2026

MARCO NORMATIVO DE IT

Changelog del Estándar de Desarrollo Agencia de Sistemas de Información

Setiembre 2026

Índice

El presente documento es complementario al documento ES0901 - Estándar de Desarrollo ASI v6.4. Su finalidad es brindar detalles sobre que contenido ha sido actualizado en él.

Dado que para la versión 6.4 solo se han modificado lo detallado a continuación, también se incluyen los cambios realizados oportunamente a la versión 6. 3 del estándar.

Changelog v6.4

6.10 – Herramientas y Versiones aceptadas por la ASI

- Se modifica el criterio de homologación de herramientas, principalmente diferenciando al stack tecnológico del stack de programación.

Anexo II - Herramientas de Desarrollo y Versiones homologadas

- **Vulnerabilidad: Inyección de CRLF en la regla de correo electrónico predeterminada de Laravel permite el contrabando SMTP y la retransmisión de correo falsificado.**

  Se ha reportado una vulnerabilidad en Laravel, un framework para aplicaciones web. Previo a las versiones 12.60.0 y 13.10.0, una vulnerabilidad de inyección CRLF en la validación de correo electrónico de Laravel, en combinación con la forma en que Symfony Mailer y Symfony Mime manejan ciertas secuencias de caracteres, podía permitir que un atacante no autenticado interfiriera en el procesamiento de correos salientes en aplicaciones que envían correos a direcciones proporcionadas por el usuario. Este problema se ha corregido en las versiones 12.60.0 y 13.10.0. Su grado de severidad CVSS es 8.9 (**HIGH**).

  Para más información, se pude consultar:

  - **CVE Program - MITRE**: https://www.cve.org/CVERecord?id=CVE-2026-48019

- Dado el cambio en los criterios de homologación de herramientas detallado en el apartado *6.10 – Herramientas y Versiones aceptadas por la ASI*, se eliminan de este anexo los listados de bibliotecas.

Changelog v6.3

Anexo II - Herramientas de Desarrollo y Versiones homologadas

- **Vulnerabilidad: Ejecución de código arbitrario en NLTK StanfordSegmenter**

  Se ha reportado una vulnerabilidad crítica en la biblioteca NLTK, utilizada en Python para procesamiento de lenguaje natural. Bajo el identificador CVE-2026-0848, este fallo introduce un riesgo crítico en entornos donde se utilizan herramientas de análisis de texto o sistemas basados en inteligencia artificial, permitiendo ejecutar código remoto (RCE). Es decir, un atacante podría ejecutar instrucciones arbitrarias en un sistema vulnerable. Su grado de severidad CVSS es 10.0 (**crítico**).

  La vulnerabilidad está en cómo NLTK gestiona ciertos recursos externos: al cargar archivos sin validar correctamente su origen o su contenido, el recurso manipulado puede terminar siendo procesado como legítimo. Si un atacante consigue introducir un archivo malicioso en el flujo de datos que consume la aplicación, ese código podría ejecutarse directamente en el sistema.

  Para corregirlo, se ha actualizado la versión de esta biblioteca **NLTK** de la **3.9.2** a **3.9.4**.

  Para más información, se pude consultar:

  - **National Vulnerability Database**: https://nvd.nist.gov/vuln/detail/CVE-2026-0848.
  - **Huntr**: https://huntr.com/bounties/08b109bb-ac24-403f-9422-1c246ce60202