Tendencias en ciberseguridad

Simulación de incidentes y ciberejercicios

La simulación de incidentes y realización de ciberejercicios se enmarcan dentro de un conjunto de actividades que sirven para **evaluar y perfeccionar las acciones en ciberseguridad**. Los sistemas de simulación de escenarios e incidentes se basan en la utilización de entornos de pruebas (*testbed*) que ponen a prueba la **capacidad tecnológica y de reacción** de las herramientas y recursos de una organización. Los ciberejercicios, por su parte, permiten evaluar el estado de preparación de los participantes frente a crisis de origen cibernético, facilitando además lecciones aprendidas y recomendaciones para el futuro.

ORIGEN DE LA TENDENCIA

ECONÓMICO/EMPRESARIAL · DEMANDA · NORMATIVA · TECNOLOGÍA

En España, la **Estrategia de Ciberseguridad Nacional** pone de manifiesto la necesidad de desarrollar modelos de simulación de escenarios basado en ciberamenazas contra Infraestructuras Críticas y sus riesgos derivados, así como elaborar y ejecutar un Programa de Ejercicios de Simulación de Incidentes de Ciberseguridad. En EEUU, el Congreso ha elaborado la **Ley de Autorización de Defensa Nacional 2016**, la cual encarga al mando de Ciberdefensa la realización de "cibermaniobras", que tendrán que simular ataques informáticos con los sistemas del gobierno americano. Por otro lado, la creciente dependencia de la sociedad del ciberespacio y su fácil accesibilidad hacen que cada vez sean más comunes y preocupantes las intromisiones en este ámbito. Los ciberataques, en sus **diversas modalidades de ciberterrorismo, ciberdelito, ciberespionaje o activismo en la red, se han convertido en un potente instrumento de agresión contra instituciones públicas.**

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación · Comercialización · **Servicios**

La oferta de ciberejercicios cooperativos en ciberdefensa, de simulación y experimentación con nueva tecnología, malware y otras ciberamenazas o pruebas de ciberseguridad en un entorno controlado, se situaría en el último eslabón de la cadena de valor de la ciberseguridad como una actividad de prestación de **servicios de ciberseguridad por empresas especializadas**.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	ADMINISTRACIÓN PÚBLICA
Impacto en usuarios ○○○	Impacto en empresas ●○○	Impacto en gobiernos ●●●
El impacto en usuarios o ciudadanos de la realización de simulación de incidentes en ciberseguridad es bajo. Dichas simulaciones realizadas por los gobiernos o AAPP repercuten finalmente en una **mayor seguridad y fiabilidad** de los sistemas e infraestructuras críticas del país.	Las empresas especializadas en servicios de ciberseguridad son las encargadas de realizar el desarrollo de **plataformas o sistemas de simulación**, adaptables a los requisitos de las organizaciones y que ayuden en la programación y puesta en marcha de ciberejercicios en las instituciones.	Las simulaciones y ciberejercicios ayudan a las Administraciones Públicas y los gobiernos a **evaluar y perfeccionar** las acciones llevadas a cabo en ciberdefensa, especialmente, analizando las dependencias entre las diferentes Infraestructuras Críticas y los riesgos acumulados por éstas.

CLASIFICACIÓN DE LA TENDENCIA

SOLUCIONES DE PREVENCIÓN · SOLUCIONES DE CONTROL · SOLUCIONES DE MITIGACIÓN

Las simulaciones se encuentran entre las **principales técnicas de prevención frente a las ciberamenazas** dada la importancia que supone la experiencia previa para desarrollar capacidades de respuestas adecuadas. Las simulaciones de incidentes en ciberseguridad permiten probar lo que sucedería y a qué decisiones habría que hacer frente en caso de un ataque.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO · INTRODUCCIÓN · **CRECIMIENTO** · MADUREZ

En los 60 ya se puede mencionar el Ejercicio REFORGE, concebido por la OTAN y realizado anualmente durante la Guerra Fría. A partir de los años 80, la simulación cobra cada vez más importancia como un **medio de formación**. Aunque inicialmente, entre 2002 y 2004 el número de ciberejercicios realizados anualmente se redujo, en los últimos años ha **crecido considerablemente** por alcance, ámbito geográfico, número de sectores involucrados y por perfil de participación.

Tendencias en ciberseguridad

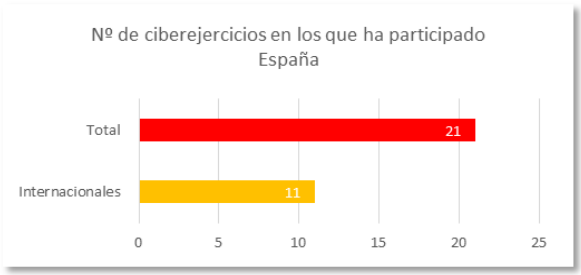
Simulación de incidentes y ciberejercicios

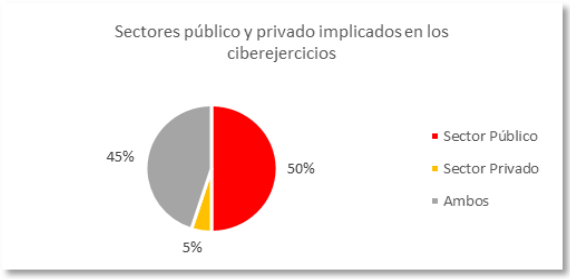
ÁMBITO DE APLICACION

El grado de dependencia de nuestra sociedad respecto de las TIC y el ciberespacio crece día a día. Conocer sus amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis e investigación constituyen elementos esenciales de la **Política de Ciberseguridad Nacional**. Además el Estado debe promover la **participación coordinada** de instituciones públicas y del sector privado en simulacros y ejercicios internacionales.

CARACTERIZACIÓN DEL SECTOR

- Se ha detectado que el **50% de los ciberejercicios** involucra solo al sector público, frente al 5% que implica solo al sector privado; el 45% de los ciberejercicios compromete a ambos sectores.
- Alrededor de un 16% de ciberejercicios internacionales han contado con la participación conjunta de hasta **20 países de la UE**, y más de 20 países de la UE han participado conjuntamente solamente en un 7% de ciberejercicios organizados a nivel internacional.
- La **participación de España** se refleja en un total de 21 ciberejercicios, de los cuáles, 11 pertenecen a ediciones de ciberejercicios internacionales y el resto, los celebrados dentro del ámbito nacional.





PREVISIONES DE DEMANDA

CRECIMIENTO

- En 2015, desde INCIBE se gestionaron **45.680 incidentes** relacionados con la seguridad cibernética de las empresas, un 180% más que en 2014. De todos estos incidentes, 11.400 fueron relacionados con el **fraude electrónico**.
- En 2016, INCIBE se prepara para gestionar **100.000 incidentes de ciberseguridad**, el doble que en 2015

CLIENTES

- Infraestructuras críticas.
- Empresas, fundamentalmente, de prestación de servicios financieros, TIC o energéticas.
- Empresas de demanda sofisticada de ciberseguridad.
- Administraciones Públicas y Gobiernos.
- Cuerpos y fuerzas de seguridad del Estado.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE | **DIFERENCIACIÓN EN PRESTACION DE SERVICIOS** | DIFERENCIACIACIÓN EN VALOR AÑADIDO

CASO DE ÉXITO

Deloitte.

- Deloitte lleva organizando y realizando desde hace más de cinco años **Ciberejercicios públicos y privados**, tanto a nivel nacional (INCIBE, CNPIC, ISMS Forum, grandes corporaciones) como internacional (SIFMA, ENISA).
- Estos ciberejercicios consisten en la **evaluación de procedimientos con los equipos de tecnologías de la información**, de seguridad y de respuesta ante incidentes. Para ello, Deloitte desarrolla metodologías de evaluación o marco de control, y ejecución de pruebas, tanto en un entorno real como simulado.
- Gracias a estos ciberejercicios, las empresas participantes logran conocer el **grado de madurez y eficacia de su organización** en la gestión de la ciberamenazas e identificar puntos de mejora, ponen a prueba sus sistemas, tecnologías y capacidades humanas y procedimiento técnicos y de coordinación para responder a un ciberataque en un escenario realista y pueden evaluar cómo impactaría un ciberataque en sus infraestructuras TIC.