CiberMS 2015

# 12 COMPAÑÍAS ESPAÑOLAS DEMUESTRAN SU COMPROMISO CON LA CIBERSEGURIDAD

- ***Por cuarto año consecutivo ISMS Forum Spain ha llevado a cabo los Ejercicios de Ciberseguridad multi-sectoriales con la participación de 12 grandes empresas españolas.***
- ***El objetivo de las pruebas ha sido medir la capacidad de las empresas para resistir ante un ciberataque.*** **La evaluación de las empresas participantes ha sido satisfactoria**.
- ***La evaluación de los ejercicios ha sido realizada por Deloitte y el equipo atacante lo han formado Grupo SIA, S21sec, Telefónica y Mnemo. Además se ha contado con la colaboración de ECIX y el apoyo del Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) como observadores.***

**Madrid, 03 de marzo de 2016**. La **Asociación Española para el Fomento de la Seguridad de la Información**, **ISMS Forum Spain**, ha llevado a cabo **CiberMS2015**, la cuarta edición del programa de ciberejercicios multi-sectoriales con la colaboración de **Deloitte** en calidad de evaluador, y de ***Grupo SIA, S21sec, Telefónica y Mnemo***, en calidad de equipos atacantes, así como con el apoyo de **INCIBE y CNPIC** como observadores, y **ECIX** como asesor legal. Las 12 grandes empresas españolas que han puesto a prueba sus capacidades de ciberseguridad en un examen práctico pertenecen a los sectores de banca, energía, retail, seguros, telecomunicaciones y transporte.

**La evaluación de las empresas participantes en CiberMS2015 ha sido satisfactoria**. La puntuación obtenida refleja un buen nivel de madurez e implantación de medidas destinadas a responder a posibles ciberataques. Esta puntuación responde a una serie de 65 controles estructurados en varias áreas para evaluar a cada una de las entidades participantes en función de tres líneas fundamentales: la **respuesta ante los ataques**, las **medidas organizativas** -en cuanto a concienciación, compromiso de la dirección y procedimientos de respuesta a incidentes- y, por último, las **medidas técnicas** implementadas -en cuanto a prevención, detección, contención y forense.

En lo relativo a los ataques realizados cabe destacar que los **vectores de entrada por ingeniería social siguen siendo muy eficaces** para obtener información sensible de las entidades. A través de estos ataques las personas son engañadas, y los hackers lo aprovechan para introducir malware en su empresa o terceros con la intención de obtener información, cometer fraude o conseguir acceso a un sistema o una red. Uno de los ataques por ingeniería social más conocido es el *phishing,* en el que se envía un correo electrónico en el que se solicita información o que se descargue y ejecute algún tipo de archivo haciéndose pasar por un tercero confiable de manera fraudulenta.

En cuanto a las medidas organizativas de las empresas, se concluye que **existe un alto compromiso en esta materia por parte de la Dirección** de las entidades participantes; al igual que, en lo que respecta a las medidas técnicas, ha destacado un **nivel alto de capacidad de detección** ante posibles ciberataques por parte de las empresas participantes.

Entre las conclusiones extraídas del ciberejercicio de este año destaca la **mejora**, por un lado, en la **capacidad de detección de ataques por parte de las empresas** -gracias, principalmente, a la mayor dotación de medios técnicos y equipos humanos-, y, por otro lado, en la elaboración de procedimientos asociados.

En cambio, el aspecto donde **todavía deben concentrarse los esfuerzos** es la **concienciación,** ya que el factor humano tiene un gran peso en los riesgos de ciberseguridad. Aunque es habitual la realización de un curso de concienciación para empleados en la mayoría de las empresas, en general no se contemplan en las políticas de seguridad la inclusión de métricas asociadas a las acciones de concienciación de cara a conocer el nivel de concienciación real de los empleados. Los resultados de los ataques de ingeniería social han puesto de nuevo de manifiesto que el factor humano es el eslabón más débil de la cadena. En este sentido, nuevos enfoques y actividades de concienciación, como puedan ser ejercicios prácticos para todos los empleados, pueden contribuir a que cale el mensaje de la importancia de la seguridad en todos los empleados de la organización.

Este es el cuarto año que ISMS Forum, en colaboración con Deloitte, realiza estos ejercicios de ciberseguridad. En todas las ediciones, el objetivo ha sido obtener una visión del nivel de ciberseguridad que muestran compañías españolas de distintos sectores evaluando la capacidad de resiliencia ante posibles ataques a sus sistemas informáticos e infraestructuras críticas, a fin de mejorar su capacidad de respuesta. Para obtener esta visión cada año se han evaluado las capacidades de las empresas utilizando una metodología que permite hacer la comparación entre empresas y con los resultados de años anteriores, de forma que se pueda seguir su evolución. Durante los ejercicios se separa el rol de los atacantes y de los evaluadores. Los ataques técnicos son ejecutados por el mismo equipo de personas (Grupo SIA, S21sec, Telefónica y Mnemo, coordinados por ISMS Forum Spain), mientras que la evaluación la realiza un equipo independiente (Deloitte).

## Sobre ISMS Forum Spain

La Asociación Española de la Seguridad de la Información, ISMS Forum Spain, es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España. Creada con una vocación plural y abierta, se configura como un foro de debate especializado para empresas, organizaciones públicas y privadas, investigadores y profesionales, donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. ISMS Forum Spain tiene ya a más de 120 empresas y más de 800 profesionales asociados. La Asociación es, por tanto, la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España en la actualidad.

**PARA MÁS INFORMACIÓN:**
DEPARTAMENTO DE COMUNICACIÓN DE ISMS FORUM
Tel.: 91 563 50 62
Email: comunicacion@ismsforum.es
www.ismsforum.es
Síguenos en Twitter @ISMSForum