Seguridad en equipos informáticos

IFCT0109 – Seguridad informática

MF0486_3 (90 horas)

Análisis de impacto de negocio

- Introducción
- Identificación de procesos de negocio soportados por sistemas de información
- Valoración de los requerimientos de confidencialidad, integridad, y disponibilidad de los procesos de negocio
- Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad
- Resumen

Introducción

En el contexto actual, los equipos informáticos son vitales para las operaciones empresariales, dado el valor crítico de la información que gestionan y las repercusiones de cualquier fallo en su seguridad.

La creciente sofisticación de las amenazas informáticas y la omnipresencia de las vulnerabilidades hacen que la seguridad de la información sea una preocupación primordial para las organizaciones.

La gestión efectiva de la seguridad informática implica comprender y mitigar los riesgos asociados con las amenazas, evaluando tanto el daño potencial como la probabilidad de ocurrencia.

Para lograrlo, se emplea un enfoque basado en el riesgo, que consiste en analizar los riesgos, determinar la aceptabilidad de los mismos y aplicar medidas de protección adecuadas. Este proceso continuo busca garantizar la confidencialidad, integridad y disponibilidad de la información, con el objetivo final de asegurar la continuidad del negocio y maximizar el retorno de la inversión en seguridad.

Identificación de procesos de negocio soportados por sistemas de información

- Los procesos empresariales dependen de múltiples activos, como datos, servicios, aplicaciones, equipos, redes y personas.
- Se realizan análisis de dependencia para comprender cómo afecta el fallo de un activo al funcionamiento general.
- El Business Impact Analysis (BIA) evalúa los activos críticos, determina su impacto en los procesos de negocio y define los requisitos de seguridad.

<u>Principales puntos:</u>

- BIA: Identifica activos informáticos críticos, evalúa su impacto y define requisitos de seguridad.
- ISO 22317: Ayuda en la realización efectiva del BIA, priorizando productos y servicios, y proporcionando un marco detallado.

Identificación de procesos de negocio soportados por sistemas de información

El Business Impact Analysis (BIA) y la Continuidad del Negocio

- El BIA es fundamental para desarrollar el Plan de Continuidad del Negocio (BCP) y, a menudo, incluye un Plan de Recuperación de Desastres (DRP).
- El BCP abarca todas las áreas de la empresa, no solo la información, considerando instalaciones, contratos, seguros, financiación, clientes y stock de productos.
- La norma ISO 22301:2020 establece un Sistema de Gestión de la Continuidad de Negocio, abordando los riesgos generales y siguiendo el ciclo de mejora continua (PDCA).
- La ISO 22301 define requisitos para la planificación, implementación, operación, supervisión, revisión, prueba, mantenimiento y mejora del Sistema de Gestión de Continuidad de Negocio (SGCN).

Identificación de procesos de negocio soportados por sistemas de información

Metodologías para identificar procesos de negocio:

- Formularios: Recopilación de información estructurada sobre los procesos empresariales y su criticidad.
- Entrevistas: Diálogo con usuarios avanzados para comprender sus necesidades y la importancia de los procesos.
- Reuniones conjuntas: Colaboración entre personal de TI y usuarios avanzados para identificar y evaluar los procesos críticos.

Enfoque:

- Identificación de procesos vitales.
- Análisis de activos involucrados.
- Implementación de medidas proporcionales para minimizar riesgos y garantizar la continuidad del negocio.

Identificación de procesos de negocio soportados por sistemas de información

Metodologías para identificar procesos de negocio (Formularios)

- Los formularios son una herramienta clave para realizar el Business Impact Analysis (BIA) en un Sistema de Gestión de la Seguridad de la Información (SGSI).
- Se distribuyen a todos los trabajadores o a los responsables de área para recopilar información sobre las funciones clave y su criticidad.
- Los datos recopilados se unifican y valoran según criterios comunes de criticidad.
- Los formularios permiten identificar procesos críticos y ordenarlos por prioridad.
- Se consideran los daños e impactos según el tiempo de recuperación del servicio.
- Se debe tener en cuenta la externalización de servicios de TI y los contratos con proveedores.

Identificación de procesos de negocio soportados por sistemas de información

Metodologías para identificar procesos de negocio (Formularios)

- La información recopilada en los formularios se utiliza para diseñar estrategias de recuperación.
- Los formularios se dividen en secciones para recopilar datos sobre la criticidad, el impacto y el coste de recuperación.
- Se incluyen secciones específicas para evaluar el daño de la información no recuperable y para determinar cómo restaurar el servicio.

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 día	2 d.	4 d.	7 d.	15 d.	TOTAL

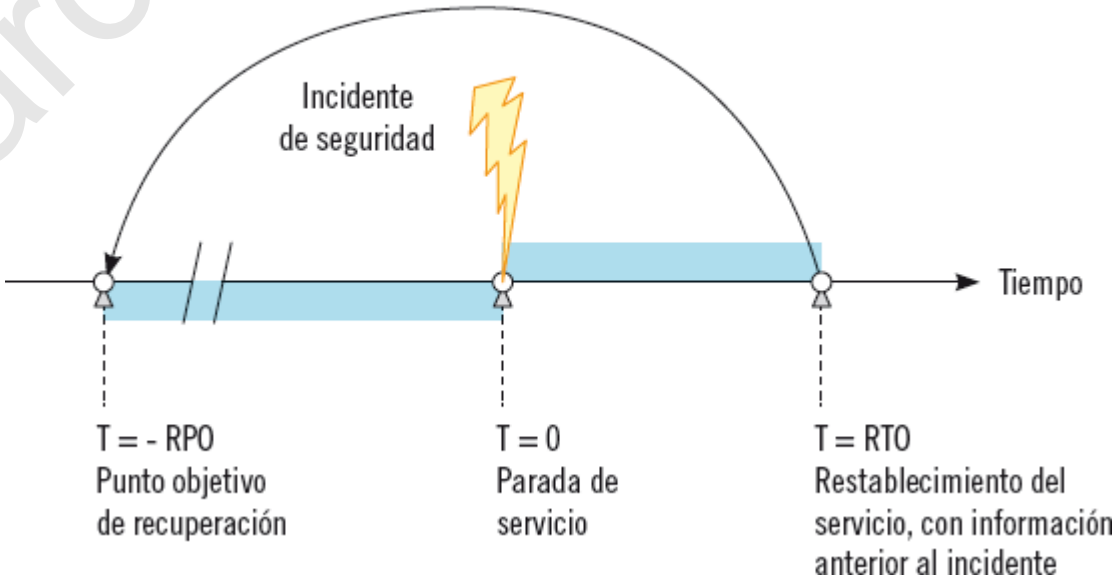
B.2 Impacto en la función. (RTO) Valore el daño en la interrupción de la función durante los siguientes periodos de tiempo

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					

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.

RPO (B.1) y RTO (B.2)



Desde que se produce un incidente, hasta que se restablece el servicio, pasa un tiempo sin servicio (RTO). El servicio se recupera, pero con la información que se tenía un tiempo (RPO) previo a la ocurrencia del incidente. El periodo de tiempo total que retrocede la empresa es RPO+RTO.

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		

Identificación de procesos de negocio soportados por sistemas de información

Metodologías para identificar procesos de negocio (Formularios)

Introducción al BIA y Formulario de Evaluación

El Business Impact Analysis (BIA) es una metodología para identificar y evaluar los procesos de negocio críticos para la continuidad de la empresa.

Se puede utilizar el "Formulario de Evaluación BIA 1" para recopilar información sobre la importancia y dependencia de los sistemas de información en los procesos de negocio.

El formulario se distribuye a los responsables de área para recoger datos relevantes sobre la relación entre los procesos y los sistemas de información.

Identificación de procesos de negocio soportados por sistemas de información

Metodologías para identificar procesos de negocio (Formularios)

Análisis de los Apartados del Formulario BIA

El apartado A.2 del formulario evalúa la importancia que los usuarios asignan a la función dentro de la empresa, aunque esta podría no estar relacionada con los sistemas de información.

El apartado B.1 define el tiempo máximo que el usuario está dispuesto a perder información, lo que ayuda a determinar la criticidad de los sistemas de información en el proceso.

La valoración de la pérdida en diferentes periodos de tiempo indica la dependencia del proceso de los sistemas de información.

Identificación de procesos de negocio soportados por sistemas de información

Metodologías para identificar procesos de negocio (Formularios)

Evaluación de la Criticidad de la Función

El apartado B.2 del formulario ayuda a valorar la criticidad de la función midiendo el daño que sufriría debido a una interrupción en términos financieros, de reputación y de satisfacción.

Se analizan cinco aspectos para determinar el impacto de la interrupción en la función y en otras áreas dependientes de ella.

El análisis de estas tablas permite asignar valores a las respuestas y calcular totales para determinar la criticidad de la función.

Identificación de procesos de negocio soportados por sistemas de información

Metodologías para identificar procesos de negocio (Formularios)

Objetivos y Métodos de Evaluación

El objetivo del BIA es ordenar los procesos en función de su criticidad, evaluar el daño de una interrupción y determinar la adecuación de las estrategias de recuperación.

La valoración puede realizarse de manera cuantitativa o cualitativa, utilizando criterios coherentes para futuras revisiones del BIA.

Se pueden emplear métodos de estimación sencillos para calcular el impacto de la interrupción, como asignar valores a las respuestas del formulario y sumarlos para obtener una puntuación total.

Identificación de procesos de negocio soportados por sistemas de información

Metodologías para identificar procesos de negocio (Entrevistas a usuarios clave)

Las entrevistas son una herramienta útil para recopilar información sobre la importancia de los procesos de negocio.

Se prepara un conjunto de preguntas similares a las del formulario anterior para guiar la entrevista.

Las entrevistas son adecuadas cuando se desconocen todos los aspectos de valoración de un proceso.

Es importante acotar las entrevistas para evitar tomar demasiada información y consumir recursos excesivos (p.e. sesión de 30 min)

Identificación de procesos de negocio soportados por sistemas de información

Actividad

Ordena de mayor a menor criticidad los siguientes procesos o funciones de una librería.

- Venta de libros.
- Pedidos de material.
- Presentación de impuestos a Hacienda.

Calcula el coste (impacto), teórico, de no poder realizar alguna de ellas, durante: una hora, un día, una semana, y dos o más semanas

Busca alternativas que se podrían emplear para reanudar cada función lo antes posible.

Identificación de procesos de negocio soportados por sistemas de información

Actividad (solución posible)

Orden de criticidad (mayor a menor):

1. Venta de libros: Es el proceso central de la librería, genera ingresos y permite la satisfacción del cliente.
2. Presentación de impuestos a Hacienda: Si no se cumple, se pueden generar multas e incluso el cierre del negocio.
3. Pedidos de material: Es importante para mantener el inventario y ofrecer variedad a los clientes, pero su impacto es menor a corto plazo.

Identificación de procesos de negocio soportados por sistemas de información

Actividad (solución posible)

Cálculo del coste de no realizar las funciones:

Venta de libros:

1 hora: Pérdida de ventas directas, clientes insatisfechos, daño a la reputación.
1 día: Pérdidas significativas, mayor insatisfacción, impacto en la imagen del negocio.
1 semana: Pérdidas considerables, riesgo de perder clientes, daño a la rentabilidad.
2 o más semanas: Crisis financiera, posible cierre del negocio.

Presentación de impuestos a Hacienda:

1 hora: Retraso en la presentación, posible multa.
1 día: Multa considerable, riesgo de sanción mayor.
1 semana: Multa significativa, posible suspensión de actividades.
2 o más semanas: Multa grave, cierre del negocio.

Pedidos de material:

1 hora: Posible falta de stock para algunos libros, ventas perdidas.
1 día: Mayor falta de stock, insatisfacción de clientes.
1 semana: Impacto en la variedad de libros, pérdida de clientes potenciales.
2 o más semanas: Dificultad para mantener el negocio operativo.

Identificación de procesos de negocio soportados por sistemas de información

Actividad (solución posible)

Alternativas para reanudar las funciones:

Venta de libros:
Implementar un sistema de venta online temporal.
Ofrecer pedidos por teléfono o correo electrónico.
Habilitar un punto de venta alternativo (kiosco, mercado).

Presentación de impuestos a Hacienda:
Contactar con un asesor fiscal para resolver el problema.
Solicitar una prórroga para la presentación.
Buscar ayuda financiera para pagar la multa.

Pedidos de material:
Contactar con proveedores alternativos para obtener libros.
Priorizar los pedidos de libros más vendidos.
Buscar soluciones de impresión bajo demanda.

Identificación de procesos de negocio soportados por sistemas de información

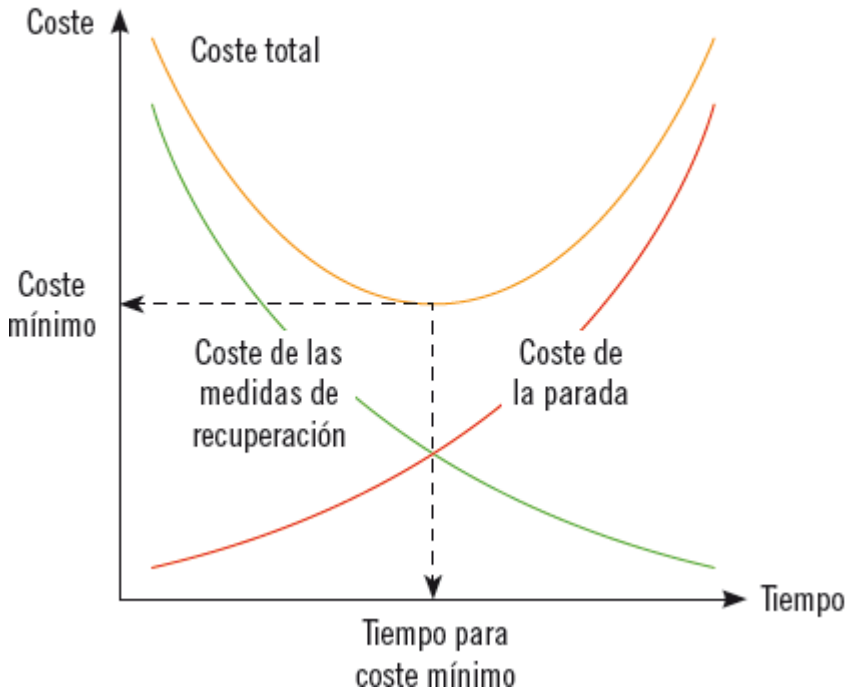
Metodologías para identificar procesos de negocio

(Reuniones 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.

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



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

Valoración de los Requerimientos de Seguridad (Confidencialidad, Integridad y disponibilidad)

La fiabilidad o seguridad se basa en tres principios esenciales: confidencialidad, integridad y disponibilidad de la información.

- Confidencialidad: la información solo debe ser accesible para quienes estén autorizados.
- Integridad: la información debe ser exacta y completa, solo modificable por personal autorizado.
- Disponibilidad: la información debe estar accesible cuando sea necesaria para su uso.

Estos principios, conocidos como **la triada de la seguridad o CIA**, resumen los objetivos de seguridad.

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

Valoración de los Requerimientos de Seguridad

Evaluación de Salvaguardas

Es crucial evaluar las necesidades específicas de cada proceso de negocio en términos de confidencialidad, integridad y disponibilidad.

Las salvaguardas óptimas pueden variar según el nivel de cada requisito de seguridad.

Por ejemplo, para garantizar la confidencialidad de las nóminas, una salvaguarda efectiva puede ser mantener copias cifradas en un servidor externo, pero su efectividad dependerá del nivel de seguridad requerido para acceder a esos datos. O algo así!!!!

La evaluación cuidadosa de las salvaguardas garantiza una protección integral de la información y minimiza los riesgos de seguridad en los procesos de negocio.

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

Valoración de los Requerimientos de Seguridad (CIA)

Es esencial evaluar los requisitos de confidencialidad, integridad y disponibilidad de los procesos de negocio para determinar las salvaguardas adecuadas.

Por ejemplo, la misma salvaguarda puede ser válida para garantizar la integridad de los datos en un proceso, pero no necesariamente para proteger su confidencialidad, lo que resalta la importancia de evaluar cada requisito por separado.

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

Procesos

Un proceso se define como el conjunto de fases sucesivas de un fenómeno natural o de una operación artificial.

En el contexto empresarial, un proceso de negocio representa las actividades realizadas para generar un producto o servicio.

Un proceso involucra tres elementos principales: personas, equipos (que incluyen aplicaciones) e información.

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

Procesos

Relaciones en un Proceso

En el procesamiento automático de la información, se encuentran personas que utilizan equipos con información de entrada para generar información de salida.

En la fabricación de un producto, el proceso se relaciona con la información de los sistemas informáticos de control de las máquinas.

Para la prestación de un servicio, el proceso termina con el conjunto de información necesario para su ejecución.

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

Procesos

Valoración de la Seguridad en los Procesos

La valoración de los requisitos de seguridad de un proceso comienza con la evaluación de los requisitos de información que genera.

La seguridad de un proceso se determina por la importancia y sensibilidad de la información involucrada en su ejecución.

Cuando no es posible valorar la información resultante, se requiere emplear otro enfoque para evaluar la seguridad del proceso.

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

Valoración CIA de la información

La importancia de la información varía en una empresa, por lo que es crucial clasificarla y asignar recursos adecuados para su protección.

El propietario de la información es responsable de clasificarla, y esta clasificación debe revisarse anualmente.

La información se clasifica en confidencial, interna y pública, según su importancia y el daño que su difusión sin control podría causar a la empresa.

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

Valoración CIA de la información

Es esencial evaluar los requisitos de confidencialidad, integridad y disponibilidad de los procesos de negocio para determinar las salvaguardas adecuadas.

Por ejemplo, la misma salvaguarda puede ser válida para garantizar la integridad de los datos en un proceso, pero no necesariamente para proteger su confidencialidad, lo que resalta la importancia de evaluar cada requisito por separado.

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

Valoración CIA de la información

Información Confidencial

Su difusión sin control conlleva incumplimientos legales y graves daños financieros o de imagen para la empresa.

El acceso debe basarse en la necesidad de conocer, con permisos otorgados según las funciones de cada persona y autorización del propietario.

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.

Ejemplos: contratos con clientes, datos personales protegidos por la ley, información sobre productos o servicios nuevos.

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

Valoración CIA de la información

Información Interna

Su difusión sin control no causa daños graves a la empresa, pero puede afectarla financieramente o en su imagen.

Acceso libre para empleados internos, con políticas internas establecidas.

Ejemplos: circulares internas, políticas de empresa, material formativo.

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

Valoración CIA de la información

Información Pública

Su difusión no tiene consecuencias negativas para la empresa.

Requiere calificación expresa para su difusión pública, normalmente por el área de comunicación o marketing.

Ejemplos: notas de prensa, presentaciones comerciales, publicidad.

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

Valoración CIA de la información

Determinación de Requisitos de Seguridad

Los requisitos de seguridad se determinan según el daño que la degradación de una propiedad de la información podría causar a la empresa.

Es esencial evaluar los requerimientos de confidencialidad, integridad y disponibilidad de la información para implementar medidas de seguridad adecuadas.

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

Valoración CIA de la información

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:

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.
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.

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

Valoración CIA de la información

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.

Puede tener un nivel de confidencialidad medio un directorio telefónico, o un organigrama de la empresa.

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

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

Valoración CIA de la información

La integridad se refiere a la completitud y exactitud de la información. La integridad se pierde cuando se realizan cambios no autorizados. Los criterios para determinar los requisitos de integridad de la información, podrían ser los siguientes:

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.

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

Valoración CIA de la información

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. Los periodos indicados son orientativos, y se espera que difieran de una empresa a otra:

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.

Identificación de procesos de negocio soportados por sistemas de información

Valoración CIA de la información

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.

Puede tener un nivel de confidencialidad medio un directorio telefónico, o un organigrama de la empresa.

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

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

Valoración de los procesos a partir de sus componentes

Enfoque Simple:

- El enfoque anterior se centra en evaluar los requisitos de seguridad de un proceso coincidiendo con los requisitos de su información resultante.
- En ocasiones, este enfoque puede no ser posible o conveniente.

Enfoque Componentes:

- Los requisitos de seguridad del proceso se pueden determinar a partir de los requisitos de seguridad de sus componentes: personas, información de entrada y sistemas de procesamiento.
- La seguridad del proceso es una combinación de los requisitos de seguridad de las personas, sistemas e información involucrada.

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

Valoración de los procesos a partir de sus componentes

Agregar Requisitos de Componentes:

- Para agregar los requisitos de los componentes, existen opciones cuantitativas (1,2,3,…)y cualitativas (**A**lto,**M**edio,**B**ajo)

- Puede sumarse los niveles en cada dimensión si la valoración es cuantitativa, o simplemente emplear el nivel máximo de cada componente si es cualitativa.

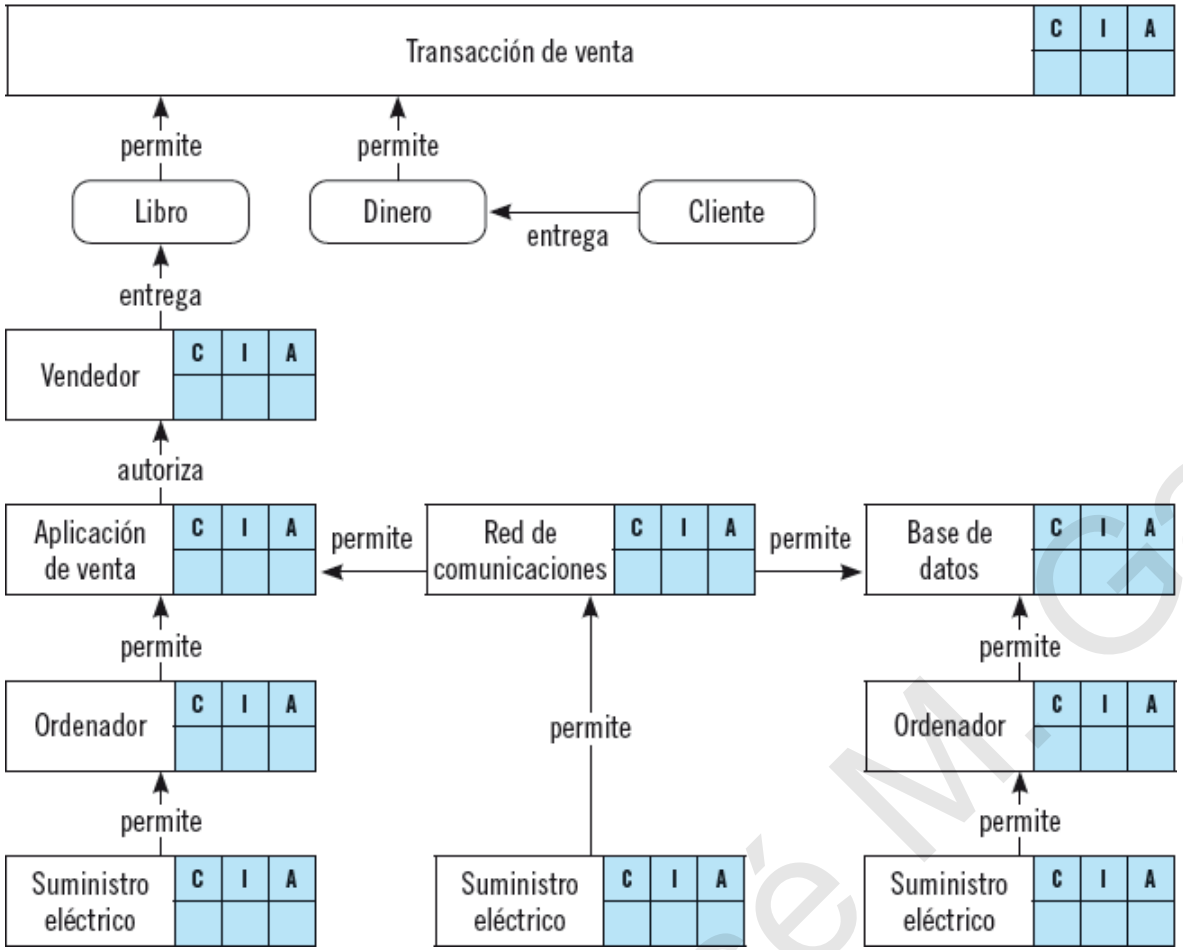
Valoración de los requerimientos de confidencialidad, integridad, y disponibilidad de los procesos de negocio

Valoración de los procesos a partir de sus componentes

Combinación de Valores:

- En ocasiones, es necesario combinar los valores de Confidencialidad (C), Integridad (I) y Disponibilidad (A) para obtener un único valor de seguridad para el proceso.
- La suma puede ser ponderada o no ponderada, dependiendo de si se desea otorgar diferentes pesos a cada dimensión.
- En valoraciones cualitativas, se suele elegir el valor máximo alcanzado en alguna de las dimensiones como representante de seguridad del proceso.

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



Cada elemento va añadiendo sus requisitos CIA según se asciende hasta el proceso final. 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.

El proceso crítico de una empresa es la venta por internet. Resumidamente, un comprador accede desde internet a la web de venta online, alojada en un servidor ubicado en la sede de la empresa. El servidor se comunica a través de un firewall con una base de datos interna, que solo sabe administrar una persona del departamento de informática. La venta tiene interrupciones breves, como sucede durante los trabajos de mantenimiento en la base de datos, que se advierten en la página web.

Los elementos del servicio y sus valoraciones CIA (bajo = 1, medio = 2, alto = 3) son:

Venta Online

SERV. WEB

Firewall

BBDD

ADM BBDD

B=1 M=2 A=3

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

En el apartado anterior se establecieron pautas para determinar los requisitos de seguridad de la información.

Otros elementos importantes en un proceso son las personas y los sistemas.

En este apartado nos enfocaremos en los requisitos de seguridad de las personas.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de las personas

- Las personas que manejan la información deben ser identificadas y sus requisitos de seguridad evaluados en las dimensiones de Confidencialidad (C), Integridad (I) y Disponibilidad (A).
- Los responsables de procesos son los encargados de identificar a las personas involucradas en ellos.
- Se pueden emplear formularios o reuniones con los dueños de los procesos para realizar esta identificación y valoración.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de las personas

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.

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.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de las personas

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.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de las personas

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.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de sistemas físicos, programas y servicios de soporte

En esta categoría, se deben clasificar los componentes que intervienen en el proceso, excluyendo a las personas y la información. Esto incluye los requisitos para:

- Equipos físicos (hardware): Esto abarca ordenadores, equipos de comunicaciones y soportes de almacenamiento como CD y discos duros extraíbles.
- Aplicaciones o programas (software): Esto incluye sistemas operativos y otras aplicaciones necesarias para el proceso.
- Servicios de soporte: Esto comprende suministro eléctrico, climatización, alojamiento y otros servicios necesarios para el funcionamiento adecuado de los equipos y aplicaciones.

Cada uno de estos componentes debe ser clasificado y evaluado en términos de sus requisitos de seguridad.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de sistemas físicos, programas y servicios de soporte

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.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de sistemas físicos, programas y servicios de soporte

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.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de sistemas físicos, programas y servicios de soporte

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 las personas
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.

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Valoración CIA de sistemas físicos, programas y servicios de soporte

Elementos en un Proceso de Negocio (necesario evaluar y protegerlos para garantiaar la continuidad y seguridad de las operaciones empresariales)

- Equipos hardware de procesamiento: Servidores, estaciones de trabajo críticas, ordenadores portátiles, dispositivos móviles (tablet-PC, PDA, smartphones), e impresoras.
- Equipos de comunicaciones de red: Router, switch, firewall, líneas de comunicaciones, centralitas telefónicas, faxes, terminales telefónicos fijos y móviles.
- Programas: Sistemas operativos, aplicaciones y utilidades, y códigos fuente de programas.
- Soportes de información: Backup de sistemas operativos y aplicaciones, backup de código fuente de programas, y backup de datos (bases de datos y archivos).
- Servicios de soporte: Sistema eléctrico y de alimentación ininterrumpida, aire acondicionado, y elementos de fijación (armarios de rack y otra mecánica).

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Herramientas de ayuda para determinar los componentes

Descripción del Proceso:

- Iniciar con una narrativa o descripción textual del proceso.
- Puede recogerse mediante formularios BIA o entrevistas.
- Para procesos complejos, dividirlos en fases o subprocesos.

Elementos a Identificar:

- Enumerar los elementos de cada tipo: personas, sistemas e información de entrada.
- Garantizar completitud: ¿qué, quién, cuándo, cómo, dónde, por qué y para qué?

Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

Herramientas de ayuda para determinar los componentes

Relación entre Componentes:

- Relacionar cada elemento con otros mediante acciones verbales.
- Establecer una jerarquía de dependencia y progreso.

Representación Gráfica:

- Graficar la estructura jerárquica con un diagrama de árbol invertido.
- Hojas: componentes; nodos intermedios: resultados o hitos; raíz: resultado final.

Esta metodología proporciona una forma sistemática de identificar y relacionar los componentes de un proceso, facilitando la comprensión de su estructura y dependencias. La representación gráfica ayuda a visualizar claramente cómo se desarrolla el proceso y cuáles son los resultados esperados.

RESUMEN

Sistema de Gestión de Seguridad de la Información (SGSI)

Objetivo del SGSI:

- Asegurar la continuidad del negocio.
- Minimizar riesgos y maximizar retorno de inversión en seguridad.

Podría permitir nuevas oportunidades para la empresa.

Análisis y Gestión de Riesgos:

- Proceso esencial para conocer riesgos.
- Punto de partida para el Business Impact Analysis (BIA).
- Permite identificar procesos críticos y áreas de enfoque.

RESUMEN

Sistema de Gestión de Seguridad de la Información (SGSI)

Resultados del BIA:

- Ordena criticidad de funciones y procesos.
- Evalúa el coste de interrupción.
- Determina estrategias de recuperación y contramedidas.

Requisitos de Seguridad:

- Confidencialidad, Integridad, Disponibilidad.
- Se evalúan a través de la información resultante o de los componentes del proceso.
- Homogeneidad en la aplicación de criterios para medir la evolución de la seguridad a lo largo del tiempo.

En este resumen se destaca la importancia del SGSI para la continuidad del negocio, detalla el proceso de análisis de riesgos y el BIA, y subraya la necesidad de criterios consistentes en la evaluación de la seguridad.