



# SEGURIDAD INFORMÁTICA

---

JOSÉ PABLO  
HERNÁNDEZ

# SEGURIDAD INFORMÁTICA

1.2.1. Capítulo 2  
Parte 2 de 2

Análisis de impacto de negocio

JOSÉ PABLO HERNÁNDEZ

## 4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD

**Otros elementos que pueden intervenir en un proceso son:**

- **las personas**
- **los sistemas**

**Vamos a profundizar en sus requerimientos de seguridad.**

## 4.1. VALORACIÓN CIA DE LAS PERSONAS

La información es manejada por personas, y resulta importante tener identificadas a dichas personas, que serán empleados de la empresa, o externos (proveedores, clientes, visitas, y otros).

El responsable de identificar las personas que acceden a la información de un proceso, es el responsable de dicho proceso; y puede coincidir habitualmente con el responsable o jefe del área o departamento que desempeña dicho proceso en la empresa.

## 4.1. VALORACIÓN CIA DE LAS PERSONAS

**La valoración para cada persona que intervenga en el proceso se evalúa en las tres dimensiones de la seguridad: (C, I, A).**

**Se pueden emplear formularios similares a los usados en el BIA, o reuniones con los dueños de los procesos, para identificar a todas las personas que intervengan en dichos procesos.**

# 4.1. VALORACIÓN CIA DE LAS PERSONAS

## 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)
Describe 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 día	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 día					
2 días					
4 días					
7 días					
> 15 días					

## 4.1. VALORACIÓN CIA DE LAS PERSONAS

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)		
<b>A. Recuperación (cuánto cuestan las opciones de restablecimiento)</b>		
Nombre de la solución		
Tiempo objetivo de la recuperación		
Descripción	<div></div> <div></div> <div></div>	
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		

## 4.1. VALORACIÓN CIA DE LAS PERSONAS

### Confidencialidad

Los requisitos de confidencialidad para cada individuo atienden a la clasificación de la información del proceso (confidencial, interno, o público), a la que tenga restringido su acceso. Se clasifican en 3 niveles, y pueden asignarse de acuerdo a la mejor descripción de las necesidades del proceso.

#### Requerimientos de confidencialidad para las personas

- **Nivel alto** Cuando las personas acceden a información calificada como confidencial o crítica para la empresa.  
Un incidente de seguridad causado por una persona con un requisito de confidencialidad alto tendría un impacto grave/desastroso en el proceso.
- **Nivel medio** Cuando las personas acceden a información calificada como interna.  
Un incidente de seguridad tendría un impacto moderado en el proceso.
- **Nivel bajo** Cuando las personas acceden a información calificada como pública.  
Un incidente de seguridad tendría una repercusión ninguna/bajo en el proceso.



## 4.1. VALORACIÓN CIA DE LAS PERSONAS

### Integridad

Los requisitos de integridad para las personas atienden al nivel de la información que pueden modificar en el proceso, y a la capacidad para modificar completamente o no dicha información.

#### Requerimientos de integridad para las personas

- **Nivel alto** Cuando las personas modifican información calificada como confidencial o crítica para la empresa.  
Un incidente de seguridad causado por una persona tendría un impacto grave/desastroso en el proceso.
- **Nivel medio** Cuando las personas pueden modificar completamente información calificada como interna e información calificada como pública.  
Un incidente de seguridad tendría un impacto moderado en el proceso.
- **Nivel bajo** Cuando las personas tienen restricciones para modificar la información calificada como interna e información calificada como pública.  
Un incidente de seguridad tendría una repercusión ninguno/bajo en el proceso.

## 4.1. VALORACIÓN CIA DE LAS PERSONAS

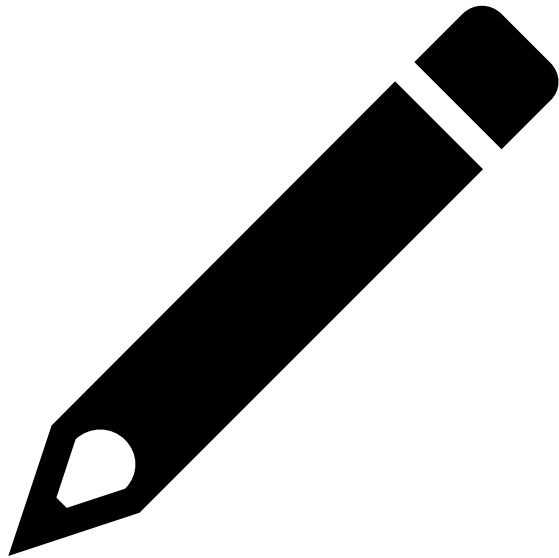
### Disponibilidad

Los requisitos de disponibilidad para las personas atienden al daño que genera al proceso el que la persona no esté disponible.

#### Requerimientos de disponibilidad para las personas

- **Nivel alto** Cuando la no disponibilidad de la persona tendría un impacto grave/desastroso en el proceso.
- **Nivel medio** Cuando la no disponibilidad de la persona tendría un impacto moderado en el proceso.
- **Nivel bajo** Cuando la no disponibilidad de la persona tendría un impacto ninguno/bajo en el proceso.

# Actividades



PIENSE LA VALORACIÓN CIA QUE PODRÍA TENER EL ÚNICO ADMINISTRADOR DE LA RED DE ORDENADORES DE UN DESPACHO DE ABOGADOS.

## 4.2. VALORACIÓN CIA DE SISTEMAS FÍSICOS, PROGRAMAS Y SERVICIOS DE SOPORTE

Se clasifican aquí los requisitos para:

- **Equipos físicos (hardware):**
  - Ordenadores
  - Equipos de comunicaciones
  - Soportes de almacenamiento (CD, discos duros extraíbles, etc.),
- **Aplicaciones o programas:**
  - Sistemas operativos
  - Aplicaciones
- **Servicios de soporte necesarios:**
  - Suministro eléctrico
  - Climatización
  - Alojamiento.

# Ampliación



LOS SOPORTES DE ALMACENAMIENTO SON UNA PIEZA ESENCIAL DE UN SISTEMA DE INFORMACIÓN, Y EN CONCRETO, DEL SISTEMA DE COPIAS DE SEGURIDAD. SI LA INFORMACIÓN TIENE UN NIVEL ALTO DE CONFIDENCIALIDAD, TAN IMPORTANTE ES CONSERVARLOS LIBRES DE ACCESOS NO PERMITIDOS, COMO DESTRUIRLOS DE MANERA IRRECUPERABLE AL FINALIZAR SU PERIODO DE VIGENCIA, PORQUE LAS COPIAS NO PUEDEN ALMACENARSE INDEFINIDAMENTE. SI LA INFORMACIÓN TIENE UN NIVEL DE INTEGRIDAD ALTO, LAS COPIAS DEBEN PROTEGERSE DE MODIFICACIONES, YA QUE EN CASO DE RESTAURARLAS SE INTRODUCIRÁ INFORMACIÓN ALTERADA; PARA ELLO PUEDE SERVIR CONSERVAR EL HASH DE LA INFORMACIÓN GUARDADA, QUE SE EMPLEARÁ COMO ELEMENTO DE VERIFICACIÓN DE LA COPIA ANTES DE RESTAURARLA.

[HTTPS://WWW.YOUTUBE.COM/WATCH?V=NU8WN1EFTUI](https://www.youtube.com/watch?v=NU8WN1EFTUI)

## 4.2. VALORACIÓN CIA DE SISTEMAS FÍSICOS, PROGRAMAS Y SERVICIOS DE SOPORTE

### Confidencialidad

Los requisitos de confidencialidad de los sistemas atienden al servicio que prestan, y heredan la confidencialidad de la información procesada o almacenada por el sistema.

#### Requerimientos de confidencialidad para los sistemas

- **Nivel alto** Cuando la información procesada, almacenada, o el servicio prestado, tiene un nivel de confidencialidad alta.
- **Nivel medio** Cuando la información procesada, almacenada, o el servicio prestado, es de confidencialidad media.
- **Nivel bajo** Cuando la información procesada, almacenada, o el servicio prestado, es de confidencialidad baja.

## 4.2. VALORACIÓN CIA DE SISTEMAS FÍSICOS, PROGRAMAS Y SERVICIOS DE SOPORTE

### Integridad

Los requisitos de integridad de los sistemas heredan la integridad de la información procesada o almacenada por el sistema, y además, reflejan la confianza o fiabilidad (predictibilidad) de los servicios prestados por el sistema en el proceso.

### Requerimientos de integridad para los sistemas

- **Nivel alto** La confianza y fiabilidad de los servicios prestados es alta.  
La información procesada o almacenada tiene un nivel de integridad alto.
- **Nivel medio** La confianza y fiabilidad de los servicios prestados es media.  
La información procesada o almacenada tiene un nivel de integridad medio.
- **Nivel bajo** La confianza y fiabilidad de los servicios prestados es baja.  
La información procesada o almacenada tiene un nivel de integridad bajo.

## 4.2. VALORACIÓN CIA DE SISTEMAS FÍSICOS, PROGRAMAS Y SERVICIOS DE SOPORTE

### Disponibilidad

Los requisitos de disponibilidad heredan la clasificación de disponibilidad de la información del proceso, y se basan en el impacto que tendría para el proceso que estos no estuviesen disponibles.

### Requerimientos de disponibilidad para los sistemas

- **Nivel alto** La información procesada o almacenada tiene un nivel de disponibilidad alto.  
Cuando la no disponibilidad de los sistemas tendría un impacto grave/desastroso en el proceso.
- **Nivel medio** La información procesada o almacenada tiene un nivel de disponibilidad medio.  
Cuando la no disponibilidad de los sistemas tendría un impacto moderado en el proceso.
- **Nivel bajo** La información procesada o almacenada tiene un nivel de disponibilidad bajo.  
Cuando la no disponibilidad de los sistemas tendría un impacto ninguno/bajo en el proceso.



## 4.2. VALORACIÓN CIA DE SISTEMAS FÍSICOS, PROGRAMAS Y SERVICIOS DE SOPORTE

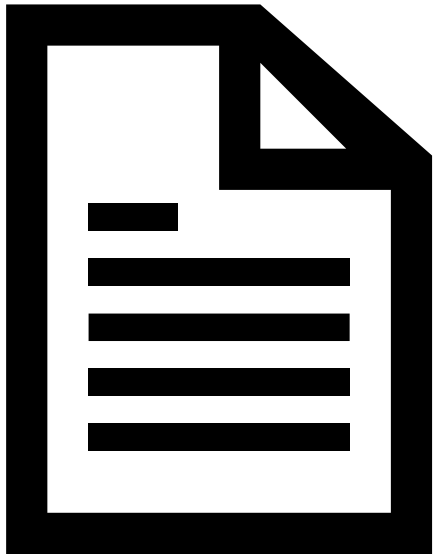
### Disponibilidad

Los requisitos de disponibilidad heredan la clasificación de disponibilidad de la información del proceso, y se basan en el impacto que tendría para el proceso que estos no estuviesen disponibles.

### Requerimientos de disponibilidad para los sistemas

- **Nivel alto** La información procesada o almacenada tiene un nivel de disponibilidad alto.  
Cuando la no disponibilidad de los sistemas tendría un impacto grave/desastroso en el proceso.
- **Nivel medio** La información procesada o almacenada tiene un nivel de disponibilidad medio.  
Cuando la no disponibilidad de los sistemas tendría un impacto moderado en el proceso.
- **Nivel bajo** La información procesada o almacenada tiene un nivel de disponibilidad bajo.  
Cuando la no disponibilidad de los sistemas tendría un impacto ninguno/bajo en el proceso.

# Ejemplo



1.2.2.MF0486\_3-CAPITULO2-PARTE2\_EJEMPLO.DOCX