ANALISIS DE IMPACTO

- Para asegurar la continuidad del negocio, hay que asegurar en todas sus dimensiones el sistema de información, empleando un criterio de evaluación de riesgos, con una etapa de análisis, y una etapa de gestión de riesgos.

- Para asegurar la continuidad del negocio, el punto de partida recomendado es un análisis de impacto del negocio (o BIA a partir de sus iniciales en inglés, *Business Impact Analysis)*. En el BIA se estudian **los procesos o funciones vitales del negocio, que dependan en cualquier medida de los sistemas de información**

- Resiliencia:
- Capacidad de los sistemas para seguir operando pese a estar sometidos a un ciberataque, aunque sea en un estado degradado o debilitado. Así mismo, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un ataque.

PASOS

- 1. Recopilación de información
- 2. Identificación de las funciones y los procesos
- 3. Evaluación de impactos operacionales
- 4. Establecimiento de los tiempos de recuperación
- 5. Optimización de los recursos
- 6. Enumeración de procesos alternativos
- 7. Generación de un Informe de Impacto de Negocio

1. Recopilación de información
Técnicas

- Formularios.
- Entrevistas a los usuarios avanzados o dueños de los procesos.
- Reuniones entre personal de TIC y los usuarios avanzados.

Formularios

- En todos los casos, la información recogida debe permitir evaluar los siguientes resultados del BIA:
- Cuáles son los procesos críticos, u ordenarlos por prioridad.
- Cuál es el daño/impacto, en función del tiempo que se tarde en restablecerse el servicio.
- Cuál es el coste de las diferentes estrategias de recuperación, que proporcionarán un tiempo y un punto objetivo de recuperación.

Formularios

Entrevistas a usuarios clave

- Una entrevista resulta adecuada **cuando no haya certeza de que las preguntas previstas identifiquen todos los aspectos de valoración de la importancia de un proceso: las entrevistas dan cabida a recoger información bajo criterios desconocidos a priori.**

Reuniones entre personal de TIC y usuarios clave

- informáticos: back up
- información, ¿al día? ¿consistente?
- sw: programas y configuraciones
- tradicionales: papel
- personal técnico y directivo
- ¿dónde se sienta? ¿cómo habla?
- Procedimientos
- Pruebas regulares y mantenimiento

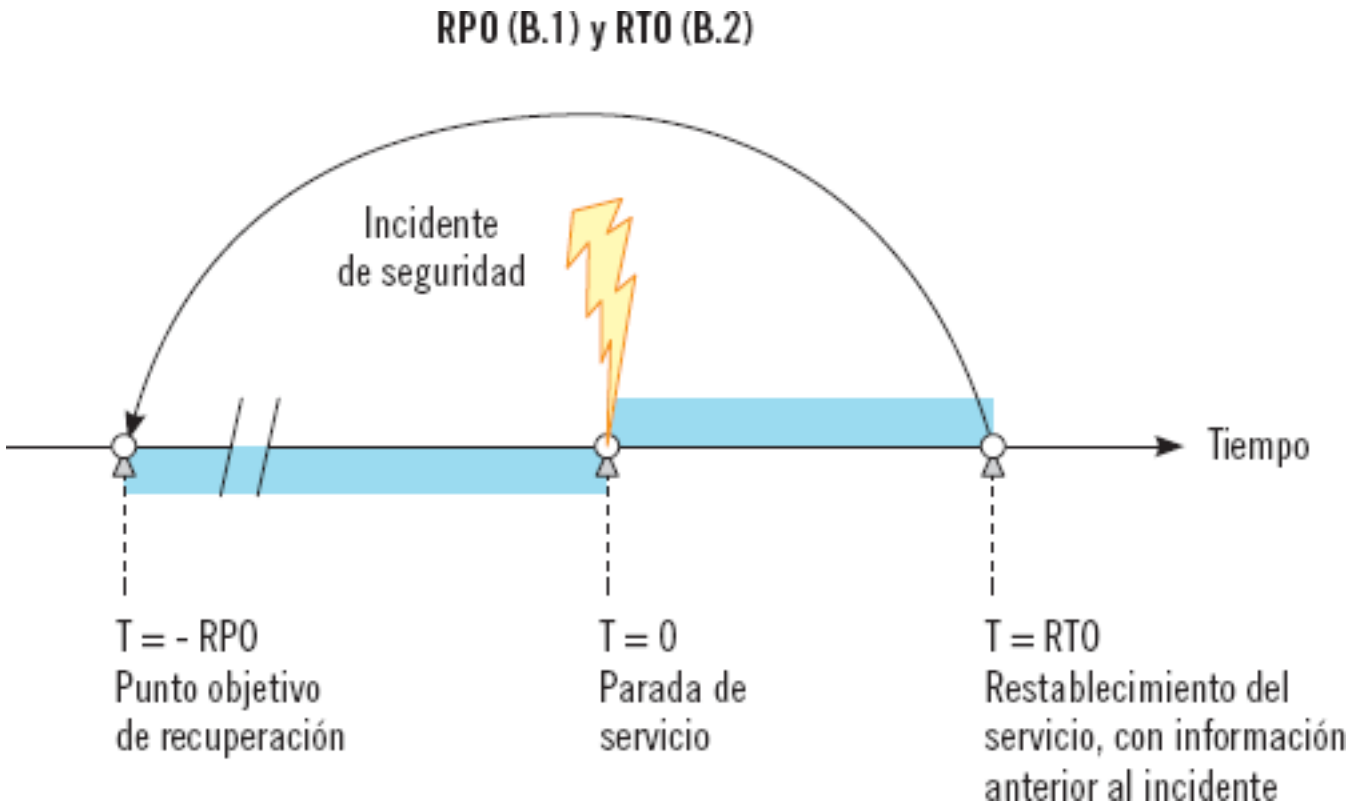
2. Identificación de las funciones y los procesos
Identificación de procesos de negocio soportados por sistemas de información

- BIA es **el estudio de las consecuencias que tendría en el negocio en una parada de sus procesos vitales por un determinado tiempo: qué hay que recuperar, cuánto cuesta hacerlo, y cómo hay que recuperarlo.**

- El BIA es una herramienta para elaborar el plan de continuidad de la empresa (o BCP, por las iniciales de *Business Continuity Plan).*
- Frecuentemente, el BCP incluirá un plan para la recuperación de desastres (o DRP, por las iniciales de *Disaster Recovery Plan).*
- Dentro de una empresa, la realización de un BCP debe incluir no solo los aspectos de la información, sino todas las facetas que se necesitan para la actividad de la empresa (instalaciones, contratos, seguros, financiación, clientes, *stock* de productos, etc.).

Análisis de impacto en el negocio (Business Impact Analysis-BIA):

4. Establecimiento de los tiempos de recuperación



- RPO es el objetivo de punto de recuperación, y representa el último instante de tiempo previo al incidente al que los sistemas son capaces de regresar. Vendrá dado. por ejemplo, por la frecuencia con que se realicen copias de seguridad.

- RTO es el objetivo de tiempo de recuperación, y representa el tiempo que se tarda en restablecer el servicio, al menos a los niveles mínimos acordados.

- MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.
- • RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.
- • RPO (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.
- • WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

- El objetivo del BIA es ordenar los procesos en función de su criticidad, valorar el daño de una interrupción, y ayudar a determinar si una estrategia de recuperación es adecuada.

- La valoración puede hacerse de manera cuantitativa, por ejemplo con las pérdidas económicas (€) generadas por la parada; o en términos cualitativos mediante niveles tipo bajo, medio o alto. El criterio debe mantenerse ,para que futuras revisiones del BIA sean coherentes.

- Por ejemplo, puede emplearse una estimación sencilla como:
- Impacto RPO (B.1) = Impacto RTO (B.2) =
- Número de apariciones de “desastre” × 10 +
- Número de apariciones de “grave” × 5 +
- Número de apariciones de “medio” × 2 +
- Número de apariciones de “bajo” × 1

Criticidad = valor función (A.2) × impacto RPO (B.1) × impacto RTO (B.2)

5. Optimización de los recursos

Valoración de los requerimientos de confidencialidad, integridad, y disponibilidad de los procesos de negocio

- La fiabilidad o seguridad, se apoya en tres aspectos o **principios de seguridad** esenciales:
- **La confidencialidad,** es decir, que la información solo esté accesible para quien esté autorizado a ello.
- **La integridad,** es decir, que la información sea exacta y completa, de manera que solo pueda modificarla quien esté autorizado a ello.
- **La disponibilidad,** es decir, que la información esté accesible cuando sea necesario.

6. Enumeración de procesos

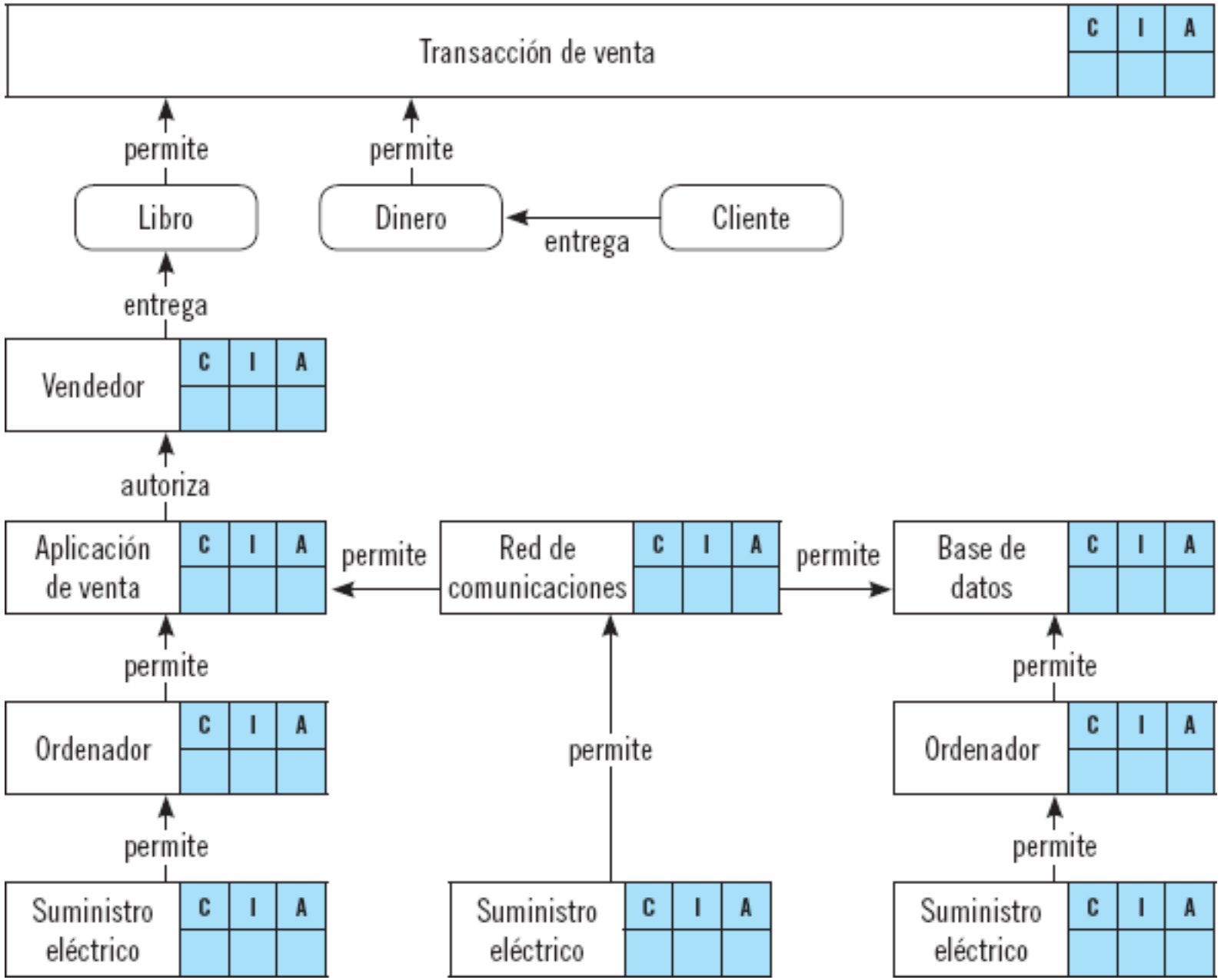
- proceso de negocio representa al conjunto de trabajos que se realizan para generar un producto o servicio

CATEGORIAS DE IMPACTO	EJEMPLOS DE IMPACTOS
Financiero	Pérdidas causadas por multas, sanciones, pérdida de beneficios o reducción de la cuota de mercado
Reputacional	Opiniones negativas o daño a la imagen de marca
Legal y regulatorio	Responsabilidades judiciales y retirada de licencias comerciales
Contractual	Incumplimiento de contratos o de obligaciones entre organizaciones
Objetivos de negocio	Incumplimiento de los objetivos o imposibilidad para sacar partido de las oportunidades
Operativo	Extensión y duración de la disrupción en el flujo de las operaciones de negocio

Valoración de los procesos a partir de sus componentes

- un proceso puede observarse como **la combinación de unas personas, una información de entrada, y unos sistemas de procesamiento para generar una información de salida**

Ejemplo de posibles componentes en la función de venta de una librería



Herramientas de ayuda para determinar los componentes

- Para determinar los sistemas de información que intervienen en un proceso, puede servir de ayuda partir de una narrativa del mismo, o una **descripción textual.** Habitualmente, esta descripción puede solicitarse por escrito, por ejemplo en un formulario de un BIA, o recogerse en el transcurso de una entrevista o reunión mixta.

- Dividirlo en fases, …

7. Generación de un Informe de Impacto de Negocio

- Resumen ejecutivo
- Objetivos y alcance
- Metodologías utilizadas para recopilar datos y evaluación
- Detalles de cada departamento: incluidos los procesos críticos, el impacto de la interrupción, sus prioridades, el listado de tiempos y los procesos alternos
- Recomendaciones para la recuperación

¿Qué aspecto tiene un BIA?

Fecha Modificación 11/03/2021 12:23:06

Impactos en el Negocio

Tabla de impactos

Impacto / Tiempo	1.00 horas	4.00 horas	8.00 horas	24.00 horas	2.00 dias	1.00 semanas	2.00 semanas	3.00 semanas	4.00 semanas	Criticidad
	Muy Bajo	Muy Bajo	Medio	Medio	Alto	Muy alto	Muy alto	Muy alto	Muy alto	5
Impacto económico. Pérdida de beneficios (%)	Muy Bajo	Muy Bajo	Bajo	Bajo	Alto	Alto	Alto	Alto	Alto	26
Impacto económico. Incremento de costes y/o gastos (%)	Muy Bajo	Muy Bajo	Medio	Medio	Medio	Alto	Alto	Muy alto	Muy alto	29
Impacto comercial	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Medio	Alto	Alto	Alto	Alto	24
Impacto operacional	Muy Bajo	Bajo	Bajo	Bajo	Bajo	Medio	Alto	Alto	Muy alto	25
Impacto reputacional	Muy Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Medio	Medio	Medio	20
Impacto legal										

Aplicación práctica

- El proceso crítico de una empresa es la venta por internet. El BIA determina que el impacto de una parada es de 100 € a la hora.
- El personal de seguridad considera tres posibles estrategias para restablecer el servicio:
- a. Con un plazo de puesta en marcha de 7 días, disponer un servidor nuevo en el que montar las copias de seguridad. El importe es de 2000 €.
- b. Con un plazo de 3 días, alquilar un servidor alojado por terceros para montar las copias de seguridad. El contrato mínimo es por un mes, con un importe de 1000 €.
- c. Con un plazo de 5 días, arreglar el servidor averiado. El importe de la reparación es de 100 €.
- Seleccionar la mejor opción.