# DESAFÍO UNIVERSIDAD - EMPRESA

***Esta necesidad tecnológica forma parte del Concurso de Proyectos de I+D+i y/o consultoría en colaboración Universidad – Empresa "Desafío Universidad Empresa" 2018 organizado por la Fundación Universidades y Enseñanzas Superiores de Castilla y León.***

## TÍTULO DE LA DEMANDA TECNOLÓGICA A RESOLVER

**Referencia:**

NT54

**Título de la demanda tecnológica propuesta**

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

**Acrónimo:**

DEEPWEB

**Áreas de interés de la demanda tecnológica**

(Principal) Tecnologías de la Información y Comunicación, Energía y Sostenibilidad

Otros (Ciberseguridad)

**Resumen:**

El reto consiste en la investigación y posterior desarrollo de una prueba de concepto de una o varias herramientas orientadas a 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 servicios de monitorización e incrementar el conocimiento de la red TOR.

*PALABRAS CLAVE:* Ciberseguridad, deepweb, tor, dominios, detección

## DESCRIPCIÓN DE LA NECESIDAD DEMANDADA

**1.- Descripción de la demanda tecnológica**.

El reto consiste en la investigación desarrollo de una prueba de concepto orientada a la detección de dominios .onion que no estén siendo indexados por fuentes públicas.

En el apartado de "Posibles Enfoques", se proponen unos Casos de Uso en los que basar las propuestas de solución tecnológica (proyecto de investigación) que se planteen como respuesta a este desafío.

**2.- Antecedentes.**

Es necesaria la detección de amenazas en el ciberespacio, como puede ser la obtención de información relativa a servicios ilícitos ocultos en la red TOR. Una aproximación consiste en la detección de nuevos servicios ilícitos ocultos no indexados por las principales fuentes de datos públicas (Ahmia, Bdpuqvsqmphctrcs, tt3j2x4k5ycaa5zt, etc.).

**3.- Posibles enfoques del proyecto de investigación.**

CASO DE USO 1

Precondiciones:

Teniendo en cuenta que:

(1) 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.

(2) 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 TOR. (b) El sistema de monitorización TOR comprueba su existencia y el resultado es positivo

CASO DE USO 2

Precondiciones:

Análisis de formas de obtención de dominios en TOR no indexados por fuentes públicas. Por ejemplo: establecimiento de nodos de salida 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.

**4.- Enfoques sin interés.**

n/d

***Si desea remitir una propuesta de solución tecnológica*** *(proyecto de investigación y/o consultoría)* ***deberá enviar el formulario de participación*** *(ANEXO II), descargable en* ***www.redtcue.es/desafio*** ***a una de las direcciones de correo electrónico que se indican en las bases del concurso antes del 29/06/2018.***

*Acceso a información general del concurso*