Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Análisis y gestión de riesgos

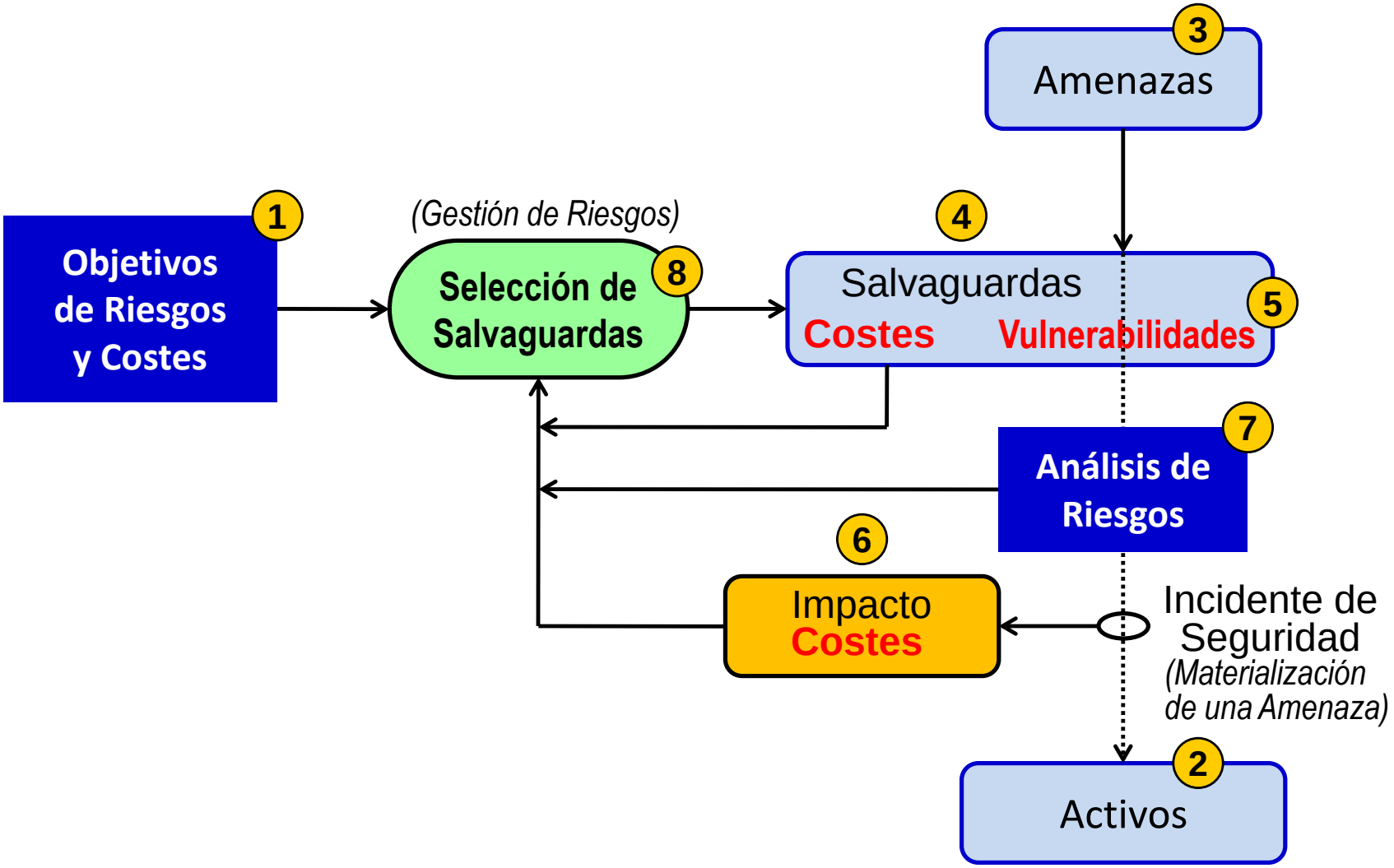
Presentación

Daniel F. García

Fases del análisis y la gestión de riesgos

1. Identificación de **objetivos y restricciones**
2. Inventariado y valoración de **activos**
3. Identificación y valoración de las **amenazas**
4. Identificación de las **medidas** de seguridad existentes
5. Identificación y valoración de **vulnerabilidades**
6. Determinar el **impacto**
7. Determinar el **riesgo**
8. Identificación y selección de las **medidas** de protección

Proceso de análisis y gestión de riesgos



Fase 1: Objetivos de riesgos y restricciones 1

Identificación de objetivos

1. Identificar lo que se espera del Plan de Seguridad
2. Analizar los objetivos estratégicos definidos en la Política de Seguridad
3. Establecer objetivos específicos cualitativos y cuantitativos referentes a un activo o grupo de activos
4. También pueden definirse objetivos en relación a los niveles de Integridad, Confidencialidad y Disponibilidad necesarios
5. Pueden identificarse fases limitando el alcance, teniendo en cuenta las restricciones identificadas

Fase 1: Objetivos de riesgos y restricciones 2

Las restricciones afectan y limitan las medidas de seguridad a implantar

Identificación de restricciones

1. **Restricciones técnicas:** Mejor implantar medidas en fase de diseño que en explotación
   Si no existen medidas, implantar alguna mediante procedimientos o seguridad física
2. **Restricciones financieras:** El coste de las medidas de seguridad no debe ser mayor que el de los activos que protegen
3. **Restricciones temporales:** Debe ser aceptable limitar el tiempo máximo para gestionar un riesgo específico
4. **Restricciones sociológicas:** Costumbres, cultura y mentalización del personal
   Aceptación de la organización → Ante la negatividad, las medidas serán inoperativas
5. **Restricciones ambientales:** Superficie y espacio disponible, entorno, etc.
6. **Restricciones legales:** Legislaciones informáticas y otras (laboral, edificios, ...)
   Suelen ser medidas impulsoras más que restricciones

Fase 2: Inventariado y valoración de activos 1

Los activos son los elementos valiosos de una organización que hay que proteger

Relación de los principales tipos de activos:

- Hardware: servidores, estaciones de trabajo, PCs portátiles, impresoras, escáneres, sistemas de back-up (discos, cintas, robot, cartuchos)
- Software: sistemas operativos, herramientas ofimáticas, software de gestión, herramientas de desarrollo, aplicaciones comerciales y propias
- Equipos de comunicaciones: routers, hubs, switches, cableados, armarios con paneles de conexiones, líneas de comunicación con el exterior
- Locales y oficinas donde se ubican los sistemas informáticos
- Personas que utilizan y se benefician directa o indirectamente del sistema
- Información: ficheros, bases de datos (Activos de Naturaleza Intangible)
- Documentación: procedimientos operativos, manuales de los sistemas, planes de contingencia
- Imagen y reputación de la organización
- Confianza de los clientes

Fase 2: Inventariado y valoración de activos 2

Valoración de activos:

El valor representa la importancia de un activo en la organización

El valor NO tiene por que ser de tipo económico (Ej. Imagen de la organización)

El método usado debe permitir la valoración
- Cualitativa (Alto, Medio, Bajo)
- Cuantitativa (Euros)

Identificar y valorar activos críticos

El valor debe incluir todos los aspectos →
- Adquisición
- Desarrollo
- Mantenimiento
- Sustitución, …

Resumen de esta fase → TABLA

Código	Nombre	Descripción	Criticidad	Coste adquisición	Coste reposición	Confidencialidad	Integridad	Disponibilidad

Otros campos → Propietario Administrador Usuarios Control_Acceso ···

Fase 3: Identificación y valoración de amenazas 1

Definición de amenaza

Una amenaza es cualquier causa potencial (accidental o intencionada) que puede ocasionar daños en un sistema informático provocando perdidas materiales, financieras, etc., a una organización

Identificación de las amenazas

Desastres naturales: Tormentas, Rayos, Terremotos, Inundaciones

Fallos de infraestructuras: Cortes de electricidad, agua, refrigeración, comunicaciones

Accidentes: Inundaciones, Incendios

Averías y fallos del SI: Hardware (Fallo de servidores, estaciones de trabajo, etc)
Software (SO, BD, Aplicaciones)
Red (LAN interna, WAN ajena, Routers)

Agentes externos: Ataques y sabotajes de organizaciones cibercriminales
Virus informáticos
Intrusos en el sistema
Robos, estafas

Agentes internos: Errores en el uso de herramientas y recursos
(Causa: Accidentales, Deliberados, Por mala formación)

Ver ISO/IEC 27005 Annex C: Examples of typical threats

Fase 3: Identificación y valoración de amenazas 2

Valoración de las amenazas

Para cada amenaza hay que identificar:

- El origen (Actor): Quién o que puede violar las salvaguardas de seguridad
- El blanco (Activo): Elementos que pueden ser afectados por la amenaza

En una fase posterior del análisis se identificará:

- La probabilidad de ocurrencia
- El impacto y las consecuencias de su ocurrencia

Hay que clasificar su importancia en 3 o 5 niveles:

- Alta, Media, Baja
- Muy Alta, Alta, Media, Baja, Muy Baja

Fase 4: Identificar la seguridad existente 1

Acciones a realizar:

- Identificar las medidas (controles) de seguridad existentes
- Conocer su grado de efectividad
- Identificar a los activos a los que se aplican
- Clasificar las medidas existentes:

  1. Medidas organizativas
  2. Medidas de seguridad física
  3. Medidas de seguridad lógica (tecnológicas)
  4. Medidas legales

- Estimar la criticidad de las medidas
- Estimar el estado de las medidas → { Bueno / Mejorable / Malo }

Fase 4: Identificar la seguridad existente 2

Medidas organizativas

- Política de seguridad
- Procedimientos, recomendaciones y normas
- Formación y concienciación del personal

Medidas de seguridad física

- Acceso a edificios y salas (vigilancia)
- Sistemas anti-intrusión → Puertas blindadas, Arcos detectores, Control de acceso (llave, tarjeta)
- Sistemas anti-incendio y anti-inundación
- Sistemas de alimentación eléctrica → Red eléctrica, Generadores, Baterías
- Aire acondicionado
- Suministro de agua para refrigeración

Fase 4: Identificar la seguridad existente 3

Medidas de seguridad lógica

- Confidencialidad de la información: cifrado en { Almacenamiento / Transmisión
- Integridad en los sistemas
- Disponibilidad: redundancia existente
- Autenticación de usuarios → { Estándar / Fuerte
- Auditorias: habilitación de registros

Medidas legales

- Identificación de la legislación aplicable
- Cumplimiento con RGPD, LSSI, y otras leyes y normas

Fase 5: Vulnerabilidades 1

Definición de vulnerabilidad

UNE-ISO 27000 Sección 2.89

Una vulnerabilidad es cualquier debilidad de un activo o de un control que puede ser explotada por una o más amenazas causar daños y producir pérdidas en la organización

Las vulnerabilidades suelen estar relacionadas con deficiencias en los sistemas físicos y lógicos

También pueden tener su origen en deficiencias de ubicación, configuración y mantenimiento

Identificación de vulnerabilidades

Primero han de identificarse las vulnerabilidades generales para la organización

Después han de identificarse las vulnerabilidades específicas para cada activo o grupo de activos inventariados
(especialmente para los identificados como críticos)

Conviene clasificar las vulnerabilidades por categorías
(Utilizando las mismas categorías que para las amenazas)

Ver ISO/IEC 27005 Annex D.1: Examples of vulnerabilities

Fase 5: Vulnerabilidades 2

Valoración de vulnerabilidades

Hay que evaluar la importancia de cada vulnerabilidad

- Identificando si existe una medida de protección contra ella y
- Evaluando la eficacia de la medida cuando existe

Conviene ampliar el estudio con pruebas

- Test de intrusión (hacking ético) interno y externo
- Ingeniería social

Establecer tres o cinco niveles de valoración cualitativa

- Alta, Media, Baja
- Muy Alta, Alta, Media, Baja, Muy Baja

Resumen de esta fase → TABLA

Código	Nombre	Descripción	Activo(s) a los que afecta	Importancia	Valoración	Recomendaciones

Fase 6: Evaluación del impacto 1

Un **incidente de seguridad** es cualquier evento que produce:

- Pérdidas físicas de activos o financieras y/o
- La interrupción de los servicios suministrados por el sistema informático

Generalmente, un incidente es la materialización de una amenaza

---

El **impacto** es la medición o valoración de las consecuencias (daños, pérdidas) que se derivan de un incidente de seguridad

Considerar los daños en activos → { Tangibles; Intangibles (incluye la información) }

Hay que realizar entrevistas con los responsables de cada { Departamento; Función; Proceso }
para que ayuden a determinar el impacto real de los incidentes

La valoración del impacto sirve para seleccionar las medidas de protección de modo racional ←→ La medida debe costar menos que el impacto

Fase 6: Evaluación del impacto 2

Clasificación del impacto: valoración y tipos

Valoración	Tipos de impacto
ALTO (grave)	Pérdida o destrucción de activos críticos no reparables Interrupción de los procesos de negocio Robo o revelación de información estratégica y muy confidencial Daños en la imagen y/o reputación de la organización (intangible)
MEDIO (moderado)	Pérdida o destrucción de activos críticos pero se dispone de respaldos Caída notable del rendimiento de los procesos de negocio Robo o revelación de información confidencial pero no estratégica
BAJO (leve)	Pérdida o inhabilitación de activos secundarios Disminución moderada del rendimiento de los procesos de negocio Robo o revelación de información interna no publicada

Fase 7: Análisis de riesgos 1

Definición de riesgo

El riesgo es la posibilidad de que una amenaza aproveche una vulnerabilidad del sistema causando un determinado impacto en la organización

Se mide en términos de una combinación de la probabilidad de un evento y su consecuencia

El nivel de riesgo depende de
- Las amenazas
- Las vulnerabilidades
- El impacto de las amenazas

- Amenaza SIN Vulnerabilidad NO IMPLICA riesgo
- Vulnerabilidad SIN Amenaza NO IMPLICA riesgo
- SI una Amenaza explotando una Vulnerabilidad NO GENERA impacto NO ES NECESARIO mejorar las medidas de seguridad

Tipos de estimaciones del riesgo

1. Inherente: estimado sin tener en cuenta las medidas de protección existentes
2. Actual: estimado teniendo en cuenta las medidas de protección existentes
3. Residual: estimado teniendo en cuenta las medidas de protección existentes Y las nuevas medidas planificadas

Las diferencias entre 1, 2 y 3 indican la efectividad de las medidas de protección

Fase 7: Análisis de riesgos 2

Clasificación cualitativa de las probabilidades

Para amenazas naturales (4 niveles)

Alta (A): 1 ocurrencia cada año
Media (M): 1 ocurrencia cada 5 años
Baja (B): 1 ocurrencia cada 10 años
Muy Baja (MB): 1 ocurrencia cada 20 años

Para amenazas accidentales o intencionadas (5 niveles)

Extremadamente Frecuente (EF): 1 cada día = 365/año
Muy Frecuente (MF): 1 cada semana = 54/año
Frecuente (F): 1 cada mes = 12/año
Frecuencia Normal (FN): 1 cada trimestre = 4/año
Poco Frecuente (PF): 1 cada año = 1/año

Metodologías de evaluación de riesgos

ISO 27005 framework de ISO
https://www.iso.org/

SP 800 30 framework de NIST
https://csrc.nist.gov/pubs/sp/800/30/r1/final

Risk IT framework de ISACA
https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2

MAGERIT Utilizada en la administración pública española
Metodología de Análisis y Gestión de Riesgos de los SI
https://pilar.ccn-cert.cni.es/

Fase 8: Selección de medidas 1

Definición de medida de seguridad

Una defensa, salvaguarda, control, o medida de seguridad es cualquier medio empleado para eliminar o reducir un riesgo

Objetivos:

1. Reducir las vulnerabilidades de los activos
2. Reducir la probabilidad de ocurrencia de las amenazas
3. Reducir el nivel del impacto en la organización

Clasificación de las medidas de seguridad

- **ACTIVAS:** Cualquier medida utilizada para anular o reducir el riesgo de una amenaza
  - **Medidas de prevención** Se aplican ***antes*** del incidente
    - Ej. La autenticación de usuarios, el control de accesos a los recursos, el cifrado de datos sensibles, la formación de los usuarios, etc.
  - **Medidas de detección** Se aplican ***durante*** el incidente
    - Ej. Los Sistemas de Detección de Intrusiones (IDS), los antivirus, los cortafuegos, etc.
- **PASIVAS:** Cualquier medida utilizada para reducir el impacto de un incidente
  - **Medidas de corrección** Se aplican ***después*** del incidente
    - Ej. las copias de seguridad, el plan de respuesta a incidentes y de continuidad del negocio

Fase 8: Selección de medidas 2

Otra clasificación de las medidas de seguridad

- **FÍSICAS:** Medidas para controlar el acceso físico a los recursos y las condiciones ambientales en las que se utilizan los recursos
- **LÓGICAS:** Proporcionan protección mediante herramientas y técnicas informáticas (autenticar usuarios, controlar el acceso a ficheros, cifrar datos)

Proceso de selección de medidas

- Inicialmente definir una lista de medidas de seguridad lo más amplia posible (sin restricciones)
- Identificar las medidas existentes, evaluando su mejora si fuese necesaria
- Las medidas han de abarcar y considerar todos los aspectos:

Organizativos:	Políticas, procedimientos, documentación
Técnicos:	Hardware, software, comunicaciones
Humanos:	Formación y concienciación del personal
Legislativos:	Cumplimiento de la legislación vigente

- **Usar estándares** internacionales (ISO) que definen una relación de controles de seguridad
- Seleccionar finalmente en función de los objetivos pero respetando las restricciones
- Considerar que tras la selección hay que IMPLANTAR y VERIFICAR las medidas

Fase 8: Selección de medidas 3

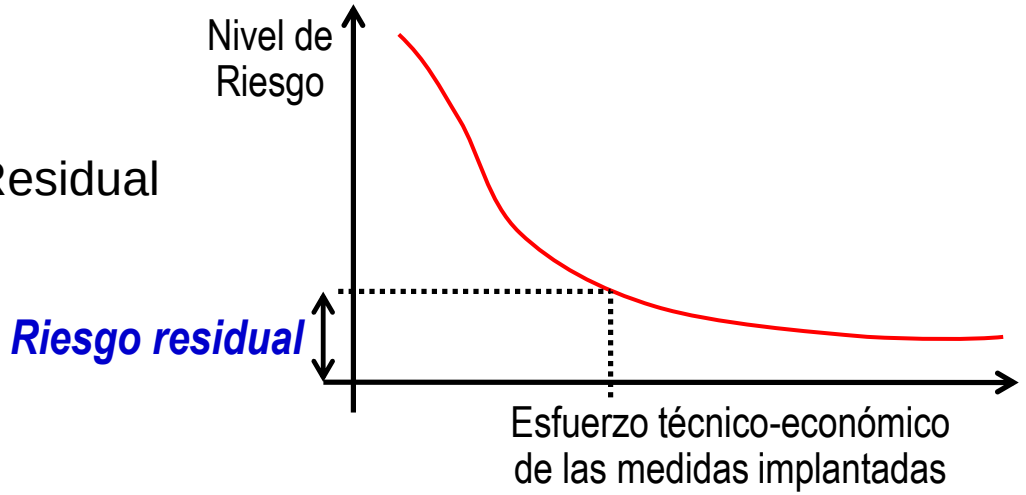
Tras la correcta implantación …

La organización debe determinar el "*nivel de riesgo residual*"

Realizando un nuevo proceso de evaluación de riesgos que considera las nuevas medidas

SI (Riesgo residual > Objetivo de riesgo) para algún activo
Seleccionar medidas de seguridad adicionales y repetir el proceso

Tras múltiples repeticiones
Siempre queda un Riesgo Residual



Nivel de riesgo residual == Nivel de riesgo que una organización está dispuesta a asumir
(Porque no es viable técnica/económicamente reducir más el riesgo)

Establecer un compromiso: Riesgo ←→ Esfuerzo

Fase 8: Selección de medidas 4

Reevaluación

Es recomendable hacer nuevas evaluaciones del riesgo de forma periódica

- Para contemplar cambios en el sistema …
  - La integración de nuevos recursos y aplicaciones
  - La puesta en marcha de nuevos servicios
  - Incorporación de nuevo personal, etc.
- Para considerar nuevas vulnerabilidades …
  - Nuevos fallos detectados en las aplicaciones informáticas
- Para considerar nuevas amenazas

Considerar la externalización

Se puede contratar una empresa que proporcione los servicios de seguridad informática

Modalidad de gestión de la seguridad → Servicio de seguridad gestionado
Managed Security Services (MSS)

Planteamiento similar al de la seguridad física → empresa encargada de vigilar instalaciones

Considerar si la externalización mejora la gestión de la seguridad y/o reduce sus costes

Ejercicio – Análisis de riesgos

Activos (inventario en una tabla)		C	I	A
1) Servidor de Ficheros	Valor:	1000€ Muy Bajo	10000€ Muy Alto	5000€ Medio
	frecuencia	degradación del valor		
A1 Robo info por hacker	4 veces/año	100%	0%	0%
C1 Cifrado comunicaciones	Eficacia red frecuencia	Eficacia reduciendo degradación (impacto)		
C2 Contraseña autenticación	0,9	0	0	0
Impacto = Valor x Degradación x (1-EficaciaRI) →		1000	0	0
Riesgo = Impacto x Frecuencia x (1-EficaciaRF) →		400	0	0
	frecuencia	degradación del valor		
A2 Fallo HW (disco)	2 veces/año	0%	100%	100%
C1 Copia de seguridad	Eficacia red frecuencia	Eficacia reduciendo degradación (impacto)		
	0	0	0,8	0,9
Impacto = Valor x Degradación x (1-EficaciaRI) →		0	2000	500
Riesgo = Impacto x Frecuencia x (1-EficaciaRF) →		0	4000	1000

Frecuencia efectiva: 4 x (1-0,9) = 0,4 veces/año

Frecuencia efectiva: 2 x (1-0) = 2 veces/año

2) Otro activo …

Ejercicio – Análisis de riesgos

Cada activo sufre N amenazas

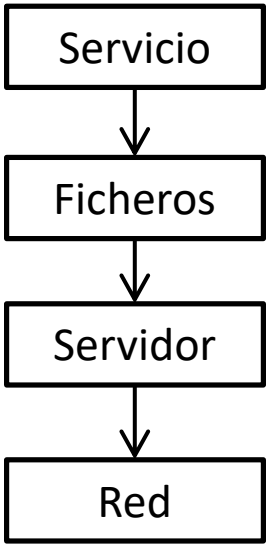
¿Cuál es el riesgo total que sufre el activo?

Opción 1: Sumar todos los riesgos en cada dimensión

Opción 2: Quedarse con el mayor riesgo en cada dimensión

Dependencias entre activos

En el método elemental previo se analiza cada activo independientemente de los otros



Pero en la realidad hay dependencias
Suelen modelarse mediante grafos

Ej. Si el servidor es atacado queda inoperativo …
NO se puede proporcionar el servicio