¿Estáis preparados?

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_ 2006-2016 TRABAJANDO POR LA CONFIANZA DIGITAL

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Índice

1 Descripción del juego

Ha ocurrido un incidente de seguridad en vuestra empresa y tenéis que:

1. Averiguar qué ha pasado.
2. Identificar qué pasos hay que dar para remediarlo.

2 ¿Qué hace falta?

1. Un equipo de personas para debatir sobre el incidente y cómo resolverlo.
2. Un lugar de reunión.
3. Una pizarra o un sitio dónde pegar post-it.
4. Material de apoyo:

   - esta presentación cómo guía para analizar lo ocurrido
   - una descripción de cada reto
   - un cuestionario de respuesta a incidentes
   - la solución de cada reto que se desvelará al final

5. Un PC con conexión a internet, para consultar opcionalmente las secciones del portal de Incibe:

   - ¿Qué te interesa?
   - Testimonios del Blog
   - Guías

3 ¿Qué hay en las instalaciones de la empresa?

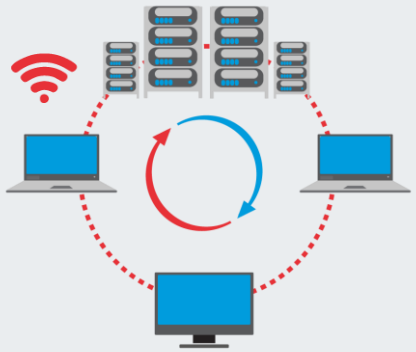
- Imaginad, en una empresa como la vuestra, **una oficina** con:

  - puestos de trabajo: PC, impresoras, teléfonos,...
  - dispositivos móviles: portátiles, móviles y tabletas
  - sistemas de almacenamiento externo: discos, pendrives,...

3 ¿Qué más hay en las instalaciones de la empresa?

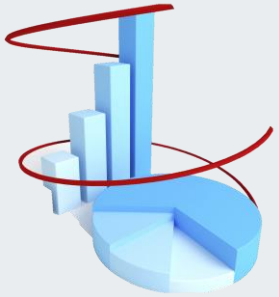
- **En las instalaciones de la empresa también hay:**

  - servidores de correo electrónico
  - servidores de archivos y aplicaciones
  - conexión a Internet, *routers*,..., wifi



- **Y distintos tipos de datos e información:**

  - datos personales de clientes y proveedores
  - datos de funcionamiento y gestión de la empresa
  - propiedad intelectual
  - procesos internos en aplicaciones CRM, ERP, etc. en los servidores o en la nube



3 Y además...

- Se utilizan servicios en la nube (almacenamiento).
- Tenéis una página web o tienda online (alojada en un proveedor externo).
- Se utilizan las redes sociales.

1

2

3

4 ¿Cuáles son los activos (físicos) de la empresa?

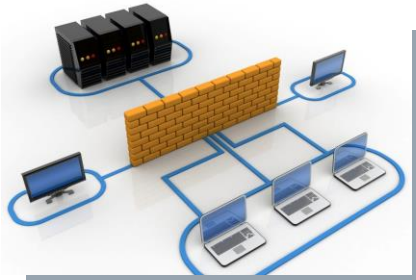
- Puestos de trabajo
- Ordenadores personales
- Impresoras
- Teléfono fijo

Dispositivos móviles:

- Teléfono
- Tableta
- Portátiles

Sistemas de almacenamiento externo:

- Pendrives
- Discos duros externos



- Sevidores de correo electrónico
- Servidores de aplicaciones
- Router de Internet

- Página web / Tienda online
- Servicios externalizados
- Servicios en cloud

Los datos, información y programas son parte de los activos lógicos.

5 Fases del ejercicio ¿estás preparado?

6 ¿Qué ha pasado?

- En este momento los participantes reciben la descripción del incidente.

Se inicia el debate sobre lo que ha ocurrido

Entre todos tenéis que:

- identificar qué ha podido ocurrir respondiendo a las preguntas de la diapositiva siguiente.

6 ¿Qué ha pasado? – Preguntas guía

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? ¿Podemos valorarlos?
6. ¿Tendremos que avisar a nuestros clientes o usuarios?
7. ¿Tiene consecuencias sobre nuestra reputación?
8. ¿Tiene implicaciones legales?

(a continuación tienes 3 diapositivas de apoyo)

¿Qué ha podido pasar y dónde?

Incidente / Activo	Robo o pérdida	Avería	Infección por malware	Infección con extorsión	Botnet	Denegación de servicio
Puesto de trabajo						
Dispositivos móviles						
Sistemas de almacenamiento externo						
Servidores y redes						
Página web, servidores externalizados o en cloud						

Marcad la(s) casilla(s) que correspondan.

¿Quién ha facilitado o iniciado el incidente?

- **Alguien desde dentro de la empresa:**

  - por despiste, inconsciencia e ingenuidad;
  - descontento o con afán de revancha o lucro;
  - sin mala intención pero descuidado, por no aplicar las políticas o no cumplir los procedimientos

- **Desde fuera:**

  - un exempleado descontento o con afán de revancha o lucro;
  - un ciberdelincuente que quiere llevarse datos de la empresa para venderlos, causar daño de imagen o introducir malware;
  - un grupo de ciberdelincuentes organizado que nos utiliza como a otras empresas para sus fines delictivos;

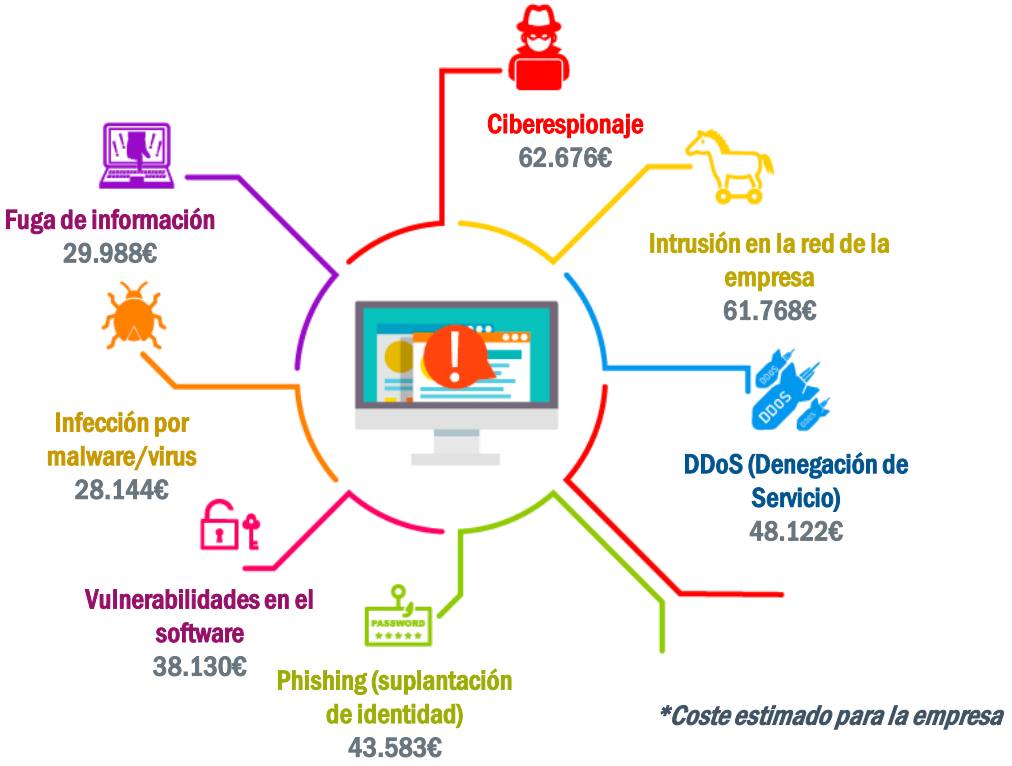
6 ¿Cuáles son las consecuencias?

Valorar las consecuencias no es fácil, tendréis que echar mano de vuestra experiencia y de la de otros.

- A modo orientativo considerad:

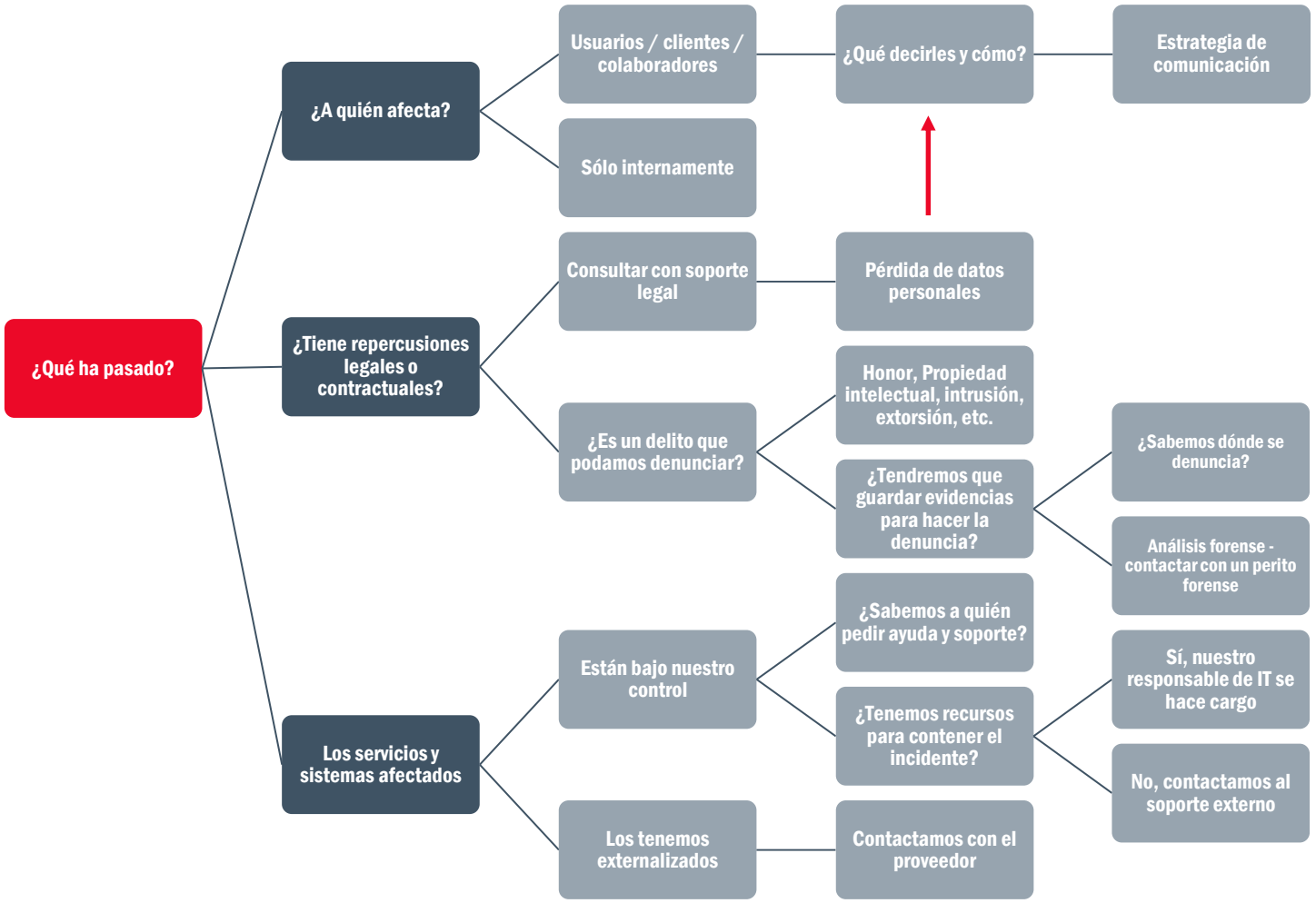
  - pérdidas financieras;
  - costes de reparación o sustitución de equipos:
  - costes por interrupción del servicio;
  - pérdida de reputación y confianza de los clientes;
  - disminución del rendimiento;
  - infracciones legales (multas) o ruptura de condiciones contractuales con terceros;
  - pérdida de ventaja competitiva;
  - daños personales.

6 El coste de los incidentes en la pymes



Las cifras son pérdidas medias totales por tipo de incidente en una pyme según el informe: Kapersky Labs

6 ¿Sobre qué más tenemos que reflexionar?



7 El juego continua, ¿qué ha fallado?

- Una vez identificado qué ha podido pasar y dónde, tenéis que identificar el motivo del incidente.

¿Qué mecanismo/protocolo de seguridad ha fallado?

(Consulta la tabla de la diapositiva siguiente)

- Anotad las conclusiones en post-it (o en una pizarra) para poder comprobarlas al final.

7 ¿Qué error hemos cometido?

Incidente / Errores	Robo o pérdida	Avería	Infección por malware	Infección con extorsión	Botnet	Denegación de servicio
Uso de equipos o servicios no autorizados						
Contraseña poco segura, por defecto o a la vista						
Dejar los dispositivos desatendidos o sin bloquear						
Acceso desde redes no seguras						
Ser víctima de engaños de ingeniería social						
Mala configuración de los equipos / dispositivos						
Gestión de proveedores sin acuerdos de seguridad y confidencialidad						
Equipos con software no actualizado						
Acceso desde redes wifi públicas a recursos de la empresa						
Dispositivos con información confidencial no cifrada						
Routers o redes con contraseña por defecto o comunicaciones con cifrado débil						
Mala gestión de usuarios (permisos excesivos, cuentas sin uso,...)						
Control de accesos físicos insuficiente						
Equipos viejos y sin mantenimiento						

8 ¿Cómo salimos de esta?

- Una vez hayáis determinado el carácter del incidente, sus implicaciones y los errores cometidos.

Ahora, hay que resolver el incidente

- Se abre un debate sobre qué hacer para resolverlo.

  - ¿Qué hay que hacer?
  - ¿Qué no hay que hacer?
  - ¿Qué tendríamos que hacer para evitarlo en el futuro?

- A continuación, tenéis algunas pistas.

8 ¿Cómo resolvemos el incidente?

- ¿Tenemos que avisar a alguien para que nos ayude?, ¿sabemos a quién?
- ¿Tenemos que detener el incidente o evitar que se propague?, ¿sabemos cómo?
- ¿Podremos recuperar la información o los equipos/servicios afectados?, ¿cómo?
- Si tenemos que denunciar, ¿cómo hacemos para guardar las evidencias?
- ¿Tendremos que avisar a los medios o a los clientes o colaboradores afectados?, ¿qué les vamos a decir?
- ¿Cómo evitamos que vuelva a suceder? *(consulta la siguiente diapositiva)*

¿Qué tenemos que hacer para evitarlo?

Activos/medidas	Puesto de trabajo	Dispositivos móviles	Sistemas de almacenamiento	Servidores y redes	Pág. Web externalizada, o servicios en cloud	Varios activos
Actualizaciones software						
Antimalware						
Cortafuegos						
Sistema de control de accesos físicos						
Sistema de control de accesos lógico						
Gestión de proveedores						
Protocolo uso puesto de trabajo						
Protocolo uso móviles y portátiles						
Protocolo uso dispositivos almacenamiento						
Aplicaciones y servicios permitidos						
Procedimiento gestión usuarios						
Procedimiento clasificación y cifrado de información						
Procedimiento copias de seguridad						
Seguros externos						
Procedimiento configuración segura equipos						
Formación acceso desde redes externas						
Formación ingeniería social						
Formación uso cuentas y contraseñas						

9 ¿Qué hemos aprendido?

Es hora de hacer repaso de todo lo que habéis debatido.

- Comprobad que habéis respondido a todas las preguntas y que todos estáis de acuerdo con las respuestas.
- Repasad los fallos que técnicos, de procedimiento o de formación que han permitido que ocurriera este incidente.
- Haced un listado con todo lo que habéis aprendido y con las actuaciones que vais a poner en marcha para que no vuelva a ocurrir.
- Contrastar vuestras respuestas con la solución del reto.

Y también ...

- Seguro que os habéis planteado que es necesario que haya un **responsable** para resolver estas circunstancias.
- Si aún no lo tenéis, es necesario definir un **plan de respuesta ante incidentes** (el cuestionario puede servir para iniciarse).
- Tendréis que hacer un listado con los **contactos** que puedan ayudaros a resolver incidentes.
- Quizá no tengas implantados, activos o actualizados todos los **mecanismos técnicos** necesarios para evitar que ocurran estos incidentes.
- Tendréis que revisar los **procedimientos** para que no vuelva a suceder.
- La **formación** en ciberseguridad de todos los empleados nunca está de más.

Gracias por vuestra atención

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2005-2015
TRABAJANDO POR LA CONFIANZA DIGITAL