

# **IFCT0109. SEGURIDAD INFORMÁTICA**

## **MF0486\_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS**



# **UD02**

## **ANÁLISIS DE IMPACTO DE NEGOCIO**

# CONTENIDOS

## 1. INTRODUCCIÓN

2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN
3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO
4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD

## 1. INTRODUCCIÓN

**EL OBJETIVO DE UN SGSI ES 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.**



## 1. INTRODUCCIÓN

**LA CONTINUIDAD DEL NEGOCIO** ESTARÁ MUY ESTRECHAMENTE RELACIONADA CON **LA DISPONIBILIDAD** DE LA INFORMACIÓN.

TAMBIÉN INTERVIENE **LA INTEGRIDAD**, PUES LA EMPRESA NO PODRÁ OPERAR SI LA INFORMACIÓN ESTÁ DISPONIBLE, PERO NO ESTÁ COMPLETA NI ES EXACTA.

TAMBIÉN SE PRECISA DE **LA CONFIDENCIALIDAD**, PUES LA OPERACIÓN DE LA EMPRESA PUEDE PERDER SU VALOR SI LA INFORMACIÓN ESTÁ EXPUESTA A QUIEN NO DEBE CONOCERLA.



## 1. INTRODUCCIÓN

PARA ASEGURAR LA CONTINUIDAD DEL NEGOCIO, HAY QUE REALIZAR UNA **EVALUACIÓN DE RIESGOS**, CON UNA ***ETAPA DE ANÁLISIS***, Y UNA ***ETAPA DE GESTIÓN DE RIESGOS***.

EN ESTA EVALUACIÓN DE RIESGOS, ***SE ESTUDIAN LOS ACTIVOS QUE, BAJO UNA AMENAZA, PUEDAN SUFRIR UN IMPACTO O UN DAÑO.***

SI EN LA EMPRESA EXISTE UN **CATÁLOGO DE ACTIVOS**, DEBERÍA **REVISARSE** PARA CONFIRMAR QUE ESTÁ ACTUALIZADO; SI NO EXISTE, HABRÍA QUE CONFECCIONARLO.



## 1. INTRODUCCIÓN

PARA ASEGURAR LA CONTINUIDAD DEL NEGOCIO, EL PUNTO DE PARTIDA ES UN **ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)**.

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.**

Impacto	Alto	Considerar	Planificar Respuesta	Planificar Respuesta
	Medio	Desatender pero monitorizar	Considerar	Planificar Respuesta
	Bajo	Desatender pero monitorizar	Desatender pero monitorizar	Considerar
		Baja	Media	Alta
		Probabilidad		

## CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN
3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO
4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD



## **2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN**

**PARA CADA PROCESO DE LA EMPRESA, EL ACTIVO ESENCIAL SERÁ LA INFORMACIÓN. PERO LOS DATOS SOLO EXISTEN EN DEPENDENCIA CON OTROS ACTIVOS, COMO:**

- **LOS SERVICIOS** (QUE SE PRESTAN GRACIAS A LOS DATOS, O QUE SON NECESARIOS PARA PRODUCIRLOS)
- **LAS APLICACIONES** (QUE PROCESAN LOS DATOS)
- **LOS EQUIPOS** (QUE EJECUTAN LAS APLICACIONES)
- **LOS SOPORTES** (QUE ALMACENAN LOS DATOS)
- **LAS REDES DE COMUNICACIONES** (QUE TRANSMITEN LOS DATOS)
- **LAS INSTALACIONES** (QUE ALBERGAN LOS EQUIPOS)
- **LAS PERSONAS** (QUE OPERAN LOS DATOS)

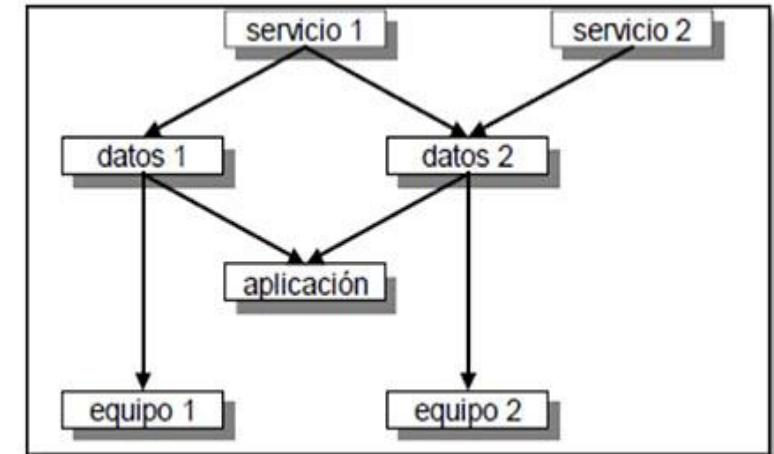


## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

ES HABITUAL CONSTRUIR ARBOLES DE DEPENDENCIA, QUE ILUSTREN CÓMO UN ACTIVO DEPENDE DE OTROS PARA SU CORRECTO FUNCIONAMIENTO.

LA DEPENDENCIA PROVOCA ASÍ QUE EL IMPACTO Y RIESGO DE LOS ACTIVOS SE VAYA ACUMULANDO HACIA EL ACTIVO PRINCIPAL INTEGRADOR, BAJO ESTUDIO.

LA EVALUACIÓN DE RIESGOS PARA LOS EQUIPOS INFORMÁTICOS PERMITIRÁ CONOCER EL COSTE DE RECUPERACIÓN DEL SERVICIO.



## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

EN GENERAL, EXISTIRÁN SALVAGUARDAS DE DIFERENTES PRECIOS, QUE CONDUCIRÁN A DIFERENTES TIEMPOS DE RECUPERACIÓN.

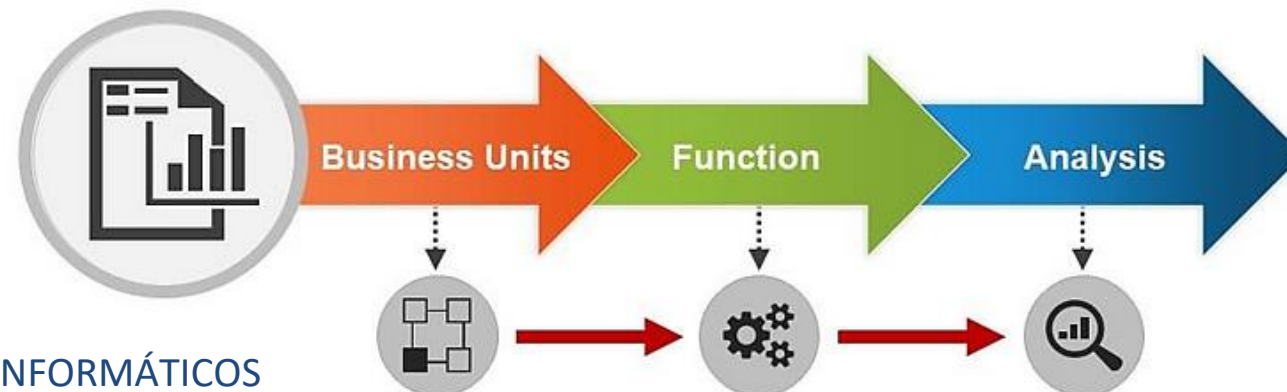
**MINIMIZANDO EL COSTE TOTAL** (SUMA DEL COSTE DE LA PARADA DEL SERVICIO Y DEL COSTE DE LA RECUPERACIÓN), SE DETERMINA EL TIEMPO DE RECUPERACIÓN, LAS SALVAGUARDAS A IMPLEMENTAR, Y OTROS REQUERIMIENTOS DE SEGURIDAD.



## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

EL BIA (BUSINESS IMPACT ANALYSIS) ES EL ESTUDIO DE LAS CONSECUENCIAS QUE TENDRÍA EN EL NEGOCIO UNA PARADA DE SUS PROCESOS VITALES POR UN DETERMINADO TIEMPO:

*¿QUÉ HAY QUE RECUPERAR?, ¿CUÁNTO CUESTA HACERLO?  
Y ¿CÓMO HAY QUE RECUPERARLO?.*

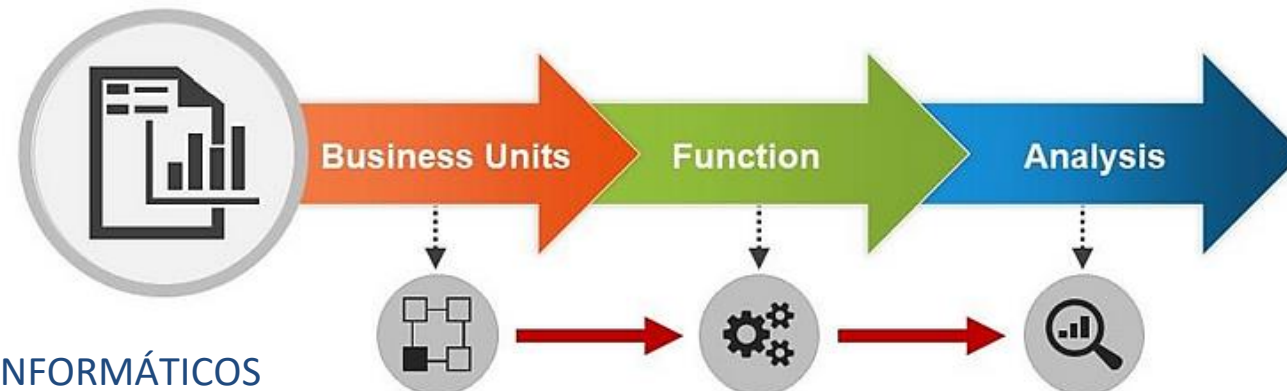


## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

DEL BIA SE OBTIENEN RESULTADOS DE MUCHÍSIMO VALOR:

*CONOCER CUÁLES SON LOS ACTIVOS INFORMÁTICOS QUE INTERVIENEN EN LOS PROCESOS CRÍTICOS DEL NEGOCIO, SER CAPACES DE EVALUAR SU IMPACTO, Y CONOCER CUÁLES SON LOS REQUISITOS DE SEGURIDAD PARA ESTOS ACTIVOS.*

**ESTE ES UN ENFOQUE MUY ADECUADO PARA IDENTIFICAR RIESGOS, LOGRANDO APLICAR RECURSOS DE MANERA PROPORCIONAL, MINIMIZANDO EL RIESGO, Y CON UN ÓPTIMO RETORNO DE LA INVERSIÓN.**



## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

EL PUNTO DE PARTIDA DEL BIA ES IDENTIFICAR LOS PROCESOS DE NEGOCIO Y SU CRITICIDAD.

EL BIA PERMITE ASÍ DESCUBRIR COMPONENTES FRECUENTEMENTE OLVIDADOS, PERO IMPORTANTES PARA LAS FUNCIONES O PROCESOS CRÍTICOS DEL NEGOCIO.

EL BIA ES UNA HERRAMIENTA PARA ELABORAR EL PLAN DE CONTINUIDAD DE LA EMPRESA (BCP).





## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

FRECUENTEMENTE, EL BCP INCLUIRÁ UN PLAN PARA LA RECUPERACIÓN DE DESASTRES (DRP).

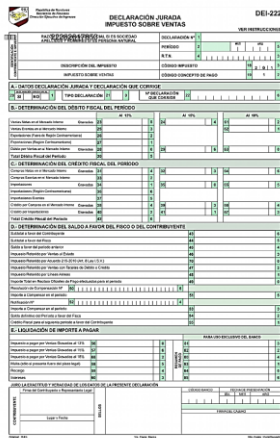
DENTRO DE UNA EMPRESA, LA REALIZACIÓN DE UN BCP *DEBE INCLUIR NO SOLO LOS ASPECTOS DE LA INFORMACIÓN, SINO TODAS LAS FACETAS QUE SE NECESITAN PARA LA ACTIVIDAD DE LA EMPRESA* (INSTALACIONES, CONTRATOS, SEGUROS, FINANCIACIÓN, CLIENTES, STOCK DE PRODUCTOS, ETC.).



## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

EXISTEN 3 TÉCNICAS 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. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN**

### **2.1 FORMULARIOS**

SE PUEDE **DISTRIBUIR UN FORMULARIO** A LOS TRABAJADORES, O SOLO A LOS RESPONSABLES DE ÁREA, EN LOS QUE RESPONDAN A UNA SERIE DE PREGUNTAS QUE AYUDEN A IDENTIFICAR LAS FUNCIONES CLAVE PARA ESA ÁREA.

EL **BIA** PUEDE ENTONCES PROSEGUIR, PARA AQUELLAS FUNCIONES QUE SE ELIJAN, DE MANERA QUE LAS FUNCIONES NO CUBIERTAS EN PRIMERA INSTANCIA SE TRATEN EN FUTURAS ITERACIONES DEL **SGSI**.

SI SE HUBIERAN EXTERNALIZADO SERVICIOS DE **TI** A PROVEEDORES, HABRÍA QUE CONSIDERAR LOS CONTRATOS PARA DICHOS SERVICIOS.

## **2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN**

### **2.1 FORMULARIOS**

NO EXISTE UN FORMULARIO ÚNICO, POR EL CONTRARIO, DEPENDERÁ DE CADA EMPRESA, O DE LO EXHAUSTIVO QUE SE PUEDA SER.

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. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

### 2.1 FORMULARIOS (EJEMPLO)

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

FORMULARIO DE EVALUACIÓN BIA — 1 (PARA EL CLIENTE)

#### 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					

## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

### 2.1 FORMULARIOS

PARA RESPONDER A LAS PARTES A Y B (**CRITICIDAD DE LAS FUNCIONES, Y DAÑO DE LA INTERRUPCIÓN**) EXISTIRÁ UN FORMULARIO A *RELLENAR POR LOS RESPONSABLES DEL PROCESO*. AUNQUE ES UN DATO QUE SE NECESITA PARA DISEÑAR LAS ESTRATEGIAS DE RECUPERACIÓN, SE PREGUNTARÁ AQUÍ POR EL DAÑO DE LA INFORMACIÓN QUE NO SE PUEDA RECUPERAR (B.1), YA QUE ESTA VALORACIÓN DEBE DARLA EL PROPIETARIO DE LA INFORMACIÓN.

PARA RESPONDER A LA PARTE C, REFERENTE A **CÓMO RECUPERAR EL SERVICIO**, ADEMÁS DE LA PARTE B.1 DEL FORMULARIO ANTERIOR, SE EMPLEARÁ OTRO FORMULARIO NUEVO, EN ESTA OCASIÓN A *RELLENAR POR EL PERSONAL DE SEGURIDAD DE LA INFORMACIÓN*.

## 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN

### 2.1 FORMULARIOS (EJEMPLO)

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	

FORMULARIO DE EVALUACIÓN BIA — 2 (PARA SEGURIDAD DE LA INFORMACIÓN)

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		



## **2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN**

### **2.2 ENTREVISTAS A USUARIOS CLAVE**

**SE REALIZAN ENTREVISTAS PARA RECOPILAR INFORMACIÓN PARA SU ANÁLISIS. SE DISPONE DE UN CONJUNTO DE PREGUNTAS PREPARADAS.**

**LAS ENTREVISTAS DAN CABIDA A RECOGER INFORMACIÓN BAJO CRITERIOS DESCONOCIDOS A PRIORI.**

**CONVIENE TENER CLARO LAS PERSONAS A LAS QUE SE LES REALIZA LA ENTREVISTA (USUARIOS CLAVE), EL ALCANCE DE LA ENTREVISTA, Y LA DURACIÓN DE LA MISMA.**



## **2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN**

### **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.**





## CONTENIDOS

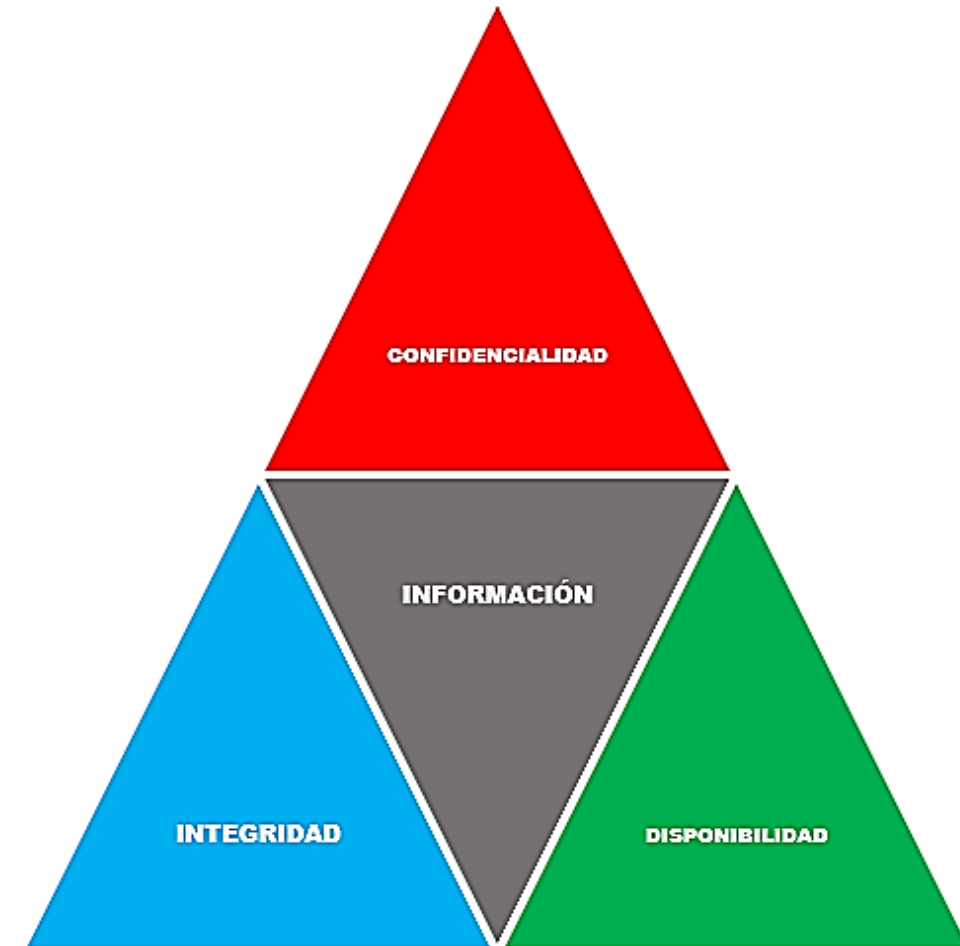
1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN
3. **VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO**
4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD

### 3. 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
- LA INTEGRIDAD
- LA DISPONIBILIDAD

ES NECESARIO EVALUAR LOS REQUISITOS DE *CONFIDENCIALIDAD*, *INTEGRIDAD* Y *DISPONIBILIDAD* DE LOS PROCESOS DE LA EMPRESA, A FIN DE DETERMINAR CUÁLES SON LAS SALVAGUARDAS ÓPTIMAS.



La triada de la seguridad o CIA

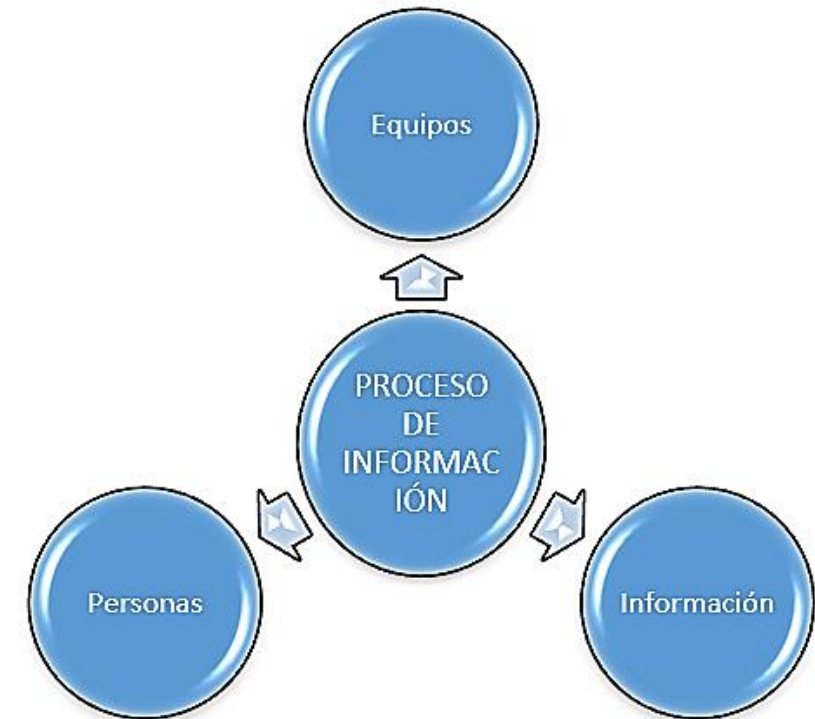
### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.1 PROCESOS

UN PROCESO 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)
- INFORMACIÓN

LAS POSIBLES RELACIONES ENTRE ESTOS TRES ELEMENTOS SON MÚLTIPLES.

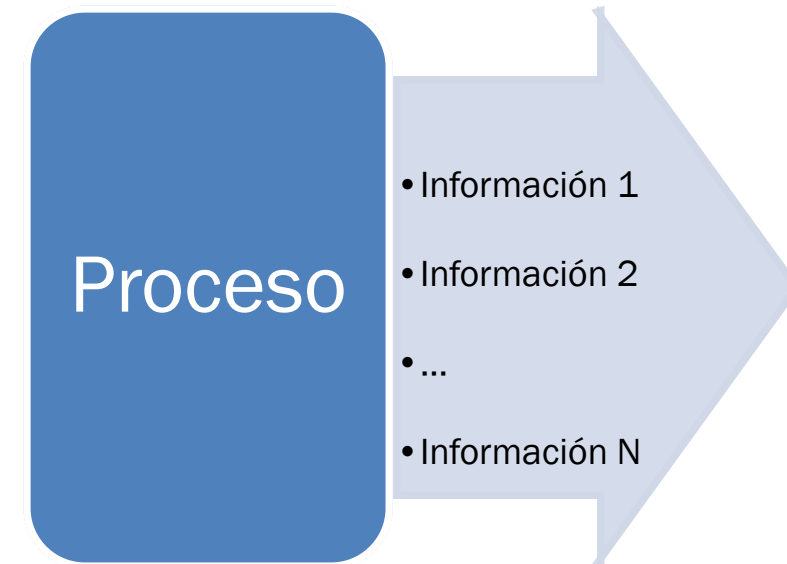


### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.1 PROCESOS

SI EL PROCESO DE NEGOCIO FUERA LA FABRICACIÓN DE **UN PRODUCTO**, SE LLEGARÍA HASTA LA INFORMACIÓN DE LOS SISTEMAS INFORMÁTICOS DE CONTROL DE LAS MÁQUINAS DE FABRICACIÓN.

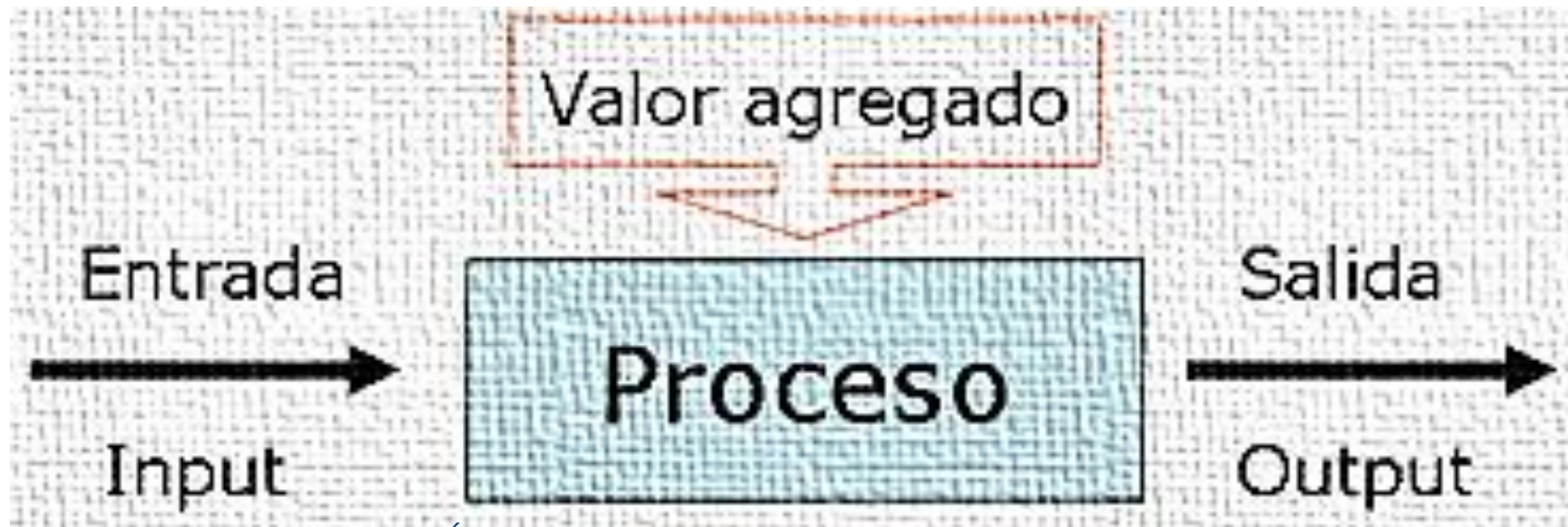
SI EL PROCESO ES LA ENTREGA DE **UN SERVICIO**, EL PROCESO TERMINA EN EL CONJUNTO DE INFORMACIÓN QUE ES NECESARIO PARA LA PRESTACIÓN SATISFACTORIA DEL SERVICIO.



### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.1 PROCESOS

UN PROCESO TIENE VALOR POR SU RESULTADO. UNA PRIMERA APROXIMACIÓN PARA VALORAR LOS REQUISITOS DE SEGURIDAD DE UN PROCESO ES VALORAR LOS REQUISITOS DE INFORMACIÓN QUE ENTREGA.





### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.1 PROCESOS

UN PROCESO DE LA ORGANIZACIÓN ES EL MÉTODO CON EL QUE SE DESARROLLA UNA TAREA EN CONCRETO, CUANDO ESA TAREA DE INFORMATIZA SE DEBE ESTUDIAR CON ANTERIORIDAD CÓMO FUNCIONA PERFECTAMENTE PARA POSTERIORMENTE DESARROLLAR EL SOFTWARE NECESARIO Y ADAPTADO A ESE PROCESO.



### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.1 PROCESOS

MIENTRAS QUE CON LAS TÉCNICAS TRADICIONALES LOS DESARROLLADORES SE CENTRABAN EN ANALIZAR Y MODELAR UN SISTEMA ORIENTADO A CASOS DE USO.

CON ESTE NUEVO ENFOQUE, SE INCIDE **EN ANALIZAR Y OBTENER UN CONOCIMIENTO PLENO DE CADA UNO DE LOS PROCESOS DE NEGOCIO**, CONSIGUIENDO UN MODELO DEL SISTEMA QUE SE ADAPTA MEJOR A SUS NECESIDADES.





### **3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO**

#### **3.2 VALORACIÓN CIA DE LA INFORMACIÓN**

**ES NECESARIO CLASIFICAR LA INFORMACIÓN PARA POSTERIORMENTE ASIGNAR UNOS RECURSOS U OTROS A SU PROTECCIÓN. EL RESPONSABLE DE CLASIFICAR LA INFORMACIÓN ES SU PROPIETARIO. 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. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.2 VALORACIÓN CIA DE LA INFORMACIÓN

DESDE LA PERSPECTIVA DE LA SEGURIDAD, LA INFORMACIÓN SE CLASIFICA EN:

- **CONFIDENCIAL**
- **INTERNA**
- **PÚBLICA**



### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.2 VALORACIÓN CIA DE LA INFORMACIÓN CONFIDENCIAL

SU DIFUSIÓN SIN CONTROL:

- SUPONE *INCUMPLIMIENTOS LEGALES*.
- SUPONE *INCUMPLIMIENTOS DE LAS NORMATIVAS O REGLAMENTOS A LOS QUE LA EMPRESA SE SUJETA.*
- *SI SE HACE PÚBLICA, GENERA UN DAÑO GRAVE/DESASTROSO PARA LA EMPRESA, FINANCIERA-ECONÓMICAMENTE O EN SU IMAGEN.*



### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.2 VALORACIÓN CIA DE LA INFORMACIÓN

## CONFIDENCIAL

PARA SU **GESTIÓN**, SE RECOMIENDA:

- LOS PERMISOS SE CONCEDEN BASÁNDOSE EN LA **NECESIDAD DE SABER** POR SUS FUNCIONES.
- LA DIFUSIÓN REQUIERE SIEMPRE LA **AUTORIZACIÓN DEL PROPIETARIO**.
- LA DIFUSIÓN A TERCEROS EXIGE UN **ACUERDO DE CONFIDENCIALIDAD**.



### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.2 VALORACIÓN CIA DE LA INFORMACIÓN INTERNA

SU DIFUSIÓN SIN CONTROL:.

- NO GENERA UN DAÑO GRAVE PARA LA EMPRESA.
- SI SE HACE PÚBLICA, GENERA UN **DAÑO BAJO** PARA LA EMPRESA.

PARA SU **GESTIÓN**, SE ACEPTA:

- ACCESO LIBRE PARA LOS EMPLEADOS O PERSONAL INTERNO DE LA EMPRESA.





### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.2 VALORACIÓN CIA DE LA INFORMACIÓN PÚBLICA

- LA NO DISPONIBILIDAD NO TIENE NINGUNA CONSECUENCIA.
- SU DIFUSIÓN NO GENERA NINGÚN DAÑO NI PÉRDIDA A LA EMPRESA

PARA SU **GESTIÓN**, SE ACEPTA:

- ESTA INFORMACIÓN DEBE SER CALIFICADA EXPRESAMENTE PARA DIFUSIÓN PÚBLICA.



### **3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO**

#### **3.2 VALORACIÓN CIA DE LA INFORMACIÓN**

A CONTINUACIÓN, SE EXPONEN INDICACIONES HABITUALES QUE AYUDARÁN A **DETERMINAR LOS REQUISITOS DE SEGURIDAD** DE LA INFORMACIÓN EN SUS 3 DIMENSIONES HABITUALES.

- **CONFIDENCIALIDAD.** ESTÁ RELACIONADA CON LA AUTORIZACIÓN DE DIFUSIÓN.
- **INTEGRIDAD.** SE REFIERE A LA COMPLETITUD Y EXACTITUD DE LA INFORMACIÓN.
- **DISPONIBILIDAD.** SE REFIERE A QUE LA INFORMACIÓN ESTÉ DISPONIBLE CUANDO SE NECESITE



### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.2 VALORACIÓN CIA DE LA INFORMACIÓN

#### CONFIDENCIALIDAD. ESTÁ RELACIONADA CON LA AUTORIZACIÓN DE DIFUSIÓN

---

##### Requerimientos de confidencialidad para la información

---

	Información confidencial, muy sensible o privada, de máximo valor para la empresa, y autorizada a ser accesible solo a individuos concretos reconocidos.
Nivel alto	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.
Nivel medio	Información interna, propiedad de la empresa, que no debe tener difusión pública. Un incidente de seguridad tendría un impacto moderado.
Nivel bajo	Información pública, no sensible, dispuesta para difusión pública. Una difusión no autorizada no debería tener ningún daño, o este sería muy bajo.

---

### 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.2 VALORACIÓN CIA DE LA INFORMACIÓN

**INTEGRIDAD.** SE REFIERE A LA COMPLETITUD Y EXACTITUD DE LA INFORMACIÓN

---

##### 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. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO

#### 3.2 VALORACIÓN CIA DE LA INFORMACIÓN

**DISPONIBILIDAD.** SE REFIERE A QUE LA INFORMACIÓN ESTÉ DISPONIBLE CUANDO SE NECESITE

---

##### Requerimientos de disponibilidad para la información

---

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.

---

### **3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO**

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

EL APARTADO ANTERIOR DA UN ENFOQUE SENCILLO PARA EVALUAR LOS REQUISITOS DE SEGURIDAD DE UN PROCESO. EN OCASIONES ESTO NO SERÁ POSIBLE O CONVENIENTE.

EN ESTOS CASOS PUEDEN DETERMINARSE LOS REQUISITOS DE SEGURIDAD DEL PROCESO A PARTIR DE LOS REQUISITOS DE SEGURIDAD DE SUS COMPONENTES.

LOS REQUISITOS DE SEGURIDAD PARA LOS PROCESOS PUEDEN OBSERVARSE ENTONCES COMO ***UNA COMBINACIÓN DE LOS REQUISITOS DE SEGURIDAD DE LAS PERSONAS, DE LOS SISTEMAS, Y DE LA INFORMACIÓN QUE INTERVENGA.***

```

graph TD
    Cliente[Cliente] -- entrega --> Dinero[Dinero]
    Cliente -- permite --> Transaccion[Transacción de venta]
    Dinero -- permite --> Transaccion
    Dinero -- permite --> Vendedor[Vendedor]
    Vendedor -- entrega --> Libro[Libro]
    Libro -- permite --> Transaccion
    Vendedor -- autoriza --> Aplicacion[Aplicación de venta]
    Aplicacion -- permite --> Transaccion
    Aplicacion -- permite --> OrdenadorI[Ordenador]
    OrdenadorI -- permite --> SuministroI[Suministro eléctrico]
    Red[Red de comunicaciones] -- permite --> Aplicacion
    Red -- permite --> Base[Base de datos]
    Red -- permite --> SuministroC[Suministro eléctrico]
    Base -- permite --> OrdenadorB[Ordenador]
    OrdenadorB -- permite --> SuministroB[Suministro eléctrico]
  
```

El diagrama ilustra el flujo de una transacción de venta de un libro, mostrando la interacción entre el cliente, el vendedor, el dinero, el libro, la aplicación de venta, la red de comunicaciones, la base de datos y los ordenadores, todos ellos controlados por un sistema de suministro eléctrico. Cada entidad tiene un cuadro de control con botones C, I y A.

SI LAS RELACIONES QUE SE EMPLEA SON EN SENTIDO CONTRARIO (“**NECESITA**” EN LUGAR DE “**PERMITE**”), SE PUEDE REALIZAR EL PROCESO INVERSO, Y PROPAGAR LOS REQUISITOS CIA DEL PROCESO HACIA SUS INTEGRANTES.



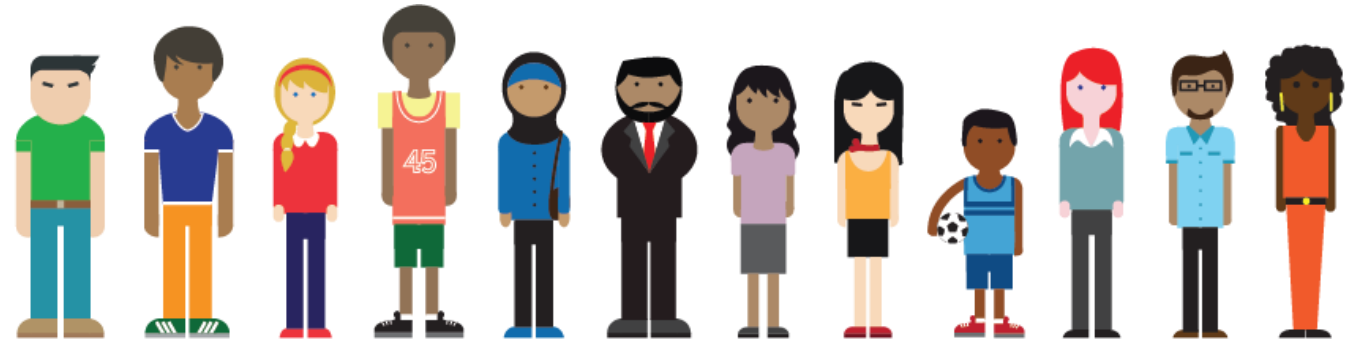
## CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN
3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO
4. **DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD**

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

HEMOS VISTO LAS PAUTAS PARA DETERMINAR LOS REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN.

LOS OTROS ELEMENTOS QUE PUEDEN INTERVENIR EN UN PROCESO SON **LAS PERSONAS Y LOS SISTEMAS.**



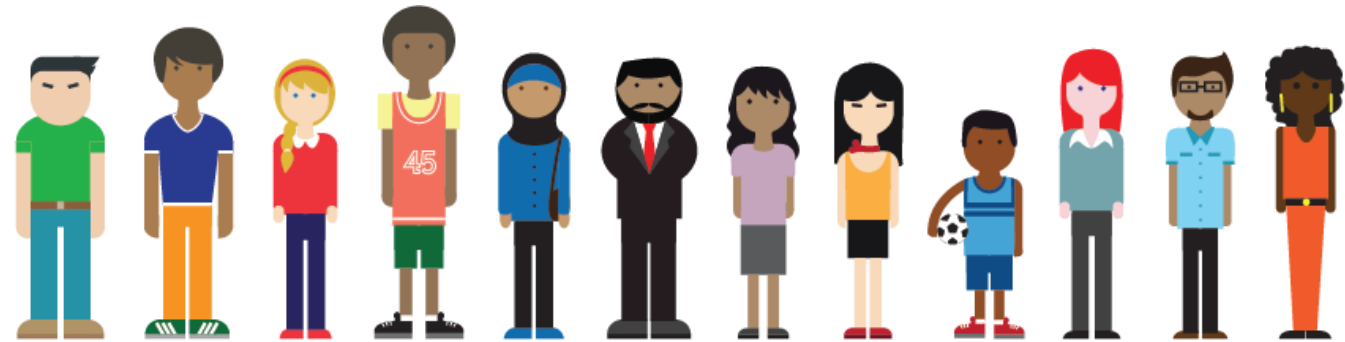
## 4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD

### 1. VALORACIÓN CIA DE LAS PERSONAS

LA INFORMACIÓN ES MANEJADA POR PERSONAS, Y RESULTA IMPORTANTE TENER IDENTIFICADAS A DICHAS PERSONAS.

*EL RESPONSABLE DE IDENTIFICAR LAS PERSONAS QUE ACCEDEN A LA INFORMACIÓN DE UN PROCESO ES EL RESPONSABLE DE DICHO PROCESO.*

LA VALORACIÓN PARA CADA PERSONA QUE INTERVENGA EN EL PROCESO SE EVALÚA EN LAS TRES DIMENSIONES DE LA SEGURIDAD (CIA).



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

### 1. VALORACIÓN CIA DE LAS PERSONAS

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

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

### 1. VALORACIÓN CIA DE LAS PERSONAS

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



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

### 1. VALORACIÓN CIA DE LAS PERSONAS

**DISPONIBILIDAD.** 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.
------------	--

---

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

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

EN ESTA CATEGORÍA SE DEBEN CLASIFICAR LOS COMPONENTES QUE INTERVIENEN EN EL PROCESO, AL MARGEN DE LAS PERSONAS Y DE LA INFORMACIÓN. SE CLASIFICAN AQUÍ LOS REQUISITOS PARA LOS EQUIPOS FÍSICOS, PARA LAS APLICACIONES O PROGRAMAS, E INCLUSO PARA LOS SERVICIOS DE SOPORTE NECESARIOS



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

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

**CONFIDENCIALIDAD.** 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 <b>alta</b> .
Nivel medio	Cuando la información procesada, almacenada, o el servicio prestado, es de confidencialidad <b>media</b> .
Nivel bajo	Cuando la información procesada, almacenada, o el servicio prestado, es de confidencialidad <b>baja</b> .

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

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

**INTEGRIDAD.** HEREDAN LA INTEGRIDAD DE LA INFORMACIÓN PROCESADA O ALMACENADA POR EL SISTEMA, Y ADEMÁS, REFLEJAN LA CONFIANZA O FIABILIDAD 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 <b>alto</b> .
Nivel medio	La confianza y fiabilidad de los servicios prestados es media. La información procesada o almacenada tiene un nivel de integridad <b>medio</b> .
Nivel bajo	La confianza y fiabilidad de los servicios prestados es baja. La información procesada o almacenada tiene un nivel de integridad <b>bajo</b> .

---



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

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

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



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

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

LA SIGUIENTE ES UNA ENUMERACIÓN DE LOS POSIBLES ELEMENTOS QUE INTERVIENEN EN UN PROCESO DE NEGOCIO:

- EQUIPOS HARDWARE DE PROCESAMIENTO.
- EQUIPOS DE COMUNICACIONES DE RED.
- PROGRAMAS.
- SOPORTES DE INFORMACIÓN.
- SERVICIOS DE SOPORTE.

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

### **3. 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 EN UN FORMULARIO DE UN **BIA**, O RECOGERSE EN UNA ENTREVISTA O REUNIÓN MIXTA.

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

## **3. HERRAMIENTAS DE AYUDA PARA DETERMINAR LOS COMPONENTES**

**CUANDO EL PROCESO ES COMPLEJO, CONVIENE DIVIDIRLO EN FASES O SUBPROCESOS**

PARA INTENTAR ASEGURAR LA COMPLETITUD EN LA NARRATIVA PUEDE AYUDAR PREGUNTARSE SI SE ENCUENTRAN RESPONDIDOS SIETE ASPECTOS FUNDAMENTALES:

**QUÉ, QUIÉN, CUÁNDO, CÓMO, DÓNDE, POR QUÉ, Y PARA QUÉ**

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

### **3. HERRAMIENTAS DE AYUDA PARA DETERMINAR LOS COMPONENTES**

POSTERIORMENTE, SE ENUMERAN EN LISTAS INDEPENDIENTES LOS **ELEMENTOS** DE CADA TIPO QUE INTERVENGAN EN CADA CATEGORÍA: *PERSONAS, SISTEMAS, E INFORMACIÓN DE ENTRADA.*

SEGUIDAMENTE, CADA UNO DE ESTOS ELEMENTOS SE RELACIONA CON LOS **DEMÁS MEDIANTE UNA ACCIÓN** (*GENERA, AUTORIZA, PROCESA, TRANSMITE, ETC.*).

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

### **3. HERRAMIENTAS DE AYUDA PARA DETERMINAR LOS COMPONENTES**

DE ESTA MANERA, SE PUEDE ORDENAR DE MANERA JERÁRQUICA LA DEPENDENCIA DE LOS COMPONENTES HASTA EL RESULTADO FINAL.

GRÁFICAMENTE, LA ESTRUCTURA SE APROXIMARÁ A LA DE UN **ÁRBOL INVERTIDO** DONDE **LAS HOJAS SERÁN LOS COMPONENTES**, LOS **NODOS INTERMEDIOS SERÁN SUBTAREAS O SUBPROCESOS**, Y EN LA **RAÍZ O PUNTO MÁS ALTO DEL DIAGRAMA**, SE **ENCONTRARÁ EL RESULTADO O INFORMACIÓN DE SALIDA DEL PROCESO**.



## **CONTENIDOS**

- 1. INTRODUCCIÓN**
- 2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN**
- 3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO**
- 4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD**

## RESUMEN

**EL OBJETIVO DE UN SGSI ES ASEGURAR LA CONTINUIDAD DEL NEGOCIO, MINIMIZANDO LOS RIESGOS Y MAXIMIZANDO EL RETORNO DE LA INVERSIÓN EN SEGURIDAD. PARA ELLO, HAY QUE CONOCER LOS RIESGOS MEDIANTE UN PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS.**

ESTE ANÁLISIS PUEDE EMPLEARSE COMO PUNTO DE PARTIDA PARA REALIZAR EL **BIA, O ANÁLISIS DEL IMPACTO EN EL NEGOCIO** QUE TENDRÍA UN INCIDENTE DE SEGURIDAD QUE DETUVIERA LA ACTIVIDAD.

EL **BIA** SE PUEDE REALIZAR MEDIANTE LA PROPIA INFORMACIÓN QUE SE RECOJA EN FORMULARIOS, Y QUE PERMITIRÁ DETERMINAR CUÁLES SON LOS PROCESOS O FUNCIONES PRINCIPALES DE LA EMPRESA DONDE FOCALIZAR LOS ESFUERZOS EN LAS SALVAGUARDAS.

## RESUMEN

EL RESULTADO DE UN BIA ES MUY VALIOSO, PORQUE PERMITE CONOCER LA ACTIVIDAD DE LA EMPRESA, ORDENANDO LA CRITICIDAD DE SUS FUNCIONES Y PROCESOS.

TAMBIÉN PERMITE **CONOCER EL COSTE DE UNA INTERRUPCIÓN**, Y RECOGE LOS REQUISITOS DE PUNTO OBJETIVO DE RECUPERACIÓN.

EL BIA AYUDA A DETERMINAR LAS ESTRATEGIAS O MÉTODOS DE RECUPERACIÓN, Y LAS SALVAGUARDAS O CONTRAMEDIDAS QUE SE APLICARÍAN.

**LOS REQUISITOS DE SEGURIDAD** SERÁN CALIFICACIONES, NÚMEROS, O GRADOS, ALCANZADOS EN CADA UNA DE LAS DIMENSIONES DE LA SEGURIDAD (**LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD**).

## RESUMEN

LOS REQUISITOS DE SEGURIDAD DEL PROCESO DE NEGOCIO PUEDEN OBTENERSE EVALUANDO LOS REQUISITOS DE LA INFORMACIÓN RESULTANTE DEL PROCESO O ANALIZANDO LOS COMPONENTES DEL PROCESO, Y **VALORANDO LOS REQUISITOS DE SEGURIDAD DE CADA COMPONENTE.**

UNA VEZ DISPUESTOS JERÁRQUICAMENTE, **LOS REQUISITOS DE SEGURIDAD SE AGRUPAN DE MANERA ASCENDENTE**, MEDIANTE ALGUNA FÓRMULA O MÉTODO DEFINIDO.

LAS CATEGORÍAS EN QUE SE VALORE LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD, ASÍ COMO LA FORMULA O MÉTODO DE AGREGACIÓN DE LOS REQUISITOS DE LOS COMPONENTES DE UN PROCESO, NO ES ESPECIALMENTE RELEVANTE.

## RESUMEN

ESTOS INDICADORES PERSIGUEN COMPARAR LA EVOLUCIÓN DE LA EMPRESA EN DIFERENTES INSTANTES DEL TIEMPO.

**POR LO TANTO, LO IMPORTANTE ES QUE ESTOS CRITERIOS SE DEFINAN POR ESCRITO, Y SE APLIQUEN CON HOMOGENEIDAD A LO LARGO DEL SGSI, PORQUE SOLO ASÍ SE PODRÁ RECONOCER LA TENDENCIA DE MEJORA EN LA SEGURIDAD OBTENIDA POR CADA ITERACIÓN DEL MISMO (PLANIFICACIÓN, EJECUCIÓN, MEDIDA, Y CORRECCIÓN).**

