**Spread the love**

Según lo solicitado en la Orden Ejecutiva de Ciberseguridad («EO») del 12 de mayo de 2021 publicada por la Administración de Biden ( aquí ), el *National Institute for Standards and Technology,* NIST ha publicado su definición de «software crítico» dentro del plazo de 45 días que establecía la OE. Esta definición de «software crítico» representa un requisito, conforme a la OE, para dotar de seguridad a la cadena de suministro de software, especialmente en lo relativo a los proveedores de servicios para el ejecutivo Federal de Estados Unidos. Eventualmente, se reflejará en un  futuro Reglamento Federal de Adquisiciones obligatorio para los proveedores de software. Como es sabido, los documentos sobre seguridad del NIST acaban constituyendo una referencia de definiciones y estándares en todo el mundo, y muy especialmente en el ámbito de la ciberseguridad.

acrobacias2015

La definición de NIST de «software crítico» como se establece en su documento técnico publicado el 25 de junio de 2021 incluye a cualquier software  que influye directamente sobre otro software o sobre componentes de otro software («dependencias directas» y cuenta con al menos uno de estos atributos:

- está diseñado para ejecutarse con permisos o privilegios o para administrar privilegios;
- tiene acceso directo o privilegiado a redes o recursos informáticos;
- está diseñado para controlar el acceso a datos o tecnología operativa;
- realiza una función fundamental para los servicios «críticos

de confianza»; o,

- opera fuera de los límites de confianza normales, con acceso privilegiado.

El documento técnico especifica además, que  esa definición se aplica a software muy variado, como software independiente, software integral para dispositivos o componentes de hardware específicos, software basado en la nube; y tanto cuando ha sido adquirido por compra como cuando es desarrollado en sistemas de producción y utilizado para fines operativos. Sin embargo,  cuando se trata de software utilizado únicamente para investigación o pruebas , es decir, que no se implementa en sistemas de producción, estaría fuera del alcance de esta definición.

By M.A. Díaz

NIST proporciona también información sobre cuestiones terminológicas de la propia definición. Por ejemplo las «Dependencias directas sobre otro software" significa, para un componente o producto dado, "otros componentes de software (por ejemplo, bibliotecas, paquetes, módulos) que están directamente integrados y son necesarios para el funcionamiento de la instancia de software en cuestión. No incluye las interfaces y servicios de lo que de otra manera serían productos independientes «. En cuanto a «Crítico para la confianza» significa «categorías de software utilizadas para funciones de seguridad como control de red, seguridad de punto final y protección de red».

El documento técnico, destinado principalmente a los contratistas con la administración federal,  también ofrece un cuadro que explica cada categoría de software que considera «crítico para la EO», así como una lista de preguntas frecuentes (FAQ) y respuestas. Las categorías de software enumeradas en la tabla de NIST incluyen los destinados a gestión de identidades, credenciales y acceso (ICAM), los sistemas operativos, hipervisores, entornos de contenedores, los navegadores web, el software de control y protección de red, supervisión y configuración de redes, seguimiento y análisis operativos, copias de

seguridad, almacenamiento remiro, entre otros.