**Ciberseguridad:**

**Necesitamos un ciberespacio seguro para nuestro progreso económico y social.**

*Carmen Castro.*

**

carmencastro2010@gmail.com

doctoracarmencastro.blogspot.com

**RESUMEN**

Este artículo trata de reflexionar sobre la necesidad de un ciberespacio seguro. La relevancia de esta reflexión reside en que en este nuevo ámbito, las administraciones públicas, las empresas y los ciudadanos realizan actividades de todo tipo, transacciones, acciones formativas, comerciales, de comunicación y de ocio y al mismo tiempo existen amenazas como el ciberespionaje, la ciberdelincuencia y el hacktivismo.

La introducción describe el escenario actual, define Ciberseguridad y los conceptos relacionados con ella, también se cita la *“Estrategia de Ciberseguridad Nacional”* del 5 de diciembre de 2013.

El desarrollo del artículo explica la necesaria protección de la Información Nacional Clasificada, expone que esta es el *principal activo crítico de información* y muestra los distintos grados de clasificación en orden decreciente de importancia. La seguridad de la Información Clasificada es responsabilidad del Centro Nacional de Inteligencia (CNI). El CNI, a través de su Centro Criptológico Nacional (CCN), interviene de oficio cuando hay un incidente de seguridad sobre información clasificada. El Centro Criptológico Nacional es el CERT gubernamental, es el centro de alerta y respuesta nacional, organismo que tiene como misión contribuir a la mejora de la Ciberseguridad y responder de forma rápida y eficiente a los incidentes de seguridad de las administraciones públicas y de las empresas estratégicas. Se describen los sistemas y herramientas que utilizan para cumplir sus funciones.

Se define y clasifica el código dañino y el modus operandi de este, a la vez que se dan algunas recomendaciones para los usuarios de las computadoras y de la red.

Continúa examinando los riesgos y amenazas del nuevo fenómeno BYOD, “Traiga su propio dispositivo” y de los riesgos de seguridad en las redes sociales.

Por último se citan los organismos que velan por la Ciberseguridad en España, incluyendo al Instituto Nacional de Ciberseguridad, INCIBE, dirigido a PYMES y ciudadanos, anteriormente conocido por INTECO

|  |
| --- |
| **PALABRAS CLAVE:** Ciberseguridad, ciberespacio, ciberamenazas, ciberespionaje, ciberdelincuencia, hacktivismo, información clasificada, CERT, sistema de alerta temprana, sistema multiantivirus, sistema de análisis web, APT (amenaza persistente avanzada), gusano, troyano, rootkit, spyware, ransomware, BYOD, phishing, pharming, spam, geolocalización, sexting, ciberacoso, grooming. |

**Cybersecurity:**

**We need a secure cyberspace for our economic and social progress.**

**Abstract.**

**This article will look the need for safe cyberspace. This is relevant because public bureaucracies, businesses and individuals carry out all types of online activities, these include: transactions, training, business, communication and leisure activities; at the same time there exist threats such as: cyber-espionage, cyber-crime and hacktivism.**

**The introduction describes the current situation, defines “cyber-security” and related terms, it cites the “Estrategia de Cyberseguridad Nacional”, published on of December, 2013, as well.**

**The main part of the article will explain the necessary protection of classified information, explaining that it is the main critical principle when it comes to information and shows the degrees of classification in descending order. The Center for National Intelligence (CNI) is responsible for classified intelligence security. The CNI, through its National Cryptological Center, intervenes when there a classified information security issue. The National Cryptological Center is the Spanish government ‘s answer to CERT; it is the national alert and response center, whose mission is to contribute to the improvement of cybersecurity and to respond in a quick and efficient manner to the needs of public administration and strategic businesses. The systems and tools it uses to carry out its responsibilities will be described in the text.**

**Malicious code and its modus operandi will be defined and classified, and computer and network users will be given some recommendations on how to deal with the problem.**

**The article will continue by examining the risk and threats if the new phenomenon BYOD, Bring Your Own Device, and security risks on social networks.**

**Finally, it will cite the organizations responsible for safeguarding cybersecurity in Spain, including The National Institute of Cybersecurity, INCIBE, which deals with small-to-medium businesses and citizens, previously known as INTECO.**

**Key words:** Cybersecurity, cyberspace, cyber-threats, cyber-espionage, cybercrime, hacktivism, classified information, CERT, EWS (Early Warning System), multiantivirus system, web analysis, APT (Advanced Persistent Threat), worm, Trojan, rootkit, spyware, ransomware, BYOD (Bring Your Own Device) , phishing, pharming, spam, geolocation, sexting, cyberbullying, grooming.

**Introducción.**

La economía de nuestro país, las actividades de las empresas, las Administraciones Públicas en su misión de prestación de servicios públicos, la Educación y el ocio, los profesionales y los ciudadanos necesitan un ciberespacio seguro para acceder a la información, trabajar, formarse, comprar, crear relaciones sociales… Se necesita un ciberespacio seguro para el desarrollo económico y social, para conducir nuestras transacciones de forma eficaz y a salvo de ataques e incidentes.

La Ciberseguridad es el conjunto de métodos, procedimientos y herramientas que permiten proporcionar seguridad a los sistemas, redes, dispositivos, software y servicios. Es un requisito que precisan las Administraciones públicas, las empresas y las personas para poder desarrollar sus actividades en el entorno actual en el que las ciberamenazas son cada vez más numerosas y variadas, tanto que muchas de ellas sufren mutaciones casi a diario lo que hace que la aplicación de medidas de seguridad sea compleja.

Las amenazas más significativas que se desarrollan a través de medios electrónicos provienen del ciberespionaje, de la ciberdelincuencia y del hacktivismo.

Las acciones de ciberespionaje tratan de recopilar fraudulentamente información con alto valor estratégico, económico, tecnológico, científico…, en poder de los Gobiernos o empresas con el fin de obtener ventaja competitiva o menoscabar la seguridad y el desarrollo nacional. El ciberespionaje es la mayor de las ciberamenazas para las organizaciones públicas y privadas, puesto que los atacantes seguirán madurando y mejorando sus modelos de ataque, así como revisando métodos y herramientas, para mejorar la eficacia de sus acciones y dificultar la detección y sobre todo su identificación.

Los ciberdelincuentes son aquellos que perpetran actividades delictivas tendentes a cometer fraude y por lo general con fines lucrativos.

El hacktivismo es la utilización de herramientas digitales con fines políticos, produciendo la interrupción de los servicios públicos o de las actividades empresariales mediante ataques de denegación de servicio, desfiguración de contenidos o menoscabo de la reputación online de las víctimas.

Actualmente se detecta un aumento en el número y la sofisticación de las amenazas y ataques, nuevos actores, nuevas formas de ocultación, certificados falsos,… Es de vital importancia que las instituciones públicas, las empresas y los ciudadanos se conciencien de los riesgos que supone operar en el ciberespacio de forma que sean capaces de tomar las precauciones necesarias y en consecuencia, reducir su vulnerabilidad y la de todos.

El 5 de diciembre de 2013, fue aprobada en España la “Estrategia de Ciberseguridad Nacional” con el fin de asegurar la gobernabilidad y administración del Estado, el desarrollo de las actividades empresariales o profesionales y el normal desenvolvimiento de la vida privada.

**Información nacional clasificada.**

La Constitución establece el principio de que una participación ciudadana responsable de los asuntos públicos exige una NECESARIA INFORMACIÓN, principio que sólo encuentra excepciones en los casos en que sea necesario proteger la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas

Los responsables de la protección de las materias clasificadas deberán asegurar el adecuado tratamiento y mantener el control o registro de las mismas. La posesión o uso de información o material clasificados estará limitado a lugares donde se disponga de instalaciones para su almacenaje y segura protección. La transmisión del material clasificado se hará por medios de transmisión en forma cifrada.

**¿Qué es información clasificada?**

"Información clasificada es cualquier información o material respecto del cual se decida que requiere protección contra su divulgación no autorizada y al que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad" entendiéndose como información "todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma."

Se considera información nacional clasificada la etiquetada con algunos de los siguientes grados de clasificación, en orden decreciente de importancia:

* SECRETO.
* RESERVADO.
* CONFIDENCIAL.
* DIFUSIÓN LIMITADA.
* SINCLASIFICAR. No está clasificada con los grados anteriores. Requiere cierta protección, por ser de carácter sensible o de uso interno.

**Seguridad de la Información clasificada.**

La información clasificada, constituye el principal ACTIVO CRÍTICO DE INFORMACIÓN en la Administración. Este tipo de información para ser tratada por los sistemas, requerirá la aplicación de medidas de seguridad.

A los demás activos de información que no son información clasificada, se les aplicará las medidas de seguridad establecidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

El soporte es el medio en el que esta se encuentra en cada momento: la mente de las personas, los documentos, las TICs.

**El CNI (Centro Nacional de Información) y la información clasificada.**

De acuerdo con la Ley Orgánica 11/2002, de 6 de mayo, reguladora del CNI, en su Artículo 5, las actividades del Centro Nacional de Inteligencia, así como su organización y estructura interna, medios y procedimientos, personal, instalaciones, bases y centros de datos, fuentes de información y las informaciones o datos que puedan conducir al conocimiento de las anteriores materias, constituyen información clasificada, con el grado de secreto, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales o, en su caso, con el mayor nivel de clasificación que se contemple en dicha legislación y en los mencionados Acuerdos.

La Oficina Nacional de Seguridad (ONS), se crea en 1983, dentro del servicio de inteligencia, como órgano de trabajo del director del CNI, para auxiliarle en el cumplimiento de sus cometidos relacionados con la protección de la Información clasificada.

Además de este organismo también existe dentro del CNI el CCN (Centro Criptológico Nacional) y el CCN-CERT, encargado de dar respuesta ante incidentes de seguridad TIC. Es el CERT gubernamental. Atiende los incidentes de seguridad de las Administraciones Públicas (AAPP) y de las empresas estratégicas. Cuando surge un incidente, a petición de la Administración asesora y orienta. Si la Administración que tiene el problema no lo soluciona, interviene. En los casos de información clasificada interviene de oficio.

**¿ Qué es un CERT (Computer Emergency Response Team) .**

Un CERT es un equipo de personas dedicado a la implantación y gestión de medidas tecnológicas con el objetivo de mitigar el riesgo de ataques contra los sistemas de la comunidad a la que proporciona el servicio.

**¿Cuál es la misión del CCN-CERT?**



La misión de este organismo es la de contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional, cooperar y ayudar a responder de forma rápida y eficiente a las Administraciones Públicas y a las empresas estratégicas, y afrontar de forma activa las nuevas ciberamenazas. Asimismo establece relaciones con otros CERTs y con las Fuerzas y Cuerpos de Seguridad del Estado.

|  |  |
| --- | --- |
| C:\Users\Penelope\Pictures\articulo_ciber_DIM\la moncloa.gif | https://www.ccn-cert.cni.es/images/banners/banner-empresas-estrategicas-cabecera.jpg |

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actúa con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones Públicas. Respecto a la investigación y divulgación, el CCN-CERT emite las series de documentos **CCN-STIC** que ofrecen normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de Tecnologías de la Información de la Administración

El CNN-CERT utiliza, entre otros, los siguientes sistemas y herramientas para cumplir con sus funciones:

* SISTEMA DE ALERTA TEMPRANA (SAT): sistema para la detección rápida de incidentes y anomalías dentro del ámbito de la administración que permite realizar acciones preventivas, correctivas y de contención:
  + SAT de la red SARA. Analiza el tráfico de red que circula entre las redes de los organismos de las Administraciones Públicas conectados a la red SARA, para la detección en tiempo real de ataques y amenazas.
  + SAT de Internet, para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico que fluye entre la red interna del Organismo adscrito e Internet. Es una sonda individual en la red pública del organismo, es decir, un servidor de alto rendimiento, que se encarga de detectar y recolectar la información relativa a la seguridad de la red siempre que esta sea relevante. Después de un primer filtrado, envía los eventos de seguridad hacia el Sistema Central. Este realiza una correlación entre los distintos elementos y entre los distintos dominios (organismos) y después envía avisos y alertas sobre los incidentes detectados.
* Sistema Multiantivirus (MAV) / Análisis de código dañino: permite analizar todo tipo de código, haciendo uso de múltiples motores antivirus, actualizados a tiempo real.
* Sistema de Análisis Web (SAW): Servicio desarrollado e implantado para ofrecer a los responsables TIC una visión en tiempo real del estado de seguridad de sus sitios web, detectando incidentes. Se debe “reportar” un incidente; es decir, cuando se produce cualquier incidente de seguridad en una computadora o en un sistema es crítico para una organización contar con un protocolo eficaz de respuesta. La velocidad con la cual se reconozca, analice y responda a este incidente, limitará el daño y bajará el coste de la recuperación.
* Herramienta **PILAR** Procedimiento Informático Lógico para el Análisis de Riesgos.
* **CARMEN** Centro de Análisis de Registros y Minería de Datos, destinada a la mejora en la detección de un APT en curso.
* **CCNDroid.** Herramienta de Seguridad para Android.
* **LUCIA** Listado Unificado de Coordinación de Incidentes y Amenazas.
* **CLARA** Auditoria de Cumplimiento ENS/STIC en sistemas Windows.

Proyecto **INES** (Informe Nacional del Estado de la Seguridad). El Esquema Nacional de Seguridad establece la obligación de evaluar el estado de la seguridad de los sistemas por parte de las Administraciones Públicas y dispone la necesidad de establecer un sistema de medición a través de un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad (grado de implantación de las medidas de seguridad, eficacia y eficiencia de las medidas de seguridad e impacto de los incidentes de seguridad). El CNN ha desarrollado el proyecto INES con el fin de facilitar la labor a todos los organismos.

El CCN-CERT imparte formación a través de cursos presenciales y de cursos online.

El CCN-CERT también emite informes: Informes de Código dañino, Informes de Amenazas, Informes de Actualidad…

Por último destacar la organización de las Jornadas del Sistema de Alerta Temprana del CCN-CERT que se celebran en la Fábrica Nacional de Moneda y Timbre, en Madrid. El 29 de abril de 2015 se celebró la quinta edición, con la asistencia de 260 personas provenientes de la Administración Pública, central, autonómica y local, empresas de interés estratégico y Universidades.

Estas Jornadas tienen como objetivos realizar una puesta en común con todas las organizaciones implicadas, compartir conocimientos e inquietudes y facilitarles las novedades del servicio.

**Código dañino, malware o malicious software.**

Denominamos código dañino a un programa informático que tiene como objetivo comprometer de algún modo un sistema informático sin el permiso o el conocimiento del usuario. El Código dañino trata de INFECTARLO, COLONIZARLO, SECUESTRARLO.

El código dañino se clasifica de la siguiente forma:

* **Virus:** Archivo ejecutable que desempeña funciones en nuestra computadora sin nuestro consentimiento. Puede dañar archivos, reproducirse, ocultarse o también hacer que dejen de funcionar programas o incluso la máquina infectada.
* **Gusano:** se replica en archivos válidos de nuestro equipo y se replica en otros equipos utilizando la red o la libreta de direcciones.
* **Troyano:** Se disfraza para parecer un programa legítimo e incorporar funcionalidades dañinas.
* **Rootkit:** esconde su actividad al sistema y oculta procesos, carpetas, archivos, registros.
* **Spyware:** recoge información, contraseña de accesos a web, contraseñas bancarias, números de tarjetas de crédito.
* **Ransomware:** secuestra al sistema y a la información. Bloquea el acceso a los mismos hasta que se pague un “rescate”.

**APT (Advanced Persistent Threat): Amenaza persistente avanzada**. Persistentes significa residentes.

Una amenaza persistente avanzada es un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo por el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras, delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas.

Los APT tratan de realizar ataques contra un objetivo concreto, tratan de evadir las técnicas de detección, son persistentes en la máquina comprometida y su estructura es muy compleja. El origen de un APT puede ser Internet, cualquier otra fuente externa o incluso interna.

**Modus operandi de las Amenazas Persistentes Avanzadas.**

Los APT suelen tener tres fases claramente diferenciadas; es decir, el modus operandi de los APTs comprende una PRIMERA FASE de reconocimiento de la víctima, lanzamiento del ataque personalizado e infección exitosa de la víctima. Una SEGUNDA FASE de control, descubrimiento de la información de interés y persistencia en el equipo; y una TERCERA FASE de extracción de la información. Cuando una computadora va más lenta que cuando la adquirimos, existen en ella programas que ya no trabajan para nosotros. Está colonizada.

**Definiciones de virus y actualizaciones de seguridad.**

Las definiciones de virus, spyware y otro malware, son archivos que se usan para identificar software malintencionado y posiblemente no deseado en el equipo. Estas definiciones se actualizan automáticamente aunque también se puede hacer clic en “Actualizar” para obtener las versiones más recientes.

**Recomendaciones generales:**

1. No ejecutar en nuestras computadoras programas de dudosa procedencia.

2. Realizar navegación por Internet por páginas seguras.

3. Desconfiar totalmente de cualquier archivo de procedencia desconocida o dudosa.

4. Emplear para la navegación de Internet y consulta de correo electrónico un usuario

con los mínimos y necesarios privilegios, nunca como administrador o usuario avanzado.

5. Extremar el cuidado en el uso de los pendrive y discos duros portátiles, son una fuente

de colonización.

6. Poner contraseñas disminuye las probabilidades de ciberataques.

7. Apagar el equipo informático cuando terminemos de usarlo.

8. Aumentar la periodicidad de los análisis de riesgos y vulnerabilidades en nuestra

computadora.

**Riesgos y amenazas del BYOD**

****

Se denomina BYOD por ser acrónimo del inglés “Bring Your Own Device”: Traiga su propio dispositivo.

La movilidad y la necesidad o deseo de estar siempre conectado es una de las características que definen a nuestra sociedad actual. Cada vez es mayor el número de personas que utilizan la tecnología de la que son propietarios (hard o soft) para realizar tareas relacionadas con su trabajo, accediendo por 3G, 4G, wifi, etc., a servicios y datos corporativos. Todo esto produce beneficios, pero no está exento de riesgos y amenazas.

La política de seguridad BYOD son las directrices que tengan en cuenta los dispositivos, las formas de acceso y las aplicaciones y que sean aplicables en todas las capas de la organización, incluidas, por supuesto, los altos directivos. Los dispositivos móviles de última generación: tabletas, smartphones, e-readers, etc., se han convertido en un blanco fácil para los ciberataques.

**Riesgos de seguridad en las redes sociales.**

* **Ingeniería social:** proceso de manipular a usuarios legítimos para obtener información clasificada o confidencial, con el objetivo de divulgar información, cometer fraude u obtener acceso a un sistema informático.
* **Suplantación de identidad:** un atacante se hace pasar por otra persona.
* **Phishing y Pharming:** intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a web modificadas de bancos o empresas de tarjetas de crédito para que introduzcan datos personales de su cuenta bancaria.
* **Spam:** correo no deseado, molesto.

Destaco algunos términos y conceptos relacionados con esta actividad:

* **Geolocalización.** Facilitar sin intención el sitio en el que un usuario está ubicado puede ocasionar ciertos riesgos, como pueden ser desde una posible intromisión en la casa de la víctima aprovechando su ausencia, hasta el acoso digital.
* **Privacidad.** Existe el riesgo de compartir (o que otros compartan) demasiada información de uno mismo y sin ningún tipo de control.
* **Falta de control de contenidos.** Una vez que se entrega cierta información a los portales, ésta queda en manos de los propietarios de la red. Existen suspicacias sobre cómo son administrados esos datos sensibles por parte de las compañías. Todavía se producen fallos de seguridad en estas plataformas, lo que facilita el robo de información sensible.
* **Sexting.** Envío por Internet, especialmente a través de smartphones, de fotografías y vídeos con contenido sexual, tomados o grabados por el protagonista de los mismos. A partir del momento en que se envía una foto o un vídeo, se pierde el control de los mismos.
* **Reputación virtual.** Es muy importante seleccionar bien la forma y el fondo de los contenidos que se suben a la red, ya sean fotos, vídeos o comentarios, reflexionando en todo momento sobre la imagen que se está construyendo de sí mismos en la red.
* **Ciberacoso - Cyberbullying.** Uso de información electrónica y medios de comunicación para acosar a un individuo o grupo mediante ataques personales u otros medios. Puede constituir un delito penal.
* **Grooming.** Conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor de edad a través de internet y de las nuevas tecnologías, para conseguir su control a nivel emocional, con el fin último de obtener concesiones de índole sexual.

**Organismos implicados en la ciberseguridad.**

Los organismos encargados de la ciberseguridad de nuestro país son:

El **CCN-CERT CNI**, que tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico.



**CNPIC** (Centro Nacional para la protección de las Infraestructuras Críticas).

Las infraestructuras críticas son infraestructuras estratégicas, es decir, aquellas que proporcionan servicios esenciales, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales:

Administración, Agua, Alimentación, Energía, Espacio, Industria química, Industria nuclear, Instalaciones de Investigación, Salud, Sistema Financiero y Tributario, Tecnologías de la Información y la Comunicación, Transporte.



El objetivo del CNPIC es impulsar y coordinar los mecanismos necesarios para garantizar la seguridad de las infraestructuras que proporcionan los servicios esenciales a nuestra sociedad, fomentando para ello la participación de todos y cada uno de los agentes del sistema en sus correspondientes ámbitos competenciales.

**INCIBE** (Instituto Nacional de Ciberseguridad, anteriormente denominado INTECO, Instituto Nacional de Tecnologías de la Comunicación), dirigido a ciudadanos y PYMES y que posee un CERT, centro de respuesta a incidentes de seguridad TICs. Desde el 28 de octubre de 2014 el Instituto Nacional de Tecnologías de la Comunicación (INTECO) pasó a denominarse INCIBE, perfilándose como el centro nacional de referencia en Ciberseguridad.



INCIBE trabaja para la protección de la privacidad de los usuarios, entendiéndose por usuarios las empresas y profesionales que hacen uso de las TICs, los expertos en seguridad y los ciudadanos.

La Oficina de Seguridad Internauta OSI, es el servicio gratuito que proporciona información y soporte al usuario final para evitar y resolver los problemas de seguridad que le puedan surgir al navegar por Internet.

El recientemente creado en octubre de 2013, **MCCD (Mando Conjunto de Ciberdefensa de las Fuerzas Armadas).**



Es el órgano responsable de programar y ejecutar las acciones relativas a la Ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas.

Contribuye a dar respuesta adecuada en el ciberespacio a las amenazas o agresiones que puedan afectar a la Defensa Nacional.

WEBGRAFÍA:

<http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf>

[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)

[www.cnpic.es](http://www.cnpic.es)

[www.incibe.es](http://www.incibe.es)

[www.emad.mde.es/CIBERSEGURIDAD/](http://www.emad.mde.es/CIBERSEGURIDAD/)

**Madrid, mayo de 2015**