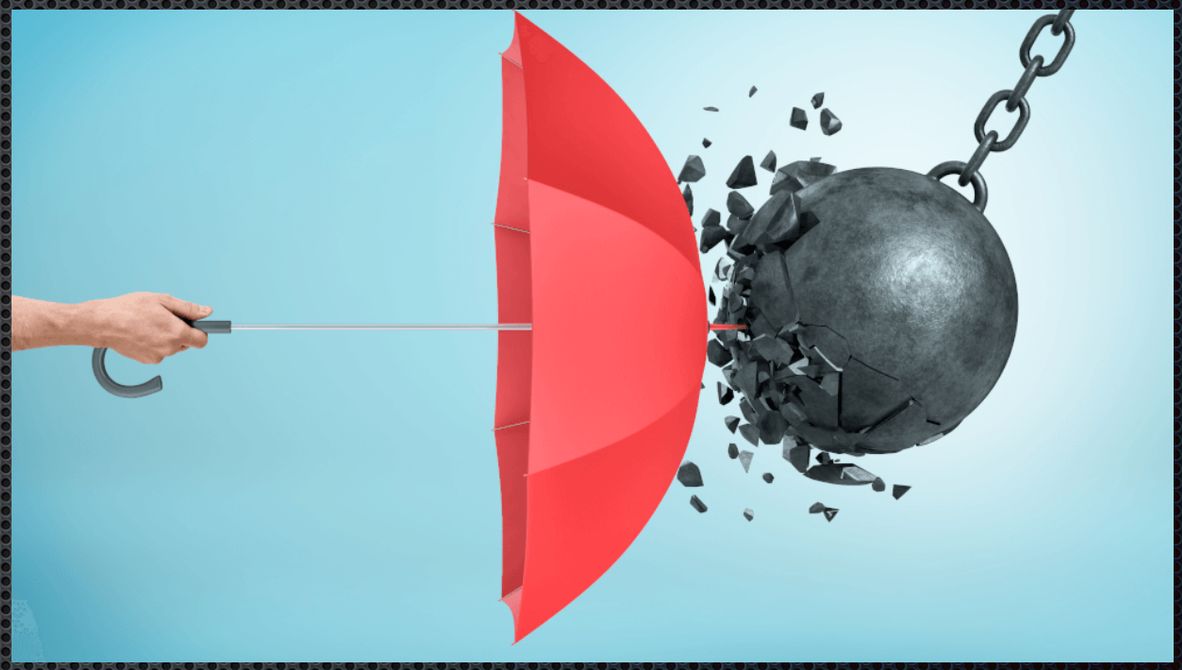
UT4 Implementación de medidas de ciberseguridad

- Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, **eliminar o contener los tipos de incidentes.**
- Implantar capacidades de ciberresiliencia.
- Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados.



- Tareas para reestablecer los servicios afectados por incidentes.
- Documentación
- Seguimiento de incidentes para evitar una situación similar.

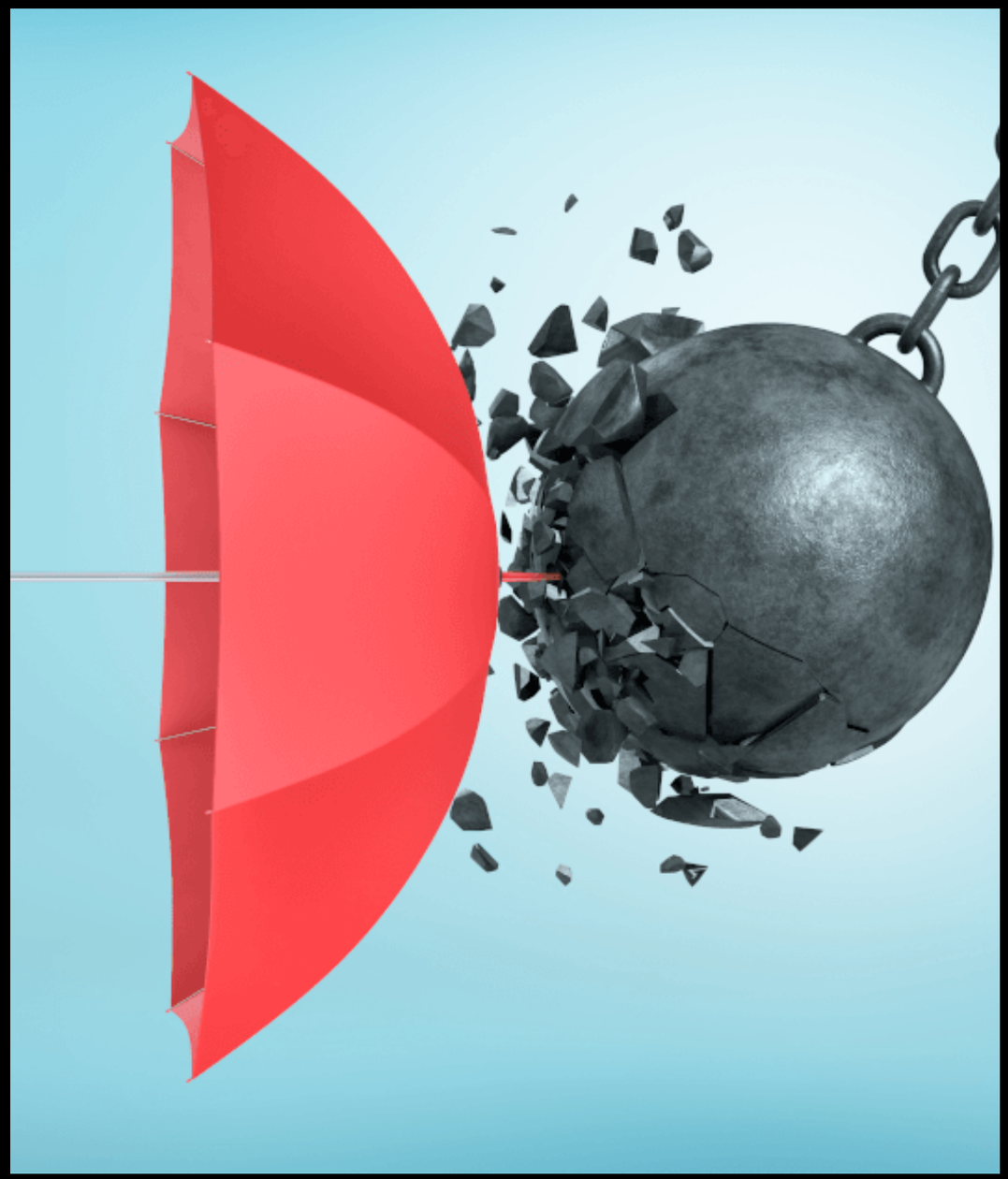
.

Tarea online

- Realizar el test sobre ciberresiliencia para una determinada organización ,elaborar un plan de crisis y un plan de continuidad del negocio:
  - IES Trassierra
  - O bien otra organización (que se conozca)

Ciberesilicencia

- Qué es?
- ¿Cómo se consigue?
- La **ciber-resiliencia** es la capacidad de una empresa de adaptarse y continuar con sus funciones y su trabajo en situaciones de riesgo. Cómo actuar y cómo gestionar la situación de forma eficiente afectando el mínimo posible al desempeño general de la empresa.



Cibersesilicencia

- las capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua, frente a las distintas ciberamenazas.

- El conjunto de dichas capacidades y su operación cuando son necesarias define realmente la disposición de una organización a construir y mantener la ciber-resiliencia.

- Dentro de estas metas, objetivos y técnicas se pueden encontrar capacidades:
  - detectivas y preventivas,
  - de gestión y respuesta,
  - de recuperación y continuidad,
  - de trazabilidad y mejora.

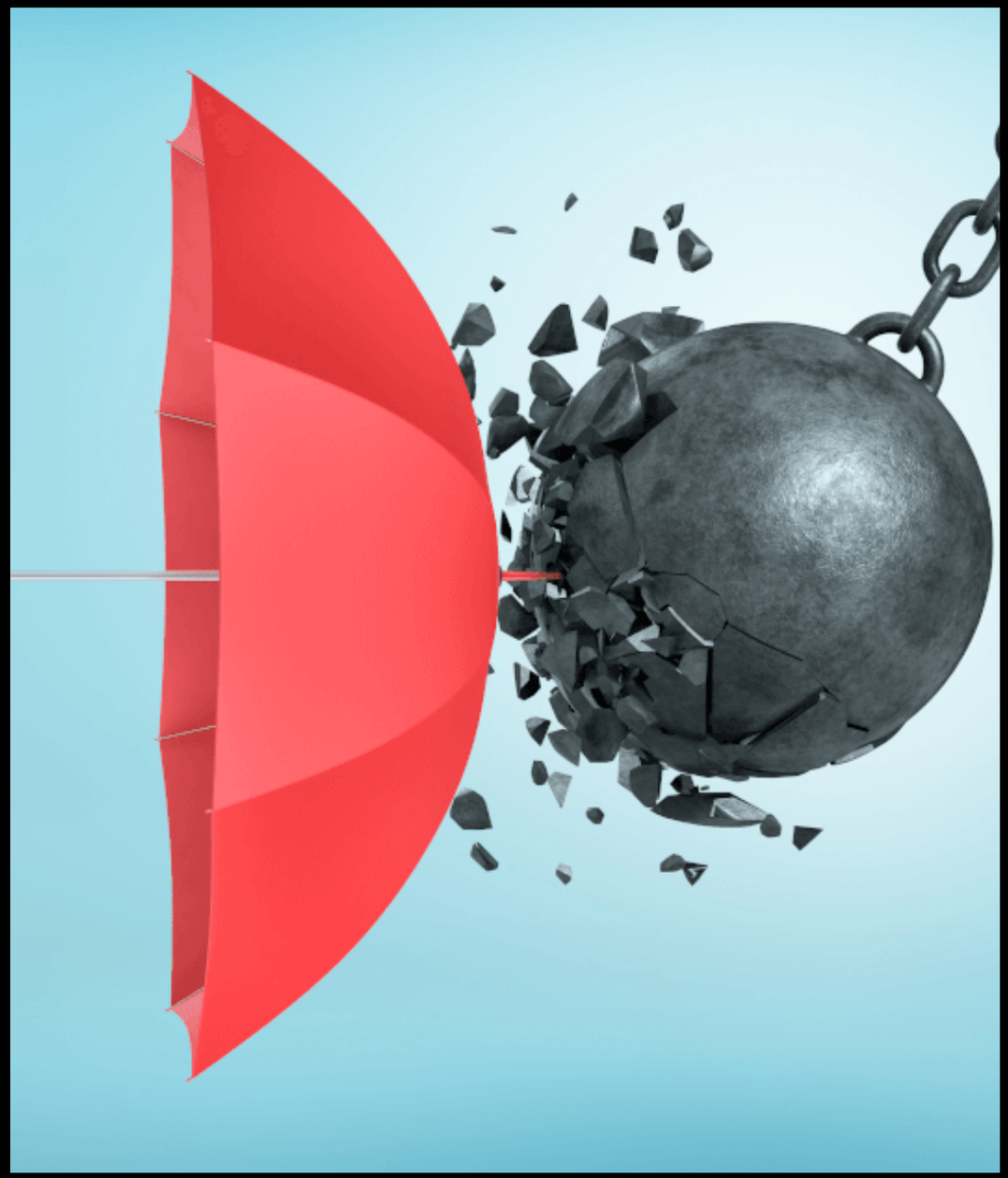
Ciberseguridad

- Existen múltiples tipos de ciberataques:
  - interrumpir los servicios que prestan
  - ataques que explotan las vulnerabilidades de sus sistemas para acceder a información valiosa con fines delictivos
    - Ciberespionaje, poniendo en riesgo los intereses nacionales y la vulneración de la confianza de sus clientes.
- Para conseguir debemos ser capaces de medir,
  - de una manera eficiente, coordinada y metodológica,
  - garantizar que las organizaciones tienen adoptadas unas medidas razonables que garanticen la protección de sus datos, sistemas y equipos.

Cibersesilicencia

Plan de crisis

- En el momento en el que todo falla, hay que tener un plan.
- Improvisar en ese momento es la garantía para el caos y el camino al desastre.
- cómo debe ser éste? La respuesta es: práctico, operativo y real.



Plan de crisis

- Práctico y operativo:
    - Información clara:
        - Terminología, definiciones o listas interminables de responsabilidades, innecesarias
        - Evitar incluir información extra. Por ejemplo: en la gestión de la crisis : dónde están las copias de seguridad, quién las custodia y como obtenerlas.
        - (La política de copias, la descripción del software y hardware, los registros de las copias o los procedimientos de copias de seguridad son importantes, pero no pertenecen al plan de crisis) .

Plan de crisis

- Real: describir el flujo de decisiones, los roles de cada persona, los comités, las vías de comunicación o los tiempos de respuesta, han de ser ajustados a la realidad.

- Por ejemplo: la activación del centro de respaldo sea decidida el responsable del departamento de informática.

    - (no debemos establecer que en caso de desastre se creará un comité donde esté el director general, personal de recursos humanos, el director financiero y el responsable de informática, porque eso introducirá confusión)

- A medida que se vayan introduciendo cambios organizativos, deberemos actualizar el plan de crisis para que se adapte a la realidad de la empresa.

Plan de crisis: Contenido.

- Información general sobre los sistemas y los elementos más críticos:
    - Las copias de seguridad, el acceso a las salas de servidores, la localización de las contraseñas, personal autorizado para el acceso fuera de horario, turnos, etc.
- Información sobre el personal potencialmente implicado en una situación de crisis, con sus datos de contacto:
    - Figurar aquellas personas con responsabilidad y capacidad de decisión para la activación de la contingencia, además del personal técnico que pudiera estar implicado.
- Si nuestra organización es compleja: Proceso de escalado, en caso de que no sea posible localizar a parte del personal.
- Información de emergencias: Aunque dispongamos de un plan de emergencias: teléfono de los servicios públicos necesarios en una posible contingencia: bomberos, policía, hospitales cercanos, etc.

Plan de crisis: Pasos a seguir.

- Es el núcleo del documento: listado de los pasos a seguir en la situación de crisis.
    - Cada paso debe contener la información básica y quién debe ejecutar el paso.
- Por ejemplo, tras la detección de una potencial contingencia: “Notificación al Responsable de Informática por parte del personal de guardia:Consultar su teléfono en el apartado X.X de este documento”
- Evitando fórmulas complejas, excesivamente burocráticas o que no sean operativas.
- ¿Qué pasos incluir en un plan de crisis? depende de la organización, al menos estos grandes bloques:
    - Detección y evaluación de la incidencia o contingencia.
    - Notificación, escalado y toma de decisiones.
    - Activación de la crisis.
    - Comienzo y finalización de las tareas de recuperación.
    - Restablecimiento del servicio a un estado que nuestra organización considere aceptable.

Escenarios de desastre

- Listado de los diferentes escenarios de desastre que consideremos que podemos sufrir, (no debemos considerar una incidencia poco crítica como un desastre)

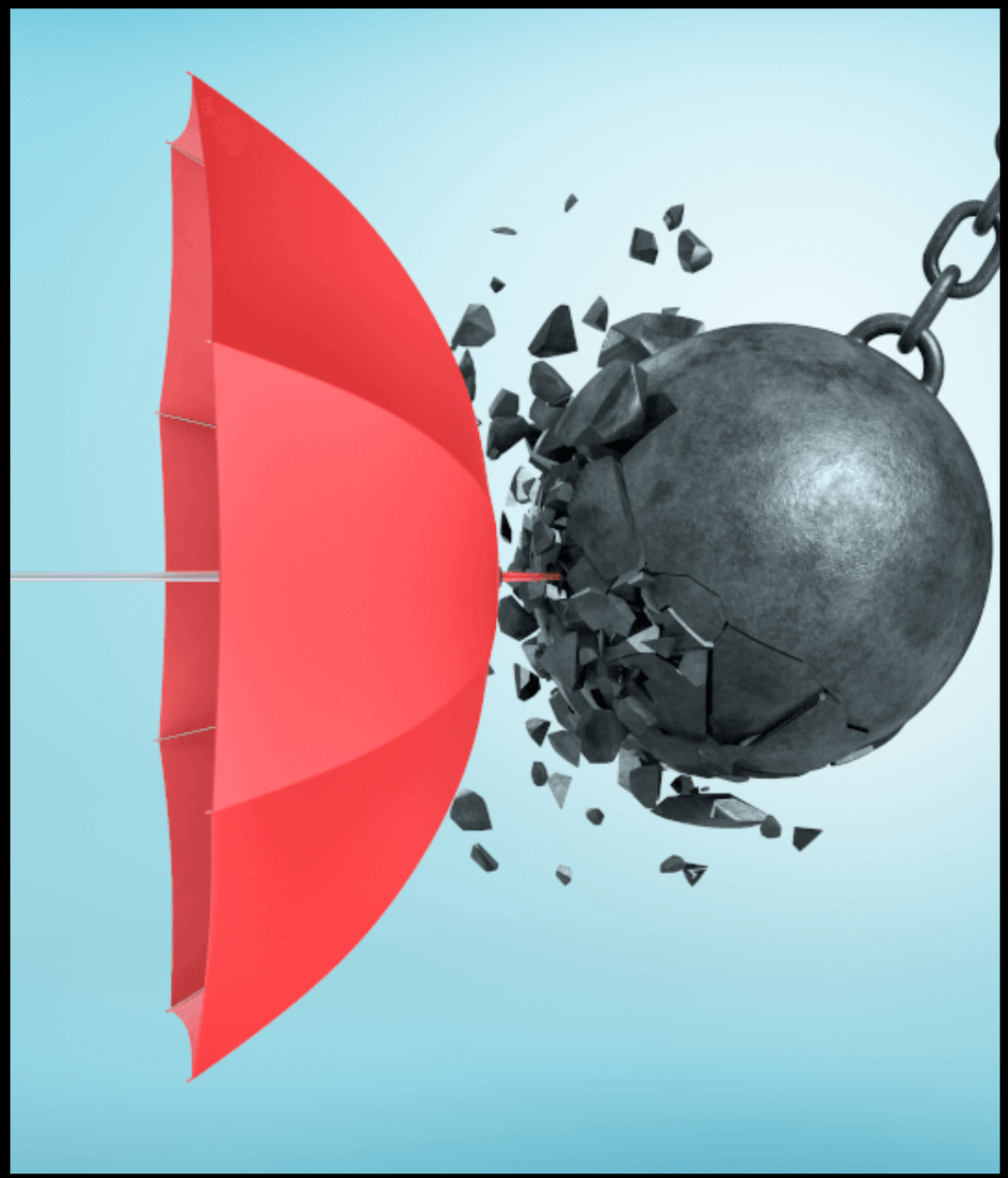
- Debemos tener en cuenta diferentes factores: coste (temporal, técnico, económico, etc.) de las medidas de contingencia, complejidad de la marcha atrás, experiencia con el procedimiento de recuperación, etc.

- La información de cada escenario debe ser la siguiente:
  - Descripción del escenario. Ej: caída de la cabina de discos central.
  - Condiciones y tiempos de disparo: bajo qué condiciones y cuánto tiempo estimamos necesario esperar antes de comenzar con las tareas de recuperación del servicio.
  - Sistemas o servicios afectados por la contingencia.
  - Personal técnico relevante.
  - Proveedores relevantes para el escenario de desastre.
  - Plan (o planes) de Recuperación asociado(s) al escenario de desastre.

Puesta en práctica

- utilización ser sencilla y casi inmediata: simplemente habrá que seguir los pasos que hemos establecido.
- El plan de crisis estará desarrollado para adaptarse al siguiente flujo:
    - Detectamos una incidencia determinando si se encuentra entre los posibles escenarios de desastres que hemos definido con anterioridad.
    - Escalamos la incidencia y notificamos al personal relevante.
    - Analizamos detenidamente la incidencia junto con el personal relevante y se decide finalmente si se trata de un escenario de desastre o no.
    - Revisamos todos los escenarios de desastre que hayamos definido en el Plan de Crisis y escogemos los que apliquen, según su descripción, las condiciones de activación y los entornos afectados.
    - Una vez ha transcurrido el tiempo de disparo, si la situación no se ha restablecido, comenzamos con la ejecución de los Planes de Recuperación asociados. En este punto comienza a trabajar el personal técnico.
    - Seguimos el proceso hasta que se alcance una situación estable.
- Al poner en marcha el plan de crisis, puede encontremos que no hemos considerado determinadas condiciones o incluso escenarios de desastre, que hay algunos errores y omisiones, o que los tiempos de activación son demasiado cortos o largos.
- Parte de estos problemas se solucionan manteniendo el plan de crisis actualizado y probándolo regularmente

Procedimientos de actuación



Restablecimiento del servicio