XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

LINCE – Adaptando la certificación de ciberseguridad

centro criptológico nacional

jtsec BEYOND IT SECURITY

- José Francisco Ruíz Gualda – CTO en jtsec
- e-mail: jruiz@jtsec.es

- jtsec Beyond IT Security - Empresa especializada en certificaciones de ciberseguridad
- Más de 10 años de experiencia trabajando como evaluador y manager en Common Criteria
- Program Director en ICCC e ICMC
- Colaborador de CCN en la creación de LINCE

Índice

1. Antecedentes
2. Certificaciones: ¿Los malos de la película?
3. Adaptación: Nuevas tendencias en certificación
4. Certificación LINCE
5. Conclusiones

Antecedentes

Antecedentes

Esquema Nacional de Seguridad (ENS)

- Art 18: “En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se **utilizarán**, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan **certificada la funcionalidad de seguridad** relacionada con el objeto de su adquisición, **salvo en aquellos casos** en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen **a juicio** del responsable de Seguridad”

ens Esquema Nacional de Seguridad

Esquema Nacional de Seguridad (ENS)

- Medidas Anexo 2: “Componentes certificados [op.pl.5]”

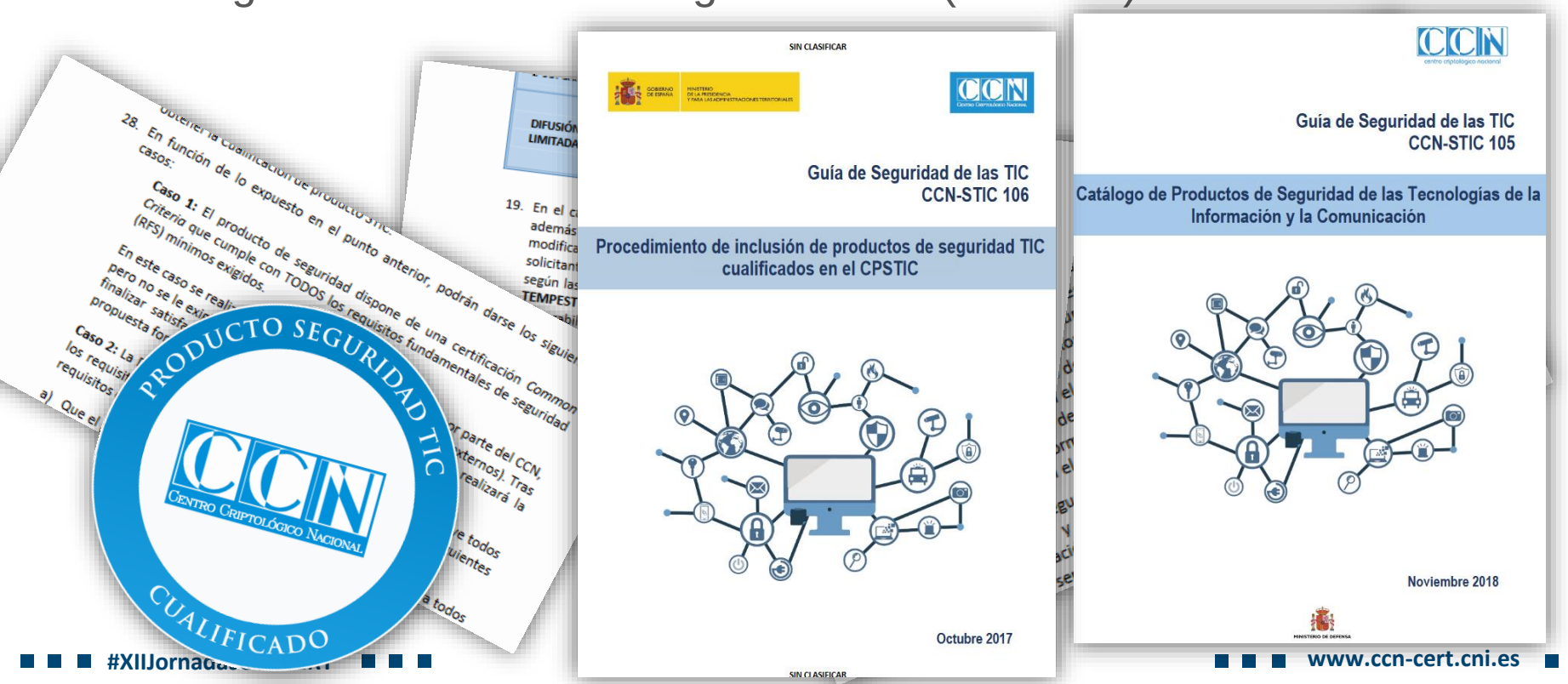
  - Categoría ALTA

  - Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a **normas europeas o internacionales** y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

ens Esquema Nacional de Seguridad

Antecedentes

Catálogo de Productos de Seguridad TIC (CPSTIC)



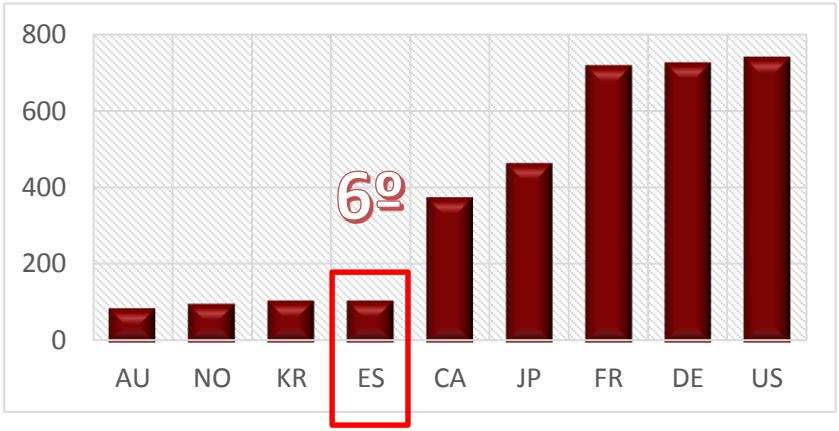
Antecedentes

Ranking PIB vs Productos certificados

Ránking mundial. PIB, en miles de millones de dólares corrientes

	2017		2019		2021		2022	
1	EEUU	19.417,14	EEUU	21.239,30	EEUU	22.886,24	EEUU	23.760,33
2	China	11.795,30	China	13.862,97	China	16.340,87	China	17.706,63
3	Japón	4.841,22	Japón	5.085,74	Japón	5.261,88	Japón	5.368,19
4	Alemania	3.423,29	Alemania	3.617,09	Alemania	3.827,70	India	3.935,27
5	Reino Unido	2.496,76	India	2.959,67	India	3.577,13	Alemania	3.923,42
6	India	2.454,46	Reino Unido	2.607,85	Reino Unido	2.780,86	Reino Unido	2.873,37
7	Francia	2.420,44	Francia	2.562,28	Francia	2.734,10	Francia	2.815,34
8	Brasil	2.140,94	Brasil	2.340,84	Brasil	2.560,12	Brasil	2.676,27
9	Italia	1.807,43	Italia	1.879,41	Italia	1.960,25	Italia	1.993,57
10	Canadá	1.600,27	Canadá	1.719,45	Canadá	1.847,90	Canadá	1.912,81
11	Rusia	1.560,71	Rusia	1.654,09	Rusia	1.781,72	Rusia	1.840,86
12	Corea	1.498,07	Corea	1.617,44	Corea	1.756,27	Corea	1.829,01
13	Australia	1.359,72	Australia	1.497,52	Australia	1.636,25	Australia	1.709,81
14	España	1.232,44	España	1.320,08	Indonesia	1.465,84	Indonesia	1.615,56
15	Indonesia	1.020,52	Indonesia	1.206,15	España	1.411,76	España	1.451,81
16	México	987,30	México	1.094,60	México	1.217,79	México	1.283,97
17	Turquía	793,70	Turquía	876,63	Turquía	982,31	Turquía	1.031,52
18	Holanda	762,69	Holanda	807,67	Holanda	855,28	Argentina	908,33
19	Arabia Saudí	707,38	Arabia Saudí	763,00	Argentina	840,35	Holanda	876,02

Fuente: FMI — Expansión



Antecedentes

TEJIDO EMPRESARIAL

DISTRIBUCIÓN POR TAMAÑO DEL TEJIDO EMPRESARIAL

2009 - 2015. En % sobre el total.

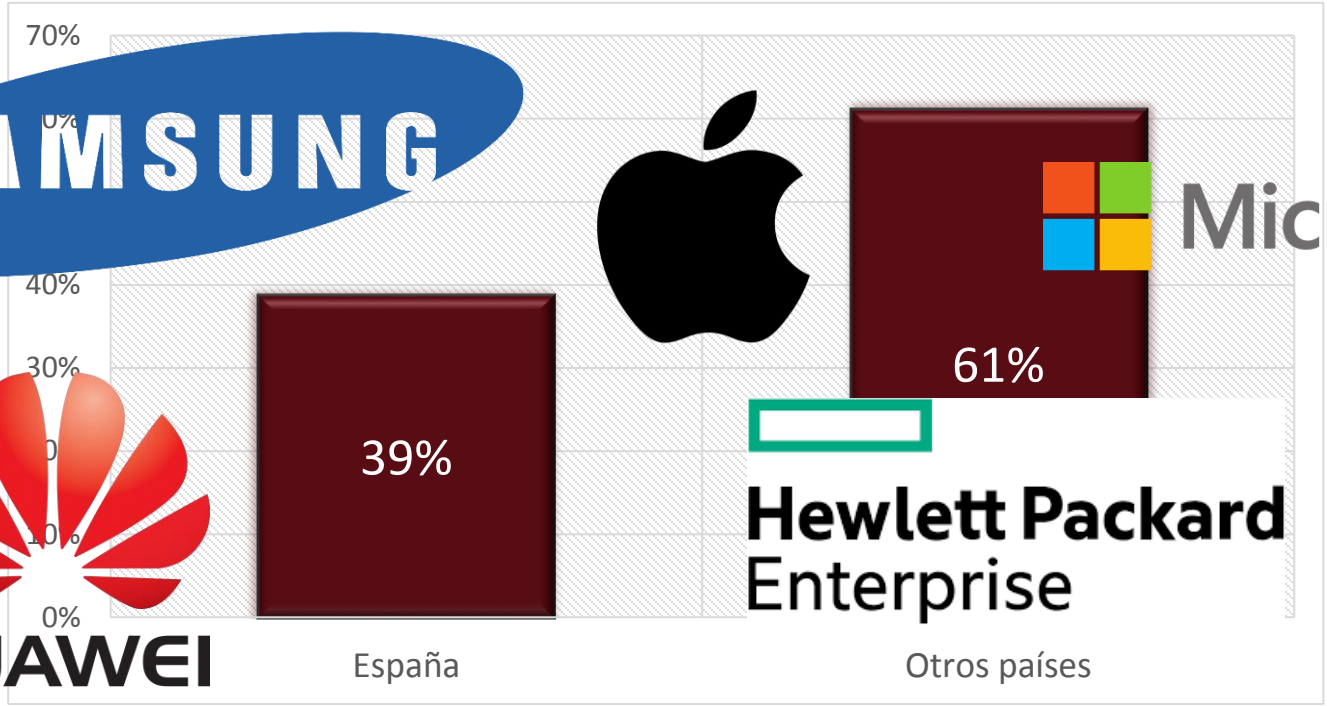
	2009				2015			
	Micro (0-9)	Pequeñas (10-49)	Medianas (50-249)	Grandes (Más de 250)	**Micro (0-9)**	Pequeñas (10-49)	Medianas (50-249)	Grandes (Más de 250)
España	**83,8**	5,4	0,7	0,1	**94,5**	4,8	0,6	0,1
Alemania	**82,8**	14,2	2,6	0,5	**81,7**	15,2	2,6	0,5
Francia	**93,2**	5,7	0,9	0,2	**93,3**	5,6	0,9	0,2
Italia	**94,5**	4,9	0,5	0,1	**94,8**	4,6	0,5	0,1
Portugal	**95,0**	4,3	0,6	0,1	**95,5**	3,8	0,6	0,1
Reino Unido	**89,1**	8,9	1,6	0,4	**88,8**	9,3	1,6	0,3

Eurostat, Círculo de Empresarios, INE. Subdirección General de Apoyo a la PYME, IESE, Ministerio de Empleo y Seguridad Social. EL PAÍS

Certificaciones: un mundo para Grandes Empresas!

Antecedentes

Procedencia de fabricantes certificados en España



Certificaciones:
¿Los malos de la película?

Certificaciones: ¿Los malos de la película?

Common Criteria

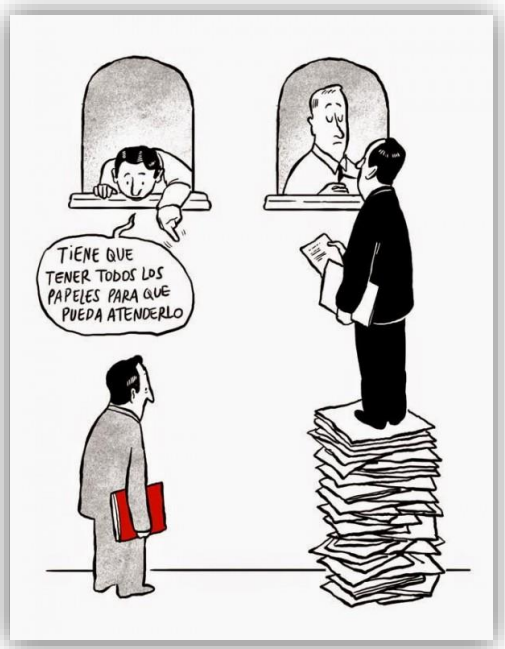
- **Metodología de evaluación – Más completa!**
  - **Potente** – An. Vulnerabilidades, Pruebas, Ciclo de Vida, Doc., etc…
  - Versátil – Aplicable a todo tipo de productos (e.g. Firewall o DNI)
  - Flexible – Distintos niveles de garantía (EALs)

- Certificados reconocidos **internacionalmente**

Certificaciones: ¿Los malos de la película?

Hacking ético vs Evaluación de producto en CC

- Diferencias:
  - Alcance de la evaluación
  - Metodología
  - Rigurosidad - Validación
  - Marketing
  - Precio
  - Complejidad



Adaptación: Nuevas tendencias en certificación

Adaptación: Nuevas tendencias en certificación

Alternativas a Common Criteria

- Esquemas privados **basados** en Common Criteria

- Iniciativa del gobierno francés: CSPN

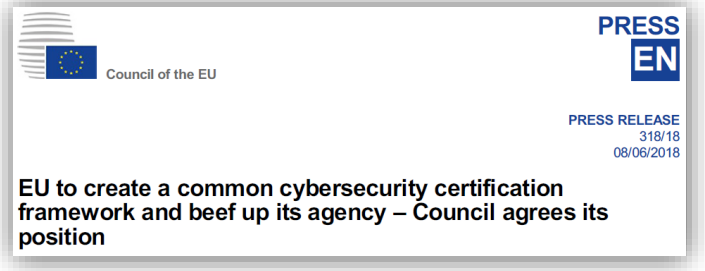
EMVCo™ FeliCa MIFARE


CPA
BSPA
BSZ
CSPN
LINCE
TSA
AISEP

Adaptación: Nuevas tendencias en certificación

Framework de certificación europeo

- Esquema de certificación que sea **común a todos los países**.
- Tres niveles de garantía: básico, **sustancial** y alto.
- Este esquema establece directrices de seguridad para cuatro categorías:
  - Productos y componentes
  - Servicios ICT
  - Proveedores de servicios y organizaciones
  - Profesionales de la seguridad


Council of the EU

PRESS
EN

PRESS RELEASE
318/18
08/06/2018

EU to create a common cybersecurity certification framework and beef up its agency – Council agrees its position

Adaptación: Nuevas tendencias en certificación

Otras iniciativas

- Smart CC
- CEN/CLC/JTC 13 WG3
  - Lightweight Evaluation Methodology Project

Certificación LINCE

Certificaciones LINCE

Introducción a LINCE

- LINCE es una metodología de evaluación de productos TIC basada en los principios de Common Criteria

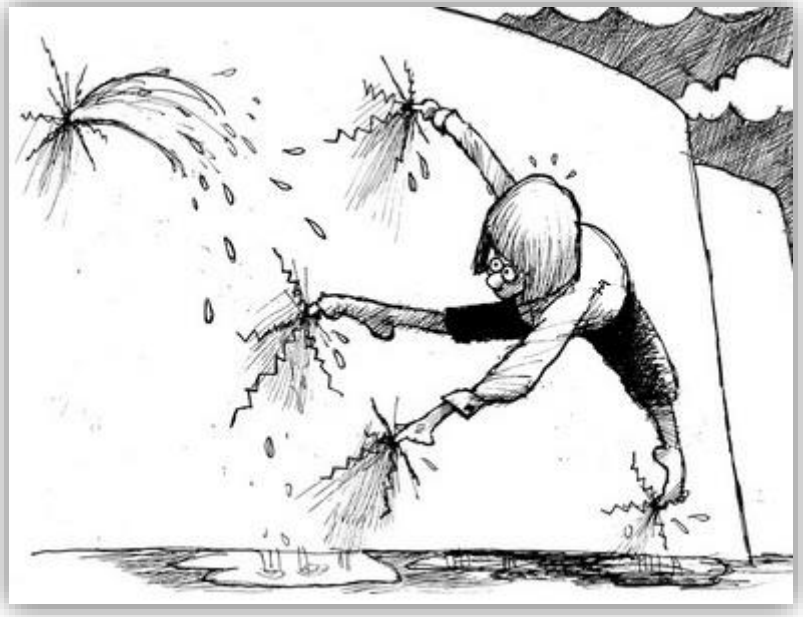
- Orientada al **análisis de vulnerabilidades y los tests de penetración**

- Diferencias con Common Criteria:
  - Esfuerzo, coste y duración **acotados**
  - Elimina complejidad
  - Reconocimiento nacional

Certificaciones LINCE

Introducción a LINCE

- LINCE no tiene la robustez de Common Criteria…



… pero permite cubrir más puntos vulnerables en menos tiempo.

Certificaciones LINCE

Introducción a LINCE

- LINCE permite el acceso al catálogo CPSTIC para niveles bajo y medio

- Metodología para pruebas complementarias STIC

Certificaciones LINCE

Estructura de la norma

- LINCE se divide en cuatro documentos:
  - CCN-LINCE-001: Definición
  - CCN-LINCE-002: Metodología de Evaluación
  - CCN-LINCE-003: Plantilla para la Declaración de Seguridad (ST)
  - CCN-LINCE-004: Plantilla del Informe Técnico de Evaluación (ETR)

Nota: Disponibles en la web del CCN

Certificaciones LINCE

Módulos de evaluación

- El módulo de evaluación básico es obligatorio y común a todas las evaluaciones (25 días / 8 semanas):
  - No incluye la preparación de la evaluación ni la formación de los evaluadores
  - Se requieren evaluadores expertos en la tecnología
  - El laboratorio debe presentar el plan de evaluación al OC
  - El laboratorio debe emitir el informe de evaluación

CCN-LINCE-004

Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE)

Certificaciones LINCE

Módulos de evaluación

- Además, LINCE ofrece dos módulos opcionales

  - Módulo de Evaluación Criptográfica (MEC):
    - Pruebas sobre algoritmos criptográficos
    - Validación conformidad de algoritmos

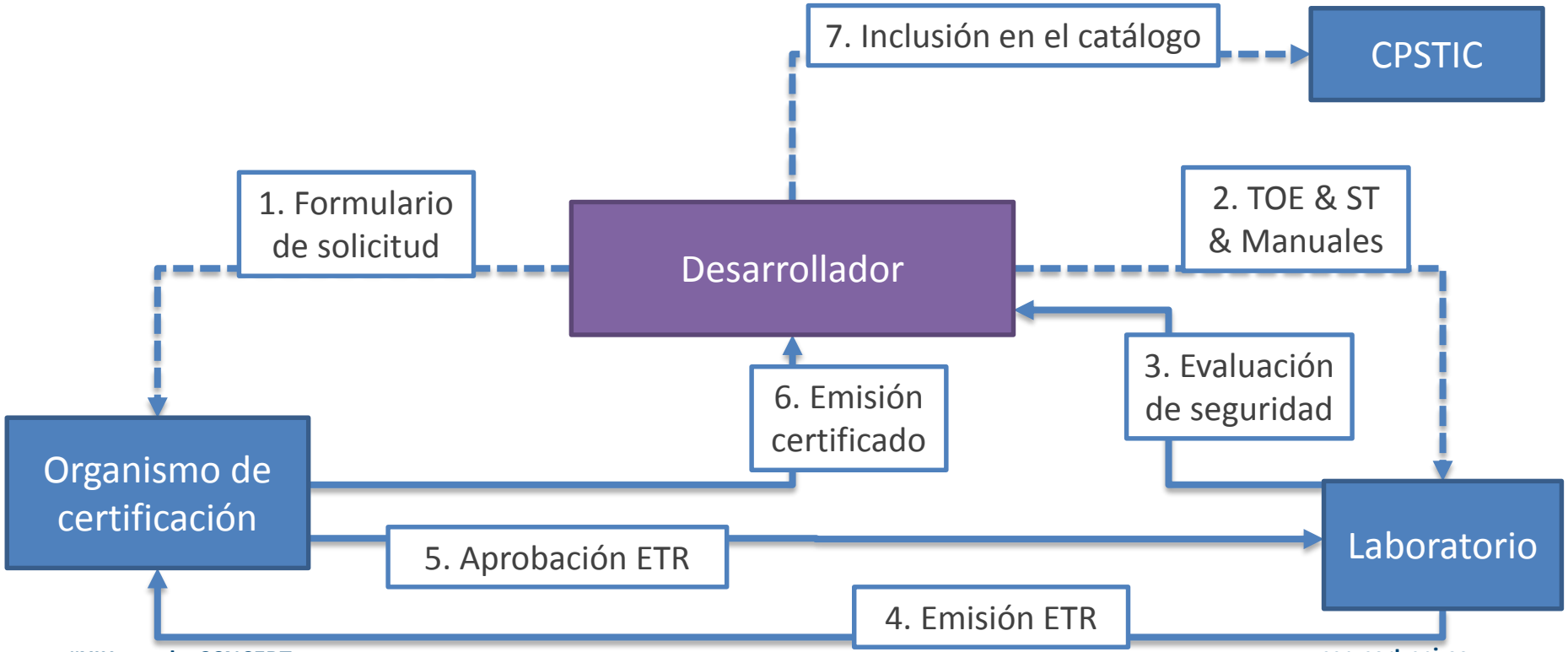
  - Módulo de evaluación de Código Fuente (MCF)
    - Pruebas caja blanca
    - Revisión de código fuente

LINCE para desarrolladores

- Para dar comienzo a la evaluación, el fabricante debe preparar:
  - Declaración de seguridad (CCN-LINCE-003)
  - Guías de instalación y operación
  - Entorno de pruebas/ejecución (en colaboración con el laboratorio)
  - (MCF) Código fuente de los mecanismos de seguridad del TOE
  - (MEC) Información de los mecanismos criptográficos

Certificaciones LINCE

Fases de la certificación:

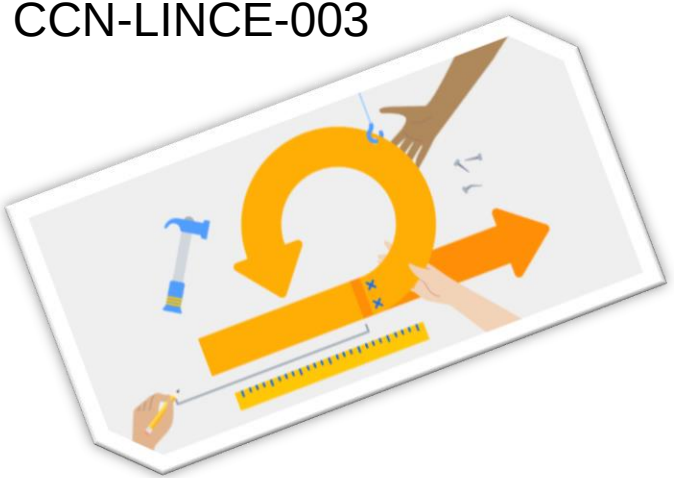


Certificaciones LINCE

Fases de la evaluación:

1. Análisis de la declaración de seguridad (1 día)
   - Comprobar que la declaración de seguridad del fabricante es correcta
   - Este documento debe seguir lo establecido en CCN-LINCE-003

2. Instalación del producto (1 día)
   - Preparar el producto para la realización de las pruebas



3. Análisis de la documentación (2 días)
   - Analizar la documentación – Ganar conocimiento del producto

Certificaciones LINCE

Fases de la evaluación:

4. Pruebas funcionales (5 días)

- Comprobar que el producto funciona conforme a la funcionalidad declarada

5. Análisis de vulnerabilidades (6 días)

- Estudio de vulnerabilidades en el dispositivo.
- Sesiones de trabajo con el fabricante.

Factor	Intervalo	Valor para identificar una vulnerabilidad	Valor para explotar una vulnerabilidad
Tiempo necesario	< 1 hora	0	0
	< 1 día	2	3
	< 1 mes	3	5
	> 1 mes	5	8
	No práctico	*	*
Experiencia del atacante	Inexperto	0	0
	Competente	2	2

Certificaciones LINCE

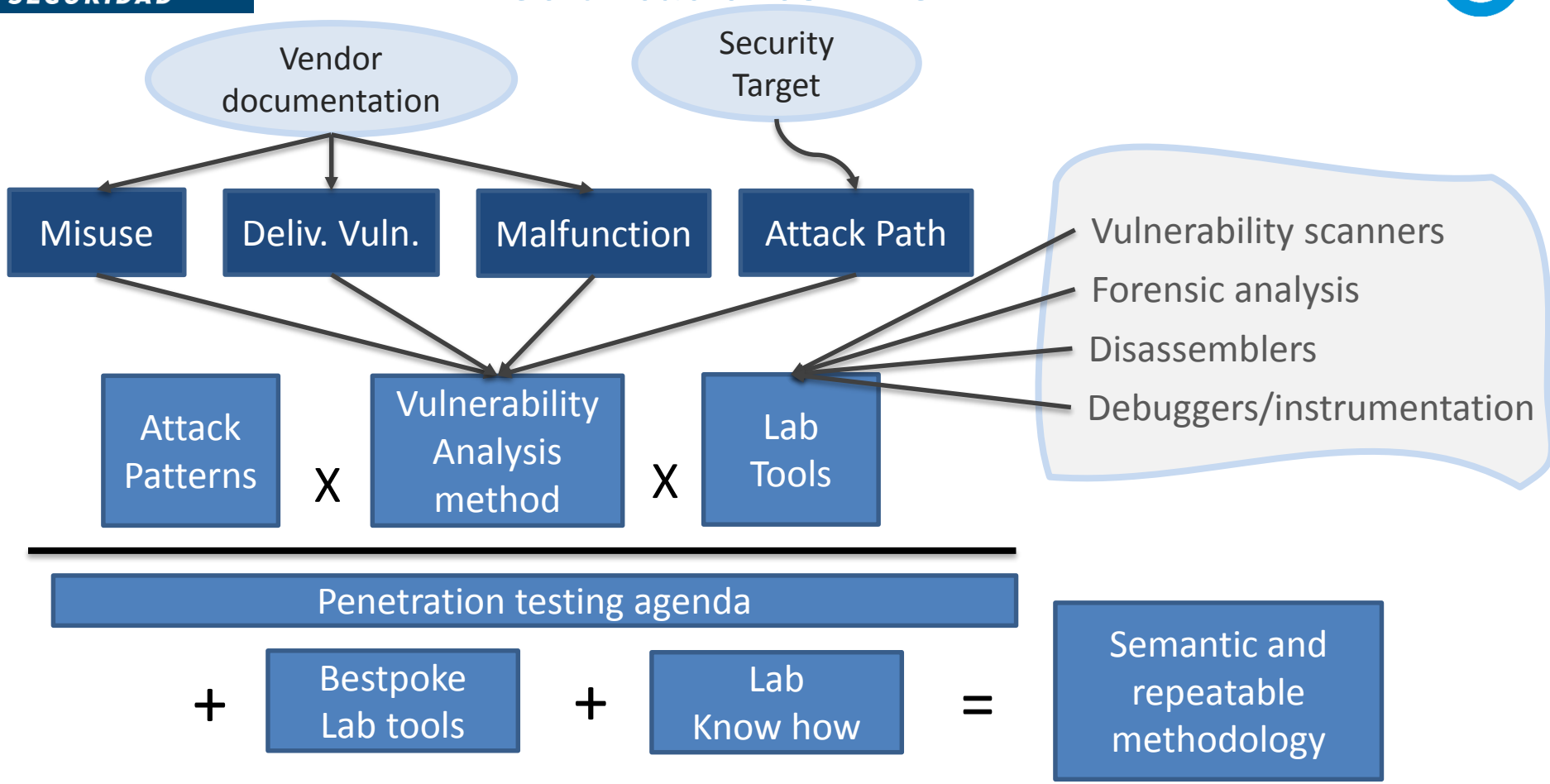
Fases de la evaluación:

6. Pruebas de penetración del TOE (10 días)

- Comprobaciones de la explotación de vulnerabilidades.
- Estas pruebas tienen un enfoque de caja negra.

Código de la prueba:	(Ej.- TEST_0xx)	
Función de seguridad probada:	Evaluador:	
	Objetivo de la prueba:	
Escenario de prueba:		
Procedimiento	Resultados esperados	Resultados obtenidos
Conclusión y veredicto:		

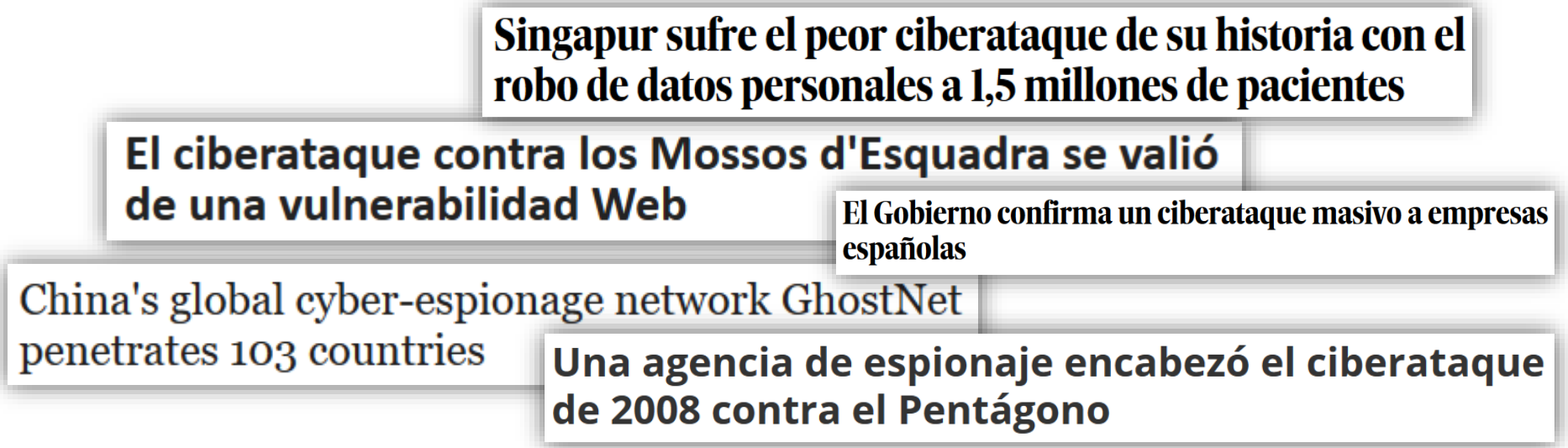
Certificaciones LINCE



Certificaciones LINCE

¿De qué nos protege LINCE?

- Las empresas y administraciones ofrecen cada vez más servicios usando productos informáticos, lo que aumenta la superficie de ataque sobre ellos.



Certificaciones LINCE

¿De qué nos protege LINCE?

- LINCE: “Orientado a Pruebas” – “Evaluar como Hackers”

Certificaciones LINCE

Evaluación de producto en CC vs LINCE

- Alcance
- Metodología
- Rigurosidad - Validación
- Marketing
- Precio
- Complejidad

Certificación Nacional Esencial de Seguridad
CCN

Common Criteria

Conclusiones

Conclusiones

Certificación de ciberseguridad

- España – Potencia en certificación de ciberseguridad

- Necesaria la inversión en certificación – Momento decisivo!

- Common Criteria es buena!
  - Potente
  - Reconocimiento internacional!!
  - Uso para High Assurance!!

Common Criteria

Conclusiones

LINCE

- Certificación ligera
  - Alineada con las iniciativas europeas
- Adaptada para PYMES
  - Menos complejidad y coste
- Ventajas para desarrolladores
  - Acceso al CPSTIC - Análisis por una tercera parte de confianza
- Ventajas para empresas/administración
  - Prevención en ciberseguridad

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **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