

ENCUENTRO

IMPACTO DEL SOFTWARE EN LA CIBERSEGURIDAD Y LA SEGURIDAD JURÍDICA DE LAS EMPRESAS

MADRID, 30 DE NOVIEMBRE 2016

SOFTWARE: RIESGOS, AMENAZAS Y OPORTUNIDADES PARA LA EMPRESA

El Software es una herramienta esencial para el funcionamiento y la productividad de cualquier negocio en cualquier sector de la economía moderna, que dependen de él para diseñar productos, gestionar y mejorar procesos, proveer servicios, comunicarse con los clientes y ahorrar costes, en definitiva, para manejar sus operaciones de manera más rápida, eficiente y competitiva.

Con un uso tan intenso y extendido de los programas de software en todas las áreas y procesos de las empresas, los problemas para la seguridad derivados de una gestión ineficiente de este activo, de un mal funcionamiento o de un uso ilícito, están aumentando en la misma proporción.

Encuentro profesional

En este contexto, CEOE, BSA The Software Alliance y la Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales (AMETIC), con el apoyo de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), organizan una jornada informativa con el fin de dar a conocer de forma práctica los riesgos para la seguridad de las compañías, desde el punto de vista tanto operativo como legal.

Dirigido a

Empresarios y directivos de empresas, responsables de informática y tecnologías de la información, asesorías jurídicas y responsables del área legal o de *compliance*.

Lugar: Sede CEOE (Sala JDN) c/ Diego de León, 50. MADRID

Fecha: Miércoles, 30 de noviembre de 2016

Hora: 9:30-12:00

Confirmación y registro: http://ametic.es/es/Impacto_Software

Más información: 91 788 32 00 (Víctor Acero / Julián Ramos)

Software
LEGAL
Valor 
SEGURO

www.softwarelegalempresa.com

PROGRAMA

MADRID, 30 DE NOVIEMBRE 2016

9:30 PRESENTACIÓN

El rol del software como activo crítico en las empresas, motor de desarrollo de la sociedad de la información y de convergencia hacia la economía digital.

Cristina Morales. Secretaria General de Contenidos de la Sociedad de la Información. Secretaria de Estado para la Sociedad de la Información y la Agenda Digital. Ministerio de Energía, Turismo y Agenda Digital.

9:45 ANEZAS PARA LA CIBERSEGURIDAD DE LA EMPRESA

El software como mecanismo para la entrada y distribución de malware en los sistemas de la empresa. Gestión de riesgos. Buenas prácticas, protocolos y medidas de ciberseguridad.

Daniel Fírvida Pereira, Coordinador de Servicios de Ciberseguridad del Instituto Nacional de Ciberseguridad INCIBE.

10:15 RIESGOS LEGALES PARA LA EMPRESA Y SUS REPRESENTANTES

Normativa y responsabilidad legal de las empresas y sus administradores ante infracciones contra la propiedad intelectual del software. Procedimientos judiciales. Medidas de control y cumplimiento eficientes para la prevención de delitos.

Carlos Pérez, socio responsable del área de IT, Risk & Compliance de ECIJA, profesor asociado Master de Propiedad Intelectual y Sociedad de la Información de ESADE

11:15 PREVENCIÓN, PRIMER PASO PARA LA SEGURIDAD DE LAS INFRAESTRUCTURAS

Como establecer una base sólida de protección de datos y activos informáticos. Análisis de vulnerabilidades e identificación de equipos y software y riesgos asociados. Evaluación de riesgos por acceso externo a los sistemas informáticos.

Carlos de la Insua, Managing Partner Softcare, experto en Software Asset Management (SAM)

11:45 TURNO DE PREGUNTAS

MALWARE

Amenaza oculta para la seguridad

Los virus y programas ocultos en webs, en ficheros o en el software sin licencia amenazan el funcionamiento y la seguridad de las empresas.

¿Qué es?

malicious + software = **malware**



VIRUS



TROJAN HORSES



SPYWARE



RANSOMWARE

El **malware** es un programa de software que introducido en los equipos y sistemas de una organización los bloquea o controla, "secuestra" información, roba o elimina datos, causa pérdidas millonarias y conlleva graves riesgos legales y de reputación.

¿De dónde proviene?

1 De descargas e instalaciones directas por empleados.

2 De enlaces o visitas a páginas web maliciosas.



3 De la ejecución de ficheros o archivos con virus camuflados.

4 De la instalación de programas de software sin licencia.

5 De grietas de seguridad de programas desactualizados.

¿Sabía que...?

26% de los EMPLEADOS descarga software no autorizado en su PC

4 de cada 10 PCs EN ESPAÑA tiene instalado software sin licencia

280 mil EUROS es la multa que puede recibir un administrador de empresa por software ilegal

3 de cada 10 PROGRAMAS SIN LICENCIA contiene malware oculto

88 mil EUROS puede costar a una pyme un ataque o infección de malware



¿Cómo prevenir?



Incorporando sistemas de seguridad, antivirus eficientes y monitorice regularmente.



Consultando con expertos en gestión de activos de software (SAM).



No instalando archivos o software de fuentes desconocidas.



Conociendo el software instalado, su procedencia y licencias de uso.

Software
LEGAL
Valor
SEGURO

www.softwarelegalempresa.com