempre que sea posible, las organizaciones deben esforzarse por forjar relaciones estratégicas con sus proveedores clave de IT. Dichas relaciones incluyen confianza en múltiples niveles de la organización y brindan vehículos para resolver problemas e identificar prioridades compartidas. La seguridad debe ser un elemento crítico de tales relaciones y las organizaciones deben esforzarse por reforzar la importancia de las prácticas seguras por diseño y seguras por defecto tanto en la dimensión formal (por ejemplo, contratos o acuerdos con proveedores) como en la informal de la relación. Las organizaciones deben esperar transparencia de sus proveedores de tecnología sobre su postura de control interno, así como su hoja de ruta para adoptar prácticas seguras desde el diseño y seguras por defecto.

Además de hacer de la seguridad una prioridad dentro de una organización, los líderes de IT deben colaborar con sus pares de la industria para comprender qué productos y servicios incorporan mejor estos principios de diseño. Estos líderes deberían coordinar sus solicitudes para ayudar a los fabricantes a priorizar sus próximas iniciativas de seguridad. Al trabajar juntos, los clientes pueden ayudar a brindar información significativa a los fabricantes y crear incentivos para que prioricen la seguridad.

Al aprovechar los sistemas en la nube, las organizaciones deben asegurarse de comprender el modelo de responsabilidad compartida con su proveedor de tecnología. Es decir, las organizaciones deben tener claridad sobre las responsabilidades de seguridad del proveedor y no sólo sobre las responsabilidades del cliente.

Las organizaciones deben priorizar a los proveedores de nube que sean transparentes en cuanto a su postura de seguridad, controles internos y capacidad para cumplir con sus obligaciones bajo el modelo de responsabilidad compartida.

# DESCARGO DE RESPONSABILIDAD



# Recursos

### CISA

- Guía de SBOM de CISA
- Objetivos de desempeño intersectoriales en materia de ciberseguridad
- Directrices sobre interoperabilidad tecnológica
- La defensa de CISA y NIST contra los ataques a la cadena de suministro de software
- El costo de la tecnología insegura y qué podemos hacer al respecto | CISA
- Dejemos de pasar la pelota en ciberseguridad: por qué las empresas deben incorporar la seguridad en los productos tecnológicos (foreignaffairs.com)
- Guía de categorización de vulnerabilidades específica (SSVC) de las partes interesadas de CISA
- Hojas informativas de MFA resistente al phishing de CISA
- Guía cibernética para pequeñas empresas | CISA

### NSA

- Hoja de información de ciberseguridad de la NSA sobre seguridad de la memoria
- El FSE de la NSA asegura la cadena de suministro de software: mejores prácticas para los proveedores

### FBI

- Comprender y responder al ataque a la cadena de suministro de SolarWinds: la perspectiva federal
- La amenaza cibernética: respuesta e informes
- La estrategia cibernética del FBI

### Instituto Nacional de Estándares y Tecnología (NIST)

- Pautas de identidad digital del NIST
- Marco de ciberseguridad del
- NIST Marco de desarrollo de software seguro (SSDF) del NIST

### Centro Australiano de Seguridad Cibernética (Australian Cyber Security Centre, ACSC)

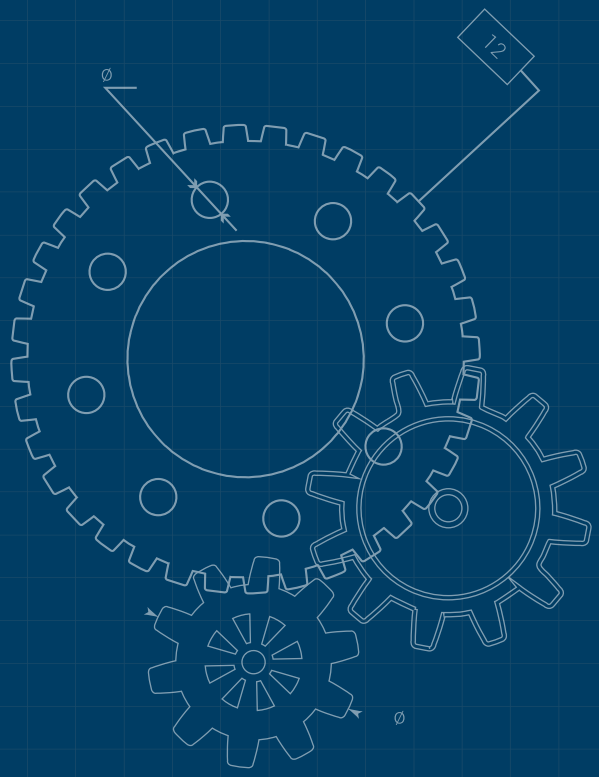
- Guía de seguridad por diseño de IoT de ACSC para fabricantes

### Centro Nacional de Seguridad Cibernética del Reino Unido(NCSC-UK)

- El marco de evaluación cibernética del NCSC-Reino Unido
- Guía de implementación y desarrollo seguro del NCSC-Reino Unido
- Guía de gestión de vulnerabilidades del NCSC-Reino Unido
- Conjunto de herramientas de divulgación de vulnerabilidades del NCSC-Reino Unido
- CHERI de la Universidad de Cambridge
- Hasta luego y gracias por todos los detalles - NCSC.GOV.UK

### Centro Canadiense de Seguridad Cibernética (Canadian Centre for Cyber Security, CCCS)

- Guía de CCCS sobre protección contra ataques a la cadena de suministro de software
- Cadena de suministro cibernética: un enfoque para evaluar los riesgos
- Guía sobre ransomware CONTI del Centro Canadiense de Seguridad Cibernética



### Oficina Federal de Seguridad de la Información (BSI) de Alemania

- Compendio de protección básica de IT de BSI Edición 2022
- La norma internacional IEC 62443, parte 4-1
- El estado de la seguridad informática en Alemania en 2022
- Seguridad de aplicaciones web: Catálogo de Medidas y Mejores Prácticas

### Centro Nacional de Seguridad Cibernética de los Países Bajos

- Hoja informativa sobre autenticación para adultos del NCSC-NL

### Centro Nacional de Preparación para Incidentes y Estrategia para la Ciberseguridad (NISC) de Japón

- La estrategia nacional de ciberseguridad de Japón

### Ministerio de Economía, Comercio e Industria de Japón (METI)

- Guía de introducción de la lista de materiales de software (SBOM) para la gestión de software
- Colección de ejemplos de casos de uso sobre métodos de gestión para utilizar OSS y garantizar su seguridad

### Agencia de Seguridad Cibernética de Singapur

- Asesoramiento Técnico sobre Desarrollo Seguro de API
- Política de divulgación de vulnerabilidades de CSA SingCERT
- Lista de verificación de respuesta a incidentes de CSA SingCERT
- Guías de respuesta a incidentes de CSA SingCERT
- Marco de seguridad por diseño de CSA
- Lista de verificación del marco de seguridad por diseño de CSA
- Guía CSA para el modelado de amenazas cibernéticas
- Esquema de etiquetado de ciberseguridad CSA

### Otro

- Cómo fallan los sistemas complejos
- La nueva mirada en fallas de sistemas complejos

## REFERENCIAS

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom y referencias de SBOM en TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] Juran sobre Calidad por Diseño de JM Jurán, 1992.