# SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

# SEGURIDAD INFORMÁTICA

1.2.0. Capítulo 2
Parte 1 de 2
Análisis de impacto de negocio

JOSÉ PABLO HERNÁNDEZ

# 1. INTRODUCCIÓN

**Recordad:**

**El objetivo último de un SGSI asegurar la continuidad del negocio, minimizando los riesgos, y maximizando el retorno de la inversión en seguridad, a la vez que se permiten nuevas oportunidades para la empresa.**

**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.**

**Una vez identificados, se determinará el coste que supone para el negocio una interrupción de esas funciones vitales.**

# 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO

**El activo esencial será la propia información (datos).**

- **Dependencia con otros activos:**
- **Servicios**
- **Aplicaciones**
- **Soportes (media)**
- **Redes de comunicaciones**
- **Personas**

# 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO

**El 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. Este en un enfoque muy adecuado para identificar riesgos, logrando aplicar recursos de manera proporcional, minimizando el riesgo, y con un óptimo retorno de la inversión.**

**El punto de partida del BIA es identificar los procesos de negocio y su criticidad. Una vez que se limite el estudio a las funciones vitales, se analizarán los activos involucrados, y de los que depende el desempeño de dichas funciones vitales. El BIA permite así descubrir componentes frecuentemente olvidados, pero importantes para las funciones o procesos críticos del negocio.**

# 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO

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.).

# 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO

**Existen 3 técnicas generalmente aceptadas para enumerar los procesos de negocio soportados por sistemas de información, junto a su criticidad, y coste de interrupción:**

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

# 2.1. FORMULARIOS

**Se pueden distribuir formularios:**

- **A todos los trabajadores**
- **Sólo a responsables de área**

**Funciones:**

- **De máximos (todas las funciones)**
- **Sólo unas pocas (las de mayor criticidad), dejando el resto para siguientes iteraciones (ciclo Deming)**
- **Incluir contratos de servicios externalizados**

# 2.1. FORMULARIOS

**En todos los casos, la información recogida debe permitir evaluar los siguientes resultados del BIA:**

A. **Cuáles son los procesos críticos, u ordenarlos por prioridad.**
B. **Cuál es el daño/impacto, en función del tiempo que se tarde en restablecerse el servicio.**
C. **Cuál es el coste de las diferentes estrategias de recuperación, que proporcionarán un tiempo y un punto objetivo de recuperación.**

# 2.1. FORMULARIOS

| **FORMULARIO DE EVALUACIÓN BIA — 1 (PARA EL CLIENTE)** | | |
|---|---|---|
| **A.1 Función principal (qué hay que recuperar)** | | |
| Área de la empresa | | |
| Número de trabajadores | | |
| Función principal única | | |
| **A.2 Impacto en la empresa** | | |
| Valore cuánto interviene esta función en el objetivo último de la empresa | Cuantitativa (1..100) | Cualitativa (no s crítico) |
| | | |
| Describa cómo interviene esa función en el objetivo último de la empresa | ..... | |
| **B.1 Impacto en la función. (RPO) Valore la pérdida completa de informa periodos de tiempo (ninguno, bajo, medio, grave, desastre)** | | |

| 10 min | 30 min | 1 h | 4 h | 8 h | 1 día | 2 d. | 4 d. | 7 d. | 15 d |
|---|---|---|---|---|---|---|---|---|---|

No sensible, sensible, vital, crítico

# 2.1. FORMULARIOS

**FORMULARIO DE EVALUACIÓN BIA — 1 (PARA EL CLIENTE)**

**A.1 Función principal (qué hay que recuperar)**

| | |
|---|---|
| Área de la empresa | |
| Número de trabajadores | |
| Función principal única | |

**A.2 Impacto en la empresa**

| | | |
|---|---|---|
| Valore cuánto interviene esta función en el objetivo último de la empresa | Cuantitativa (1..100) | Cualitativa (no sensible, sensible, vital, crítico) |
| | | |
| Describa cómo interviene esa función en el objetivo último de la empresa | ..... | |

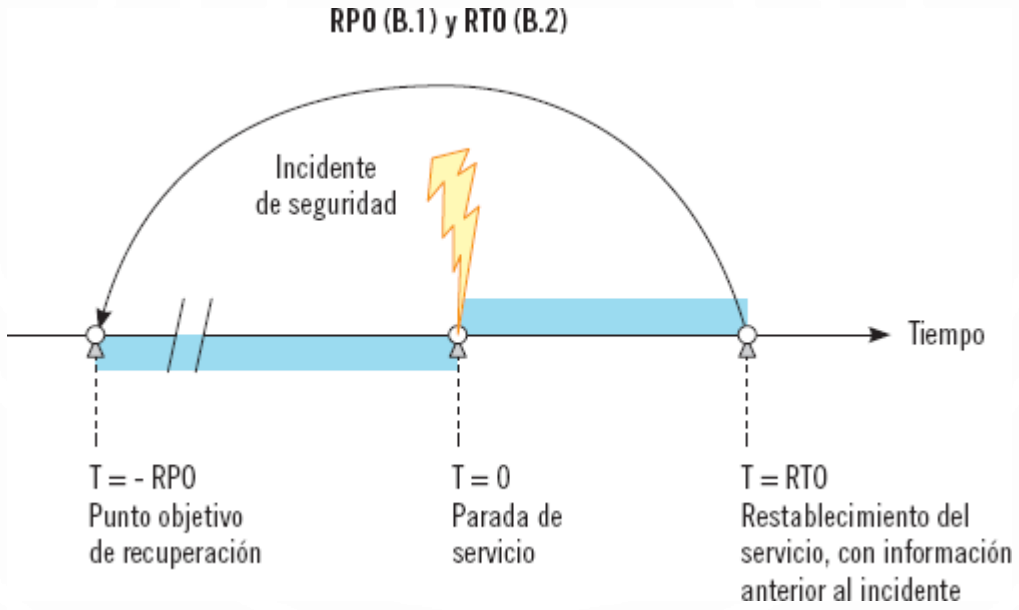
**B.1 Impacto en la función. (RPO) Valore la pérdida completa de información de los siguientes periodos de tiempo (ninguno, bajo, medio, grave, desastre)**

| 10 min | 30 min | 1 h | 4 h | 8 h | 1 dia | 2 d. | 4 d. | 7 d. | 15 d. | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

**B.2 Impacto en la función. (RTO) Valore el daño en la interrupción de la función durante los siguientes periodos de tiempo**

| Tiempo de recuperación | Daño económico (euros) o cualitativo (ninguno, bajo, moderado, grave, desastroso) en las siguientes áreas e importancia de cada área: | | | | |
|---|---|---|---|---|---|
| | Cumplir función principal | Financiero | Otras funciones vinculadas | Reputación, imagen, confianza | Satisfacción del personal |
| | ....% | ....% | ....% | ....% | ....% |
| < 10 min | | | | | |
| 30 min | | | | | |
| 1 h | | | | | |
| 4 h | | | | | |
| 8 h | | | | | |
| 1 dia | | | | | |
| 2 dias | | | | | |
| 4 dias | | | | | |
| 7 dias | | | | | |
| > 15 dias | | | | | |

# 2.1. FORMULARIOS




**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.**

# 2.1. FORMULARIOS

**Para recoger las estrategias de recuperación, además de la información B.1, el personal de seguridad de la información puede emplear un formulario similar al siguiente:**

| FORMULARIO DE EVALUACIÓN BIA — 2 (PARA SEGURIDAD DE LA INFORMACIÓN) | | |
|---|---|---|
| **A. Recuperación (cuánto cuestan las opciones de restablecimiento)** | | |
| Nombre de la solución | | |
| Tiempo objetivo de la recuperación | | |
| Descripción | ..... ..... ..... | |
| Para cada tiempo, identifique los elementos que deben recuperarse, y el coste aproximado de las salvaguardas para dicha recuperación. | | |
| Antes de: | Hay que recuperar: | Cuánto cuesta lograrlo: |
| < 10 min | | |
| 30 min | | |
| 1 h | | |
| 4 h | | |
| 8 h | | |
| 1 día | | |
| 2 días | | |
| 4 días | | |
| 7 días | | |
| > 15 días | | |

# Actividades

ORDENE DE MAYOR A MENOR CRITICIDAD LOS SIGUIENTES PROCESOS O FUNCIONES DE UNA LIBRERÍA:

PRESENTACIÓN DE IMPUESTOS A HACIENDA.
VENTA DE LIBROS.
PEDIDOS DE MATERIAL (STOCK).

A CONTINUACIÓN, PENSAR CÓMO PODRÍA CALCULARSE EL COSTE DE NO PODER REALIZAR ALGUNA DE ELLAS, DURANTE: UNA HORA, UN DÍA, UNA SEMANA, Y DOS O MÁS SEMANAS, Y QUÉ ALTERNATIVAS SE PODRÍAN EMPLEAR PARA REANUDAR CADA FUNCIÓN LO ANTES POSIBLE.

# 2.1. FORMULARIOS. FORMULARIO DE EVALUACION BIA 1

El apartado A.2 permite evaluar la importancia que los usuarios entregan a la función dentro de la empresa. Sin embargo, la función podría no tener ninguna relación con los sistemas de información.

El apartado B.1 define el periodo de tiempo para el que el usuario está dispuesto a perder información, lo que será especialmente relevante a la hora de evaluar las posibles estrategias de recuperación. Esto indica el valor que la información, y por lo tanto de los sistemas de información que la procesan, representan en el proceso. Los procesos que tengan una valoración de ninguno para el periodo de tiempo total, son los que no tienen ninguna dependencia con los sistemas de información. En el otro extremo, cuanto mayor sea la valoración de la pérdida en cualquiera de los periodos, tanto mayor será la dependencia del proceso para con los sistemas de información.

El apartado B.2 ayuda a terminar de valorar la criticidad de la función, midiendo el daño que se le produce a la propia función a consecuencia de una interrupción, en función del tiempo que duren, y de 5 aspectos:

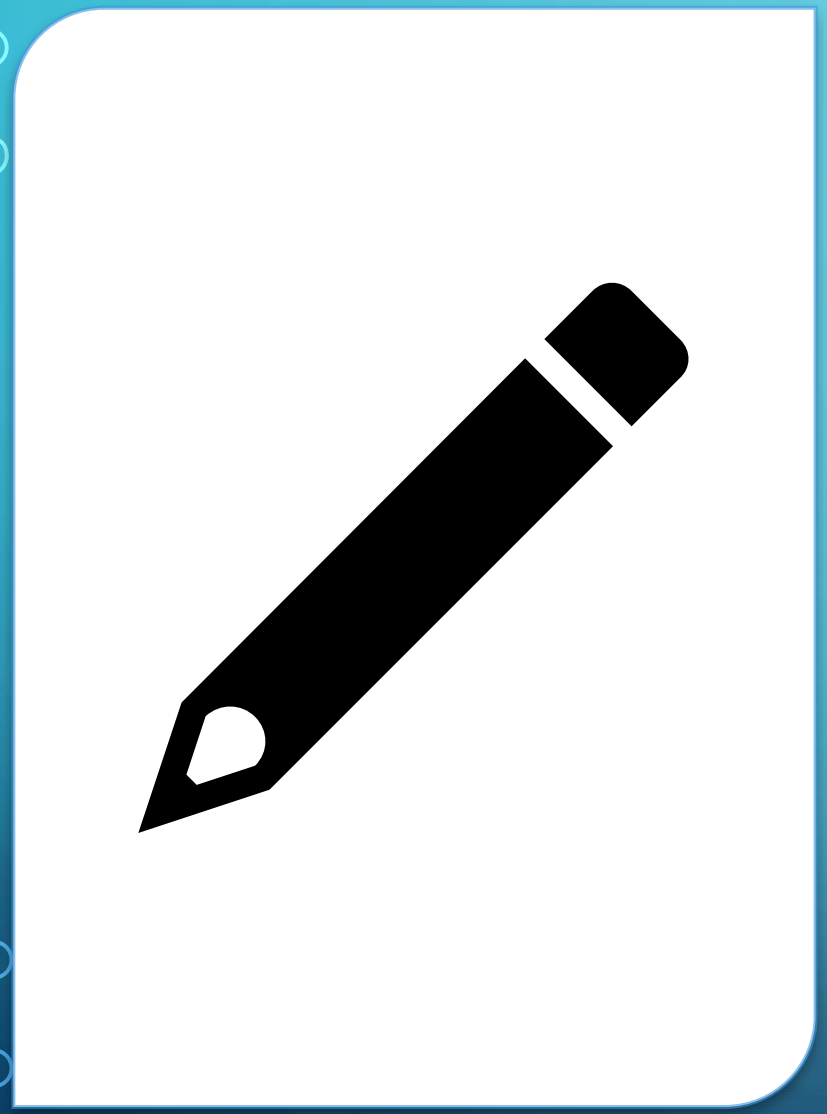
El daño para cumplir la función principal. Por ejemplo, en un proceso de fabricación, pueden existir funciones que si se interrumpen más de un día, conlleven que no sea posible reiniciar la producción. Por ejemplo, en un sistema de alimentación ininterrumpido (SAI) basado en baterías de plomo cuya recarga controla un ordenador, si este no estuviera disponible durante más de 8 horas, el daño sería desastroso, ya que a las 8 horas las baterías se agotarían por completo y su capacidad se recarga quedaría extinguida.

El daño financiero para la función, en términos económicos.

El daño para otras funciones dependientes de esta. Esta valoración excede el ámbito de la propia área o departamento, ya que valora la dependencia general que de esta función tengan las demás funciones de la empresa.

El daño que causaría, para la reputación o imagen del área o departamento que desempeña la función, la interrupción de la misma.

El daño que generaría en la comodidad y nivel de satisfacción del área o departamento la interrupción de su función.



# Actividades

RELLENE LOS FORMULARIOS DE EVALUACIÓN BIA 1 Y 2 PARA LAS SIGUIENTES FUNCIONES DE UNA LIBRERÍA, Y LAS ESTRATEGIAS DE RECUPERACIÓN EN CASO DE DESASTRE, INDICADAS PARA CADA PROCESO.

EMPLEAR SOLO LOS 4 INTERVALOS DE TIEMPO DE LA ACTIVIDAD ANTERIOR: UNA HORA, UN DÍA, UNA SEMANA, Y DOS O MÁS SEMANAS.

VENTA DE LIBROS. ESTRATEGIA DE RECUPERACIÓN: ADQUIRIR ORDENADORES NUEVOS, CONFIGURAR APLICACIONES, Y RESTAURAR COPIAS DE SEGURIDAD DE LA APLICACIÓN DE VENTA.

PEDIDOS DE MATERIAL. ESTRATEGIA DE RECUPERACIÓN: REALIZAR INVENTARIO COMPLETO, PARA RECUPERAR EL STOCK REAL DE MATERIAL.

# 2.2. ENTREVISTAS A USUARIOS CLAVE

**En este caso, se realizan entrevistas para recopilar información que posteriormente también se tabularía, y se analizaría de manera común.**

**Se debe disponer de un conjunto de preguntas preparadas, como las incluidas en el formulario anterior.**

**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.**

**Como herramienta de toma de información, siempre conviene acotar las entrevistas para evitar tomar una excesiva cantidad de información o consumir recursos excesivos tanto al recabar datos como al analizarlos. Así conviene tener claro las personas a las que se les realiza la entrevista (usuarios clave), el alcance de la entrevista (limitándolo a un proceso de negocio concreto), e incluso la donación de la misma (por ejemplo limitándolo a una sesión de 30 minutos).**

# 2.3. REUNIONES ENTRE PERSONAL DE TIC Y USUARIOS CLAVE

**Esta técnica puede emplearse después de tener datos recogidos mediante formularios.**

**Permite, de manera rápida, decidir el impacto de los diferentes procesos o funciones, y el tiempo de parada admisible en cada uno de ellos.**

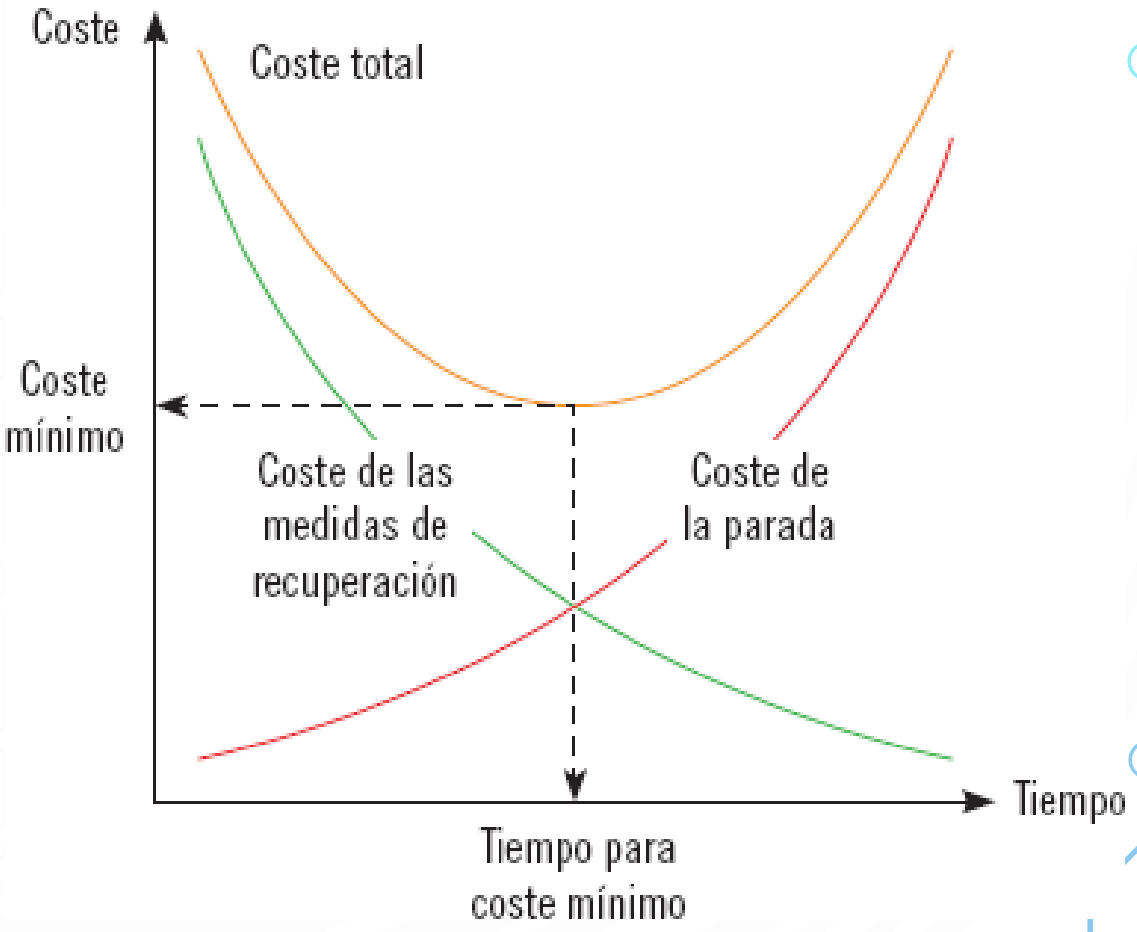
# 2.3. REUNIONES ENTRE PERSONAL DE TIC Y USUARIOS CLAVE

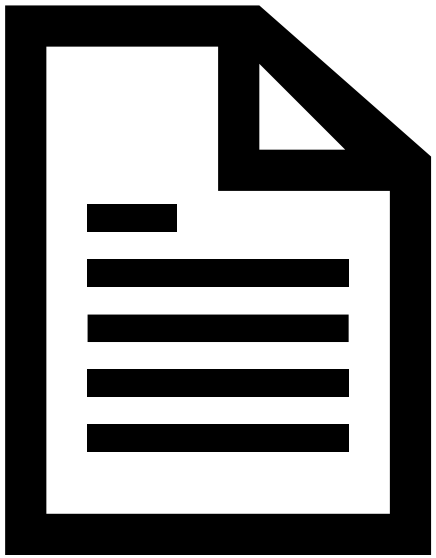
El coste de la parada, normalmente aumentará con el tiempo, de manera escalonada o gradual, como en la imagen.

El coste de las medidas de recuperación se comporta al revés, de manera que las medidas que proporcionan una recuperación muy rápida, normalmente serán más caras que las que recuperan el proceso en más tiempo.

Sumando ambos costes, se obtendrá una curva característica en "U", cuyo mínimo indicará el coste mínimo del incidente, y el tiempo de recuperación del proceso (RTO).

Representación de los costes de un incidente analizados en el BIA





# Ejemplo

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.

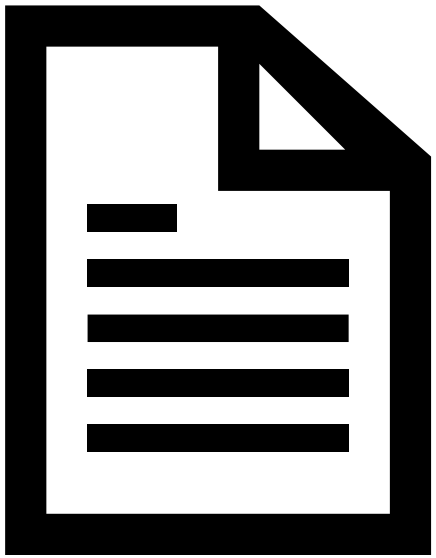
EL PERSONAL DE SEGURIDAD CONSIDERA TRES POSIBLES ESTRATEGIAS PARA RESTABLECER EL SERVICIO:

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 €.

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 €.

CON UN PLAZO DE 5 DÍAS, ARREGLAR EL SERVIDOR AVERIADO. EL IMPORTE DE LA REPARACIÓN ES DE 100 €.
SELECCIONAR LA MEJOR OPCIÓN.

# Ejemplo. Solución



ES NECESARIO EVALUAR EL COSTE DE CADA SOLUCIÓN.

COSTE SOLUCIÓN A:
COSTE PARADA = 24X7X100 = 16.800 €.
COSTE RECUPERACIÓN = 2.000 €.
COSTE TOTAL = 18.800 €.

COSTE SOLUCIÓN B:
COSTE PARADA = 24X3X100 = 7.200 €.
COSTE RECUPERACIÓN = 1.000 €.
COSTE TOTAL = 8.200 €

COSTE SOLUCIÓN C:
COSTE PARADA = 24X5X100 = 12.000 €
COSTE RECUPERACIÓN = 100 €.
COSTE TOTAL = 12.100 €.

LA SOLUCIÓN DE COSTE MÍNIMO PARA RESTABLECER EL SERVICIO ES LA SOLUCIÓN B, QUE ADEMÁS ES LA QUE PROPORCIONA EL MENOR RTO.

RESTABLECIDO EL SERVICIO, LA EMPRESA DISPONE DE UN MES PARA RESTABLECERLO POR COMPLETO, ENTENDIENDO COMO TAL VOLVER A DISPONER DE UN SERVIDOR EN PROPIEDAD:

DISPONE DE 25 DÍAS PARA REPARARLO (COSTE SOLUCIÓN TOTAL = 8.200 + 100 = 8.300 €).
DISPONE DE 23 DÍAS PARA COMPRAR UNO NUEVO (COSTE SOLUCIÓN TOTAL = 8.200 + 2.000 = 10.200 €).

# 3. VALORACIÓN DE LOS REQUERIMIENTOS

**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.**

**Por ejemplo para el proceso de nóminas, la salvaguarda frente al borrado de información podría ser mantener una copia sincronizada en un servidor externo accesible vía FTP. Sin embargo, si para el proceso de nóminas, la confidencialidad de estas es alta, resultaría la misma salvaguarda no válida.**

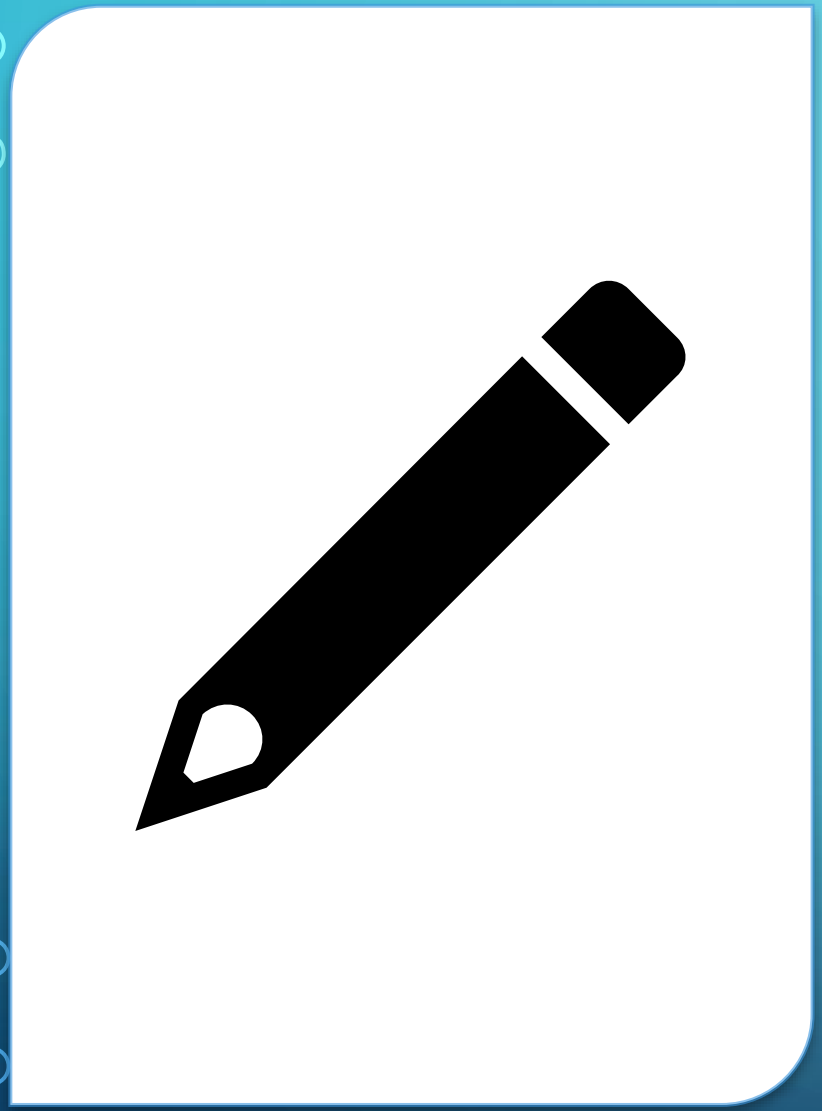
# 3.1. PROCESOS

**La definición de proceso depende del ámbito en que se emplee el término.**

**Así, un proceso de negocio representa al conjunto de trabajos que se realizan para generar un producto o servicio.**

**En un proceso, desde el punto de vista de la información, intervendrán tres elementos únicos:**

- **personas,**
- **equipos (que incluyen aplicaciones) e**
- **información.**



# Actividades

DETERMINE QUÉ ELEMENTOS INTERVIENEN EN LOS SIGUIENTES PROCESOS DE UNA LIBRERÍA:

- VENTA DE LIBROS.
- PEDIDOS DE MATERIAL.

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**No toda la información tiene la misma importancia en una empresa. En consecuencia, es necesario clasificarla, valorándola según diferentes aspectos, para posteriormente asignar unos recursos u otros a su protección.**

**El responsable de clasificar la información es su propietario. En general, esta clasificación debe revisarse, al menos anualmente. Para dicha clasificación, puede ayudar exponer a los propietarios que la información:**

- **Es un elemento concreto, definido, independiente de cómo se almacena o conserva.**
- **Es valiosa para la empresa, y no se puede reemplazar sin coste, esfuerzo, tiempo, u otros recursos.**
- **Forma parte de la empresa, sin ella la empresa sufre un daño.**

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Desde la perspectiva de la seguridad la información se clasifica en:**

- **Confidencial**
- **Interna**
- **Público**

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Confidencial:**

- **Su difusión sin control supone incumplimientos legales.**
- **Su difusión sin control supone incumplimientos de las normativas o reglamentos a los que la empresa se sujeta.**
- **Si se difunde sin control o se hace pública, genera un daño grave/desastroso para la empresa, financiera/económicamente o en su imagen.**

**Para su gestión, son recomendaciones básicas comúnmente aceptadas:**

- **El acceso a esta información debe hacerse siempre en base a la "necesidad de conocer".**
- **Nota: los permisos de acceso a la información, deben concederse a personas exclusivamente, basándose en la necesidad de conocer por sus funciones. De lo anterior, se deduce que una persona solo tendrá acceso al mínimo conjunto de información que necesite para realizar su trabajo.**
- **La difusión de la información requiere siempre de la autorización del propietario, normalmente el responsable o jefe del área o departamento donde se ejecuta el proceso.**
- **La difusión a terceros exige siempre un acuerdo de confidencialidad firmado, previo al acceso.**

**Ejemplo: contratos con clientes, datos de carácter personal según la legislación nacional de protección de los individuos aplicable, información sobre nuevos productos o servicios, información contable, etc.**

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Interna:**

- **Su difusión sin control no genera un daño grave para la empresa.**
- **Si se difunde sin control o se hace pública, genera un daño bajo para la empresa, financiera/económicamente, o en su imagen.**

**Para su gestión, comúnmente se acepta:**

- **Acceso libre para los empleados o personal interno de la empresa.**

**Ejemplo: circulares internas, políticas de diversos aspectos, material formativo, etc.**

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Público:**

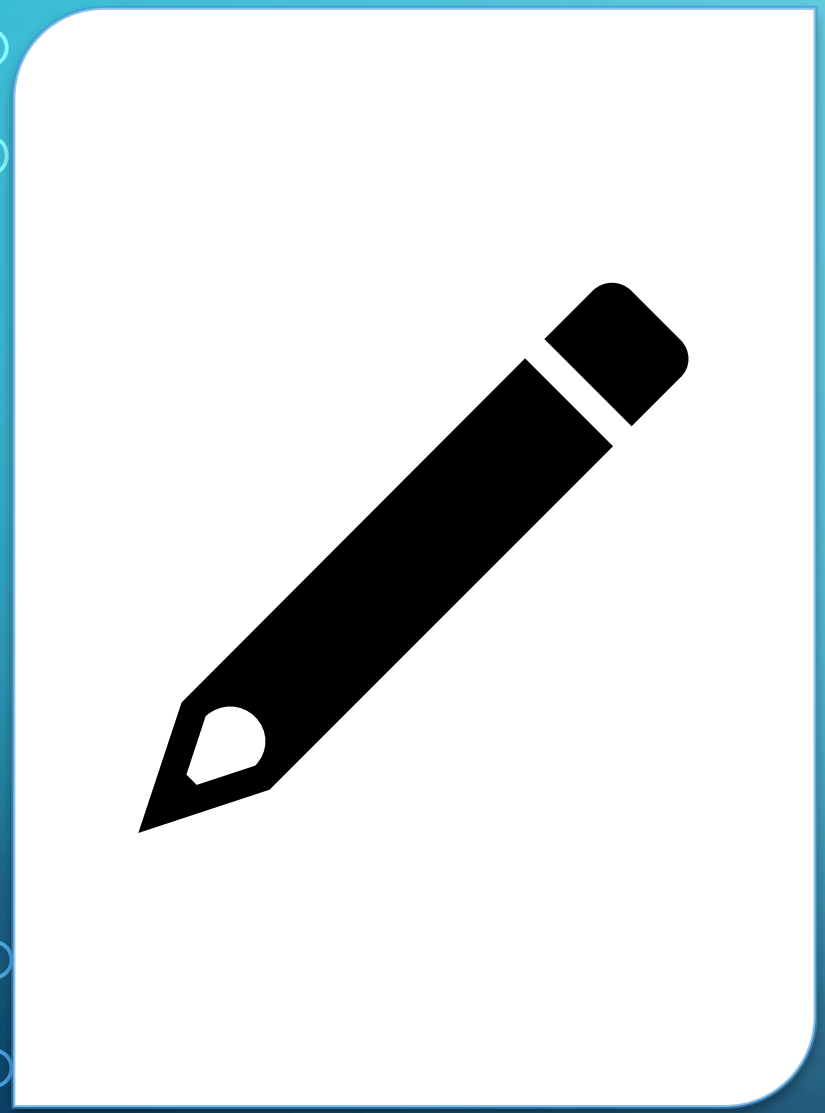
- **La no disponibilidad no tiene ninguna consecuencia.**
- **Su difusión no genera ningún daño ni pérdida a la empresa, ni económicamente, ni en su imagen.**

**Para su gestión, comúnmente se acepta:**

- **Esta información debe ser calificada expresamente para difusión pública, o por el área o responsable de comunicación de la empresa, o por el área de marketing, si se trata de información comercial.**

**Ejemplo: notas de prensa, presentaciones comerciales, catálogos de productos o servicios, publicidad comercial, etc.**

# Actividades



PIENSE EJEMPLOS DE INFORMACIÓN CONFIDENCIAL, INTERNA, Y PÚBLICA QUE PODRÍA ENCONTRAR EN UN DESPACHO DE ABOGADOS.

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Indicaciones habituales (niveles) que ayudarán a determinar los requisitos de seguridad de la información en sus 3 dimensiones habituales:**

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

**En líneas generales, el nivel viene dado por el daño que una degradación de una propiedad genera en la empresa:**

- **Nivel alto**
- **Nivel medio**
- **Nivel bajo**

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Confidencialidad**

**La confidencialidad está relacionada con la autorización de difusión.**

**Una difusión no autorizada puede presentar un daño mayor o menor.**

**Dependiendo de este daño, se categoriza la confidencialidad de la información en alto, medio o bajo.**

**La información clasificada como pública debe ser calificada expresamente para difusión pública, o por el área o responsable de comunicación de la empresa, o por el área de marketing, si se trata de información comercial**

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Confidencialidad**

**Requerimientos de confidencialidad para la información**

- **Nivel alto** Información confidencial, muy sensible o privada, de máximo valor para la empresa, y autorizada a ser accesible solo a individuos concretos reconocidos.

  La difusión no autorizada tendría un impacto grave/desastroso, por ejemplo por las repercusiones legales, por la pérdida económica derivada, por la ventaja concedida a la competencia, o por la pérdida de imagen.

  Por ejemplo, puede tener nivel de confidencialidad alto la documentación de una estrategia de marketing, la información de un proceso de adquisición empresarial, o la información de precios ofrecidos a un cliente.

- **Nivel medio** Información interna, propiedad de la empresa, que no debe tener difusión pública.

  Un incidente de seguridad tendría un impacto moderado.

  Por ejemplo, un directorio telefónico, o un organigrama de la empresa.

- **Nivel bajo** Información pública, no sensible, dispuesta para difusión pública.

  Una difusión no autorizada no debería tener ningún daño, o este sería muy bajo.

  Por ejemplo, tendrán confidencialidad baja las notas de prensa, o la información publicada en la web de la empresa.

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Integridad**

**La integridad se refiere a la completitud y exactitud de la información. La integridad se pierde cuando se realizan cambios no autorizados.**

**Requerimientos de integridad para la información**

- **Nivel alto No puede existir ninguna degradación de la integridad.**

  **La degradación tiene un impacto grave/desastroso.**

- **Nivel medio Una degradación de la información, bien en su completitud o en su precisión, o en ambos, tendría un impacto moderado.**
- **Nivel bajo La completitud o precisión de la información puede degradarse con un impacto ninguno/bajo en el proceso.**

# 3.2. VALORACIÓN CIA DE LA INFORMACIÓN

**Disponibilidad**

**La disponibilidad se refiere a que la información esté disponible cuando se necesite. Los criterios para determinar los requisitos de disponibilidad de la información podrían ser como los siguientes.**

- **Nivel alto La información se necesita de manera continua, en condiciones de 24x7.**

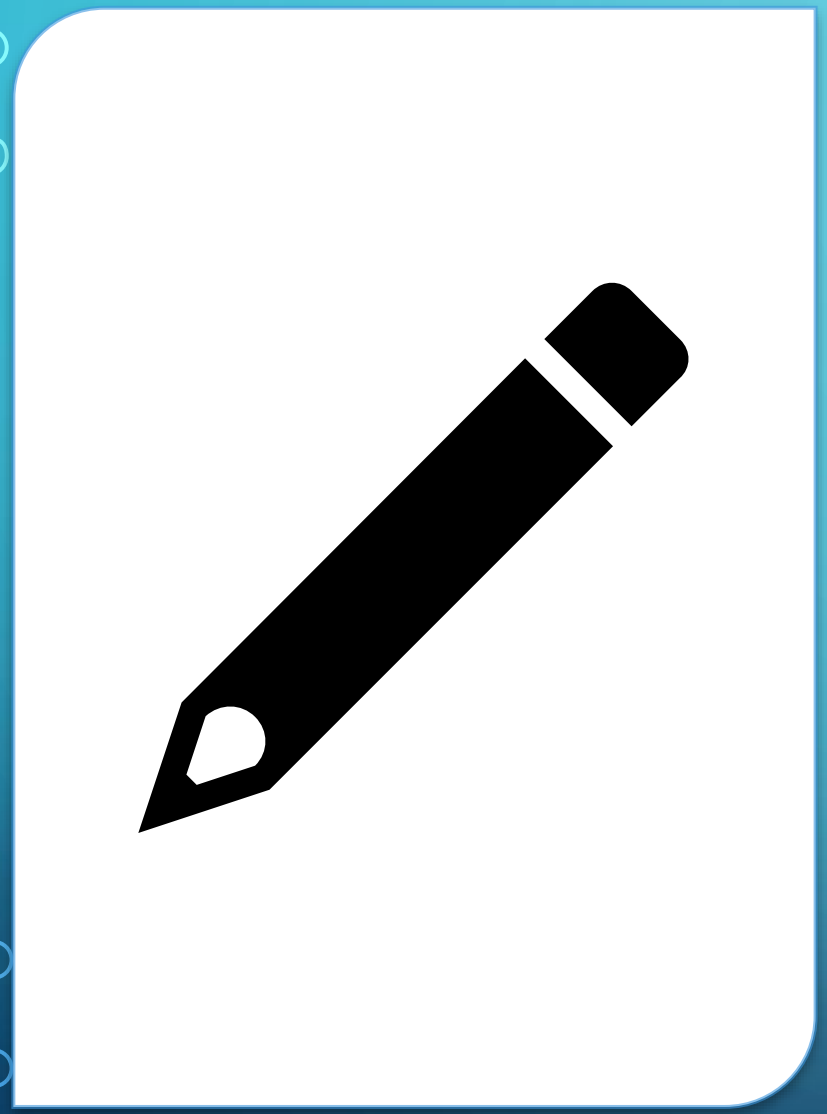
  **La indisponibilidad tiene un impacto grave/desastroso.**

- **Nivel medio La información puede no estar disponible por un periodo de uno o dos días.**

  **La indisponibilidad tiene un impacto moderado.**

- **Nivel bajo La información puede no estar disponible por un periodo de hasta 7 días.**

  **La indisponibilidad tiene un impacto ninguno/bajo.**



# Actividades

CLASIFIQUE LA SIGUIENTE INFORMACIÓN DEL PROCESO DE VENTA DE LIBROS DE UNA LIBRERÍA, Y VALORE JUSTIFICADAMENTE SUS REQUISITOS DE SEGURIDAD:

- BASE DE DATOS CON DIRECCIONES DE DOMICILIOS, TELÉFONOS E HISTÓRICO DE COMPRAS DE CLIENTES, CATEGORIZADOS POR INTERESES O AFICIONES.

- INVENTARIO.

# 3.3. VALORACIÓN DE LOS PROCESOS A PARTIR DE SUS COMPONENTES

**A veces, no es posible o conveniente la valoración según el apartado anterior.**

**En estos casos pueden determinarse los requisitos de seguridad del proceso a partir de los requisitos de seguridad de sus componentes.**

**Proceso = personas + info entrada + sistemas procesamiento = info salida**

**Entonces:**

**Req Seguridad Proceso = Req personas + Req info entrada + req sistemas procesamiento**

# 3.3. VALORACIÓN DE LOS PROCESOS A PARTIR DE SUS COMPONENTES

A la hora de agregar los requisitos de los componentes, existen varias opciones.

Por ejemplo, si la valoración es cuantitativa, pueden sumarse los niveles en cada dimensión.

Si la valoración es cualitativa, también pueden sumarse, estableciendo unas normas previas (dos niveles bajo equivalen a un nivel moderado, o dos niveles graves equivalen a un desastroso).

Una opción sencilla cuando se realizan valoraciones cualitativas, es emplear para el proceso el nivel máximo de sus componentes; tanto para la C, como para la I y la A. Por ejemplo, en un proceso en el que intervenga una información con requisitos (M, M, B), un sistema hardware con requisitos (M, A, B), y una persona con requisitos CIA de valores (A, M, B), se podría tener una clasificación de seguridad para el proceso de (A, A, B).

# 3.3. VALORACIÓN DE LOS PROCESOS A PARTIR DE SUS COMPONENTES

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