



## **INCIBE –INSTITUTO NACIONAL DE CIBERSEGURIDAD**

León, 24 de febrero de 2017.- El Instituto Nacional de Ciberseguridad (INCIBE) tiene como misión reforzar la ciberseguridad, la confianza y la protección de la privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, red académica, Administración, al sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general. INCIBE elabora para los medios informativos un boletín semanal de Seguridad, con el fin de colaborar conjuntamente en la difusión de la Seguridad de la Información.

Principales informaciones de INCIBE entre el 17 y el 23 de febrero de 2017.

### **Suplantando al centro ESTRADA de gestión de multas para propagar malware**

Se ha detectado una campaña de correos electrónicos que suplantando al Centro de Tratamiento de Denuncias Automatizadas “ESTRADA”, y tratan de infectar los equipos de los usuarios mediante un fichero adjunto que supuestamente contiene la foto de una denuncia.

Si el usuario ha recibido un correo sospechoso pero no ha ejecutado el archivo adjunto, su equipo no se habrá infectado. Pero nunca hay que bajar la guardia, ni descargar y/o ejecutar posibles ficheros adjuntos en los correos electrónicos que pudieran contener malware.

### **Tratan de infectarnos con correos que hablan de transferencias de alquileres**

Esta semana se ha detectado una intensa campaña de correos electrónicos que intentan infectar nuestro equipo con un fichero adjunto malicioso, utilizando como asuntos del email: NO RECIBÍ LA TRANSFERENCIA o ALQUILER DE FEBRERO.

No descargar archivos sospechosos adjuntos en los correos y realizar copias de seguridad en un soporte que no esté conectado al ordenador habitualmente son las principales medidas a adoptar para evitar la pérdida de información en caso de resultar infectados.

Esta información no puede ser usada en parte o en su integridad sin necesidad de citar fuentes.





## Cinco proyectos líderes en ciberseguridad, apoyados por MINETAD, mostrarán el liderazgo español en el sector en el 4YFN

El Four Years From Now (4YFN), el espacio dedicado al emprendimiento dentro del Mobile World Congress 2017, que tendrá lugar del 27 de febrero al 2 de marzo en Barcelona, contará con la presencia de cinco de los proyectos que han participado en el programa Incubadora Ciberemprende de INCIBE. 29 iniciativas emprendedoras participaron en el Certamen de 2016, recibiendo mentoring, formación online en materia de negocio, marketing y financiación y visibilidad en eventos. Por este motivo, cinco de ellas se desplazarán a Barcelona para exponer su potencial tecnológico.

## INCIBE publica su Balance de Seguridad 2016

INCIBE hace balance de su actividad en 2016, año en el que se ha cumplido el décimo aniversario de este organismo que presta sus servicios a ciudadanos y empresas.

En su balance de ciberseguridad se recogen datos referentes a servicios y soluciones para agentes y empresas estratégicas, la Oficina de Seguridad del Internauta, el Programa de Excelencia en Ciberseguridad y el apoyo al emprendimiento, promoción del talento y desarrollo de la industria.

## De la A a la Z: Glosario

INCIBE ha renovado y actualizado su glosario de términos de ciberseguridad, una recopilación de términos utilizados en el blog de seguridad, con el objetivo de aclarar a sus usuarios los conceptos que se utilizan a diario, con un lenguaje adecuado. Se trata de términos adaptados y redactados en base a las definiciones técnicas de nuestro equipo de especialistas en ciberseguridad, y de diversas fuentes internacionales especializadas de reconocido prestigio.





## Dos mejor que uno: doble factor para acceder a servicios críticos

Además de autenticarnos con una contraseña o con PIN, es decir con «algo que sé», también podemos hacerlo con «algo que tengo» (un token USB o una tarjeta de coordenadas) o con «algo que soy» (la huella, el iris, la voz o el rostro) o bien con varios de estos elementos o factores. Es lo que se llama autenticación de doble (o triple) factor. La autenticación de dos (o más) factores, al comprobar dos veces mediante mecanismos diferentes, que somos quienes decimos ser, agrega una capa de seguridad a nuestros servicios, aplicaciones y sistemas. Cualquier intento de hacerse con nuestras llaves se complica.

## RoT: Ransomware de las Cosas en SmartTV's

Cada vez hay más dispositivos conectados a Internet convertidos en nuevos objetivos para los ciberdelincuentes. Que un dispositivo sea inteligente no implica que sea seguro. El malware que tradicionalmente afectaba a ordenadores ha evolucionado y en la actualidad, con el IoT (Internet de las cosas) cada vez más presente, ha aumentado nuestra exposición a ser infectados, por lo que no debemos bajar la guardia.



Para más información en materia de Ciberseguridad visite INCIBE [www.incibe.es](http://www.incibe.es), Protege tu Empresa <https://www.incibe.es/protege-tu-empresa> y OSI <http://www.osi.es/>.

Esta información no puede ser usada en parte o en su integridad sin necesidad de citar fuentes.

