RESOLUCIÓN DE LA PRESIDENTA DEL INSTITUTO PARA LA COMPETITIVIDAD EMPRESARIAL DE CASTILLA Y LEÓN DE 20 JUL 2018 POR LA QUE SE CONVOCA UNA CONSULTA PRELIMINAR AL MERCADO EN EL MARCO DE ESTRATEGIA REGIONAL DE EMPRENDIMIENTO, INNOVACIÓN Y AUTÓNOMOS 2016-2020 DE LA JUNTA DE CASTILLA Y LEÓN

El Instituto para la Competitividad Empresarial de Castilla y León,(en adelante ICE) como ente público de derecho privado integrante de la Administración Institucional de la Comunidad de Castilla y León, de acuerdo con la Ley 19/2010, de 22 de diciembre de Medidas Financieras y de creación de ICE y el Decreto 67/2011, de 15 de diciembre, por el que se aprueba su Reglamento General, tiene entre sus competencias el desarrollo de actuaciones que promuevan la investigación, el desarrollo tecnológico y la innovación en Castilla y León.

El ICE, contempla, entre sus actuaciones, el apoyo a la **Compra Pública de Innovación (en adelante CPI) como instrumento de fomento, en este caso desde el lado de la demanda, de la innovación y del desarrollo tecnológico de las empresas**, fundamentado tanto en la Estrategia Regional de Investigación e Innovación para una Especialización Inteligente (RIS3) de Castilla y León 2014-2020, como en la Estrategia de Emprendimiento, Innovación y Autónomos de Castilla y León, que rigen las actuaciones del ICE en materia de innovación, y que incluyen objetivos y medidas de apoyo a la CPI.

La **Estrategia de Especialización Inteligente RIS3 de Castilla y León** incluye objetivos y medidas de apoyo la CPI en concreto apuesta por desarrollar nuevos instrumentos y mecanismos como la compra pública innovadora, nuevos instrumentos financieros o la prestación de servicios avanzados de innovación desde la propia Administración regional; de tal forma que empresas e investigadores encuentren soporte a su actividad, especialmente de cara a la internacionalización de nuestra ciencia y de nuestra economía. Dentro del proceso de actualización en el que se encuentra la RIS3 de Castilla y León, el ICE apuesta porque éste traiga un mayor enfoque hacia la CPI dentro de la región.

La **Estrategia Regional de Emprendimiento, Innovación y Autónomos de Castilla y León (2016-2020)** contempla la identificación de las necesidades regionales, así como las actuaciones a implementar por parte del ICE.

Entre estas actuaciones, se incluye el fomento de la CPI de las entidades públicas y privadas de Castilla y León, la participación de ICE en procesos de compra pública innovadora y el desarrollo de pilotos de CPI demostradores. Todas ellas servirán de precedente e impulso para la utilización del instrumento de la CPI como uno de los mecanismos de respuesta a los retos de la región de Castilla y León, desde el lado de la demanda, de la innovación y el desarrollo tecnológico de las empresas, fortaleciendo así el sector empresarial de la propia comunidad autónoma.

Desde el punto de vista financiero, en el actual **Programa Operativo de Castilla y León (2014-2020)**, se contempla la medida: *010b1 - OE.1.2.1. Impulso y promoción de actividades de I+D+i lideradas por las empresas, apoyo a la creación y consolidación de empresas innovadoras y apoyo a la compra pública innovadora*, y se financiarán, entre otros, operaciones de CPI concretas a través de contratos de licitación pública, así como actuaciones que fomenten la CPI en organismos públicos de la región.

EL ICE ha elaborado un plan de trabajo en materia de Compra Pública Innovadora que incluye el desarrollo de un **programa de Compra Pública Precomercial (CPP)**, que permite la adquisición de soluciones basadas en I+D+i que den respuesta a los retos planteados, sirviendo entre otros instrumentos, de fomento e impulso del sector empresarial.

Se plantea un **primer foco** de utilización del instrumento de la CPI **en Ciberseguridad** dada su importancia y potencial a nivel europeo, nacional y regional.

La ciberseguridad es un factor clave que permite el desarrollo y la explotación de la innovación y de las tecnologías digitales y, por ello, está necesariamente vinculada a las perspectivas de crecimiento, creación de empleo y respuesta a los retos medioambientales y sociales del futuro. La importancia de la ciberseguridad queda reflejada a distintos niveles:

A **nivel europeo**, además de la Estrategia de Ciberseguridad de la Unión Europea de 2013, la **DIRECTIVA (UE) 2016/1148, de Seguridad de Redes y de la Información**, y de la creación de la Organización Europea de Ciberseguridad (ECSO), se puede destacar el Programa de Trabajo de Liderazgo TIC en Habilitación y Tecnologías Industriales (LEIT) del Programa Horizonte 2020 que incluye la Ciberseguridad entre las áreas clave de desarrollo.

A **nivel nacional**, además de la Estrategia de Ciberseguridad Nacional de 2013 (pendiente de actualización, una vez que se publique la Ley sobre la Seguridad de las Redes y de Sistemas de Información, que transpondrá en España la Directiva Comunitaria), y de la Estrategia de Seguridad Nacional de 2017, actualmente se está elaborando la próxima Estrategia Digital para una España Inteligente (EDEI) que tendrá previsiblemente entre sus líneas garantizar la seguridad de la información en todos los ámbitos, tanto públicos como privados, que contribuyen a la transformación digital de nuestra economía;

A **nivel regional,** la Estrategia Regional de Investigación e Innovación para una Especialización inteligente (RIS3) de Castilla y León 2014-2020 subraya que la **Ciberseguridad** cuenta en Castilla y León con fortalezas en ámbitos muy concretos ya que dispone de **infraestructuras relevantes** y **masa crítica en áreas TIC** de carácter transversal a cualquier actividad económica y específicamente en las mencionadas en el patrón de especialización económica de la región. Durante el proceso de evaluación intermedia de la propia estrategia (año 2017), se ha identificado que es clave incorporar la Ciberseguridad, como un campo estratégico para el desarrollo de la región gracias a la tendencia

que existe a nivel nacional y europeo, hecho que ha dado lugar a la **Iniciativa Emblemática en Ciberseguridad**, liderada por ICE.

La Ciberseguridad representa un oportunidad clara de especialización para Castilla y León puesto que permite explotar dos singularidades únicas en España: el **Instituto Nacional de Ciberseguridad (INCIBE)**, sociedad estatal adscrita al Ministerio de Economía y Empresa, que es la entidad de referencia para el desarrollo de la Ciberseguridad, y la **Agrupación Empresarial Innovadora de Ciberseguridad y Tecnologías Avanzadas**, que reúne a empresas, asociaciones, centros de I+D+i y entidades públicas o privadas interesadas en la promoción del ámbito nacional de las Tecnologías de Seguridad.

A nivel regional, el ICE ha apostado por el posicionamiento como región en Europa. Por un lado, como agente facilitador, está impulsando junto con la AEI Ciberseguridad e INCIBE un **Digital Innovation Hub** de Ciberseguridad, que pretende convertirse en referente internacional, a través del desarrollo de tecnologías que den respuesta a las necesidades del mercado. Actualmente también es miembro de la European Cyber Security Organisation–**ECSO**– (Consorcio Europeo de participación público-privada en Ciberseguridad), asociación sin ánimo de lucro, cuyo objeto principal es apoyar todo tipo de iniciativas o proyectos que tengan como finalidad desarrollar, promover y fomentar la Ciberseguridad europea.

Por último el ICE participa activamente en grupos de trabajo, plataformas, y proyectos europeos de Ciberseguridad, como *CYBER: Regional policies for competitive cybersecurity SMEs* y *Ciber Valleys Pilot action*.

Por su parte, la misión del INCIBE, como entidad de referencia en este campo, es afianzar la confianza digital, elevar la Ciberseguridad y la resiliencia, y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España, así como apoyar todo tipo de iniciativas o proyectos que tengan como finalidad desarrollar, promover y fomentar la Ciberseguridad europea.

Dado este contexto en el que existen intereses comunes, y en este ámbito de actuación, se considera estratégico aunar esfuerzos entre INCIBE e ICE, hecho que se ha traducido en una relación estable de colaboración entre ambos, materializada a través de distintos convenios.

La CPI, es un concepto que ha ido evolucionando en España, desde sus inicios como Compra Pública Innovadora, soportado por la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, y el Acuerdo del Consejo de Ministros de 8 de octubre de 2010 en el marco de la Estrategia Estatal de Innovación (aprobada por Consejo de Ministros de 2 de julio de 2010) y comprometía la actuación de los poderes públicos en esta dirección.

El Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público mantiene el mismo espíritu, mediante el fomento de la contratación pública de soluciones innovadoras.

De acuerdo con lo anterior, el Ministerio de Ciencia e Innovación publicó en 2011, una "Guía sobre Compra Pública Innovadora" dirigida a las Administraciones Públicas y demás organismos y entidades del sector público contratantes para la mejor y más adecuada aplicación de los procedimientos de contratación y adjudicación de la Compra Pública Innovadora. Esta guía se actualizó en 2015, con el título de "Guía 2.0 para la compra pública de innovación".

El lanzamiento de un procedimiento de CPI, mediante el que se pretende implementar soluciones tecnológicamente innovadoras, requiere el conocimiento previo del espacio de las soluciones factibles. Es por esto, que ya en el año 2014, el Parlamento Europeo y el Consejo aprobaron la Directiva 2004/18/CE, de 31 de marzo de 2004, sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, de suministro y de servicios, que contemplaba la posibilidad de que, antes del lanzamiento de un procedimiento de adjudicación de un contrato, los poderes adjudicadores pudieran solicitar o aceptar el asesoramiento del mercado mediante un proceso de diálogo técnico. Cabe resaltar que los resultados de este diálogo podían emplearse para determinar el pliego de prescripciones técnicas del contrato de CPI, siempre que dicho asesoramiento no tenga como efecto distorsionar la competencia. En concreto, en su artículo 40, la D2014/18/CE dispone la figura de la Consulta Preliminar del Mercado que permite a los poderes adjudicadores la realización de consultas del mercado, "con vistas a preparar la contratación e informar a los operadores económicos acerca de sus planes y sus requisitos de contratación".

La Ley 9/2017 de Contratos del Sector Público, por la que se transpone al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, establece de manera explícita en su artículo 115 que los órganos de contratación podrán realizar estudios de mercado y dirigir consultas a los operadores económicos que estuvieran activos en el mismo con la finalidad de preparar correctamente la licitación e informar a los citados operadores económicos acerca de sus planes y de los requisitos que exigirán para concurrir al procedimiento. Este procedimiento aplica a todo tipo de contratos, especialmente a la CPI.

En base a los antecedentes expuestos, el ICE publica la presente resolución de Consulta Preliminar al Mercado, informando con ello a los operadores económicos acerca de los retos y necesidades a solventar en materia de Ciberseguridad.

En el marco de la colaboración señalada, se ha contado con INCIBE para el planteamiento de los Retos señalados en el anexo, pudiendo formar parte del proceso de valoración técnica de las propuestas recibidas en esta Consulta Preliminar al Mercado.

Teniendo en cuenta lo anteriormente expuesto, resuelvo:

Primero. Convocatoria

Se convoca una Consulta Preliminar al Mercado en el marco de la Estrategia Regional de Investigación e Innovación para una Especialización Inteligente (RIS3) de Castilla y León 2014-2020, de la Estrategia Regional de Emprendimiento, Innovación y Autónomos, y de la política regional de

Compra Pública de Innovación para Castilla y León, para la búsqueda de soluciones innovadoras en proyectos de innovación relacionados con la Ciberseguridad.

Segundo. Objeto

La Consulta Preliminar del Mercado tiene por objetivo promover la participación de personas físicas o jurídicas para la presentación de propuestas innovadoras destinadas a dar respuesta a cuatro retos en el campo de la Ciberseguridad, en cuya definición el ICE e INICIBE han trabajado conjuntamente. Dichos retos se detallan en el Anexo I de la presente resolución (disponible en la página web www.empresas.jcyl.es), mediante el empleo de tecnologías que superen las prestaciones de las existentes actualmente en el mercado.

Concretamente se pretende que, a partir de los resultados de la Consulta Preliminar del Mercado, el ICE pueda contar con el conocimiento suficiente sobre las soluciones más innovadoras existentes en el mercado.

Estas propuestas servirán para evaluar las capacidades del mercado y definir las especificaciones funcionales que impliquen innovación y sean factibles de alcanzarse a través de una eventual contratación de uno o varios pilotos a través Compra Pública de Innovación u otro instrumento de contratación pública posterior.

Tercero. Participantes

La convocatoria es abierta y se dirige a personas físicas o jurídicas, públicas o privadas.

Se admitirá la presentación de varias propuestas por una misma persona física o jurídica, ya sea individualmente o en forma conjunta con otras.

Cuarto. Presentación de propuestas.

Para la presentación de las propuestas, los proponentes se ceñirán a las siguientes reglas:

1. Los participantes deberán formular sus propuestas cumplimentando el formulario que se encuentra en el Anexo II de la presente resolución, y que se puede descargar en la página web www.empresas.jcyl.es. Se podrá acompañar el formulario con la documentación complementaria que se estime oportuna, donde se podrá desarrollar la propuesta con mayor detalle, pero se ruega atenerse al formulario para facilitar su análisis.
2. Las propuestas se remitirán vía plataforma electrónica ICE o en su defecto se enviarán a las siguientes direcciones de correo electrónico: (una dirección de mail por cada reto): reto1.ciber.ice@jcyl.es; reto2.ciber.ice@jcyl.es; reto3.ciber.ice@jcyl.es; reto4.ciber.ice@jcyl.es
3. Cada propuesta será identificada con el acrónimo que quedará claramente expuesto en el asunto del correo electrónico, en el caso de que se utilice esta vía.
4. Se podrán enviar sucesivas versiones de una propuesta, con el mismo acrónimo, pero cada propuesta enviada sustituirá completamente a la anterior. Por ello, la nueva propuesta deberá incluir todo lo que se considere que sigue siendo válido de las anteriores.

5. En caso de que una propuesta se presente de forma conjunta por un grupo de personas o entidades, deberá emplearse una única dirección de correo electrónico, para los efectos de identificación de la propuesta e interlocución con los proponentes.
6. Las propuestas se podrán presentar en cualquier momento a partir de la fecha de inicio indicada en la presente convocatoria, siempre que el plazo de presentación del reto al que se dirigen permanezca abierto.
7. Los costes derivados de la participación en la convocatoria correrán a cargo de los participantes. El ICE no se obliga a financiar ni a aceptar las propuestas presentadas en esta convocatoria.

Quinto. Comité Técnico

Para la ejecución de las tareas incluidas en la resolución, el ICE nombrará un **Comité Técnico** que podrá estar conformado también por personal de INCIBE, o expertos externos (con el conocimiento técnico necesario para este proceso). La composición de este comité técnico se publicará en la página web arriba indicada.

Sus principales funciones serán:

- Análisis de las diferentes propuestas presentadas. Estas propuestas servirán para evaluar las capacidades del mercado y definir las especificaciones funcionales que impliquen innovación y sean factibles de alcanzarse a través de una eventual contratación.
- Propuesta de actualizaciones de los retos de la presente Resolución mediante la publicación de una modificación sobre el Anexo I de la misma. Podrá por tanto añadir nuevos retos o reformular los retos ya publicados fruto de la evolución del propio proceso de consulta al mercado.
- Determinación del cierre de la consulta para el reto publicado, cuando se estime que:
  - Dispone de información suficiente sobre propuestas innovadoras para ese reto como para iniciar un eventual proceso de contratación pública de innovación, o
  - Considere que tal reto no ha generado suficiente interés en el mercado como para mantener la consulta, o
  - Considere que la oportunidad de plantear ese reto no sigue vigente.

Sexto. Funcionamiento de la Consulta Preliminar al Mercado.

El ICE, con el apoyo del Comité Técnico, estudiará las propuestas presentadas y podrá utilizarlas para definir las especificaciones funcionales o técnicas que se puedan emplear en los procedimientos de contratación que con posterioridad se puedan convocar, fundamentalmente a través del procedimiento de Compra Pública de Innovación (CPI, *conforme a lo establecido en el artículo 115 de la Ley 9/2017 de 8 de noviembre de Contratos del Sector Público, por la que se trasponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE de 26 de febrero de 2014 y en la Cláusula 42 de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública*).

Se podrán realizar jornadas informativas, reuniones con los participantes, y cualesquiera otras actuaciones de comunicación y difusión que se estimen oportunas.

Asimismo, si se considerara necesario, el Comité Técnico podrá contactar con participantes concretos para recabar más información sobre su propuesta, aclarar dudas o solicitar demostraciones

Se podrán añadir nuevos retos, reformular o cerrar los retos ya publicados fruto de la evolución del propio proceso de consulta al mercado. Se avisará de estas actualizaciones a todos los que hayan participado hasta ese momento en la consulta a través de la dirección de correo electrónico desde la que se envió la propuesta. Además, se publicarán, al menos, en el sitio web antes citado.

Finalizada la consulta, se publicará con suficiente antelación, el *Informe de Resultados de la Consulta al Mercado*, conforme al apartado siguiente.

Séptimo. Aplicación de los principios de transparencia, igualdad de trato y no discriminación ni falseamiento de la competencia.

La participación en la Consulta Preliminar al Mercado, los contactos mantenidos con los participantes o los intercambios de información, se regirán bajo los principios comunitarios de transparencia, igualdad de trato y no discriminación, sin que puedan tener como efecto restringir o limitar la competencia, ni otorgar ventajas o derechos exclusivos en una eventual licitación de CPI posterior en el ámbito del objeto de esta Resolución, y como consecuencia de ello, no conlleva ninguna obligación de financiación o aceptación de las propuestas presentadas.

A tal efecto, el ICE y los miembros del Comité Técnico tomarán las medidas apropiadas para garantizar el mantenimiento de los citados principios, tanto en el desarrollo de esta convocatoria como en cualquier procedimiento de contratación posterior. Su inobservancia podrá ser considerada como infracción.

Para garantizar el cumplimiento de los principios de transparencia, igualdad de trato y no discriminación ni falseamiento de la competencia, el ICE hará constar en el *Informe de Resultados de la Consulta al Mercado* las acciones realizadas incluyendo entre otros, sus responsables, las entidades consultadas y la información intercambiada con los participantes en el marco de esta convocatoria. En este informe se establecerán además los próximos pasos que se llevarán a cabo pudiendo ser, entre otros, la publicación del "Mapa de Demanda Temprana" de la futura o futuras contrataciones que se pretendan convocar, a los efectos de informar al mercado para que pueda preparar las oportunas ofertas con tiempo suficiente, facilitando la planificación y la reducción del riesgo.

Este informe se publicará en la página web citada y en la plataforma de contratación del sector público.

Octavo. Plazos de la Consulta Preliminar al Mercado.

El plazo para la presentación de propuestas comenzará el día siguiente al de publicación de esta Resolución en el Boletín Oficial de Castilla y León, permaneciendo con carácter general abierta al menos tres meses desde su publicación.

La actualización de retos, o la inclusión de alguno nuevo, supone la apertura de un nuevo plazo de presentación de propuestas, a determinar en cada caso.

El cierre de la consulta sobre un reto se anunciará con al menos quince días de antelación, publicándolo en sitio web arriba indicado, pudiendo revocarse en cualquier momento, informando de ello por los mismos medios.

.El cierre de la consulta para cada reto, podrá venir determinado por alguna de las siguientes circunstancias:

- Dispone de información suficiente sobre propuestas innovadoras para ese reto como para iniciar un eventual proceso de contratación pública de innovación, o
- Considere que tal reto no ha generado suficiente interés en el mercado como para mantener la consulta, o
- Considere que la oportunidad de plantear ese reto no sigue vigente.

Noveno. Protección de datos personales y confidencialidad.

El ICE almacenará los datos de contacto de los participantes en el procedimiento a los meros efectos de establecer un canal de comunicación con los proponentes durante el proceso de Consulta Preliminar al Mercado.

Será de aplicación el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).

Para asegurar la transparencia del proceso, la disponibilidad de la mayor información posible y el intercambio eficaz de experiencias y opiniones, los participantes harán constar expresamente su conformidad para que el ICE mantenga accesible y actualizada la información necesaria, total o parcial, sobre sus propuestas, sin perjuicio de aquella que haya sido marcada como confidencial.

Para ello, los participantes indicarán la documentación o la información técnica o comercial de su propuesta que tiene carácter confidencial, no siendo admisible que efectúen una declaración genérica o declaren que toda la información tiene carácter confidencial. Este carácter confidencial protege, en particular, a los secretos técnicos o comerciales y a los aspectos confidenciales de las soluciones. En este sentido, el contenido de la información incluida en el formulario en ningún caso podrá ser calificado como confidencial y únicamente los adjuntos a ese formulario podrán designarse como tales.

Los participantes podrán designar como confidenciales documentos, adjuntos al formulario, que aporten junto con su solicitud. Esta circunstancia deberá quedar reflejada claramente en el formulario y en el propio documento designado como tal.

A los efectos de esta convocatoria, se procederá a la cesión de los datos recabados a los miembros del Comité Técnico, previamente identificados, conforme lo establecido en el punto QUINTO para el desarrollo de las funciones previstas, de acuerdo a lo establecido la normativa aplicable a tal efecto.

Décimo. Derechos de Explotación de la Propiedad Intelectual e Industrial.

Las posibles ideas de soluciones que se presenten en el marco de la Consulta Preliminar al Mercado no podrán mencionar una fabricación o una procedencia determinada o un procedimiento concreto, ni hacer referencia a una marca, a una patente o a un tipo, a un origen o a una producción determinados.

El uso del contenido de las propuestas se limita exclusivamente a su posible inclusión en las especificaciones funcionales o técnicas de un eventual procedimiento de contratación posterior.

Undécimo. De la jurisdicción.

Contra esta Resolución podrá interponerse, conforme a lo dispuesto en los artículos 123 y 124 de la Ley 39/2015, de 1 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas, recurso de alzada ante cualquiera de los órganos que efectúan la presente convocatoria, en el plazo de un mes, o bien, directamente, recurso contencioso administrativo, en virtud de lo dispuesto en los artículos 8.3, 14.1 y 46 de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso Administrativa, en el plazo de dos meses, en ambos casos contados desde el día siguiente al de su publicación en el Boletín Oficial de Castilla y León.

Duodécimo. Contratación pública.

A partir de las ideas de soluciones innovadoras recogidas como resultado de esta convocatoria, el ICE podrá definir las especificaciones técnicas y/o funcionales, que servirán de base para la definición, con el grado de concreción necesario, del objeto de contratación del correspondiente procedimiento de contratación pública ulterior.

Este eventual procedimiento de compra pública posterior estará abierto a todas las ofertas que cumplan, en su caso, las condiciones de tal procedimiento hayan participado o no estado en esta consulta preliminar al mercado.

Arroyo de la Encomienda, 20 JUL 2018

La Presidenta

Mª del Pilar del Olmo Moro

Anexo I. RETOS

RETO 1 Detección de bots y servidores de comando y control (C&C)

1.1. Antecedentes:

Los centros especializados en seguridad cibernética están realizando investigaciones para obtención de información de bots mediante la compra de dominios obtenidos de fuentes (públicas y privadas) de DGAs (Domain Generation Algorithms).

1.2. Motivación:

Se está interesado en la obtención de información propia relativa a amenazas (en este caso concreto botnet[1]) para obtener conocimiento acerca de su funcionamiento y poder así establecer medidas de mitigación apropiadas.

1.3. Descripción del reto:

El reto consiste en la investigación y posterior desarrollo de una prueba de concepto para la detección de bots y servidores de comando y control (C&C).

1.4. Recursos de apoyo que se pondrían a disposición de posibles proveedores (data-sets, etc.):

Dominios de DGA disponibles.

1.5. Avances realizados actualmente

Investigación sobre el problema. Recopilación de conjuntos de datos para entrenar sistemas.

1.6. Alcance:

Detección de bots y servidores de comando y control (C&C)

1.7. Ejemplos de Casos de uso:

Nota: Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

Caso 01	En base a la investigación inicial se seleccionará una estrategia de detección de bots, se implantará en una PoC y se verificará su viabilidad mediante la obtención de información de bots pertenecientes a una o varias botnets. La información que se desea obtener acerca del bot es, al menos, la siguiente: IP, timestamp del momento en que se realiza la detección. También sería deseable obtener información adicional sobre el comportamiento de cada Botnet en concreto, como por ejemplo el protocolo de comunicación utilizado entre bots y servidores C&C, puertos, etc.
Caso 02	En base a la investigación inicial se seleccionará una estrategia de detección de paneles C&C, se implantará en una PoC y se verificará su viabilidad mediante la obtención de información de bots pertenecientes a una o varias botnets. La información que se desea obtener acerca del C&C es, al menos, la siguiente: IP, timestamp del momento en que se realiza la detección. También sería deseable, si es posible, obtener información adicional como, por ejemplo, el protocolo de comunicación utilizado entre bots y servidores C&C, puertos, URL completa donde se encuentra el panel, tecnología subyacente del panel, información acerca del servidor en el que está alojado, etc.

[1]Término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática

RETO 2 Detección de dominios .onion en la red TOR no indexados por fuentes públicas

2.1. Antecedentes:

Los centros especializados en seguridad cibernética trabajan en la monitorización de dominios .onion ilícitos de la red TOR.

2.2. Motivación:

Obtención de información relativa a servicios ilícitos ocultos en la red TOR.

2.3. Descripción del reto:

El reto consiste en la investigación y posterior desarrollo de una prueba de concepto para la detección de dominios .onion que no estén siendo indexados por fuentes públicas (tipo Ahmia). Se trata de descubrir nuevos servicios ilícitos ocultos para mejorar el servicio de monitorización y para incrementar el conocimiento de la red TOR y de sus usuarios.

2.4. Recursos de apoyo que se pondrían a disposición de posibles proveedores (data-sets, etc.):

Datos de las monitorizaciones diarias de dominios en TOR.

2.5. Avances realizados actualmente:

Investigación sobre el problema. Recopilación de conjuntos de datos para entrenar sistemas.

2.6. Alcance:

Detección de nuevos servicios ilícitos ocultos no indexados por las principales fuentes de datos públicas (Ahmia, Bdpuqvsqmphctrcs, tt3j2x4k5ycaa5zt, etc.).

2.6. Ejemplos de Casos de uso:

Nota: <u>Estos casos de uso se establecen como ejemplos</u>, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

Caso 01	**Precondiciones:** Teniendo en cuenta que: - Un dominio .onion tiene una longitud de 16 caracteres que puede ser creada con cualquier letra del alfabeto y con dígitos decimales que empiecen por 2 y acaben en 7. - Es posible "forzar" la generación del dominio para que incluya palabras identificativas del tipo de servicio oculto. Ejemplos: jihadlove5xhyfw3.onion; babylonxjrtoyomy.onion; drugsqfazpkaitwq.onion; weapon5cd6o72mny.onion; **Flujo del caso:** a) El sistema de generación de dominios (alcance de la investigación) genera un dominio que pasa al sistema de monitorización de TOR. b) El sistema de monitorización de TOR comprueba su existencia y el resultado es positivo **Nota**: La propuesta de solución al reto tendrá que tener en cuenta la versión 3 de TOR (diciembre de 2017). Esta nueva versión incluye mejoras importantes de seguridad y entre ellas una mejora en la seguridad de las direcciones Onion que pasan de 16 caracteres a 56 caracteres.
Caso 02	**Precondiciones**: Análisis de formas de obtención de dominios en TOR no indexados por fuentes públicas. Por ejemplo: establecimiento de nodo intermedio en TOR y obtención de metadatos, entre ellos dominios .onion a los que se conectan los usuarios. La investigación propondrá formas o métodos de obtención de dominios no indexados en fuentes públicas. **Flujo del caso**: Igual al del caso de uso 1 cambiando el sistema de generación de dominios por el método o métodos investigados.

RETO 3 Detección, categorización y predicción automatizada de ciberataques.

3.1. Antecedentes:

Se dispone de un conjunto de Honeypots de baja-media interacción para la detección temprana de ciberataques.

3.2. Motivación:

El número elevado de conexiones a los Honeypots y la baja automatización de las tareas de detección, categorización y predicción de ciberataque.

3.3. Descripción del reto:

El reto consiste es la investigación y posterior desarrollo de una prueba de concepto para la detección, categorización y predicción automática de ciberataques:

3.4. Recursos de apoyo que se pondrían a disposición de posibles proveedores (data-sets, etc.):

Conjunto amplio de datos de conexiones a los Honeypots

3.5. Avances realizados actualmente:

Investigación sobre el problema. Recopilación de conjuntos de datos para entrenar sistemas.

3.6. Alcance

Detección, categorización y predicción automatizada de ciberataques a una red de HoneyPots.

Ejemplos de Casos de uso:

Nota: <u>Estos casos de uso se establecen como ejemplos</u>, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

Caso 01	**Precondiciones** HoneyPot de baja/media interacción desplegado en servidor expuesto en internet. Intento de conexión sobre la máquina expuesta. **Flujo del caso**: a) El sistema recopila datos sobre la conexión: IP, Fecha/hora, ASN, Datos geoposicionamiento... b) El sistema etiqueta la conexión como ciberataque. Descarta las conexiones no maliciosas (ejemplo: lista blanca de escáneres conocidos). c) El sistema categoriza las conexiones etiquetadas como ciberataque. Por ejemplo: intento de intrusión, ataque DDoS, etc. d) El sistema alerta al operador proporcionándole información sobre el ciberataque.
Caso 02	**Precondiciones:** HoneyPots de baja/media interacción desplegados en servidores expuestos en internet. **Flujo del caso:** a) Sistema recopilando, analizando y correlando datos de conexiones sobre las máquinas expuestas. b) El sistema predice y alerta al operador sobre un posible ciberataque. Por ejemplo: inicio de campaña de intrusión e infección por malware.

RETO 4: Servicios avanzados para la atribución de ciber-incidentes

4.1 Antecedentes:

Se trabaja en la gestión de incidentes de ciberseguridad. Uno de los principales retos a largo plazo es la atribución de incidentes: intentar abordar las preguntas distantes y complejas que rodean al "quién" y el "por qué" de un ataque, en oposición a las preocupaciones más inmediatas de "qué", "cuándo", "dónde" y 'cómo'.

4.2 Motivación:

Los centros privados especializados en seguridad cibernética y otros organismos públicos están interesados en la obtención de conocimientos y servicios que permitan dar soporte a su nuevo modelo de inteligencia, en especial, en los aspectos relativos a la atribución de ciber incidentes.

4.3 Descripción del reto:

El reto consiste en la investigación y posterior desarrollo de una prueba de concepto, según el caso de uso que se propone, que permita generar información y conocimiento de alto valor para la atribución de ataques reales.

4.4 Recursos de apoyo que se pondrían a disposición de posibles proveedores (data-sets, etc.):

Podrán ser negociados con el proveedor, según el proyecto que se proponga y qué recursos estén disponibles.

4.5 Avances realizados actualmente:

Ejemplos de Casos de uso:

Caso 01	Entregables: 1. Una base de conocimiento inicial (KB) con las fuentes, corpus, documentales, data-sets, etc. seleccionadas para la prueba de concepto. 2. Algoritmos del sistema, tal que dado uno o más indicadores de compromiso (podrán incluir o no el sector o nombre de la entidad atacada), el sistema genere un informe de potencial atribución/motivación basado en la información almacenada en la base de conocimiento del punto 1 3. Informe con metodologías y fuentes para mantener y mejorar los puntos 1 y 2 anteriores

Anexo II. Formulario de propuesta

1. Datos Básicos

Nombre de la propuesta	
Acrónimo	

2. Datos Proponente

Persona Física		☐	
Persona Jurídica		☐	
Sector o ámbito de actividad:			
Tipo de Entidad (Autónomo, Empresa privada, Empresa pública, Centro de Investigación, Universidad, Centro Tecnológico, Otro):			
Propuesta conjunta de varias personas físicas o jurídicas Marque SÍ o NO	**SÍ ☐**		**NO ☐**
Tamaño de su entidad en la actualidad (Nº de personas en plantilla)			
Facturación total de su entidad en los últimos 3 ejercicios (€)	**2017**	**2016**	**2015**

3. Datos del interlocutor/representante

Nombre del Interlocutor (o representante de la propuesta en caso de propuesta conjunta)	
Teléfono	
Correo Electrónico	
Dirección	

4. Información adicional

¿Su entidad tiene facturación de tecnologías similares a las de la presente propuesta en últimos 3 ejercicios? Responda SÍ o NO	**SÍ** ☐	**NO** ☐
En caso de haber respondido SÍ a la pregunta anterior, **diga cuál fue la facturación aproximada de tecnologías similares a las de esta propuesta en los últimos 3 ejercicios** (dato agrupado de los 3 ejercicios)		
¿Considera que su entidad dispone de certificaciones relevantes para acometer los retos que se propone? Responda SÍ o NO	**SÍ** ☐	**NO** ☐
En caso de haber respondido SÍ a la pregunta anterior, **indique cuáles son esas certificaciones (máx. 300 caracteres)**		
¿Considera que el personal de su entidad tiene calificaciones que son específicamente relevantes para acometer los retos que se propone? Responda SÍ o NO	**SÍ** ☐	**NO** ☐
En caso de haber respondido SÍ a la pregunta anterior, indique cuáles son esas calificaciones **(máx. 300 caracteres)**		
¿Ha realizado inversión en I+D en los últimos 3 ejercicios? Responda SÍ o NO	**SÍ** ☐	**NO** ☐
En caso de haber respondido SÍ a la pregunta anterior, **indique cuál ha sido el importe de dicha inversión en los últimos 3 ejercicios** (dato agrupado de los 3 ejercicios)		
¿Su entidad ha obtenido financiación pública de concurrencia competitiva para proyectos de I+D en alguno de los 3 últimos ejercicios? Responda SÍ o NO	**SÍ** ☐	**NO** ☐

En caso de haber respondido SÍ a la pregunta anterior, **indique el volumen de financiación captada en los últimos 3 ejercicios** (dato agrupado de los 3 ejercicios)	
Para los 4 retos planteados, aportar información detallada en relación a investigaciones, desarrollo de soluciones, publicaciones, etc. realizadas o realizándose cuyo objeto sea similar al indicado.	RETO 1 Detección de bots y servidores de comando y control (C&C) 1. Investigaciones. Descripción detallada. 2. Desarrollo de soluciones. Descripción detallada. 3. Publicaciones. Descripción detallada. 4. Otros. Descripción detallada.
	RETO 2 Detección de dominios .onion en la red TOR no indexados por fuentes públicas 1. Investigaciones. Descripción detallada. 2. Desarrollo de soluciones. Descripción detallada. 3. Publicaciones. Descripción detallada. 4. Otros. Descripción detallada.
	RETO 3 Detección, categorización y predicción automatizada de ciberataques. 1. Investigaciones. Descripción detallada. 2. Desarrollo de soluciones. Descripción detallada. 3. Publicaciones. Descripción detallada. 4. Otros. Descripción detallada.
	RETO 4 Servicios Avanzados para la atribución de ciber-incidentes. 1. Investigaciones. Descripción detallada. 2. Desarrollo de soluciones. Descripción detallada. 3. Publicaciones. Descripción detallada. 4. Otros. Descripción detallada.

5. Descripción de la propuesta de solución

Breve resumen de la propuesta de solución: especificación funcional (máximo 1.250 caracteres) *Descripción de la posible idea que pueda satisfacer la necesidad planteada por parte del ICE, descrita desde un enfoque funcional*	
Duración estimada para la ejecución de la propuesta planteada (meses)	
Coste estimado del desarrollo de su solución propuesta (€):	
Beneficios aportados por la solución propuesta para el sistema público (máx. 850 caracteres)	
Beneficios aportados por la solución propuesta para otros agentes (máx. 850 caracteres)	
Elementos de innovación (nuevas tecnologías entregadas y soluciones innovadoras) o **Resultados de I+D esperados. Específicamente, diga cuáles son los elementos diferenciadores de su propuesta frente a los productos y servicios que se encuentran ya disponibles en el mercado** (máx. 850 caracteres)	
Nivel de madurez actual en el que se encuentra su solución propuesta (en caso de conocer en nivel de madurez tecnológica (TRL[2]) en el que se encuentra, indíquelo):	
Regulaciones y normativa asociada:	

[2] Los códigos TRL se pueden consultar en "HORIZON 2020 – WORK PROGRAMME 2016-2017 General Annexes: G. TRL"

6. Declaraciones Obligatorias

Autorizo al ICE al uso de los contenidos de las propuestas. Este uso se limitará exclusivamente a la posible inclusión de los contenidos en el proceso de definición de las líneas de trabajo, que se concretará en los posibles pliegos de los posibles procedimientos de contratación que se tramiten con ulterioridad bajo la fórmula de Compra Pública de Innovación:.	☒
La propuesta presentada está libre patentes comerciales, copyright o cualquier otro derecho de autor o empresarial que impida su libre uso por parte de ICE o de cualquier otra empresa colaboradora en el desarrollo de futuros proyectos:	☒

7. Autorización de uso de los datos aportados (marque SÍ o NO)

	SÍ	NO
Los datos de carácter personal serán tratados por el Instituto para la Competitividad Empresarial de Castilla y León (ICE) con NIF Q4700676B, e incorporados a la actividad de tratamiento de Actividad de Promoción, cuya finalidad es la inscripción en actividades y servicios promovidos por el ICE, finalidad basada en el cumplimiento de obligaciones legales por parte del ICE.		
Importante: Autorizo expresamente el uso de los datos personales por parte de "Instituto para la Competitividad Empresarial de Castilla y León", así como la cesión de los mismos, a los miembros del Comité Tecnico, previamente identificado, con la finalidad de gestionar los datos de los participantes en esta consulta al mercado, incluida en la actividad de tratamiento datos denominada "Actividad de Promocion". La no aceptación impedirá la inclusión de la propuesta en este proceso Puede ejercitar ante el ICE sus derechos de acceso, rectificación, supresión, limitación y oposición a su tratamiento: C/ Jacinto Benavente, nº 2, 47195 – Arroyo de la Encomienda (Valladolid), o en la dirección de correo electrónico del Delegado de Protección de Datos: dpd.ice@jcyl.es	☐	☐

8. Relación de documentación adjunta aportada

En el caso de que los hubiese, indique la documentación que acompaña a su propuesta y que proporcione mayor información acerca de la idea propuesta.

Nombre del archivo:	Breve descripción:	Confidencial*
		☐
		☐
		☐
		☐
		☐
		☐

*Marcar en el caso de que la documentación correspondiente sea confidencial