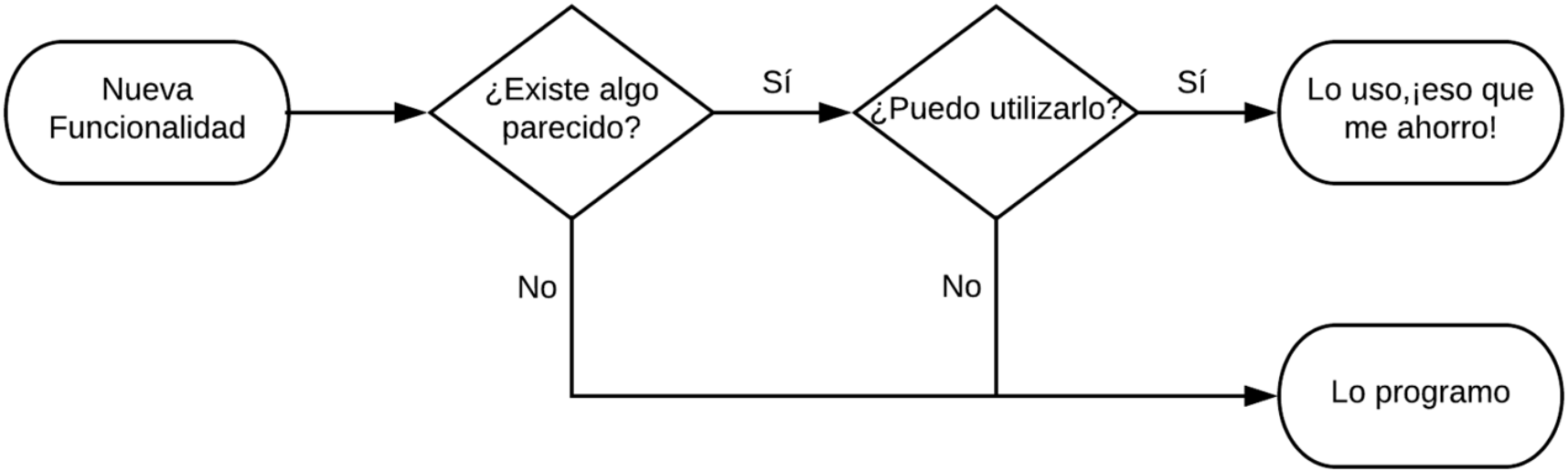
XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva

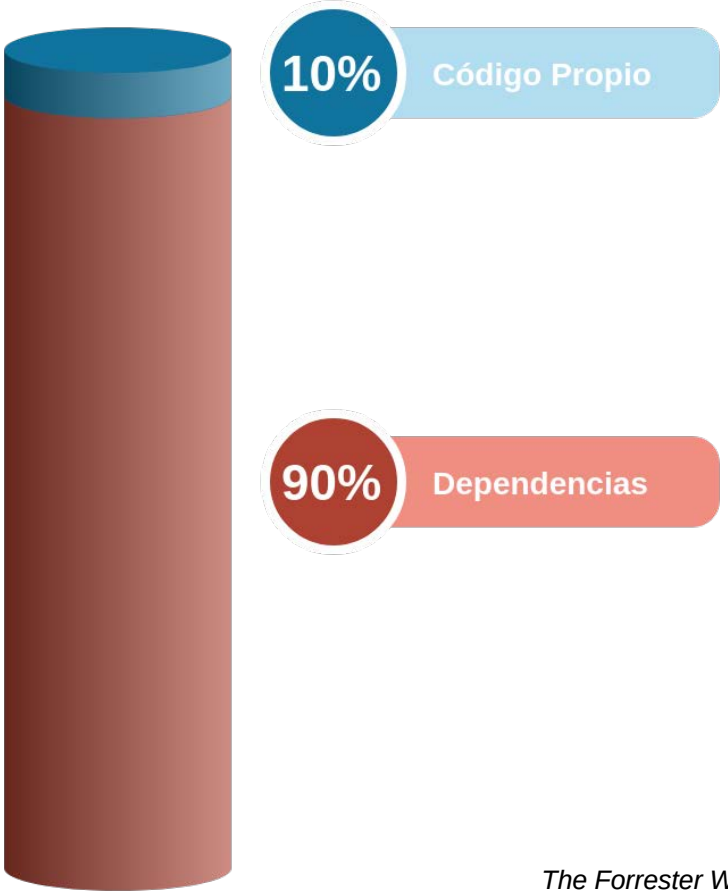
Detección de Dependencias Vulnerables en Entornos CI con Herramientas Open Source

centro criptológico nacional


Nueva Funcionalidad
¿Existe algo parecido?
Sí
¿Puedo utilizarlo?
Sí
Lo uso,¡eso que me ahorro!
No
No
Lo programo

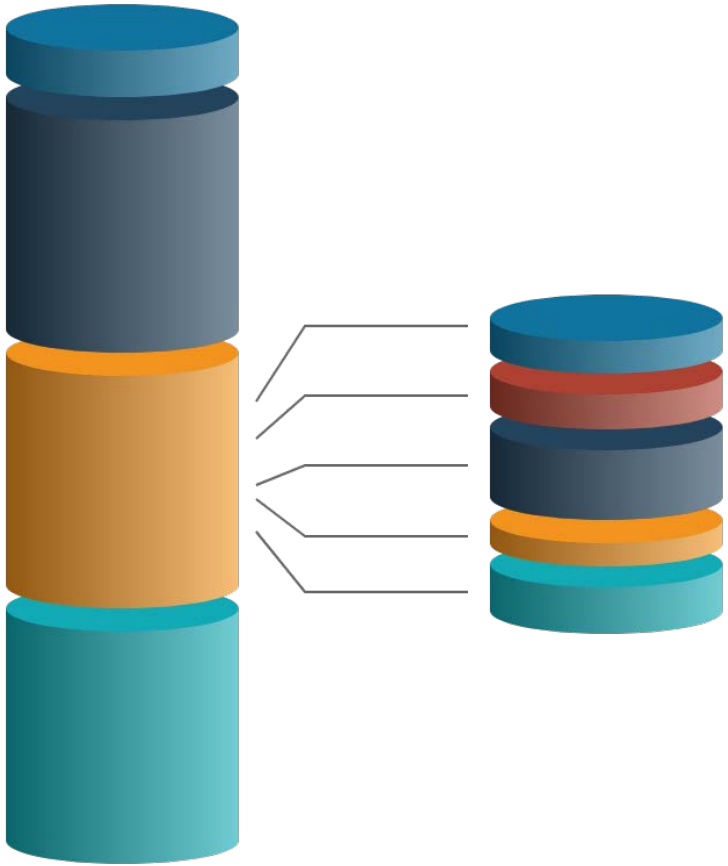
El **10% del código** de las aplicaciones es **nuevo**

El resto son componentes de **terceras partes**



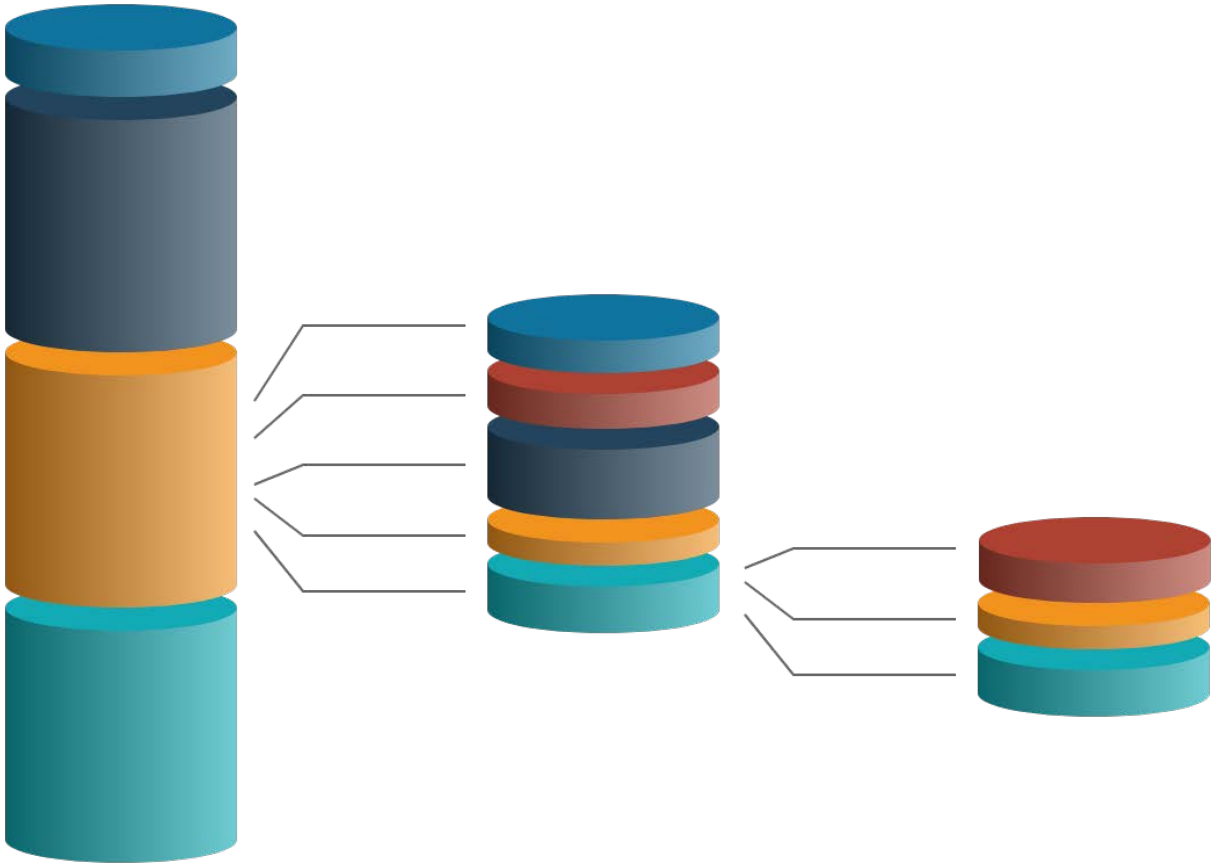
The Forrester Wave™: Software Composition Analysis, Q1 2017

Los componentes **pueden contener más** componentes



Los componentes **pueden contener más** componentes

Creando **estructuras anidadas**



Roberto Abdelkader Martínez Pérez (nilp0inter)

Desarrollador y analista de seguridad. Especialista en desarrollo de aplicaciones orientadas a la seguridad.

BBVA

BBVA Innovation Labs

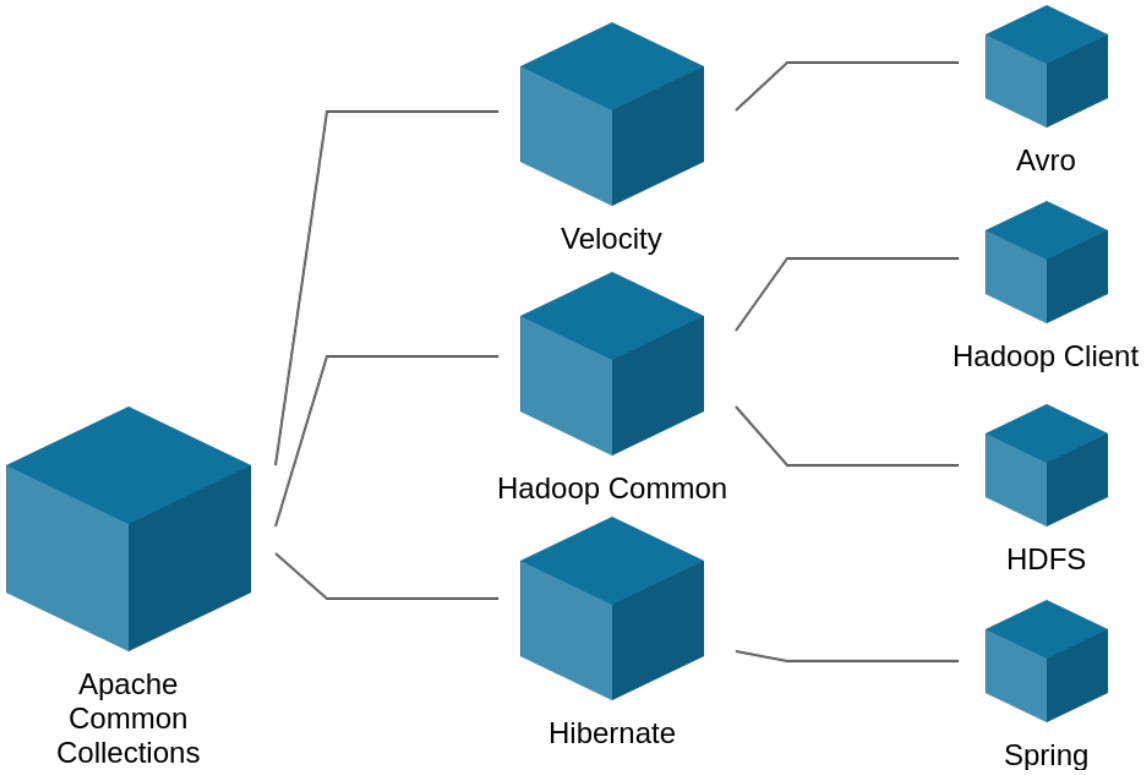
Daniel García García (cr0hn)

Investigador de seguridad, pentester y especialista en SecDevOps. Con numerosas herramientas de seguridad publicadas. Chapter Leader de OWASP Madrid.

BBVA

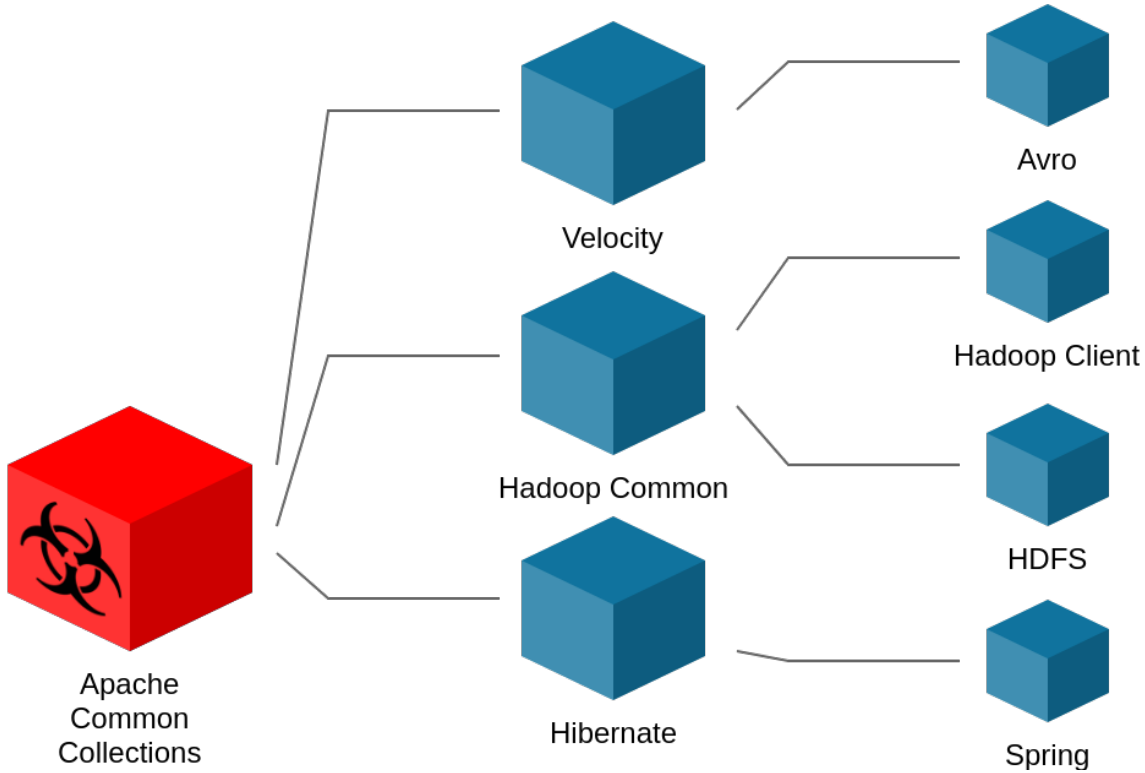
BBVA Innovation Labs

El componente ***Apache Commons Collections*** (ACC) es utilizado por **1.290 componentes**



El componente ***Apache Commons Collections*** (ACC) es utilizado por **1.290 componentes**

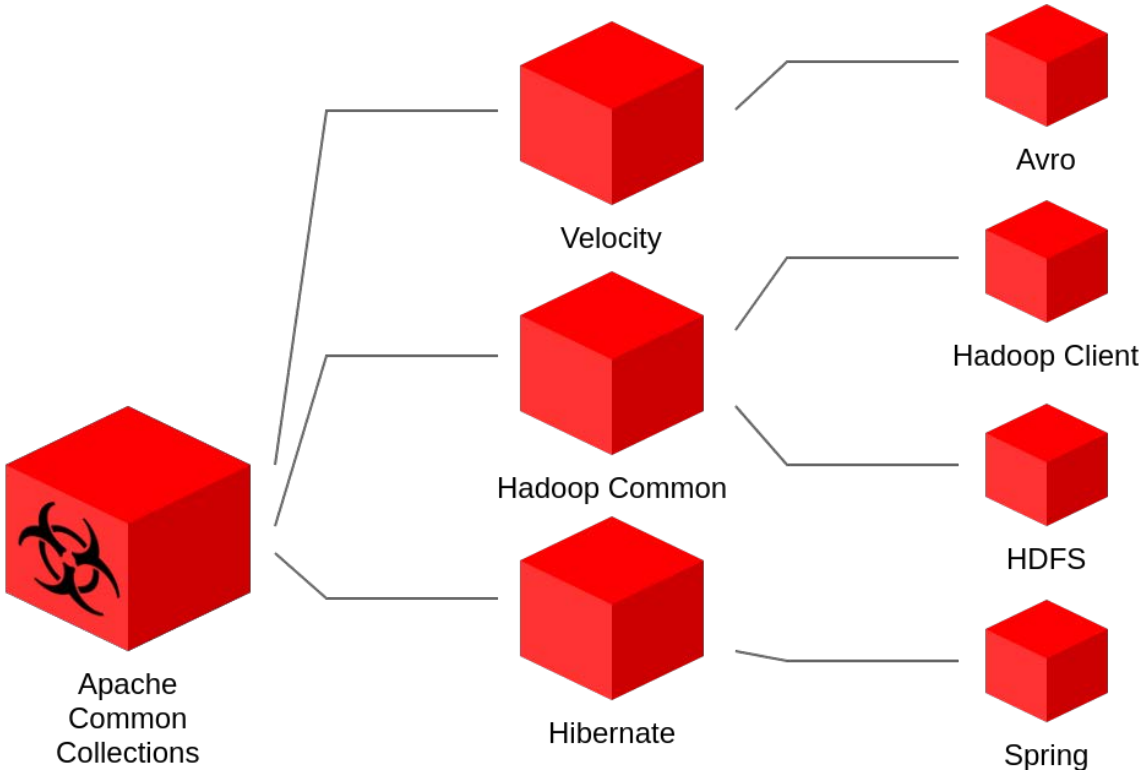
De forma indirecta **80.323 componentes**



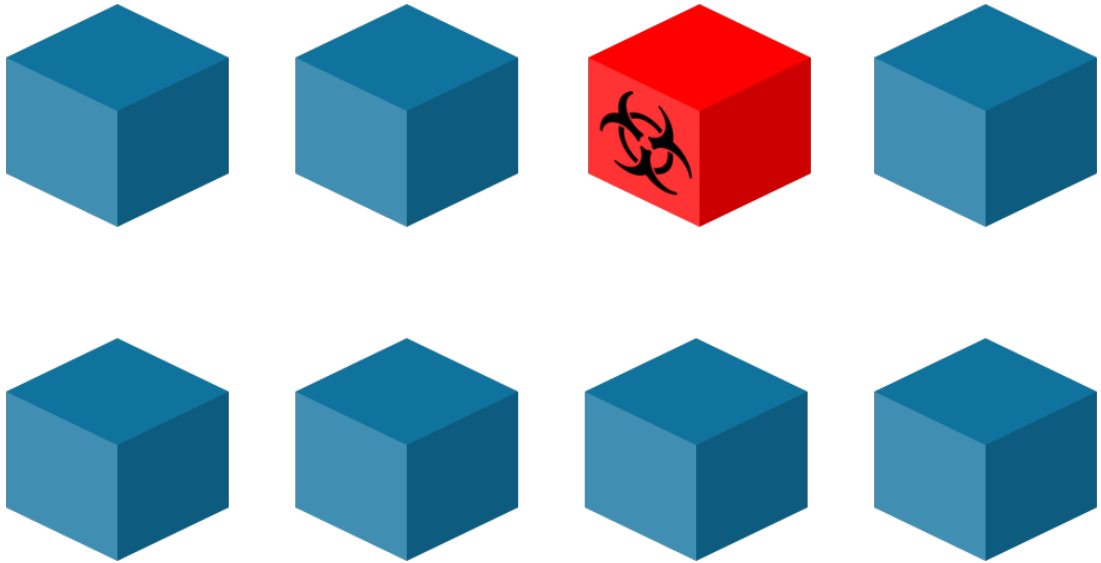
El componente ***Apache Commons Collections*** (ACC) es utilizado por **1.290 componentes**

De forma indirecta **80.323 componentes**

La **vulnerabilidad** descubierta en 2016 **afectó** a un **25% aplicaciones Java a nivel mundial**



Veracode: How One Open Source Component Put Up to 25% of Java Applications at Risk

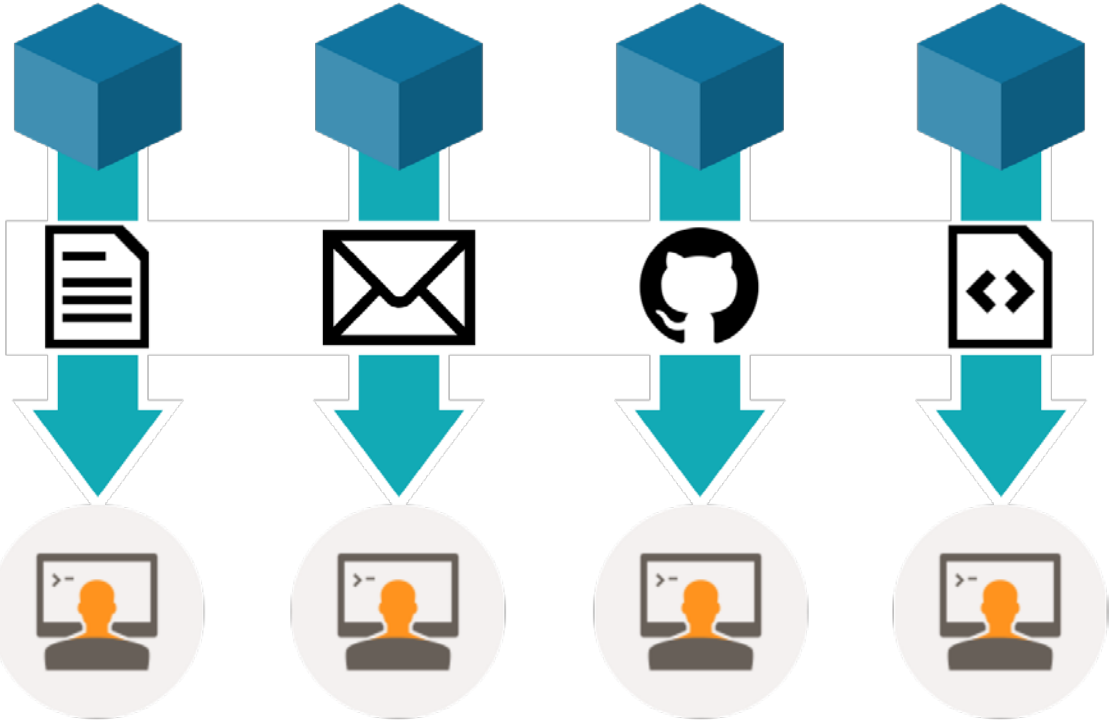


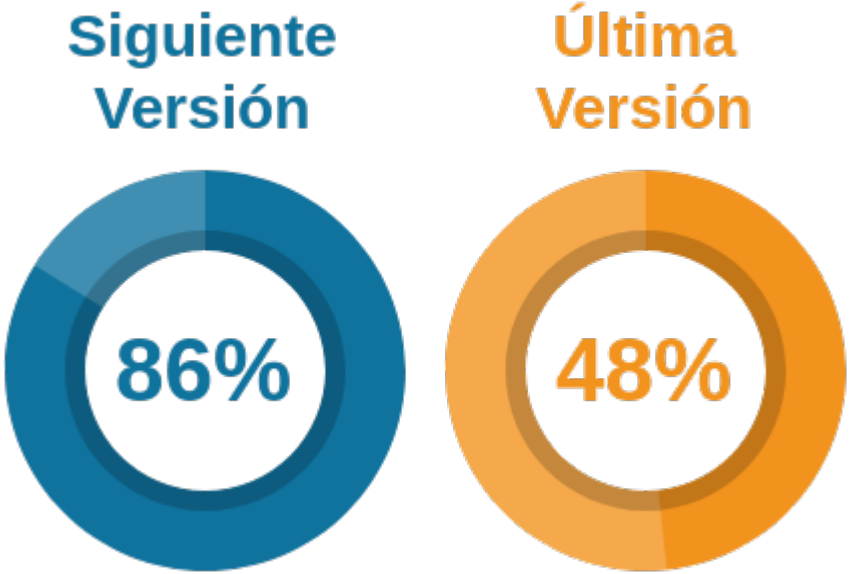
1 de cada 8 componentes descargados **en 2018** contenían algún tipo de **vulnerabilidad conocida**

Sonatype: 2018 State of the Software Supply Chain

No existe una manera estándar para **informar** a los desarrolladores de **nuevos parches de seguridad**

Cada componente utiliza su propio método: ***changelog***, ***newsletter***, ***ticketing system***...



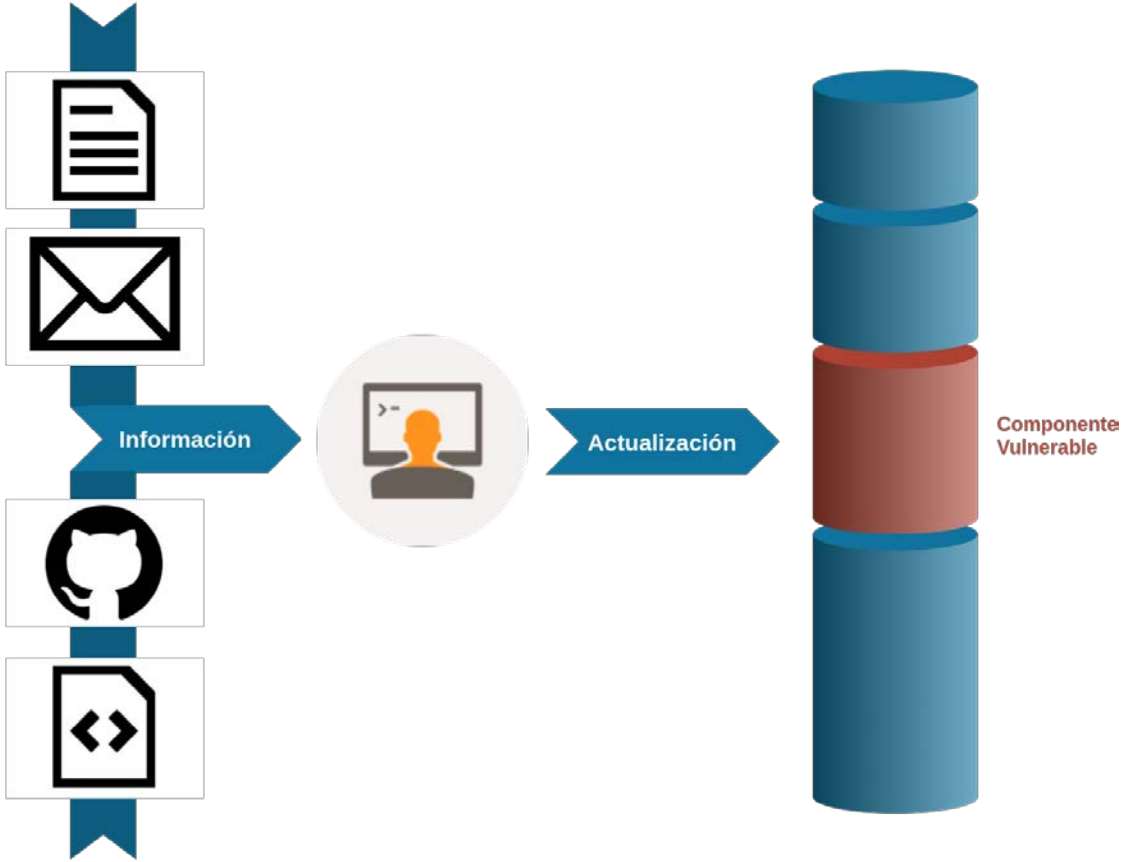


Un **86% de las aplicaciones** podrían actualizarse a la **siguiente versión** del componente **sin modificar su código**

Un **48%** podrían actualizarse **a la última versión disponible**

Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android

Es **necesario un canal único** para que los desarrolladores puedan conocer las **amenazas de seguridad** presenten en los **componentes** que utilizan



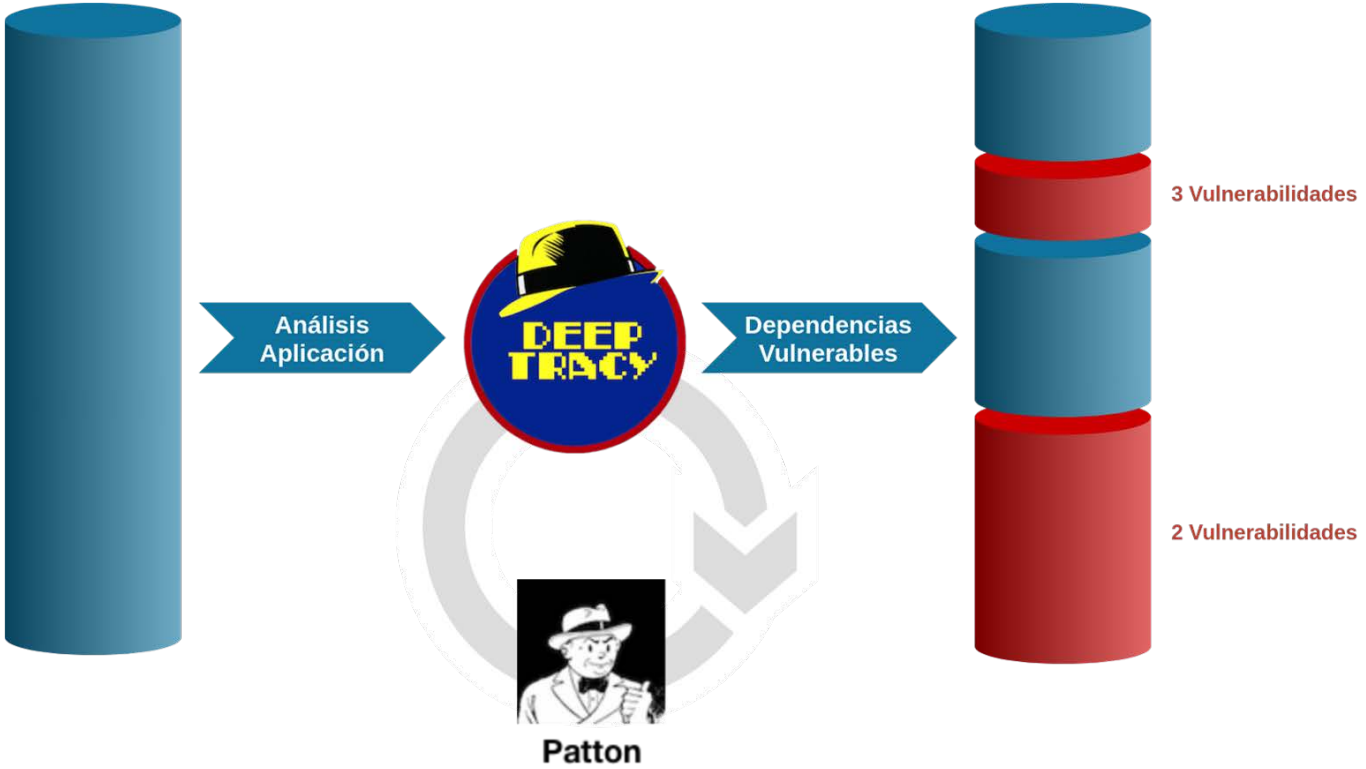
Los **nombres** de componentes **pueden colisionar** entre distintos stacks tecnológicos

NIST National Institute of Standards and Technology U.S. Department of Commerce

Las bases de datos de vulnerabilidades registran la afectación con **nombres estandarizados**, y no hacen referencia al nombre popular

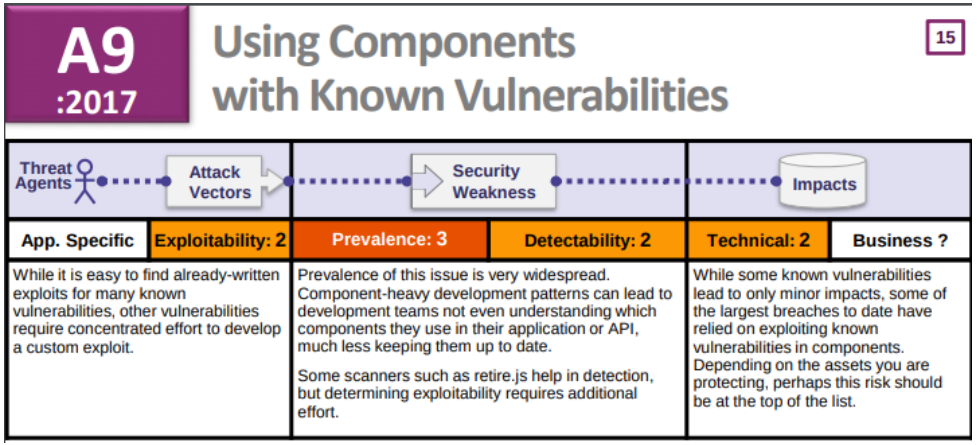
Patton es un servicio que permite **resolver las vulnerabilidades** de un componente **dado un nombre no estandarizado**

DeepTracy genera un inventario de componentes para un proyecto y utiliza ***Patton*** para descubrir sus vulnerabilidades

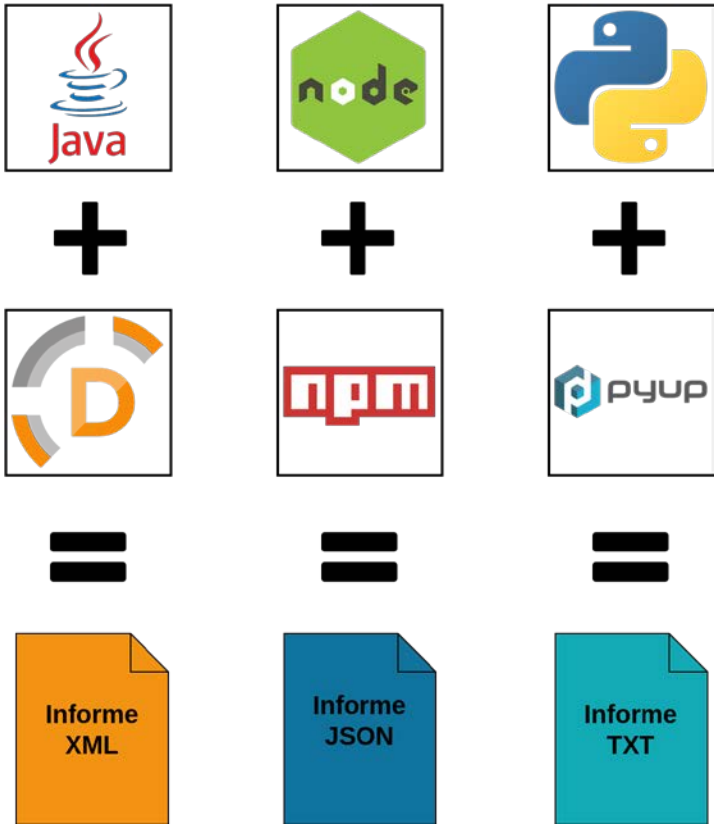


Desde **2013 OWASP** incluye el uso de componentes vulnerables entre su lista **The Ten Most Critical Web Application Security Risks**

OWASP
Open Web Application Security Project



OWASP Top 10 (2013 - 2017)



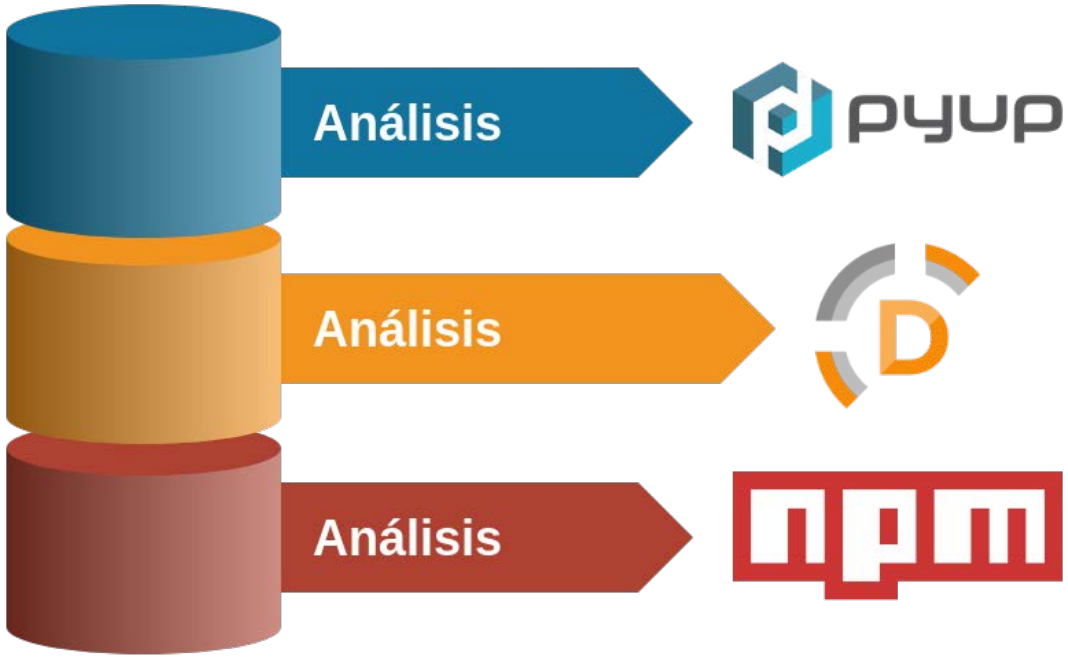
Las distintas comunidades de desarrollo han **reaccionado** a la amenaza creando diversas **herramientas para el control** de componentes en **vulnerabilidades**

Lamentablemente no existe ningún estándar y **no hay consenso** sobre cómo deberían funcionar.

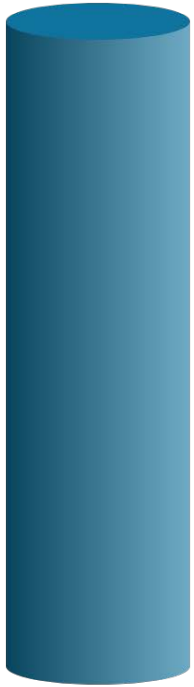
Creando un entorno **heterogéneo**

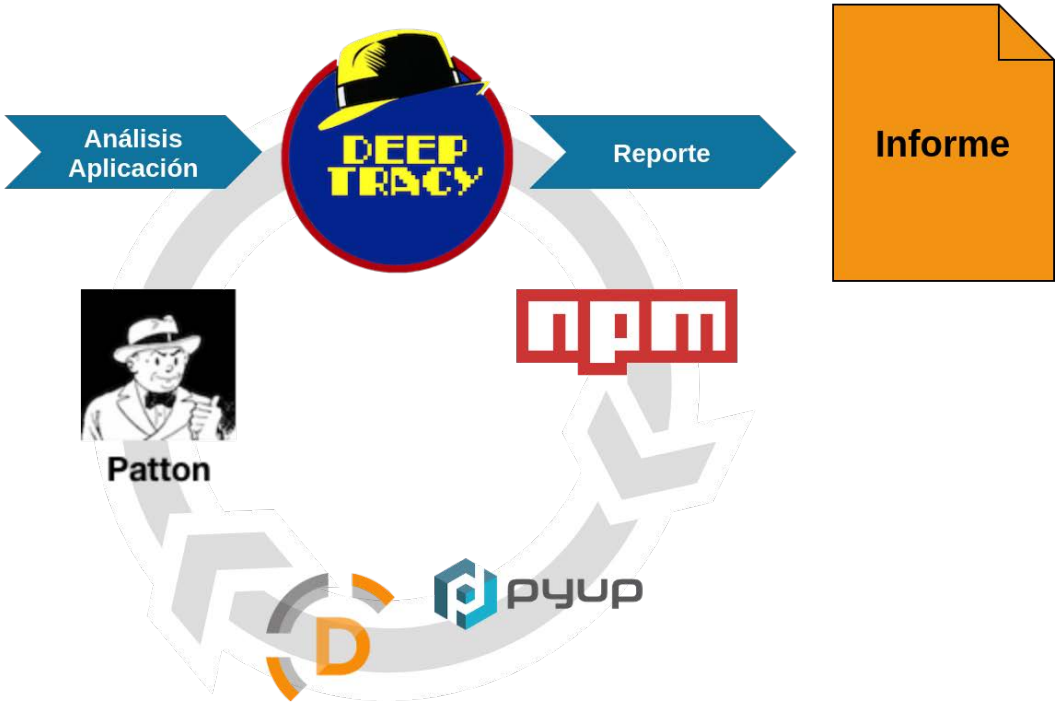
A día de hoy el **stack tecnológico** de una aplicación es a su vez **heterogéneo**

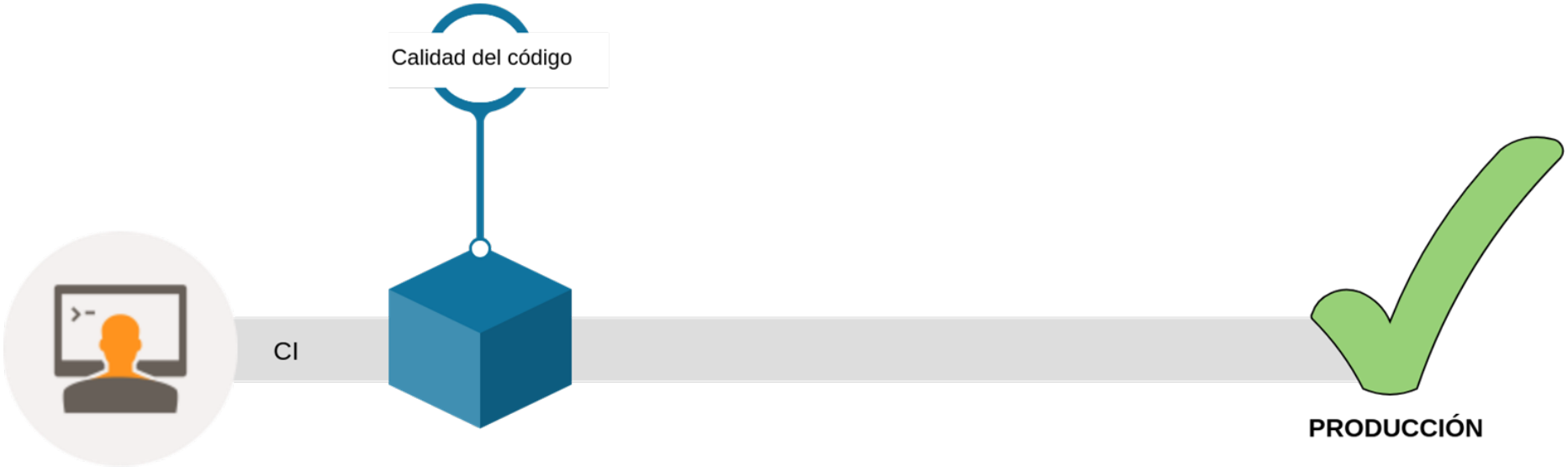
Forzando el **desarrollador** a volver a consumir **múltiples fuentes de vulnerabilidades**

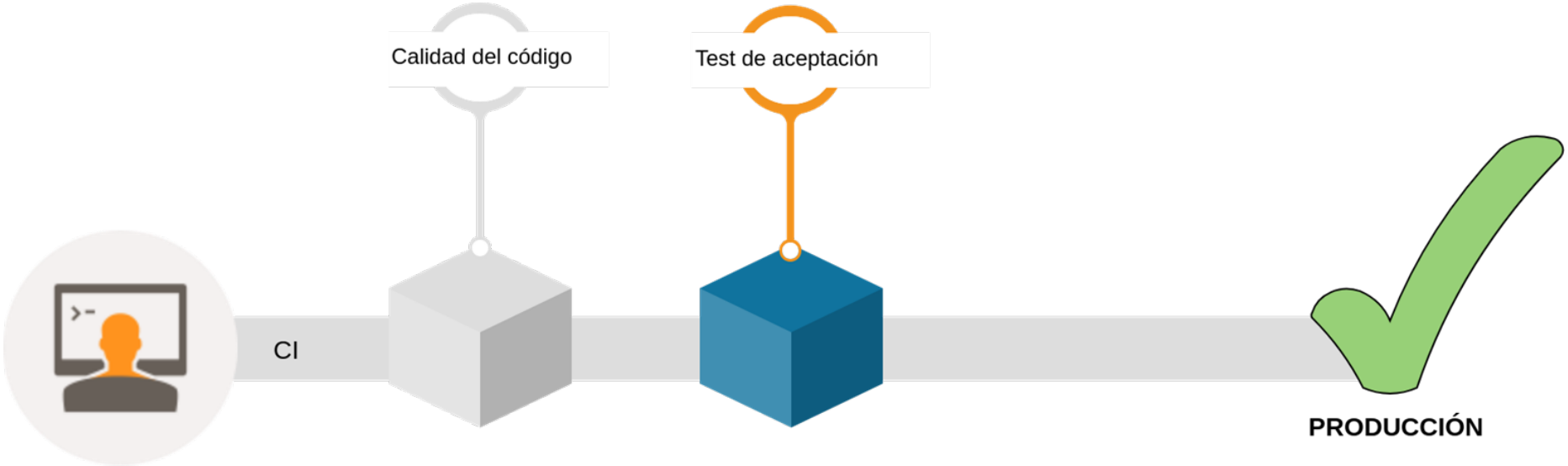


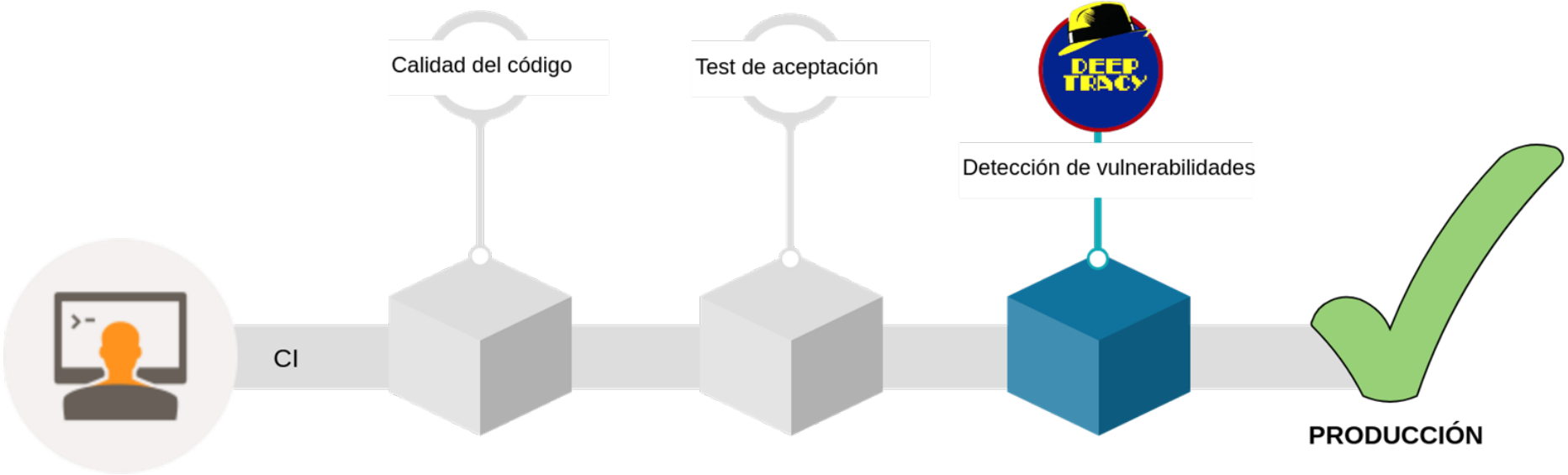
Hemos mejorado ***DeepTracy*** para incluir estas **nuevas herramientas** y facilitar la inclusión de nuevas herramientas **en el futuro**






Calidad del código
CI
PRODUCCIÓN


Calidad del código
Test de aceptación
CI
PRODUCCIÓN


Calidad del código
Test de aceptación
DEEP TRACY
Detección de vulnerabilidades
CI
PRODUCCIÓN

Casos de éxito **reales** de Deeptracy y Patton

BBVA Next Technologies

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectiva

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional