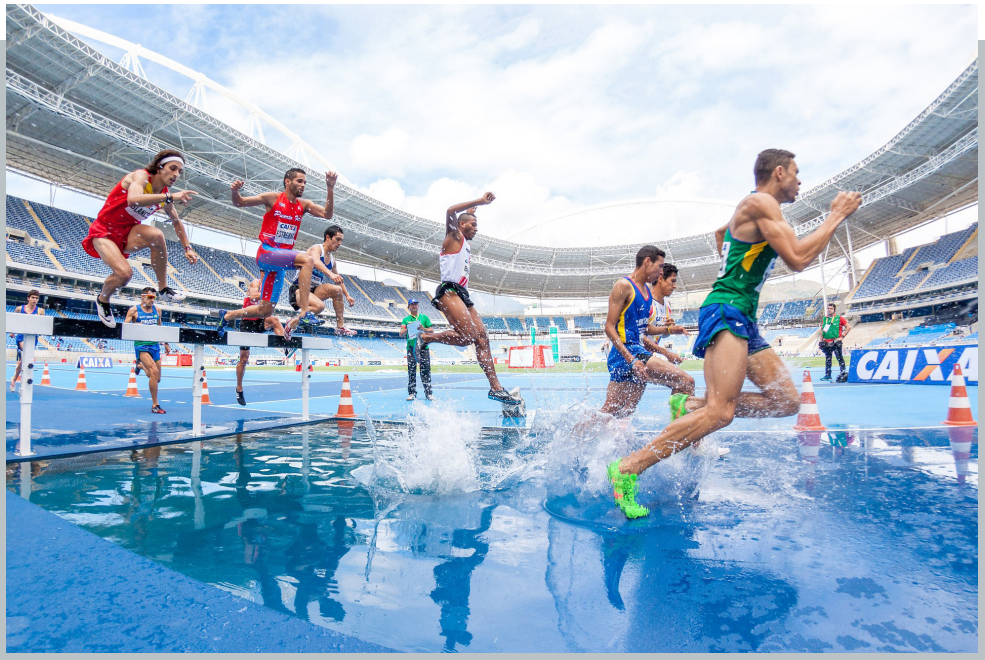
¿Estáis preparados?

Manual para el coordinador

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice



1 ¿Cómo lanzo el reto?

El coordinador de la dinámica ha de seleccionar a los participantes que formen un equipo. Cualquiera puede participar. (Si la empresa tiene suficientes empleados, se puede organizar una dinámica de competición entre equipos.)

En cada sesión se lanzará sólo un reto, a elección del dinamizador. Se puede establecer un tiempo máximo para resolverlo. Cada reto está pensado para resolverse en una sesión de una hora como máximo.

Sólo necesitaréis una pizarra dónde escribir o un lugar dónde pegar post-it (un brown paper).

El equipo tendrá acceso libre a los materiales de concienciación indicados en la web y a otros materiales que puedan aportar los participantes.

1 ¿Cómo lanzo el reto?

1.1 Formación de equipos

El equipo estará formado por perfiles variados dentro de la empresa, todos pueden participar, pues cualquiera puede verse involucrado en un incidente. Sería bueno que en el equipo participaran representantes de todos los perfiles de la empresa.

Una vez formado el equipo, el dinamizador explicará cuál es el motivo de la reunión: realizar un simulacro de respuesta ante un incidente de seguridad.

El ejercicio comienza con la selección y lanzamiento del reto. Después, continúa con un debate dónde se ha de averiguar: qué ha pasado, qué ha fallado, cómo tenemos que actuar, y qué lecciones hemos aprendido. Finalmente el equipo, con la ayuda del moderador, contrasta los resultados de los debates con la solución del reto. (Si se optara por crear varios equipos se contrastarían los resultados entre los distintos equipos.)

1.2 Lanzamiento del reto, ¿qué ha pasado?

El dinamizador traslada al equipo el **escenario del reto** elegido. Los escenarios son ejemplos de una supuesta empresa en la que ha ocurrido un incidente. El equipo tiene que ponerse en el lugar de esa empresa y comenzar la dinámica.

En primer lugar tenemos que debatir sobre **¿qué ha pasado?** Se trata averiguar entre todos, y en algunos casos imaginar, la respuesta a las siguientes preguntas:

1. ¿Qué ha ocurrido?
2. ¿Dónde se ha originado? ¿qué dispositivos están afectados?
3. ¿Cuándo o desde cuándo ocurre?
4. ¿Quién ha podido hacerlo, por qué y cómo (posibles causas)?
5. ¿Cuáles son los daños materiales, personales y económicos?, ¿cuánto costarán?
6. ¿Tendrá consecuencias sobre la reputación de imagen de la empresa?
7. ¿Tendremos que avisar a nuestros clientes, colaboradores o usuarios?
8. ¿Tiene implicaciones legales?

Si fuera necesario, se propone utilizar técnicas de *brainstorming* o lluvia de ideas para que todo el mundo participe. En el *«brown paper»*, cada participante pegará sus ideas escritas en post-it como respuesta a cada pregunta. Entre todos, con ayuda del dinamizador se han de consensuar las respuestas a las preguntas.

1 ¿Cómo lanzo el reto?

1.3 ¿Qué ha fallado?

Una vez identificado el incidente y sus consecuencias, tenemos que conocer cómo hemos llegado a esta situación.

Para ello revisaremos si lo que ha permitido que ocurriera este incidente tiene que ver con:

- la formación o concienciación de los empleados;
- la implantación o revisión de procedimientos como actualizaciones, cambios de contraseñas, cifrado, acceso remoto, etc.
- la carencia de medidas técnicas para evitarlo: antimalware, cortafuegos, etc.

1 ¿Cómo lanzo el reto?

1.4 ¿Cómo salimos de esta?

En equipo y entre todos han **de decidir y escribir en post-it tantas ideas como se les ocurran** sobre:

- qué han de hacer y cómo han de actuar;
- qué no han de hacer;
- cómo podríais haberlo evitado.

Se han de poner en común las conclusiones, decidiendo la respuesta a las preguntas, exponiéndolas por ejemplo en un *brown paper* con post-it o en la pizarra.

El dinamizador podrá lanzar al final un debate sobre la idoneidad o aplicabilidad de las soluciones mostradas en la empresa real. En este debate se deben escoger las soluciones válidas y las que no lo son.

1.5 ¿Qué hemos aprendido?

El dinamizador expone los contenidos de la solución del reto: ¿Qué puedes hacer?, ¿Qué no debes hacer?, y ¿cómo podría haberse evitado? Entre todos se debate sobre si la empresa está preparada o no para afrontar un reto real de esas características.

Como material de consulta puedes descargar un cuestionario para actuar en caso de incidente.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL