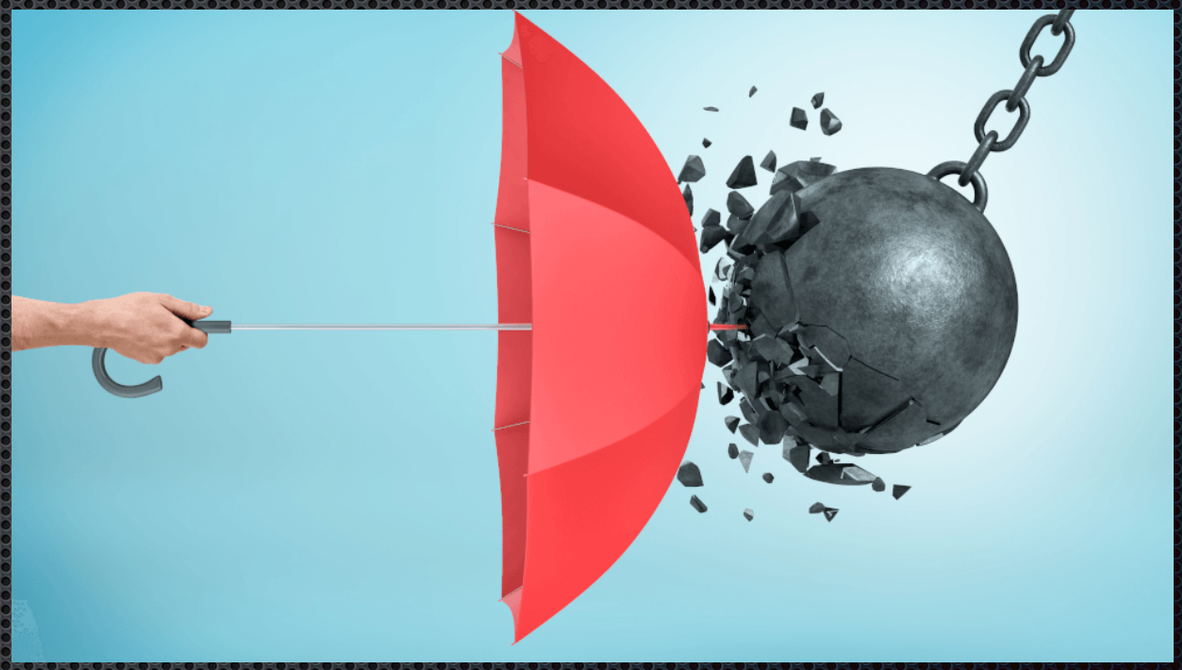
UT4 Implementación de medidas de ciberseguridad

- 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.

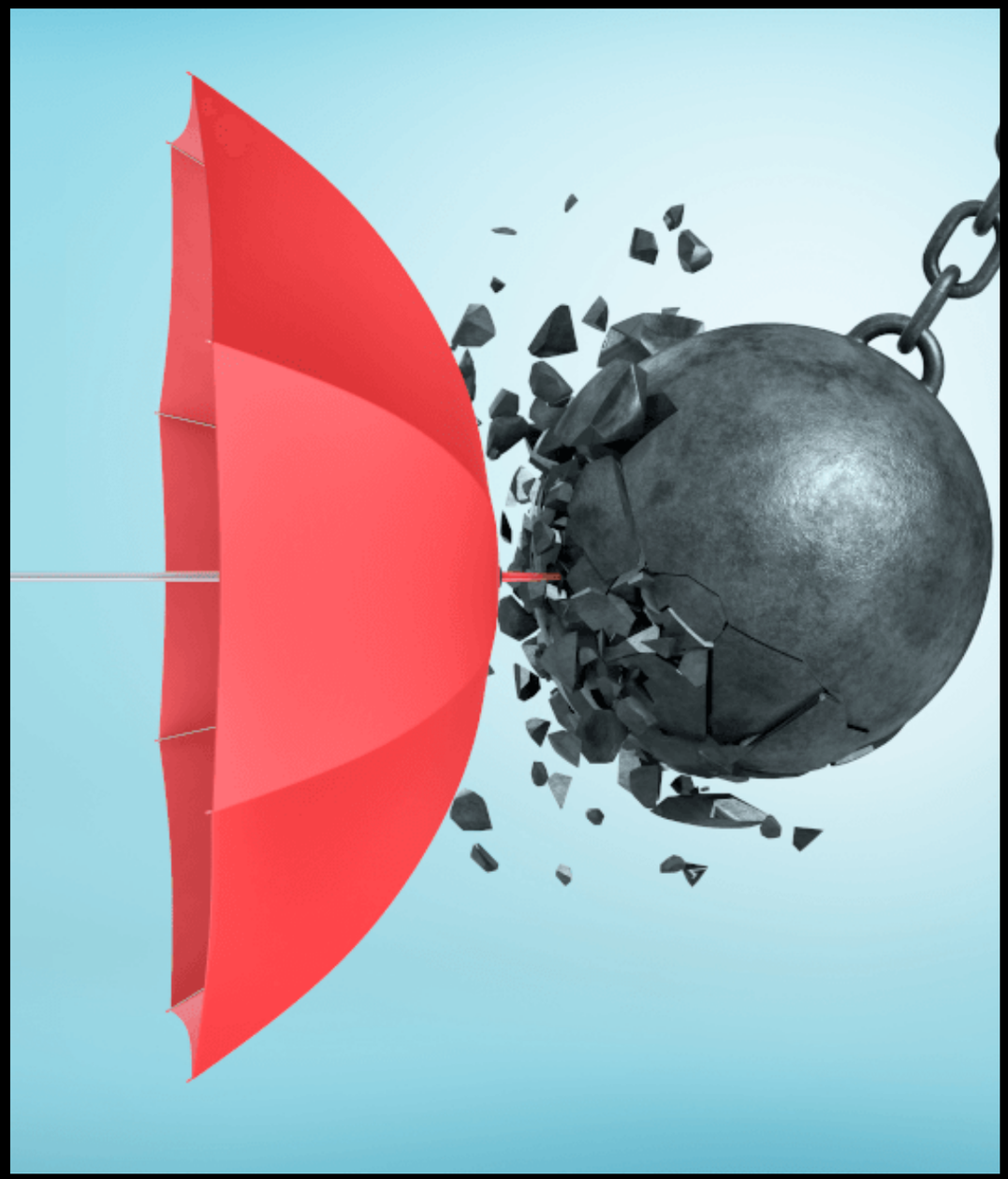
.

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.

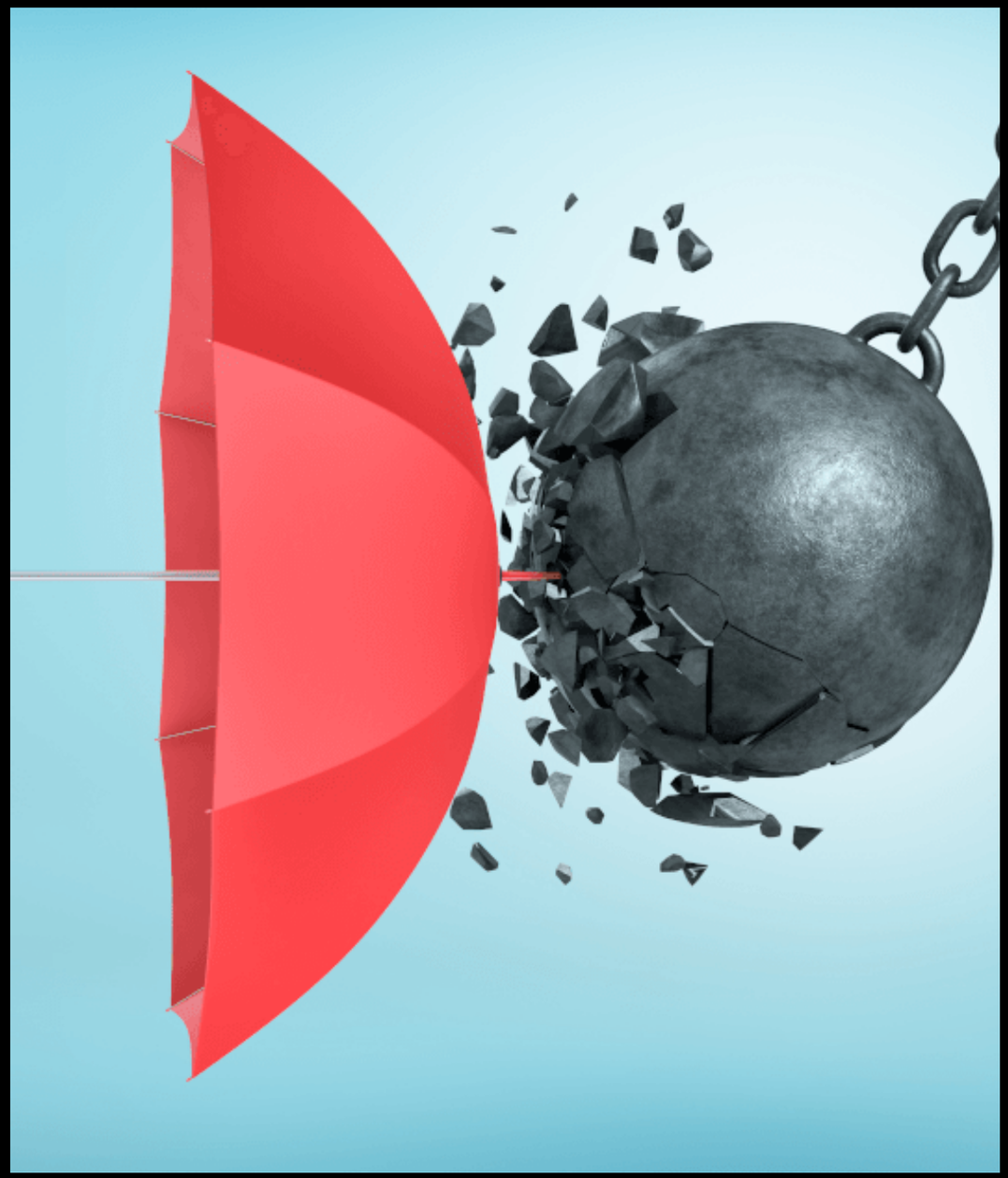
Ciberseguridad

- 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.

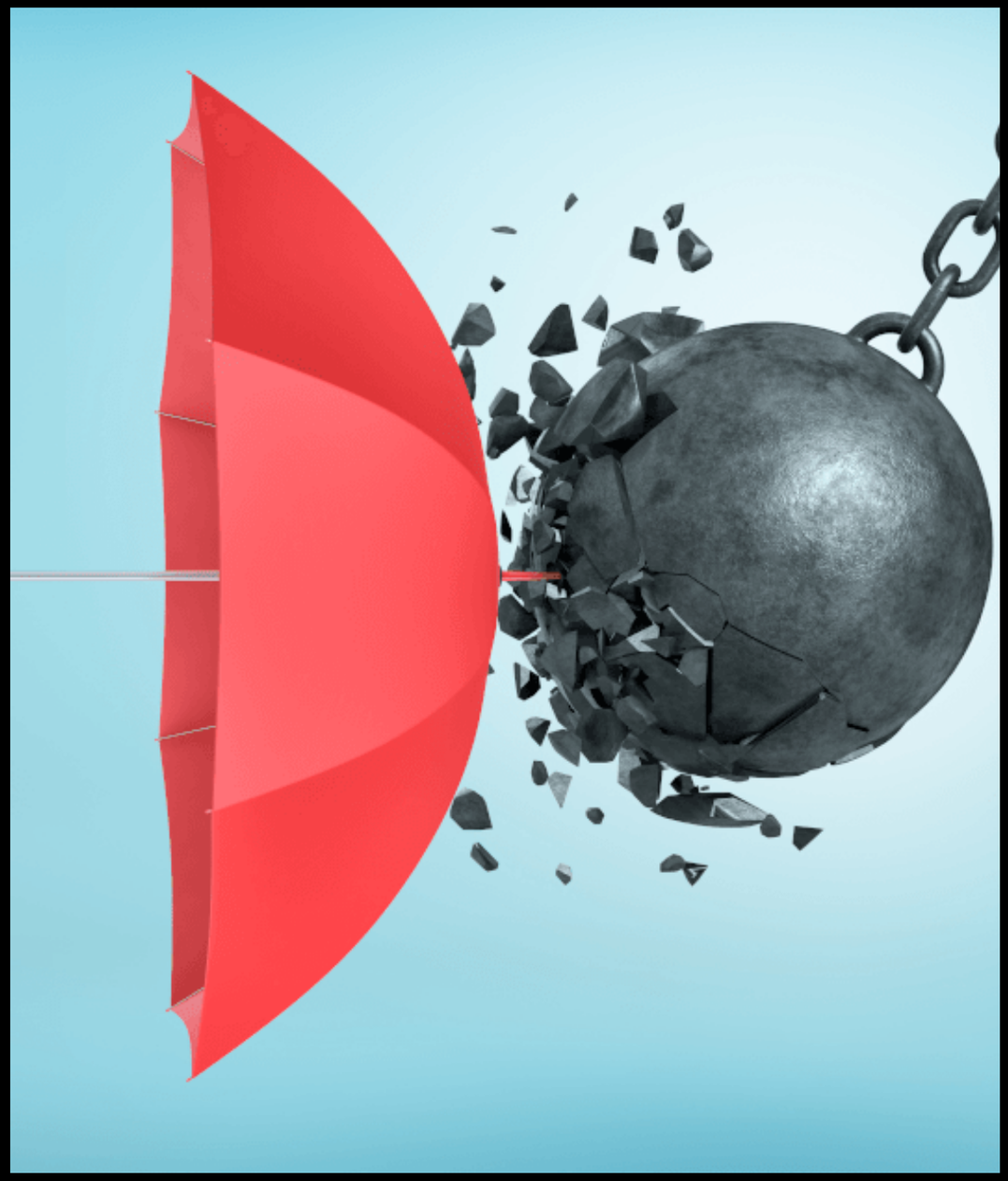
- La información de cada escenario debe ser la siguiente:
  - Descripción del escenario. Ej: caída de la cabina de discos central.
  - Condiciones y tiempos de disparo: bajo qué condiciones y cuánto tiempo estimamos necesario esperar antes de comenzar con las tareas de recuperación del servicio.
  - 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

- ¡ a pesar de las medidas que implantemos, siempre existe el riesgo de que ocurra un incidente de ciberseguridad.
- Preparar un plan de acción que nos indique cómo actuar de la manera más eficaz posible en estos casos.
-



Procedimiento actuación

- Para ejecutar correctamente el plan y evitar que el daño se extienda se deben detallar las acciones a realizar en cada momento, la lista de las personas involucradas y sus responsabilidades, los canales de comunicación oportunos, etc.

- Tras un incidente, si hemos aplicado el plan, tendremos una valiosa información para conocer y valorar los riesgos existentes, y así evitar incidentes similares en el futuro.

- En caso de que ocurran incidentes graves o desastres que paralicen nuestra actividad principal, aplicaremos el plan de contingencia y continuidad del negocio.

-

Procedimientos de actuación

- Todos los miembros de la organización conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información.

- Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la empresa.

- También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

-

Procedimientos de actuación

- Controles para revisar el cumplimiento de la política de seguridad en lo relativo a la respuesta a incidentes de ciberseguridad.

- Los controles se clasificarán en dos niveles de complejidad:

  - Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

  - Avanzado (A): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Procedimientos de actuación

- Los controles podrán tener el siguiente alcance:
  - Procesos (PRO): aplica a la dirección o al personal de gestión.
  - Tecnología (TEC): aplica al personal técnico especializado.
  - Personas (PER): aplica a todo el personal.

Procedimientos de actuación

NIVEL	ALCANCE	CONTROL	
B	PRO	**Equipo responsable** Seleccionas el equipo que se encargará de gestionar los incidentes de ciberseguridad.	☐
B	PRO	**Mejora continua** Usas la información recogida en la gestión de los incidentes para adoptar mejoras en tus sistemas.	☐
B	PRO	**Caducidad del plan de gestión** Revisas cada _____ el plan de gestión y respuesta ante incidentes de ciberseguridad.	☐
B	TEC	**Detección del incidente** Concretas las situaciones que deben ser catalogadas como incidentes de ciberseguridad.	☐
B	TEC	**Evaluación del incidente** Categorizas convenientemente el incidente y le otorgas la criticidad correspondiente.	☐
B	TEC	**Notificación del incidente** Estableces correctamente la manera de notificar un incidente.	☐
A	TEC	**Resolución de incidentes** Desarrollas procedimientos detallados de actuación para dar respuesta a cada tipología de incidente de ciberseguridad.	☐
B	TEC	**Tratamiento del registro del incidente** Registras de forma conveniente toda la información relativa a la gestión del incidente.	☐
B	PRO	**Cumplimiento del RGPD** Tienes prevista la notificación de incidentes según el RGPD en caso de brechas de seguridad que afecten a datos de carácter personal	☐

Puntos clave

- Equipo responsable. Para garantizar una respuesta eficaz durante el tratamiento de incidentes de ciberseguridad, nombraremos un equipo responsable de su gestión. Tendremos que considerar no solo al personal técnico encargado de su resolución (interno o externo), sino también personal de la dirección que debiera estar informado en todo momento del estado del incidente.

- Mejora continua. Es conveniente analizar la utilidad de usar la información recogida en la gestión de los incidentes para medir y evaluar la posibilidad de modificar procedimientos o añadir nuevas mejoras o controles para limitar futuros daños. Podemos realizar acciones preventivas con el fin de entrenar a la plantilla ante la aparición de un posible incidente .

- Caducidad del plan de gestión. Determinaremos la periodicidad con la qué debe actualizar el plan y las medidas a adoptar. También puede ser necesaria una actualización del plan tras un cambio significativo en nuestros sistemas.

-

Puntos clave

- Detección del incidente. Debemos concretar las situaciones que se considerarán incidentes. Desplegaremos herramientas con mecanismos de detección automáticos y estableceremos un sistema de alerta que nos informe detalladamente de lo sucedido en tiempo real.

- Evaluación del incidente. Una vez detectado el incidente debemos categorizarlo convenientemente y establecer la gravedad y la prioridad en su tratamiento.

- Notificación del incidente. Procuraremos establecer un punto de contacto únicodonde los empleados deben notificar los posibles incidentes o puntos débiles detectados. Asimismo, se debe indicar la información a recabar y las acciones inmediatas a seguir en el momento de la notificación. Conviene tener un listado de contactos para actuar con rapidez en caso de incidente.

Puntos clave

- Resolución de incidentes. Desarrollaremos y documentaremos procedimientos de respuesta para cada uno de los tipos de incidentes definidos previamente, poniendo especial énfasis en aquellos incidentes más habituales y peligrosos . Se detallarán al menos los procedimientos para las siguientes acciones:

    - recogida de evidencias tan pronto como sea posible tras la aparición del incidente, con cuidado de mantener la cadena de custodia, la integridad de las evidencias (cifrándolas si es necesario), soportes, etc.;

    - Tratamiento del registro del incidente. Para disponer de toda la información acerca del incidente se registrarán convenientemente.

    - Cumplimiento del RGPD: El RGPD obliga a notificar las violaciones de datos de carácter personal que podamos sufrir en la empresa a la autoridad de protección de datos competente y a las personas afectadas, salvo que sea improbable que suponga un riesgo para los derechos y libertades de los afectados.

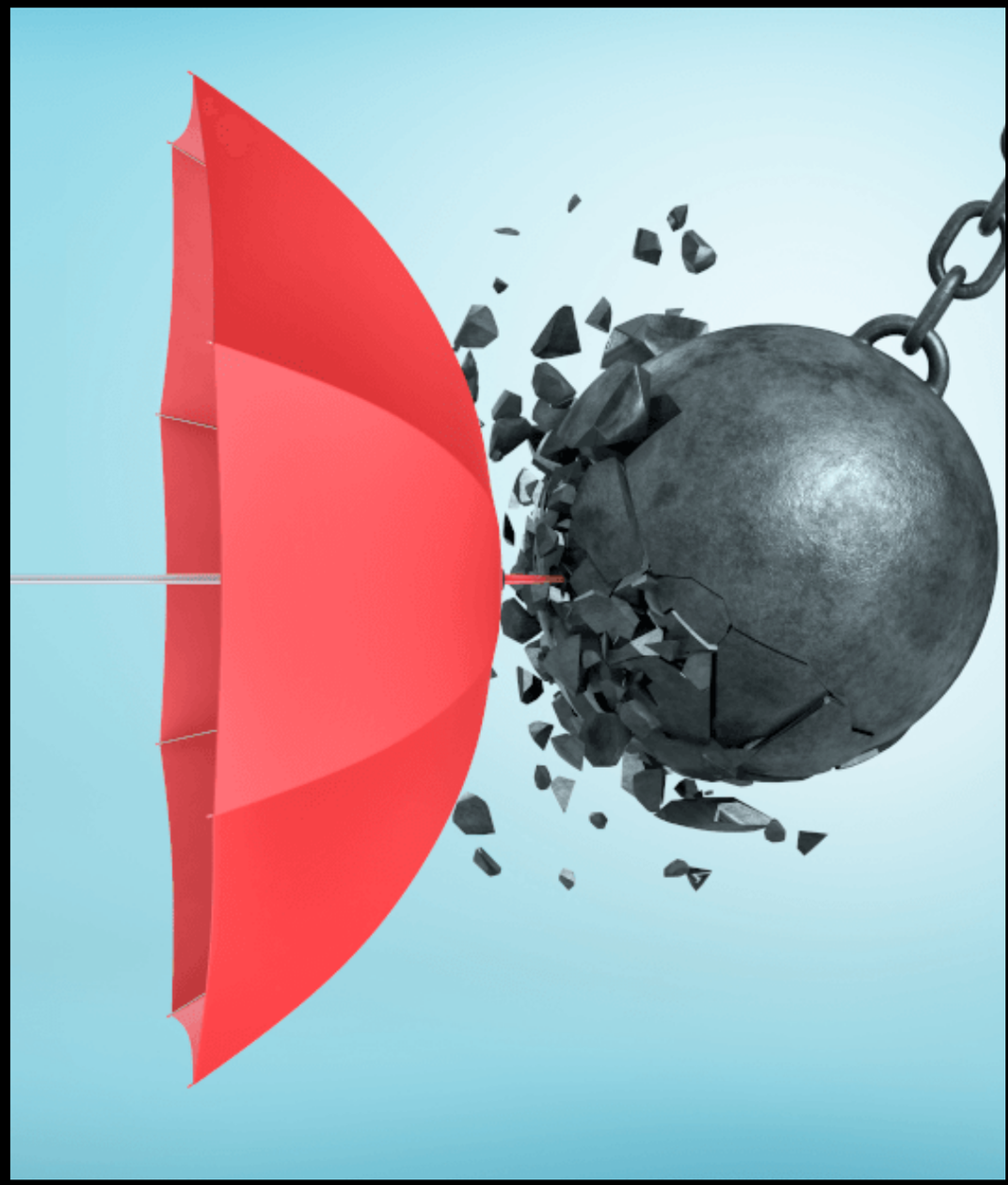
-

Restablecimiento del servicio

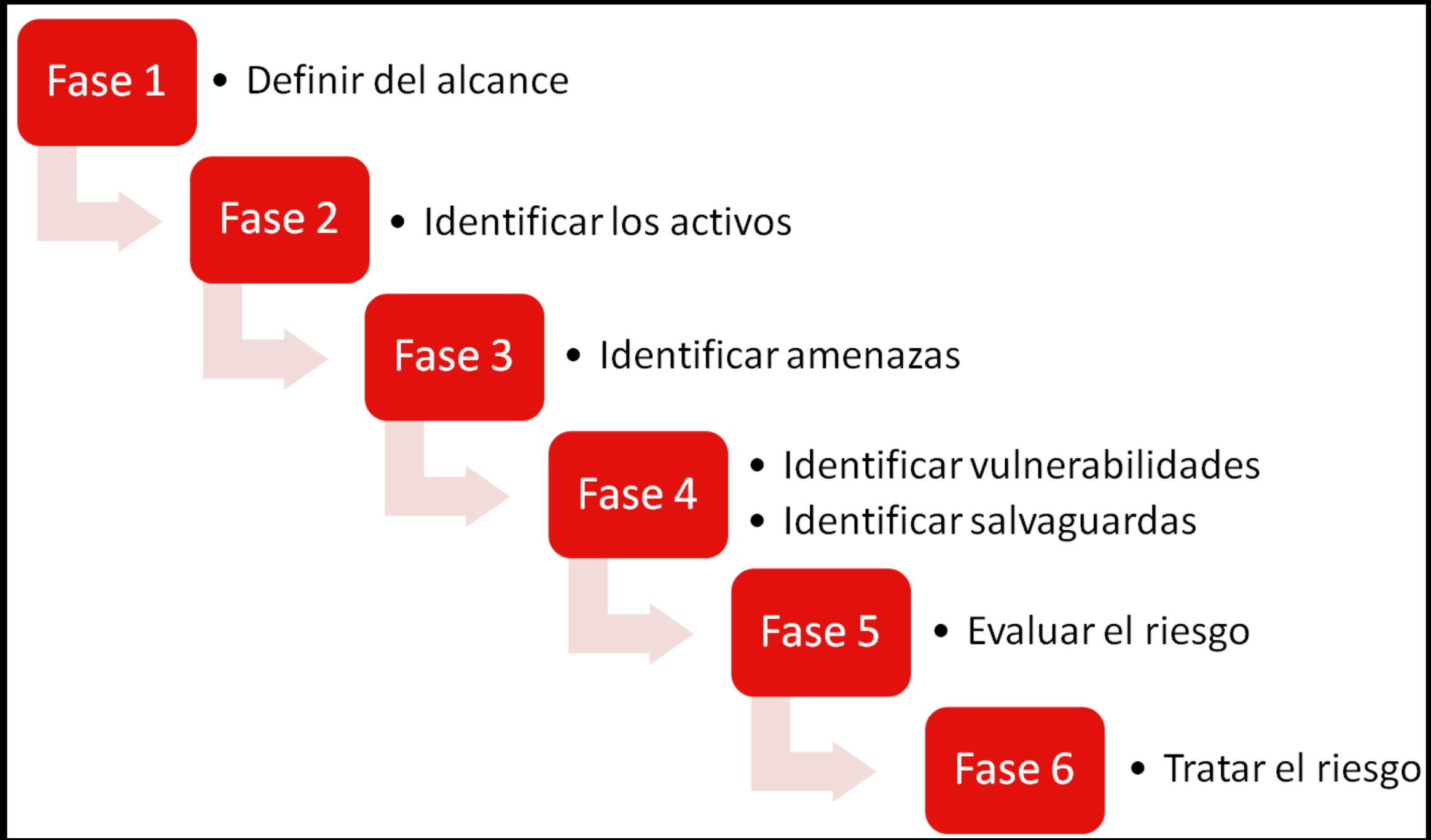
- Una propuesta para elaborar un Plan de Recuperación ante Desastres debería constar de las siguientes fases:

- Alinearlo con el plan de continuidad de negocio. Así se concentran los esfuerzos en los sistemas o aplicaciones que se consideran críticos para el negocio. Para unas empresas pueden ser los sistemas de producción y para otras, la página web o el CRM.

- Realizar una evaluación de riesgos. De este modo tendremos una visión detallada de las amenazas que pueden afectar a nuestra organización, y en particular a los sistemas o aplicaciones críticas, causando un desastre que ponga en riesgo la continuidad de negocio.



Restablecimiento del servicio



BIA

- Llevar a cabo un análisis de impacto de negocio. También conocido como BIA, por sus siglas en inglés Business Impact Analysis, tiene como principal objetivo identificar las necesidades de la organización en términos de recuperación, sobre todo en aquellos servicios que consideramos imprescindibles para el funcionamiento de la empresa.
-

BIA

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

Tiempos

- Un aspecto importante a tener en cuenta en la elaboración de un BIA son los tiempos. En este sentido, cobran especial importancia los siguientes:

- RTO (Recovery Time Objective): Tiempo de recuperación de las actividades que hemos identificado bajo unas condiciones mínimas aceptables. Por ejemplo, supongamos que el Responsable del Departamento de Administración nos indica que, en caso de que fallara la plataforma que soporta las aplicaciones para la generación y emisión de la nómina, se deberían recuperar el servicio en un plazo máximo de 24h. En este caso, estableceríamos que el RTO asociado a dicho proceso es de 24h.

- MTD (Maximum Tolerable Downtime): Tiempo máximo tolerable de caída el cual nos determina el tiempo que puede estar caído un proceso antes de que se produzcan efectos desastrosos en la compañía y repercuta en el negocio. Volviendo al caso anterior, supongamos que el proceso de gestión de nóminas no debe estar interrumpido por un periodo superior a 48h. En este caso, estableceríamos que el MTD asociado a dicho proceso es de 48h.

- RPO (Recovery Point Objective): El grado de dependencia de la actualidad de los datos determina la cantidad máxima de información que se podría perder sin llegar a tener consecuencias inaceptables, formando parte de las políticas de respaldo definidas por la organización. En este sentido, imaginemos que el Responsable del Departamento de Administración nos indica que podrían tolerar una pérdida de información siempre y cuando no se perdieran los datos generados en más de un día completo. Por lo tanto, estableceríamos que el RPO es de 24h.

BIA

- mo ejemplo de los tiempos de recuperación en un BIA, podemos observar en la siguiente tabla su implicación dependiendo del proceso de negocio, en este caso dentro del departamento de Administración:

Proceso de negocio	RTO	RPO	MTD	Criticidad
Gestión de nóminas	*24 horas*	*24 horas*	*48 horas*	*Alto*
Solicitud de viaje	*1 semana*	*24 horas*	*48 horas*	*Medio*
Validación de vacaciones	*1 semana*	*24 horas*	*48 horas*	*Bajo*

- En la tabla anterior, el proceso de Gestión de nóminas nos viene a decir que posee una criticidad alta, proyectándose en el periodo de final de mes, para el pago de las nóminas a los empleados.

- Determinamos un RTO de 24 horas como tiempo de recuperación para restablecer el servicio, y un RPO de 24 horas como tiempo de la posible pérdida de la información debido a la caída del servicio.

- Por último un MTD de 48 horas como tiempo máximo de parada del servicio sin superarlo ya que conllevaría graves riesgos a la organización.

BIA

- l BIA es una de las partes fundamentales en el plan de continuidad de negocio.
- La información que obtenida en la elaboración del BIA se validará con los distintos departamentos involucrados. Adicionalmente, contrastaremos los requisitos de recuperación con la capacidad de recuperación de los sistemas que intervienen en la prestación de servicios. En última instancia, presentaremos las conclusiones a la Dirección para hacerlos partícipes y así obtener su respaldo de cara a afrontar nuevos proyectos para mejorar la capacidad de recuperación actual.
-

BIA

- Se delimitan los procesos o actividades críticas dentro de la organización que afectan a nuestro negocio pudiendo descubrir actividades críticas que a priori no lo parecían.
- Permite identificar vulnerabilidades de una organización en materia de continuidad de negocio.
- En caso de disponer de planes de recuperación permitirá verificar si estos cubren las necesidades del negocio.
- Propicia la implicación de un mayor número de áreas de la organización a la hora de implantar planes de continuidad, no solo al personal responsable de llevar a término este tipo de proyectos.
- Reducción de costes ante posibles interrupciones del negocio.
- Aporta información de gran valor a la hora de priorizar el desarrollo de otros proyectos en materia de continuidad de negocio.
- Un mayor conocimiento de los procesos de negocio, contribuirá favorablemente a la mejora de la competitividad y seguridad en el mercado.
- La información obtenida en el desarrollo del BIA es una base fundamental para implantar estrategias de recuperación eficientes.

BIA: Objetivos

- Desarrollar las medidas para recuperación para los servicios y aplicaciones prioritarios, de manera que se puedan poner en práctica los mecanismos para volver a la operación normal lo antes posible.

- Realizar pruebas. Debemos asegurar el correcto funcionamiento de nuestro plan de recuperación y probar que las medidas que hemos considerado necesarias realmente son las adecuadas para recuperar nuestros sistemas. Por lo tanto, debemos programar pruebas periódicas (desde revisar una lista de verificación o parar completamente los sistemas para verificar que podemos recuperarlos, o transferirlos a sistemas alternativos) que nos confirmen la continuidad en caso de desastre.

- Actualizar y mejorar el plan. Las pruebas de las que hablamos en el punto anterior pueden servirnos para ver tanto los puntos fuertes como los puntos débiles de nuestro plan. Así podremos mejorar todo lo que no funcione como se esperaba y mantener el plan en una mejora continua. Además, las amenazas evolucionan constantemente por lo que debemos asegurarnos de que nuestro plan no se queda desactualizado.

- Capacitar a los encargados de ponerlo en marcha, concienciar y difundir el plan. Por último, debemos encargarnos de que todas las partes implicadas en el plan conozcan al detalle su función en el mismo así como designar a los encargados de llevarlo a cabo en caso de que sea necesario.