RENIC

Red de Excelencia Nacional de Investigación en Ciberseguridad

# Criterios de Excelencia

# 1. CRITERIOS DE EVALUACIÓN DE LA EXCELENCIA

A continuación, se presentan aquellos criterios que se evaluarán para acreditar la excelencia de los equipos de investigación procedentes del Sector Académico (Universidades) y Centros investigación, Centros tecnológicos, Centros de Apoyo a la Innovación Tecnológica (en adelante Centros tecnológicos) o AAPP que desean formar parte de la Red de Excelencia.

Dada la diversidad de la naturaleza de cada equipo de investigación, se proponen un total de catorce criterios, divididos en tres bloques genéricos de 4 criterios cada uno, y dos bloques específicos con 2 criterios adicionales: un bloque específico para Universidades, y otro también específico para Centros tecnológicos y Administraciones Públicas.

El requisito para poder superar los criterios de excelencia, y poder formar parte de la Red de Excelencia como Miembro Asociado Acreditado, es haber superado como mínimo la puntuación que muestra la siguiente tabla:

| | **Cumplimiento de criterios** | | | | | |
|---|---|---|---|---|---|---|
| | Bloque 1 | Bloque 2 | Bloque 3 | Bloque Sector Académico | Bloque C. tecnológicos. AAPP | Cumplimiento mínimo criterios |
| S. Académico | 2/4 | 2/4 | 2/4 | ½ | - | 7/14 |
| Centros tecnológicos. AAPP | 2/4 | 2/4 | 2/4 | - | ½ | 7/14 |

Todos los agentes, independientemente de su tipología, deberán superar al menos dos de los cuatro criterios existentes en cada uno de los bloques genéricos (bloques 1, 2 y 3) y, además, superar al menos uno de los dos criterios específicos indicados, según la procedencia o naturaleza del agente interesado en formar parte de la Red de excelencia.

A continuación, se indican los criterios de excelencia:

### Bloque 1: Evaluación científico-técnica de los equipos de investigación

*Bloque genérico para Universidades, Centros tecnológicos y AAPP*

1. El investigador principal o coordinador del equipo de investigación acredita una trayectoria de investigación de, al menos 5 años, en áreas TIC relacionadas con la ciberseguridad, siendo evidencias de ello tanto trabajos, como publicaciones o proyectos de investigación.

2. El equipo de investigación, o en su defecto, el organismo o la persona jurídica al que pertenece el equipo acredita uno de los siguientes:

a) Tener o haber colaborado en la obtención de, al menos, una patente (PCT o EPO).

b) Haber solicitado, al menos, una patente (PCT o EPO) durante los últimos 5 años.

c) Haber realizado, al menos, una solicitud de registro o registro de software en la Oficina de Propiedad Intelectual durante los últimos 5 años.

En todo caso la patente o registro será resultado de alguno de los proyectos de investigación relacionados con la ciberseguridad desarrollados por el propio equipo o en colaboración. En caso de que la solicitud de patente o registro no haya sido realizada por el equipo de investigación o el organismo o la personal jurídica al que pertenece el equipo, será suficiente con que entre los inventores figuren miembros del equipo de investigación

3. El equipo de investigación ha publicado en revistas científicas de reconocido prestigio, situadas en primer o segundo cuartil, como resultado de los proyectos desarrollados en los últimos 5 años relacionados con la ciberseguridad, o bien como resultado de investigaciones en ciberseguridad

4. El equipo de investigación ha publicado los resultados de sus investigaciones en congresos o eventos, nacionales o internacionales, relacionados con la ciberseguridad en los últimos 5 años, con CORE (Computing Research & Education) menor al 26%, es decir, la puntuación del congreso debe estar entre la A* – A – B.

## Bloque 2: Organización, capacidades y recursos de gestión e investigación

*Bloque genérico para Universidades, Centros tecnológicos y AAPP*

1. El equipo de investigación dispone de un programa formativo anual en ciberseguridad destinado al personal investigador.

   El programa formativo deberá identificar y definir, como mínimo, las acciones formativas específicas relacionadas con la ciberseguridad, así como el horizonte temporal en el que se han desarrollado o se desarrollarán.

2. El equipo de investigación dispone de un plan estratégico a mínimo 3 años que define los objetivos que se persiguen, las acciones a implementar para alcanzarlo y los resultados esperados de las investigaciones que participan en el plan estratégico. En el

caso de los Centros de Investigación, en caso de no disponer de un plan estratégico propio del equipo de investigación, el plan estratégico global del centro, tendrá que especificar al menos los objetivos y las acciones a desarrollar para el área de ciberseguridad.

3. El volumen de recursos procedentes de convocatorias competitivas nacionales/internacionales del equipo de investigación se ha incrementado a lo largo de los últimos 3 años.

4. El equipo de investigación dispone de una web que contiene información sobre el propio equipo, incluyendo su estructura o composición del equipo de investigación, proyectos realizados, proyectos en curso, retos, etc.

## Bloque 3: Relaciones externas

*Bloque genérico para Universidades, Centros tecnológicos y AAPP*

1. El equipo de investigación ha desarrollado en los últimos 5 años, al menos, una colaboración científico-técnica en aspectos relacionados con la ciberseguridad con otros equipos de investigación, de reconocido prestigio nacional y/o internacional, para el desarrollo de proyectos de investigación relacionados con la ciberseguridad.

2. El equipo de investigación participa o colabora con otras redes o plataformas de investigación nacional o internacional, relacionadas con la ciberseguridad, que agrupen a otros agentes públicos o privados; y cuyo objeto sea el fomento y la difusión de la I+D+i de la ciberseguridad.

3. El equipo de investigación participa o colabora con grandes consorcios de investigación internacionales para el desarrollo de proyectos de programas de la UE u otros programas internacionales.

4. El equipo de investigación o en su defecto, el organismo o la persona jurídica al que pertenece el equipo, dispone de, al menos, un contrato firmado o acuerdo de colaboración con alguna empresa o asociación empresarial para la explotación de los resultados alcanzados en la investigación, o bien, para el desarrollo de proyectos de investigación específicos de ciberseguridad.

   El objeto del contrato o acuerdo debe estar relacionado con la ciberseguridad

## Bloque específico para el Sector Académico

*Únicamente evaluable si el equipo de investigación procede de la Universidad*

1. El equipo de investigación acredita su reconocimiento como grupo de investigación consolidado o dispone de una acreditación de un reconocimiento de similares características.

   Los Reconocimientos al equipo, grupo o unidad de investigación, deberán de valorar al menos las siguientes características:

   - Composición del equipo de investigación: mínimo de cuatro investigadores, uno de los cuales actuará como director/investigador principal/ coordinador del grupo.
   - Requisitos del director/investigador principal/coordinador del grupo: disposición del título de Doctor y contar con un mínimo de dos sexenios el último activo.
   - Requisitos del equipo de investigación: acreditar el número de publicaciones científicas por los miembros del equipo de investigación, el número de proyectos en los que el equipo de investigación ha sido líder y los ingresos obtenidos por el equipo de investigación.

2. Al menos la mitad de los miembros del equipo investigador disponen de Doctorado y/o Máster en alguna de las áreas TIC relacionadas con la ciberseguridad.

## Bloque específico para Centros tecnológicos y AAPP

*Únicamente evaluable si el equipo de investigación procede de un Centro de Investigación, Centro Tecnológico, Centro de Apoyo a la Innovación Tecnológica o Administración Pública.*

1. El equipo de investigación dispone de un nivel tecnológico, según la escala *Technology Readiness Level*, superior o igual al nivel 3 en al menos uno de los proyectos de investigación desarrollados durante los últimos 5 años. TRL 3: Concepto o aplicación de la investigación probados mediante análisis y experimentación: (I+D iniciada. Se incluyen estudios analíticos para establecer la investigación en un contexto apropiado y estudios de laboratorio. Este paso recibe el nombre de “prueba de concepto”).

2. El equipo de investigación ha publicado los resultados de sus investigaciones en conferencias, congresos o eventos, nacionales o internacionales, relacionados con la ciberseguridad, en los últimos 5 años.