sedian

Seguridad Digital
de Andalucía

Webinar

Análisis de Impacto en el Negocio (BIA)

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

Índice de contenidos

Índice de contenidos

La creciente dependencia tecnológica

La disponibilidad de los recursos TI. Factor clave en el negocio

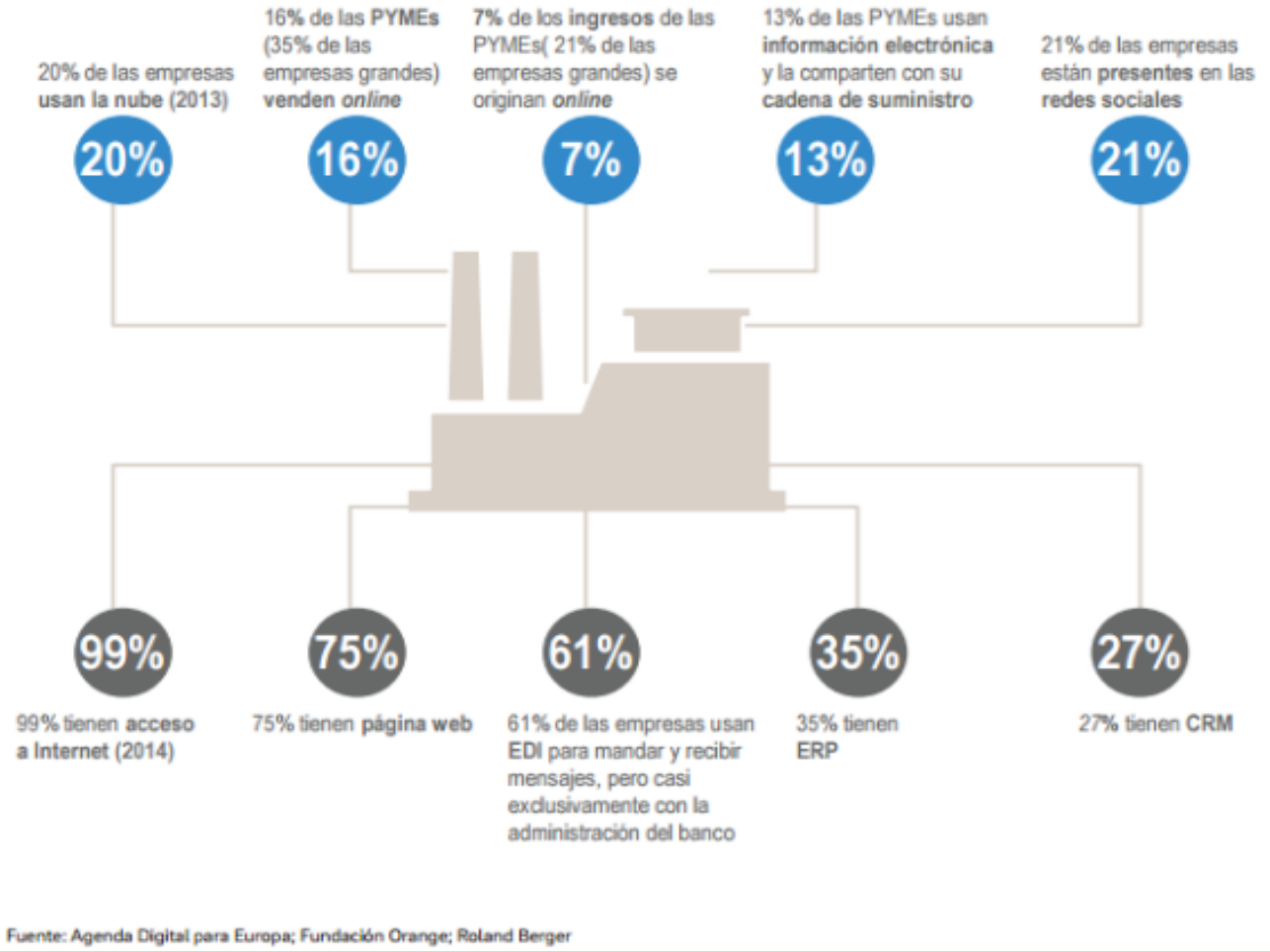
Hoy día las actividades de la Organización se apoyan fuertemente en los Sistemas de Información y en los datos que contienen, siendo, por lo tanto, la información en formato digital uno de los principales activos del negocio.

Por lo tanto, **la disponibilidad de esta información**, a través de los recursos tecnológicos que la almacenan, procesan o transportan es un factor clave para la disponibilidad de los servicios y operaciones presentados por la empresa y, por ende, para su propia supervivencia.

La creciente dependencia tecnológica

La transformación digital

Cartografía de las empresas españolas en lo que respecta a la transformación digital



Fuente: Agenda Digital para Europa; Fundación Orange; Roland Berger

Índice de contenidos

El impacto por indisponibilidad tecnológica

El impacto por indisponibilidad tecnológica

Los agentes de las amenazas más significativos durante 2018, la tipología de sus acciones y sus víctimas reflejan que la disponibilidad y la integridad (como principales dimensiones habilitantes de la continuidad) están afectadas por las amenazas más significativas.

(fuente: Informe de amenazas y tendencias del CCN)

AMENAZAS:

- Interrupción del servicio
- Sabotaje
- Manipulación de la información
- Manipulación de sistemas

Índice de contenidos

Análisis de Impacto del Negocio

Definiciones

BIA	• *Business Impact Analysis.* Tiene como principal objetivo identificar las consecuencias que un incidente en los sistemas, infraestructuras o comunicaciones de la organización tendría sobre el negocio de la misma.
RTO	• *Tiempo de Recuperación Objetivo*. Indica el lapso de tiempo máximo, tras un incidente, que un activo determinado puede estar indisponible para que el impacto sea aceptable.
RPO	• *Punto de Recuperación Objetivo.* Indica el máximo periodo de tiempo durante el cual sería admisible una pérdida de datos debido a un incidente. En otras palabras, se trata de un parámetro que fija la frecuencia de realización de *backup* de datos.
DRP	• *Disaster Recovery Plan.* Se trata de una estrategia de restablecimiento de los procesos e infraestructura TI ante cualquier eventualidad o desastre.
BCP	• *Business Continuity Plan.* Se trata de garantizar que las operaciones tengan continuidad pese a una contingencia.

Análisis de Impacto del Negocio

¿Qué es el BIA y cuál es el objetivo que persigue?

- Se trata del **Análisis de Impacto en el Negocio** que un **incidente disruptivo** en los sistemas, infraestructuras o comunicaciones de la Organización tendría sobre el negocio de la misma
- Se satisface el control **"op.cont.1"** del Esquema Nacional de Seguridad
- Determinar las plataformas de negocio más críticas (sistemas de información) , de forma que se identifiquen aquéllas que deban estar necesariamente respaldadas.
- Evaluar el impacto en el negocio que tendría una disrupción en cada una de las plataformas críticas, en función del tiempo de interrupción.
- Determinar la mejor estrategia de respaldo de aplicaciones, en base al tiempo que los sistemas de información pueden estar no-disponibles antes de que el negocio se vea afectado severamente.

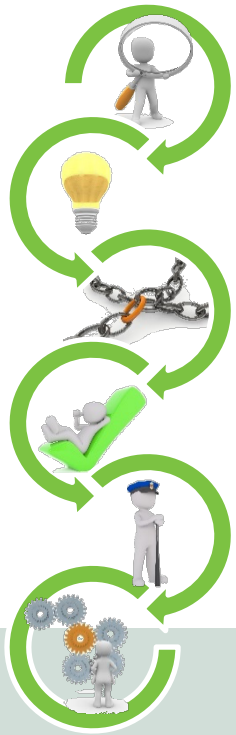
Análisis de Impacto del Negocio

¿Qué es el BIA y cuál es el objetivo que persigue?

- El BIA constituye el **primer paso para la elaboración de un Plan de Continuidad del Negocio,** el cual debe:
- Identificar las **acciones necesarias a realizar para que los procesos de negocio puedan mantenerse operativos**, con la menor degradación posible, en caso de que un incidente severo afectara a todas o parte de las infraestructuras TIC y restablecer la normalidad en el menor tiempo posible.

Análisis de Impacto del Negocio

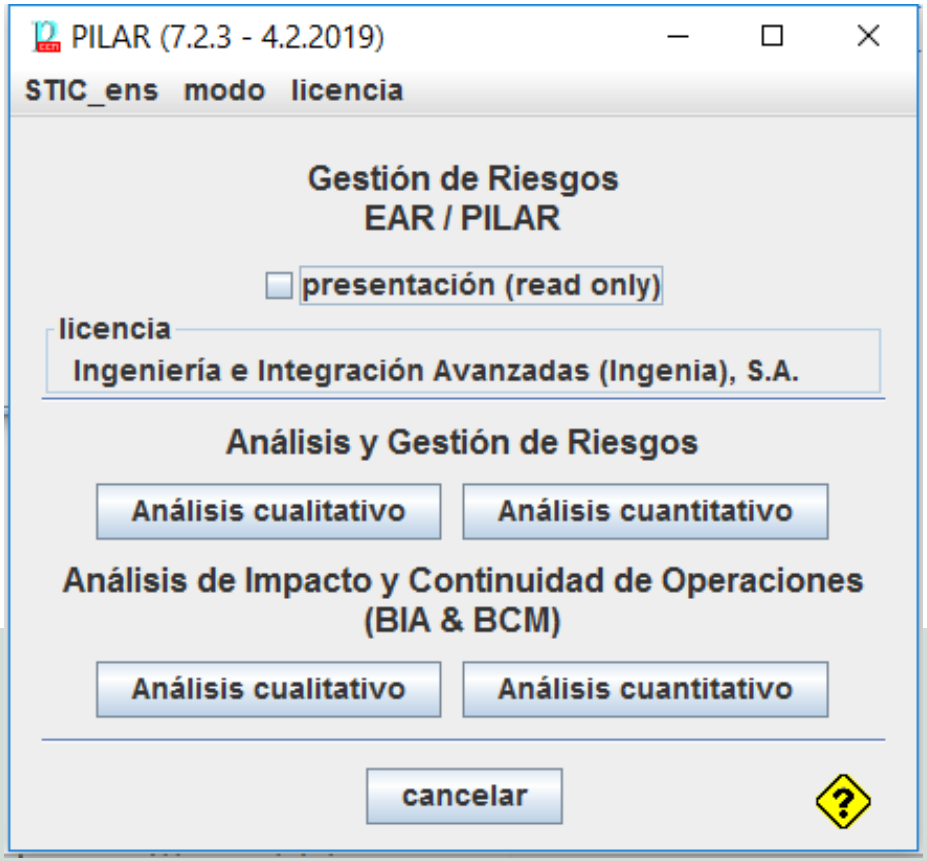
¿Cómo lo hacemos? Pasos del proceso

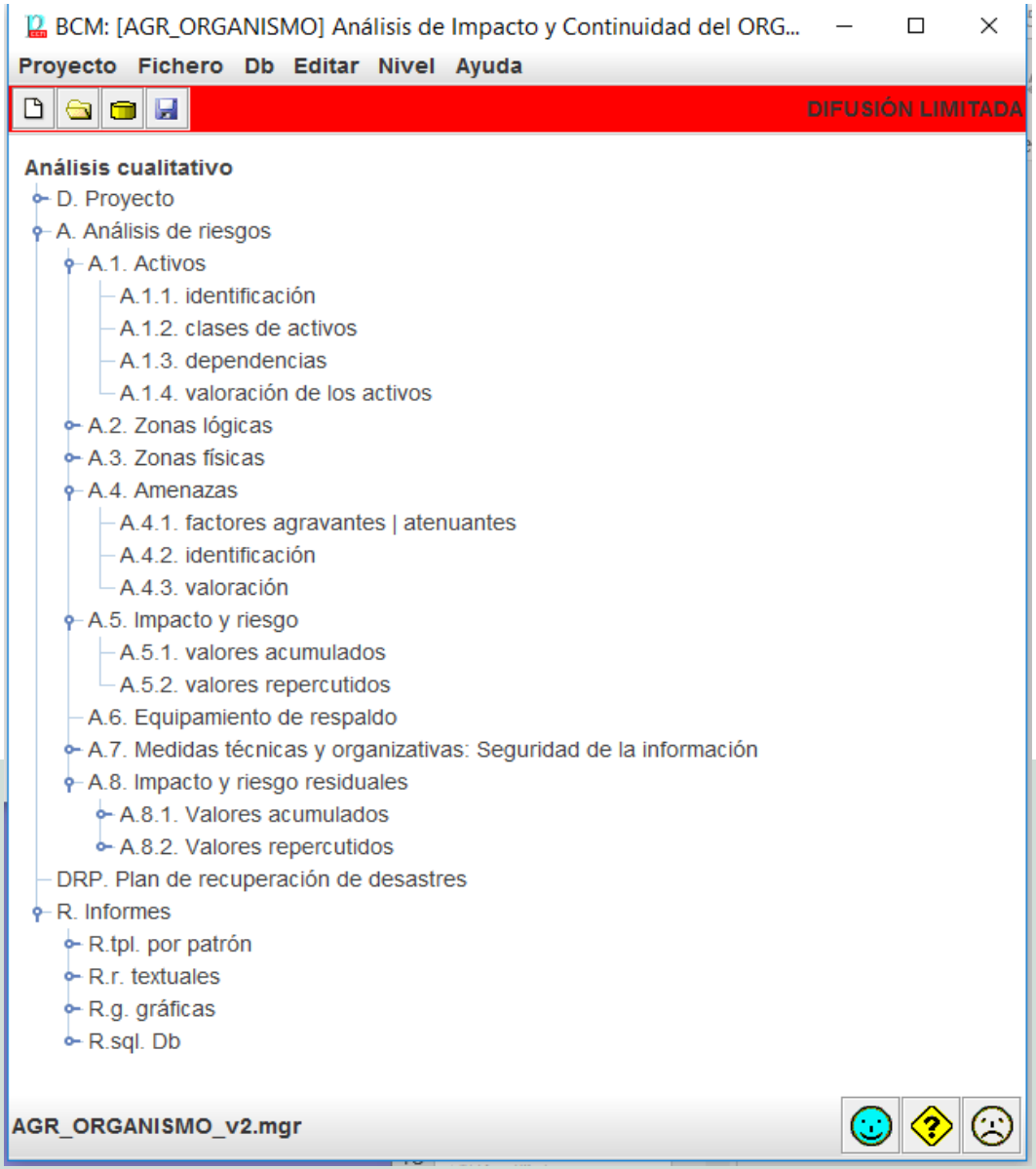


1. Identificación de los servicios	**Realizado durante el análisis de riesgos del Plan de Adecuación al ENS**
2. Valoración de los servicios en escalones temporales	**Alineado con la valoración en la disponibilidad**
3. Identificación de los activos dependientes	**Realizado durante el análisis de riesgos del Plan de Adecuación al ENS**
4. Análisis de impacto y riesgos y gestión	**Se realizará el análisis de impactos y riesgos por continuidad**
5. Estrategia de Respaldo frente a desastres	**Realizado en el proceso de conformación del BIA, se determinará el escalón de interrupción y la estrategia de recuperación**

Análisis de Impacto del Negocio

¿Cómo lo hacemos? Uso de PILAR

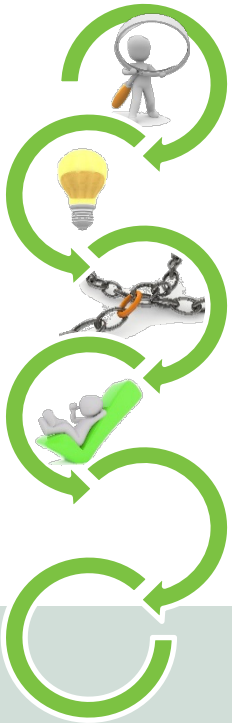




sedian Seguridad Digital de Andalucía

Análisis de Impacto del Negocio

¿Cómo lo hacemos? Pasos del proceso



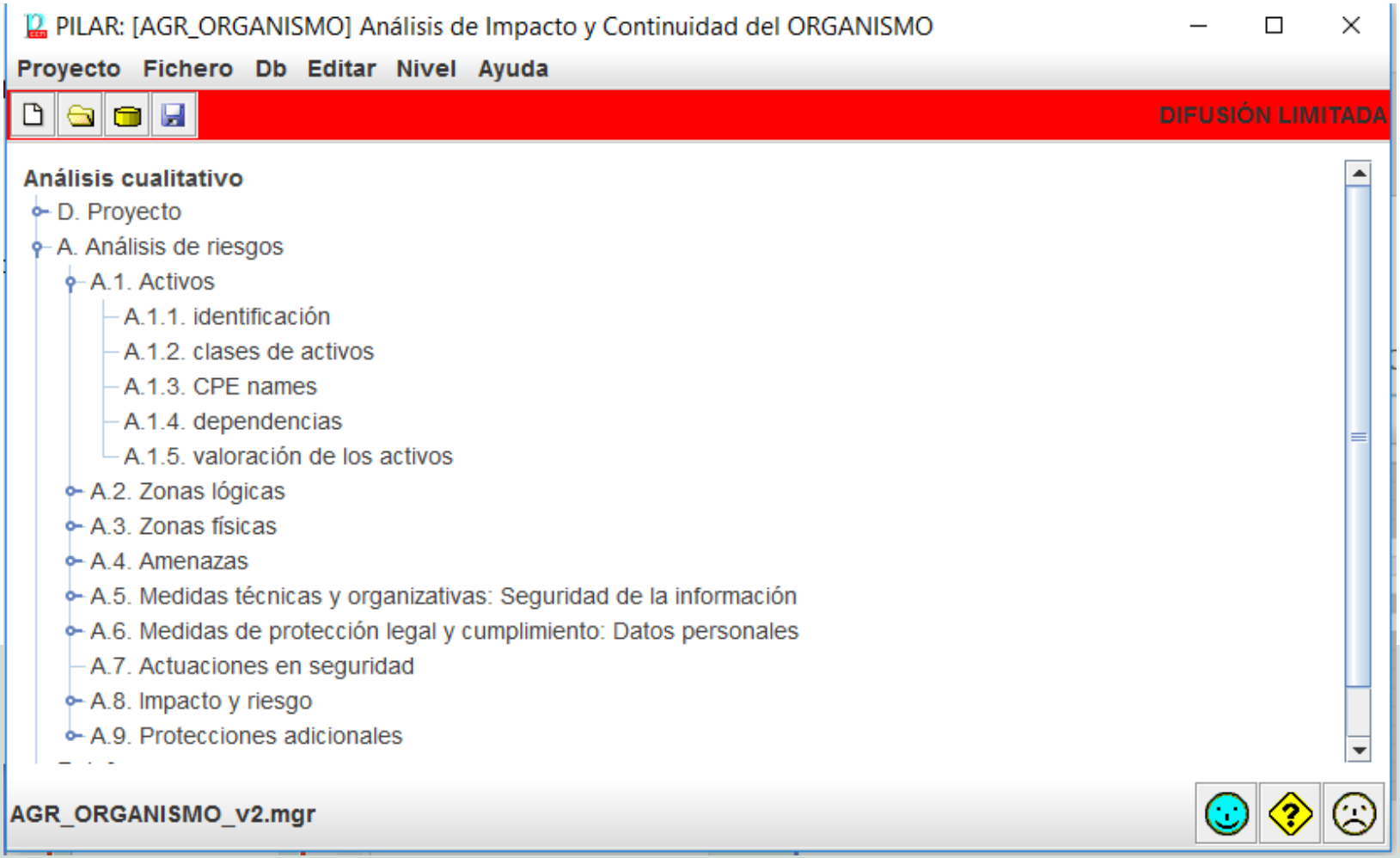
1. **Identificación de los servicios**
2. **Valoración de los servicios**
3. **Dependencias**

Para cada uno de los servicios se valora con su responsable que impacto tendría un incidente de seguridad sobre el mismo en distintos escalones temporales. Se establecen dependencias

Disponibilidad [D
¿Cómo de importante es que un activo no esté disponible?¿Se puede seguir operando con normalidad? ¿Se ve alterado el servicio?

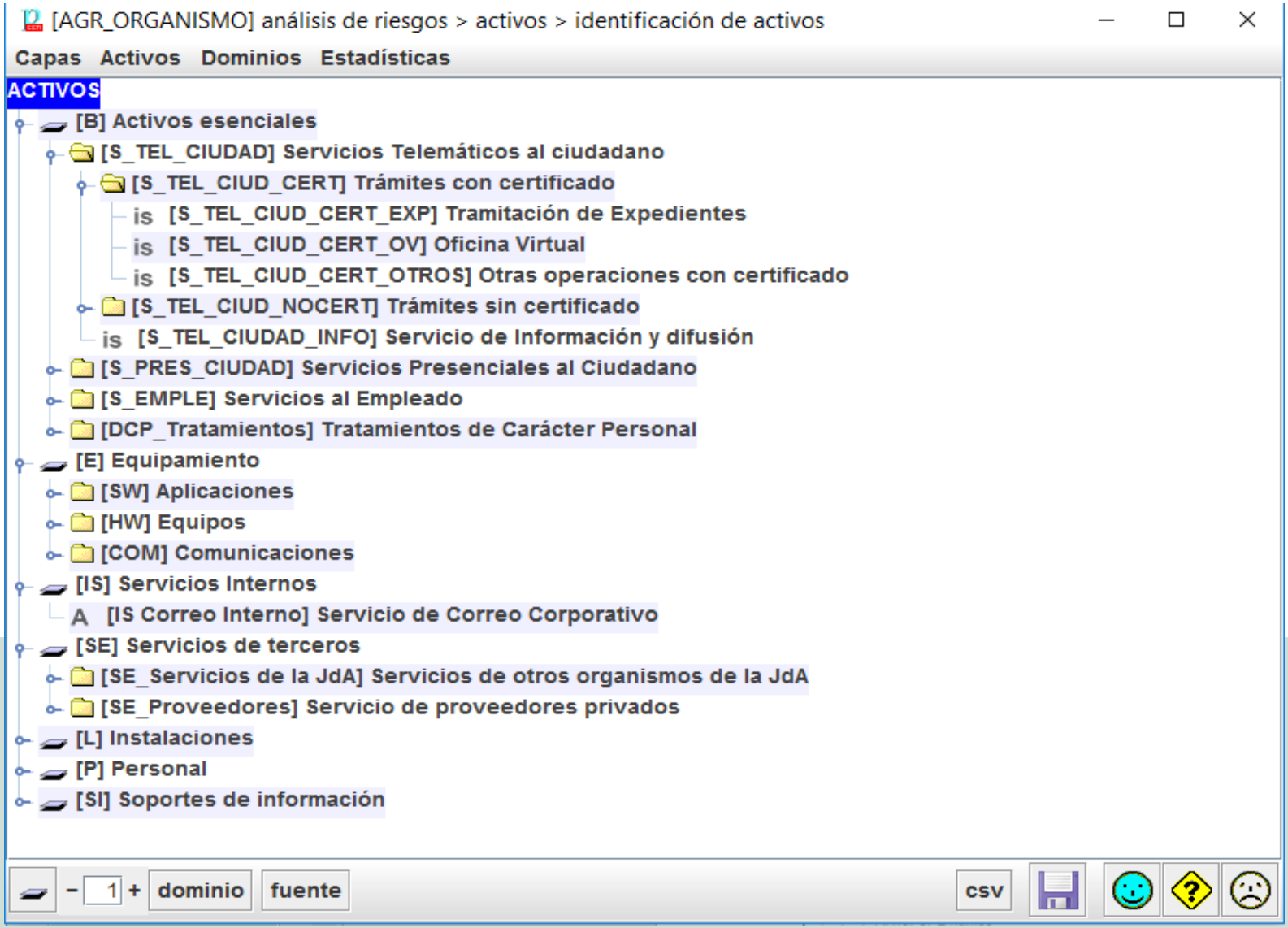
Análisis de Impacto del Negocio

Pasos del proceso. Identificación y valoración de activos



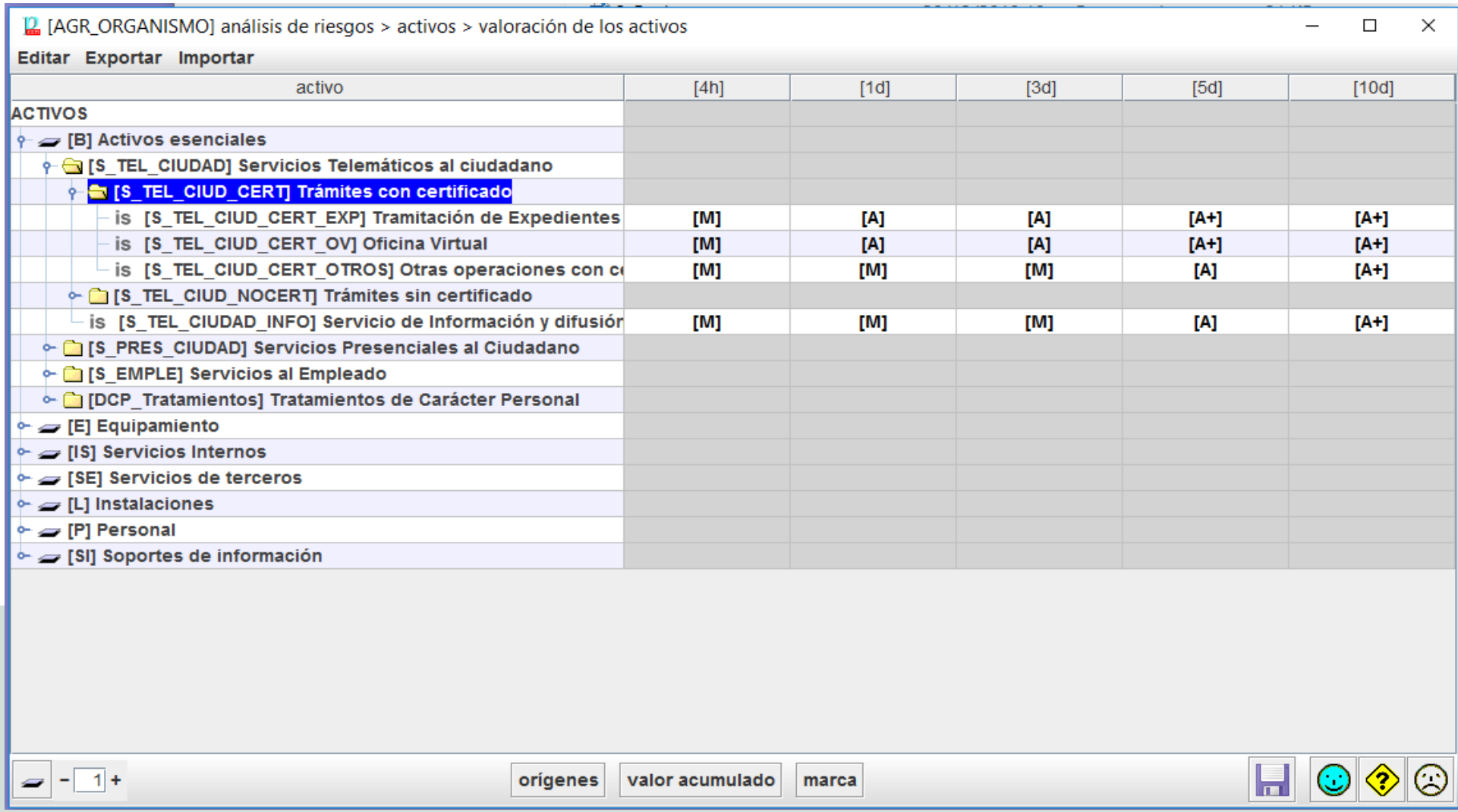
Análisis de Impacto del Negocio

Pasos del proceso. Identificación y valoración de activos



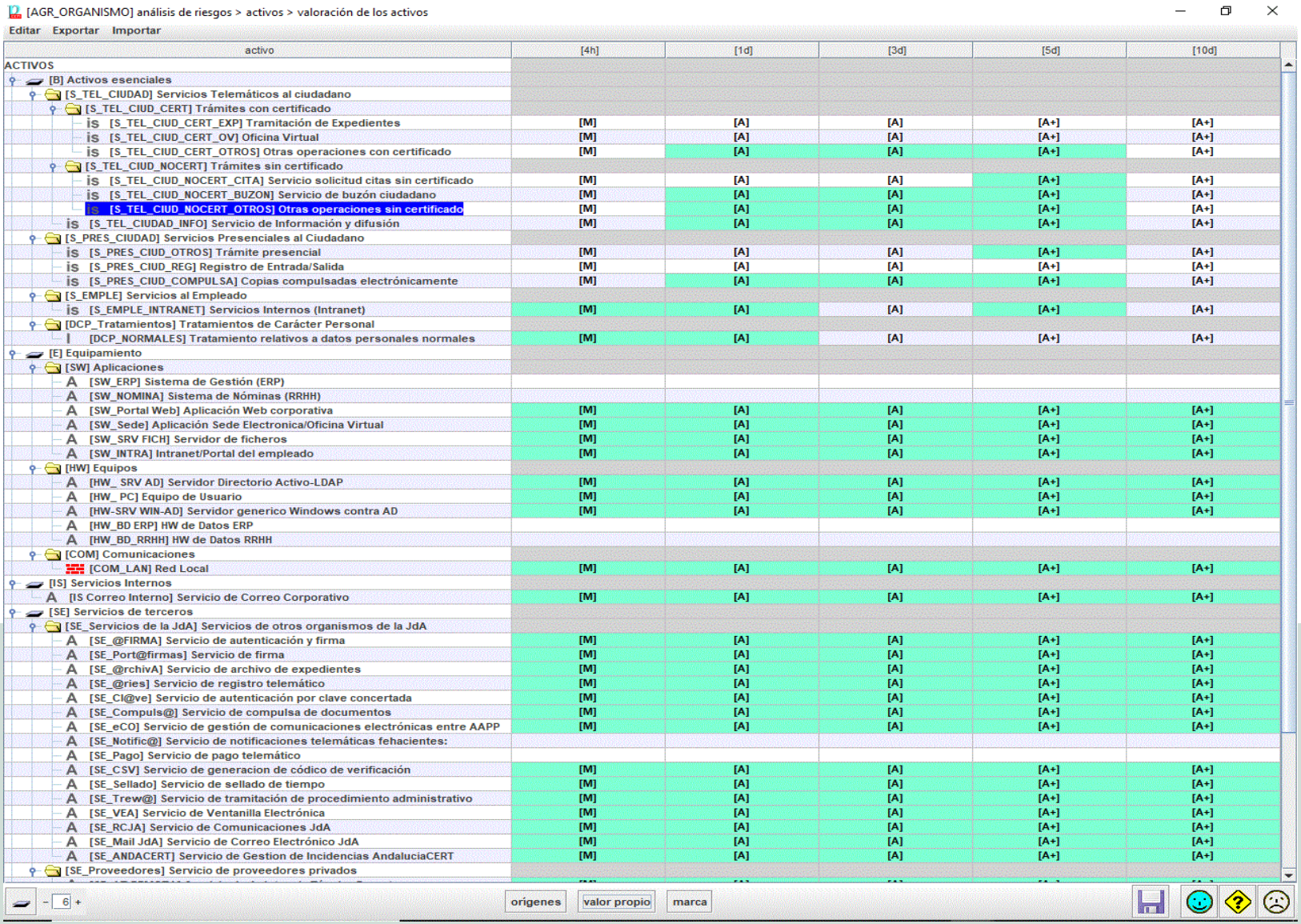
Análisis de Impacto del Negocio

Pasos del proceso. Identificación y valoración de activos



Análisis de Impacto del Negocio

Pasos del proceso. Identificación y valoración de activos

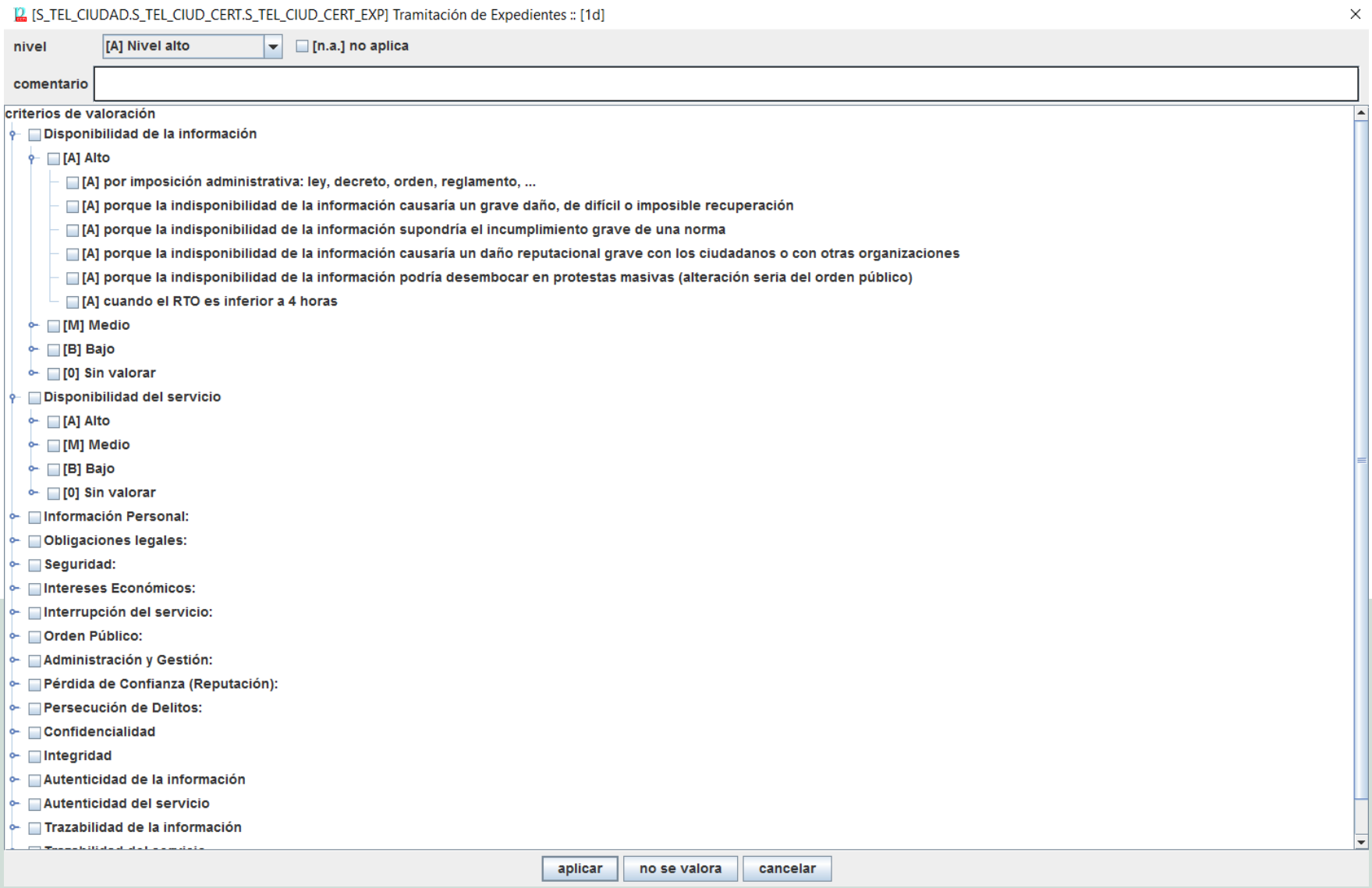


activo	[4h]	[1d]	[3d]	[5d]	[10d]
ACTIVOS					
[B] Activos esenciales					
[S_TEL_CIUDAD] Servicios Telemáticos al ciudadano					
[S_TEL_CIUD_CERT] Trámites con certificado					
[S_TEL_CIUD_CERT_EXP] Tramitación de Expedientes	[M]	[A]	[A]	[A+]	[A+]
[S_TEL_CIUD_CERT_OV] Oficina Virtual	[M]	[A]	[A]	[A+]	[A+]
[S_TEL_CIUD_CERT_OTROS] Otras operaciones con certificado	[M]	[A]	[A]	[A+]	[A+]
[S_TEL_CIUD_NOCERT] Trámites sin certificado					
[S_TEL_CIUD_NOCERT_CITA] Servicio solicitud citas sin certificado	[M]	[A]	[A]	[A+]	[A+]
[S_TEL_CIUD_NOCERT_BUZON] Servicio de buzón ciudadano	[M]	[A]	[A]	[A+]	[A+]
[S_TEL_CIUD_NOCERT_OTROS] Otras operaciones sin certificado	[M]	[A]	[A]	[A+]	[A+]
[S_TEL_CIUDAD_INFO] Servicio de Información y difusión	[M]	[A]	[A]	[A+]	[A+]
[S_PRES_CIUDAD] Servicios Presenciales al Ciudadano					
[S_PRES_CIUD_OTROS] Trámite presencial	[M]	[A]	[A]	[A+]	[A+]
[S_PRES_CIUD_REG] Registro de Entrada/Salida	[M]	[A]	[A]	[A+]	[A+]
[S_PRES_CIUD_COMPULSA] Copias compulsadas electrónicamente	[M]	[A]	[A]	[A+]	[A+]
[S_EMPLE] Servicios al Empleado					
[S_EMPLE_INTRANET] Servicios Internos (Intranet)	[M]	[A]	[A]	[A+]	[A+]
[DCP_Tratamientos] Tratamientos de Carácter Personal					
[DCP_NORMALES] Tratamiento relativos a datos personales normales	[M]	[A]	[A]	[A+]	[A+]
[E] Equipamiento					
[SW] Aplicaciones					
[SW_ERP] Sistema de Gestión (ERP)					
[SW_NOMINA] Sistema de Nóminas (RRHH)					
[SW_Portal Web] Aplicación Web corporativa	[M]	[A]	[A]	[A+]	[A+]
[SW_Sede] Aplicación Sede Electronica/Oficina Virtual	[M]	[A]	[A]	[A+]	[A+]
[SW_SRV FICH] Servidor de ficheros	[M]	[A]	[A]	[A+]	[A+]
[SW_INTRA] Intranet/Portal del empleado	[M]	[A]	[A]	[A+]	[A+]
[HW] Equipos					
[HW_ SRV AD] Servidor Directorio Activo-LDAP	[M]	[A]	[A]	[A+]	[A+]
[HW_ PC] Equipo de Usuario	[M]	[A]	[A]	[A+]	[A+]
[HW-SRV WIN-AD] Servidor generico Windows contra AD	[M]	[A]	[A]	[A+]	[A+]
[HW_BD ERP] HW de Datos ERP					
[HW_BD_RRHH] HW de Datos RRHH					
[COM] Comunicaciones					
[COM_LAN] Red Local	[M]	[A]	[A]	[A+]	[A+]
[IS] Servicios Internos					
[IS Correo Interno] Servicio de Correo Corporativo	[M]	[A]	[A]	[A+]	[A+]
[SE] Servicios de terceros					
[SE_Servicios de la JdA] Servicios de otros organismos de la JdA					
[SE_@FIRMA] Servicio de autenticación y firma	[M]	[A]	[A]	[A+]	[A+]
[SE_Port@firmas] Servicio de firma	[M]	[A]	[A]	[A+]	[A+]
[SE_@rchivA] Servicio de archivo de expedientes	[M]	[A]	[A]	[A+]	[A+]
[SE_@ries] Servicio de registro telemático	[M]	[A]	[A]	[A+]	[A+]
[SE_Cl@ve] Servicio de autenticación por clave concertada	[M]	[A]	[A]	[A+]	[A+]
[SE_Compuls@] Servicio de compulsa de documentos	[M]	[A]	[A]	[A+]	[A+]
[SE_eCO] Servicio de gestión de comunicaciones electrónicas entre AAPP	[M]	[A]	[A]	[A+]	[A+]
[SE_Notific@] Servicio de notificaciones telemáticas fehacientes:					
[SE_Pago] Servicio de pago telemático					
[SE_CSV] Servicio de generacion de código de verificación	[M]	[A]	[A]	[A+]	[A+]
[SE_Sellado] Servicio de sellado de tiempo	[M]	[A]	[A]	[A+]	[A+]
[SE_Trew@] Servicio de tramitación de procedimiento administrativo	[M]	[A]	[A]	[A+]	[A+]
[SE_VEA] Servicio de Ventanilla Electrónica	[M]	[A]	[A]	[A+]	[A+]
[SE_RCJA] Servicio de Comunicaciones JdA	[M]	[A]	[A]	[A+]	[A+]
[SE_Mail JdA] Servicio de Correo Electrónico JdA	[M]	[A]	[A]	[A+]	[A+]
[SE_ANDACERT] Servicio de Gestion de Incidencias AndaluciaCERT	[M]	[A]	[A]	[A+]	[A+]
[SE_Proveedores] Servicio de proveedores privados					

sepian

Análisis de Impacto del Negocio

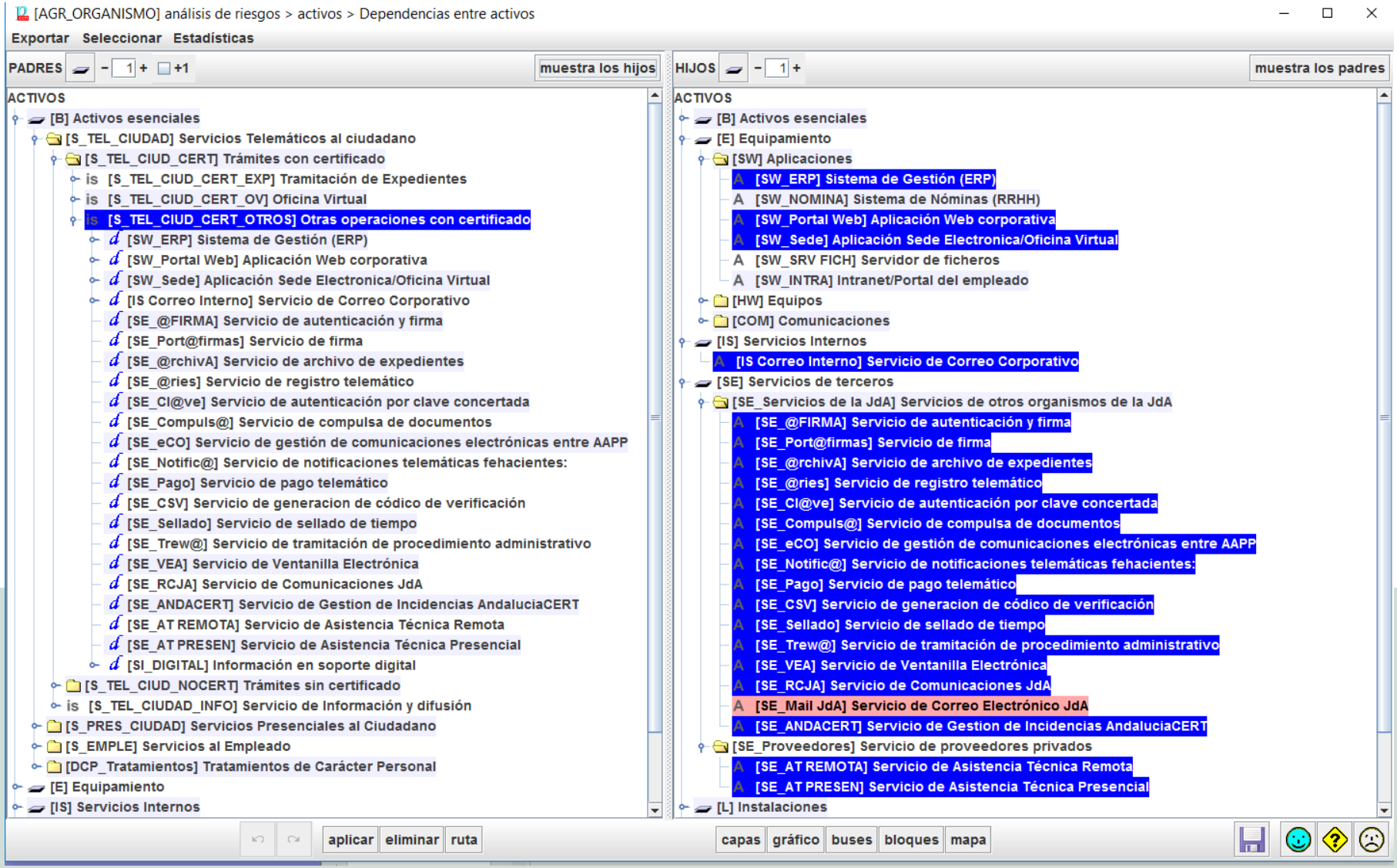
Pasos del proceso. Identificación y valoración de activos



sepian

Análisis de Impacto del Negocio

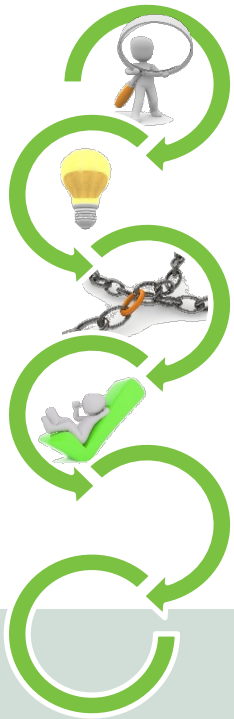
Pasos del proceso. Dependencias entre activos



sepian

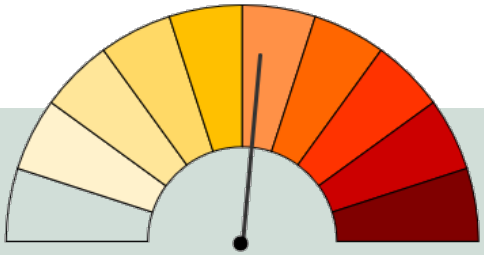
Análisis de Impacto del Negocio

¿Cómo lo hacemos? Pasos del proceso



4. Análisis de impacto y riesgos y gestión

Se evaluarán las amenazas y las salvaguardas desplegadas para calcular los impactos y riesgos de continuidad. Si no son aceptables se realizará una gestión de los mismos.



(9-10) Catástrofe
(8-9) Desastre
(7-8) Extremadamente crítico
(6-7) Muy crítico
(5-6) Crtitico
(4-5) Muy alto
(3-4) Alto
(2-3) Medio
(1-2) Bajo
(0-1) Despreciable

Análisis de Impacto del Negocio

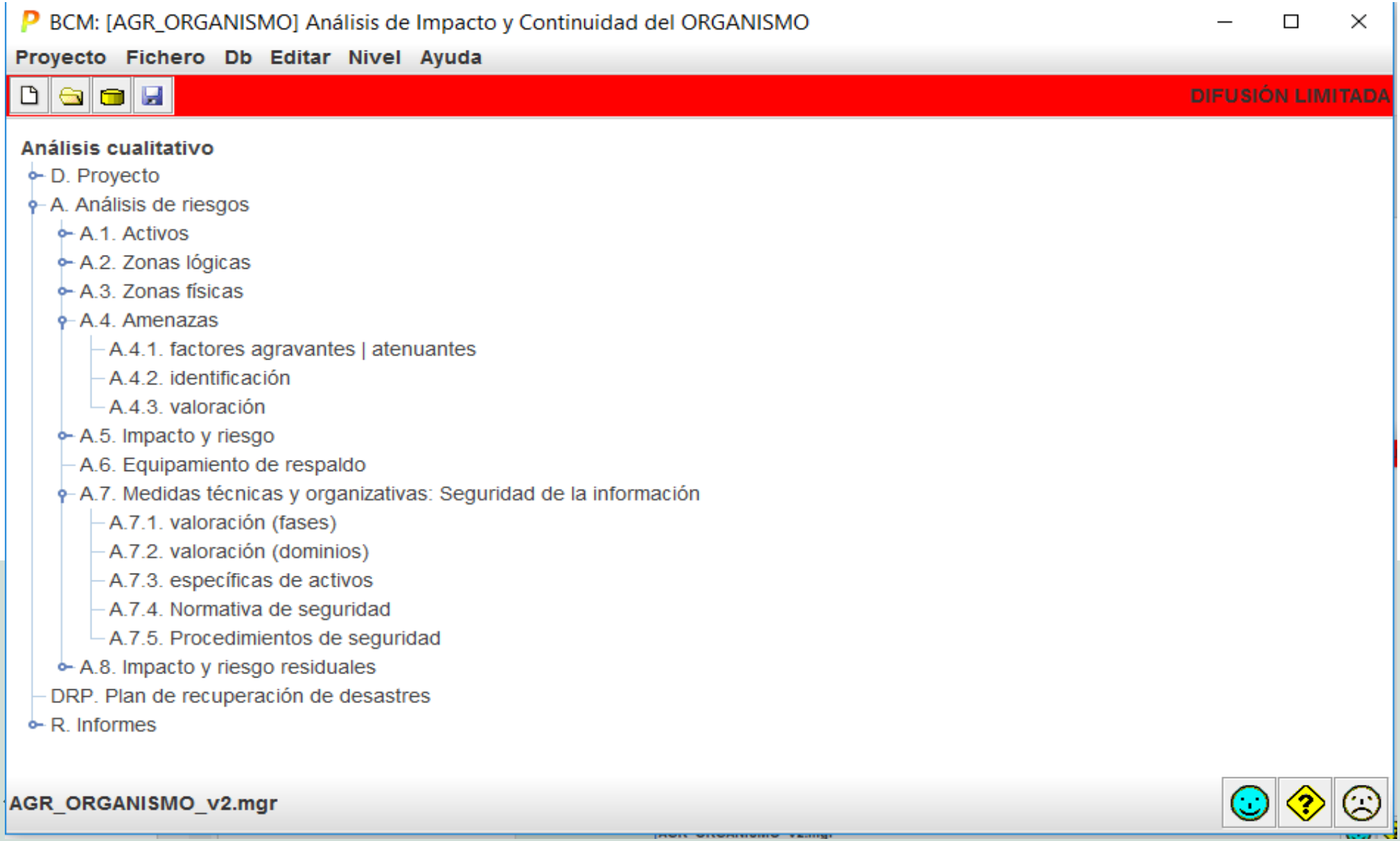
Pasos del proceso. Caracterizar amenazas

Nos centraremos en las amenazas que se relacionen con la continuidad de las operaciones, descartándose todas que tengan que ver con la confidencialidad e y privacidad, ya que nos van a parar a generar un incidente disruptivo. Pueden generar un incidente, pero no será del tipo disruptivo, asociado a la continuidad

FUENTE: INCIBE

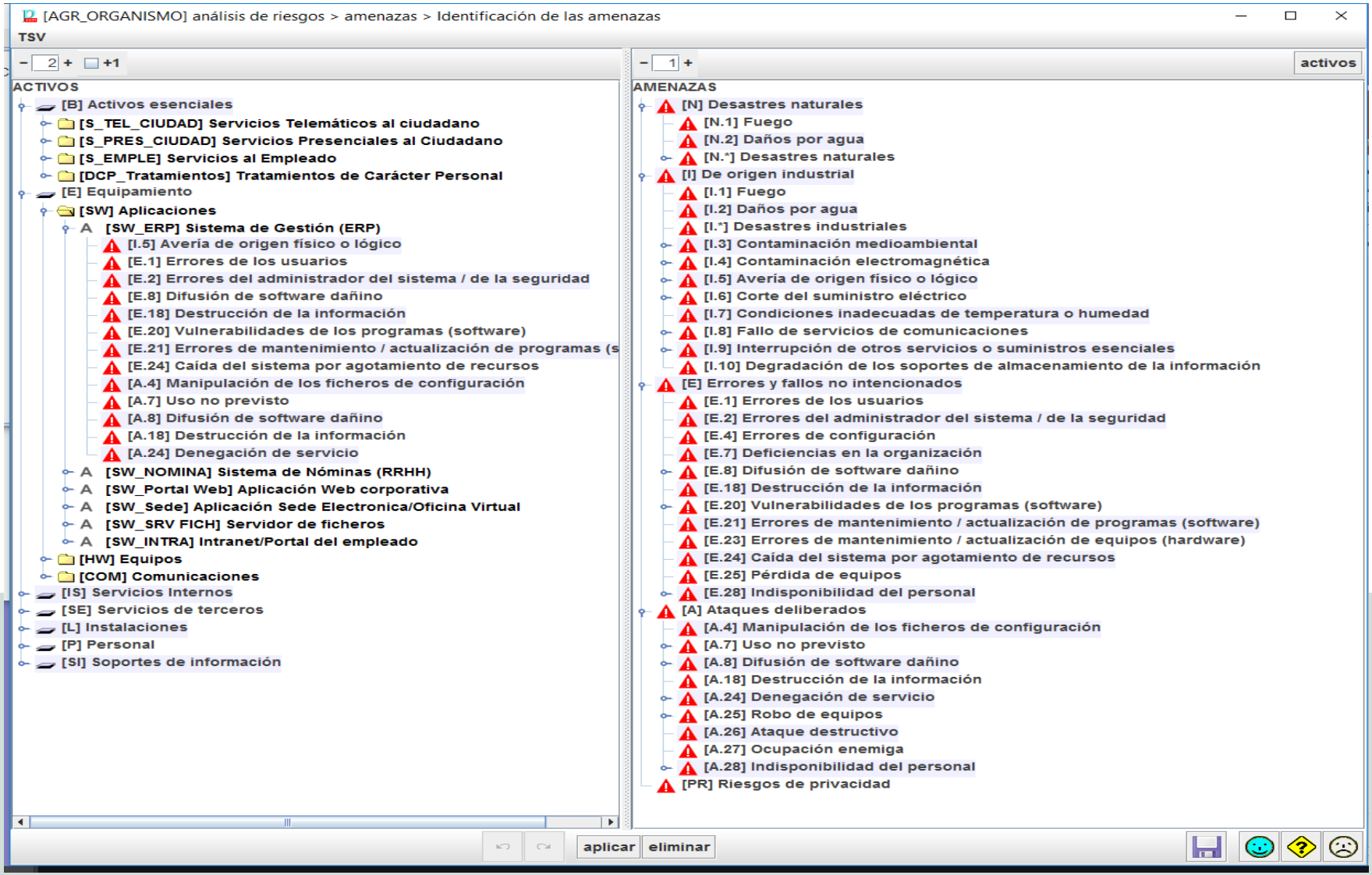
Análisis de Impacto del Negocio

Pasos del proceso. Caracterizar amenazas



Análisis de Impacto del Negocio

Pasos del proceso. Identificación de amenazas



sepian

Análisis de Impacto del Negocio

Pasos del proceso. Valoración de amenazas

- Las amenaza se sólo se valorarán en términos de su frecuencia y del escalón de (cuanto tiempo de interrupción produce si se materializa)
- El impacto será una de las variables que se calcule como resultado del análisis de **impacto**, además del grado de exposición a que las amenazas se materialicen produciendo dicho impacto, es decir, el **riesgo.**

Análisis de Impacto del Negocio

Pasos del proceso. Valoración de amenazas

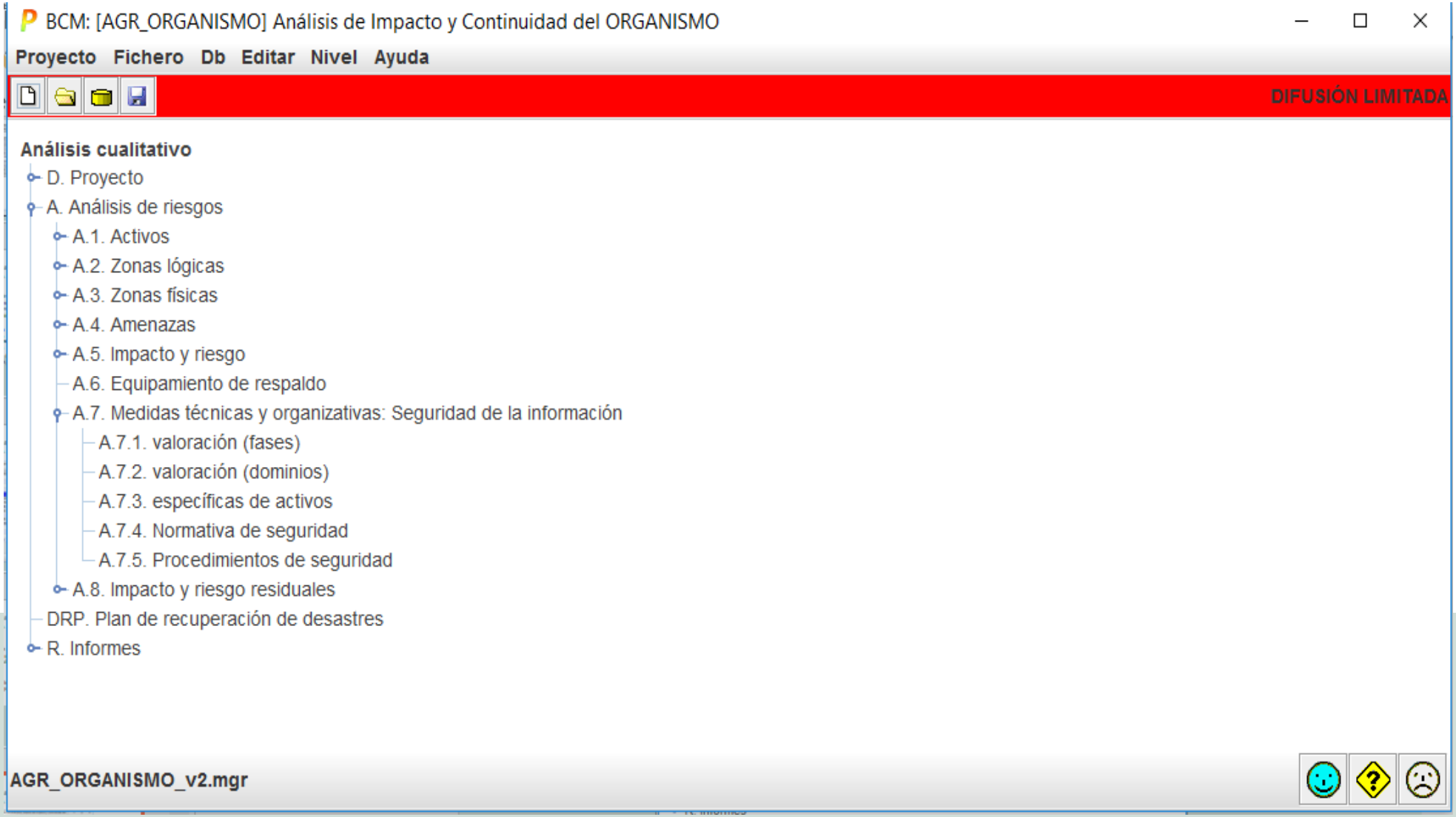
Análisis de Impacto del Negocio

Pasos del proceso. Identificación de salvaguardas

- Se considerarán sólo aquellas salvaguardas que afecten a la continuidad, básicamente las de disponibilidad
- El resto no son tenidas en cuenta para el cálculo del impacto y el riesgo de continuidad

Análisis de Impacto del Negocio

Pasos del proceso. Identificación de salvaguardas



Análisis de Impacto del Negocio

Pasos del proceso. Valoración de salvaguardas

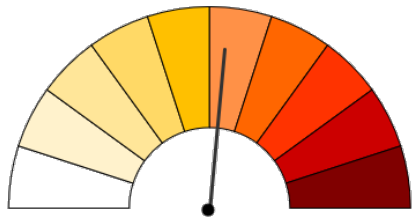
	as...	tdp	rec...		salvaguarda	du...	fue...	apli...	co...	actual	objetivo_MEDIO
					SALVAGUARDAS						
☐	G	EL			[IA] Identificación y autenticación				(*)	L1	L3
☐	T	EL			[AC] Control de acceso lógico					_-L1	_-L3
☐	G	PR	6		[D] Protección de la Información					L1	L3
☐	G	EL			[K] Protección de claves criptográficas					_-L1	_-L3
☐	G	PR	6		[S] Protección de los Servicios					_-L2	_-L3
☐	G	PR	7		[SW] Protección de las Aplicaciones Informáticas (SW)					_-L1	_-L3
☐	G	PR	7		[HW] Protección de los Equipos Informáticos (HW)					_-L1	_-L3
☐	G	PR	8		[COM] Protección de las Comunicaciones					_-L1	_-L3
☐	G	PR			[IP] Sistema de protección de frontera lógica					_-L2	_-L3
☐	G	PR	6		[MP] Protección de los Soportes de Información					_-L1	_-L3
☐	G	PR	6		[AUX] Elementos Auxiliares					_-L1	_-L3
☐	F	EL	5		[PPE] Protección física de los equipos						
☐	F	PR	7		[L] Protección de las Instalaciones					_-L1	_-L3
☐	F	EL			[PPS] Protección del perímetro físico					_-L1	_-L3
☐	P	PR	4		[PS] Gestión del Personal					_-L1	_-L3
☐	G	PR	4		[PDS] Servicios potencialmente peligrosos					_-L1	_-L3
☐	G	CR	5		[IR] Gestión de incidentes					L1	L3
☐	T	PR	8		[tools] Herramientas de seguridad					_-L1	_-L3
☐	G	CR	6		[V] Gestión de vulnerabilidades					L1	L3
☐	T	MN			[A] Registro y auditoría					_-L1	_-L3
☐	G	RC	5		[BC] Continuidad del negocio					_-L1	_-L3
☐	G	AD	4		[G] Organización					_-L1	_-L3
☐	G	AD	6		[E] Relaciones Externas						
☐	G	AD	4		[NEW] Adquisición / desarrollo					_-L1	_-L3

Análisis de Impacto del Negocio

Pasos del proceso. Cálculo del impacto y el riesgo

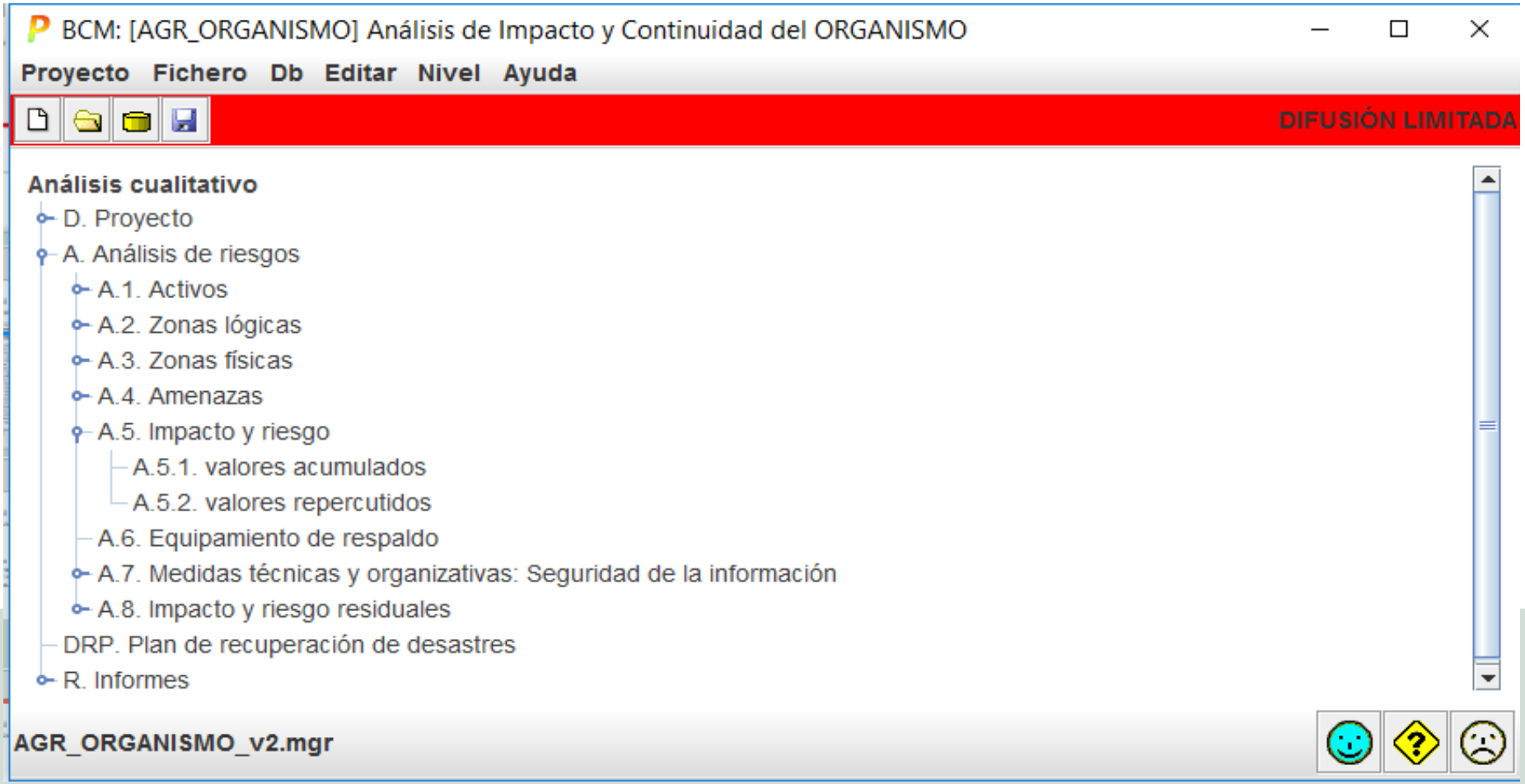
- Se calculará el impacto (daño) al negocio y el riesgo para el escalón de interrupción para el cual se ha caracterizado la amenaza

(9-10) Catástrofe
(8-9) Desastre
(7-8) Extremadamente crítico
(6-7) Muy crítico
(5-6) Crtitico
(4-5) Muy alto
(3-4) Alto
(2-3) Medio
(1-2) Bajo
(0-1) Despreciable



Análisis de Impacto del Negocio

Pasos del proceso. Cálculo del impacto y el riesgo



Análisis de Impacto del Negocio

Pasos del proceso. Cálculo del impacto y el riesgo acumulado

[AGR_ORGANISMO] impacto y riesgo > riesgo acumulado

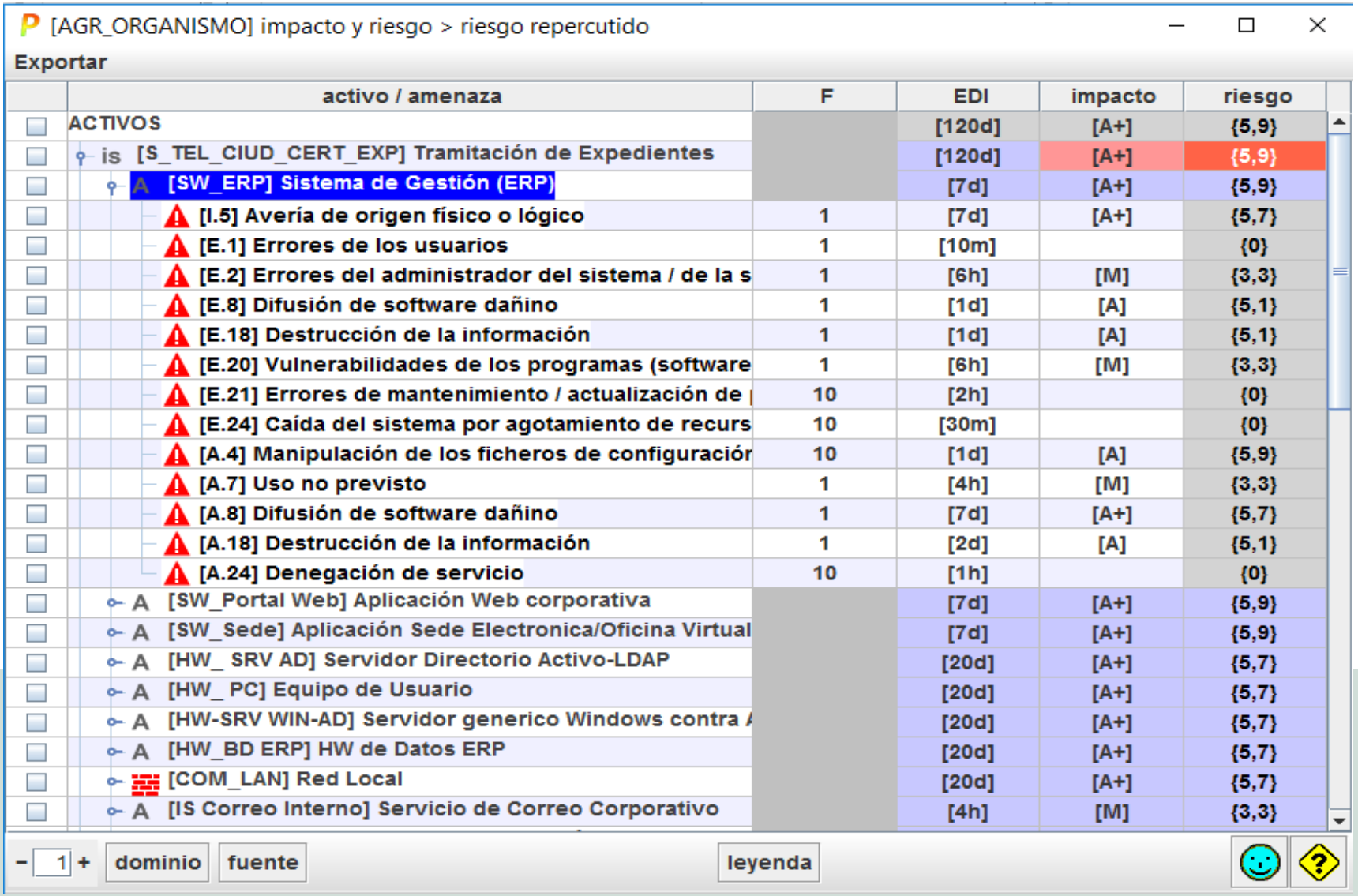
Exportar

activo / amenaza	F	EDI	impacto	riesgo
ACTIVOS		120d	[A+]	{5,9}
[B] Activos esenciales				
[E] Equipamiento				
[SW] Aplicaciones		7d	[A+]	{5,9}
A [SW_ERP] Sistema de Gestión (ERP)		7d	[A+]	{5,9}
A [SW_NOMINA] Sistema de Nóminas (RRHH)		7d	[A+]	{5,9}
A [SW_Portal Web] Aplicación Web corporativa		7d	[A+]	{5,9}
A [SW_Sede] Aplicación Sede Electronica/Oficina V		7d	[A+]	{5,9}
A [SW_SRV FICH] Servidor de ficheros		7d	[A+]	{5,7}
A [SW_INTRA] Intranet/Portal del empleado		7d	[A+]	{5,9}
[HW] Equipos		20d	[A+]	{5,7}
A [HW_ SRV AD] Servidor Directorio Activo-LDAP		20d	[A+]	{5,7}
[N.1] Fuego	0,1	[15d]	[A+]	{4,8}
[N.2] Daños por agua	0,1	[7d]	[A+]	{4,8}
[N.*] Desastres naturales	0,1	[20d]	[A+]	{4,8}
[I.1] Fuego	0,5	[15d]	[A+]	{5,4}
[I.2] Daños por agua	0,5	[7d]	[A+]	{5,4}
[I.*] Desastres industriales	0,5	[15d]	[A+]	{5,4}
[I.3] Contaminación medioambiental	0,1	[2h]		{0}
[I.4] Contaminación electromagnética	1	[10m]		{0}

EDI: Escalón de Interrupción

Análisis de Impacto del Negocio

Pasos del proceso. Cálculo del impacto y el riesgo repercutido



Análisis de Impacto del Negocio

Pasos del proceso. Gestión de impactos y riesgos

Se mejorarán los niveles de madurez de las salvaguardas actualmente (fase “actual”) hasta llegar a valores de riesgo/impacto aceptables (fase “objetivo_MEDIO”).

NISMO] análisis de riesgos > salvaguardas > Eficacia de las salvaguardas

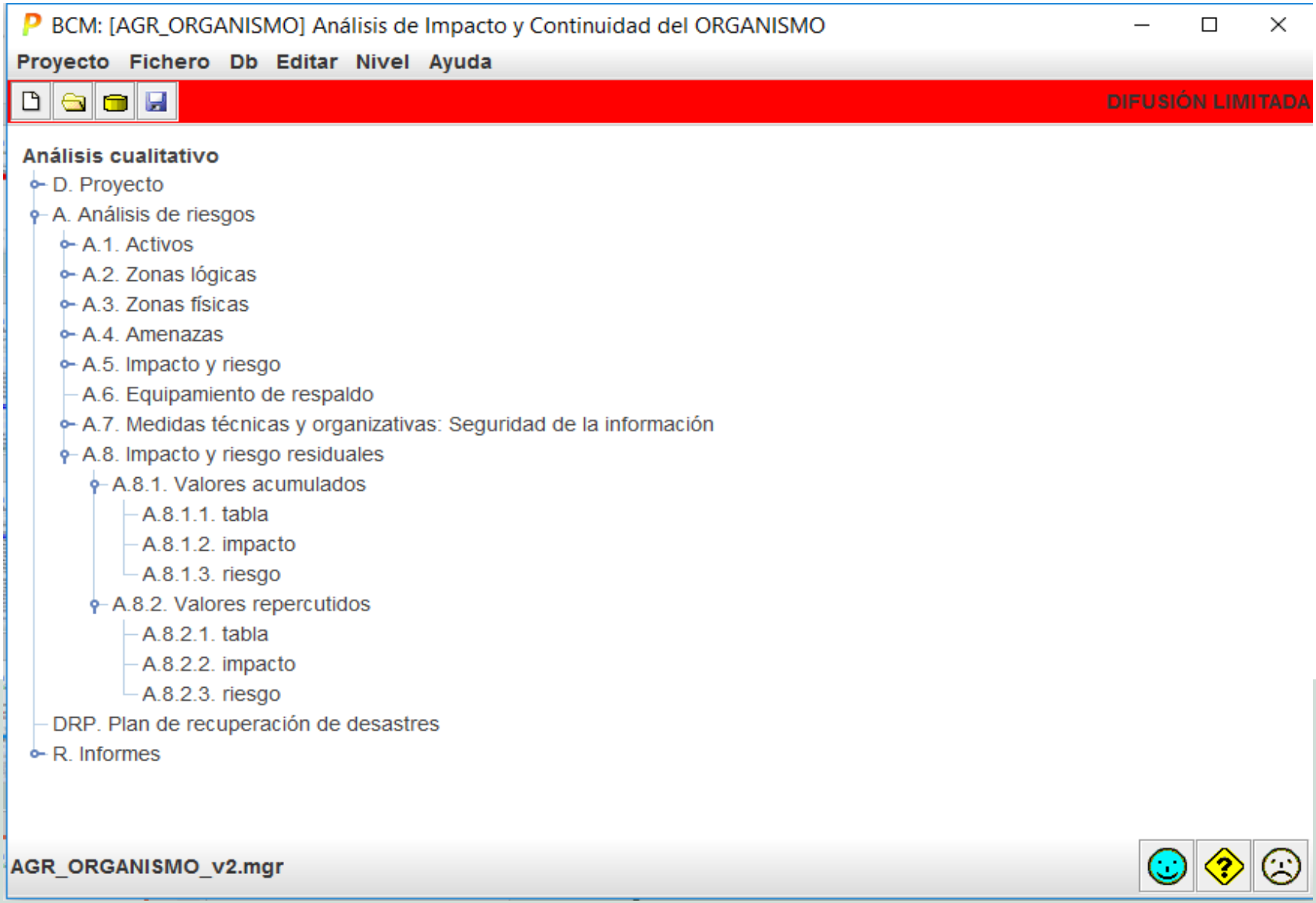
ir Exportar Importar Estadísticas

Fuentes de información

ec...		salvaguarda	du...	fue...	apli...	co...	actual	objetivo_MEDIO
		SALVAGUARDAS						
		[IA] Identificación y autenticación				(*)	L1	L3
		[AC] Control de acceso lógico					_-L1	_-L3
6		[D] Protección de la Información					L1	L3
		[K] Protección de claves criptográficas					_-L1	_-L3
6		[S] Protección de los Servicios					_-L2	_-L3
7		[SW] Protección de las Aplicaciones Informáticas (SW)					_-L1	_-L3
7		[HW] Protección de los Equipos Informáticos (HW)					_-L1	_-L3
8		[COM] Protección de las Comunicaciones					_-L1	_-L3
		[IP] Sistema de protección de frontera lógica					_-L2	_-L3
6		[MP] Protección de los Soportes de Información					_-L1	_-L3
6		[AUX] Elementos Auxiliares					_-L1	_-L3
5		[PPE] Protección física de los equipos						

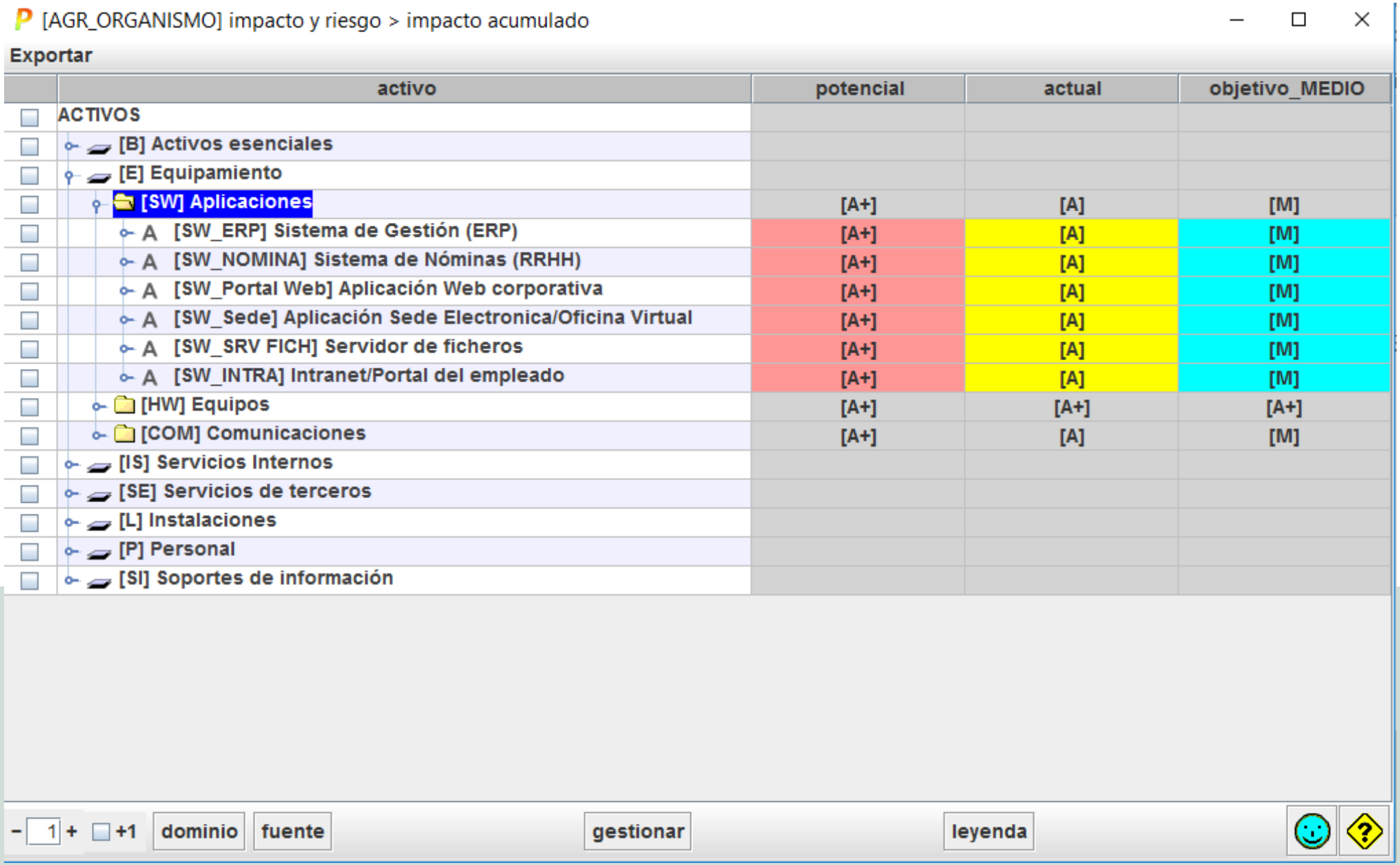
Análisis de Impacto del Negocio

Pasos del proceso. Gestión de impactos y riesgos



Análisis de Impacto del Negocio

Pasos del proceso. Impacto residual acumulado



Análisis de Impacto del Negocio

Pasos del proceso. Riesgo residual acumulado

[AGR_ORGANISMO] impacto y riesgo > riesgo acumulado

Exportar

	activo	potencial	actual	objetivo_MEDIO
	ACTIVOS			
	[B] Activos esenciales			
	[E] Equipamiento			
	[SW] Aplicaciones	{5,9}	{5,9}	{3,4}
	A [SW_ERP] Sistema de Gestión (ERP)	{5,9}	{5,9}	{3,4}
	A [SW_NOMINA] Sistema de Nóminas (RRHH)	{5,9}	{5,9}	{3,4}
	A [SW_Portal Web] Aplicación Web corporativa	{5,9}	{5,9}	{3,4}
	A [SW_Sede] Aplicación Sede Electronica/Oficina Virtual	{5,9}	{5,9}	{3,4}
	A [SW_SRV FICH] Servidor de ficheros	{5,7}	{5,0}	{2,6}
	A [SW_INTRA] Intranet/Portal del empleado	{5,9}	{5,9}	{3,4}
	[HW] Equipos	{5,7}	{5,6}	{5,0}
	[COM] Comunicaciones	{5,7}	{5,0}	{2,8}
	[IS] Servicios Internos			
	[SE] Servicios de terceros			
	[L] Instalaciones			
	[P] Personal			
	[SI] Soportes de información			

- 1 + +1 dominio fuente gestionar leyenda

Análisis de Impacto del Negocio

Pasos del proceso. Impacto residual repercutido

[AGR_ORGANISMO] impacto y riesgo > impacto repercutido

Exportar

activo	potencial	actual	objetivo_MEDIO
ACTIVOS	[A+]	[A+]	[A+]
is [S_TEL_CIUD_CERT_EXP] Tramitación de Expedientes	[A+]	[A+]	[A+]
A [SW_ERP] Sistema de Gestión (ERP)	[A+]	[A]	[M]
[I.5] Avería de origen físico o lógico	[A+]	[A]	[M]
[E.1] Errores de los usuarios			
[E.2] Errores del administrador del sistema / de la seguridad	[M]	[M]	[M]
[E.8] Difusión de software dañino	[A]	[A]	[M]
[E.18] Destrucción de la información	[A]	[A]	[M]
[E.20] Vulnerabilidades de los programas (software)	[M]	[M]	[M]
[E.21] Errores de mantenimiento / actualización de program			
[E.24] Caída del sistema por agotamiento de recursos			
[A.4] Manipulación de los ficheros de configuración	[A]	[A]	[M]
[A.7] Uso no previsto	[M]	[M]	[M]
[A.8] Difusión de software dañino	[A+]	[A]	[M]
[A.18] Destrucción de la información	[A]	[A]	[M]
[A.24] Denegación de servicio			
A [SW_Portal Web] Aplicación Web corporativa	[A+]	[A]	[M]
A [SW_Sede] Aplicación Sede Electronica/Oficina Virtual	[A+]	[A]	[M]
A [HW_ SRV AD] Servidor Directorio Activo-LDAP	[A+]	[A]	[M]
A [HW_ PC] Equipo de Usuario	[A+]	[A+]	[A+]
A [HW-SRV WIN-AD] Servidor generico Windows contra AD	[A+]	[A]	[M]
A [HW_BD ERP] HW de Datos ERP	[A+]	[A]	[M]
[COM_LAN] Red Local	[A+]	[A]	[M]
A [IS Correo Interno] Servicio de Correo Corporativo	[M]	[M]	[M]

- 1 + dominio fuente gestionar leyenda

Análisis de Impacto del Negocio

Pasos del proceso. Riesgo residual repercutido

[AGR_ORGANISMO] impacto y riesgo > riesgo repercutido

Exportar

activo	potencial	actual	objetivo_MEDIO
ACTIVOS	{5,9}	{5,9}	{5,1}
is [S_TEL_CIUD_CERT_EXP] Tramitación de Expedientes	{5,9}	{5,9}	{5,1}
A [SW_ERP] Sistema de Gestión (ERP)	{5,9}	{5,9}	{3,4}
[I.5] Avería de origen físico o lógico	{5,7}	{5,0}	{2,5}
[E.1] Errores de los usuarios	{0}	{0}	{0}
[E.2] Errores del administrador del sistema / de la seguridad	{3,3}	{3,1}	{2,2}
[E.8] Difusión de software dañino	{5,1}	{4,9}	{2,2}
[E.18] Destrucción de la información	{5,1}	{4,9}	{2,3}
[E.20] Vulnerabilidades de los programas (software)	{3,3}	{3,2}	{2,3}
[E.21] Errores de mantenimiento / actualización de program	{0}	{0}	{0}
[E.24] Caída del sistema por agotamiento de recursos	{0}	{0}	{0}
[A.4] Manipulación de los ficheros de configuración	{5,9}	{5,9}	{3,4}
[A.7] Uso no previsto	{3,3}	{3,2}	{2,3}
[A.8] Difusión de software dañino	{5,7}	{4,9}	{2,3}
[A.18] Destrucción de la información	{5,1}	{5,0}	{2,5}
[A.24] Denegación de servicio	{0}	{0}	{0}
A [SW_Portal Web] Aplicación Web corporativa	{5,9}	{5,9}	{3,4}
A [SW_Sede] Aplicación Sede Electronica/Oficina Virtual	{5,9}	{5,9}	{3,4}
A [HW_ SRV AD] Servidor Directorio Activo-LDAP	{5,7}	{5,0}	{2,7}
A [HW_ PC] Equipo de Usuario	{5,7}	{5,6}	{5,0}
A [HW-SRV WIN-AD] Servidor generico Windows contra AD	{5,7}	{5,0}	{2,7}
A [HW_BD ERP] HW de Datos ERP	{5,7}	{5,0}	{2,7}
[COM_LAN] Red Local	{5,7}	{5,0}	{2,8}
A [IS Correo Interno] Servicio de Correo Corporativo	{3,3}	{3,2}	{2,4}

- 1 + dominio fuente gestionar leyenda

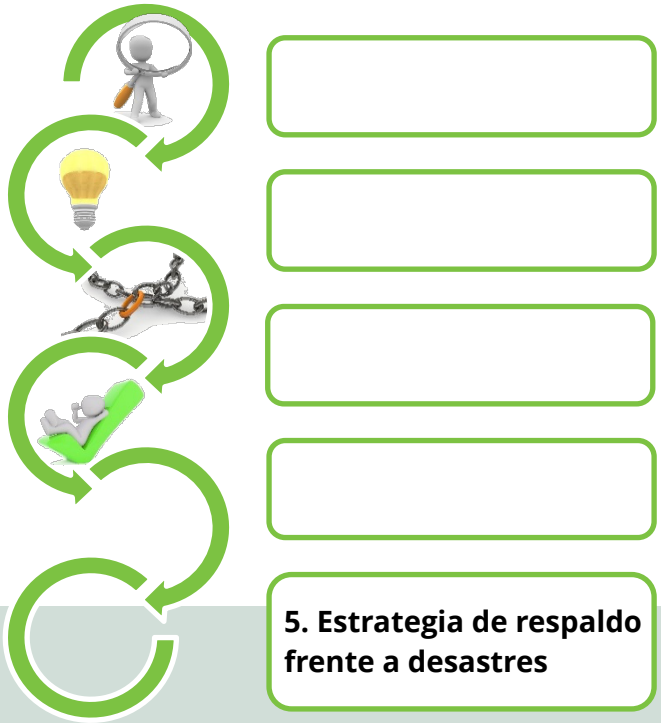
Análisis de Impacto del Negocio

Pasos del proceso. Las salidas del proceso BIA

- Una vez conocidos los impactos y los riesgos residuales para cada EDI (Escalón de Interrupción), estos marcarán los **tiempos de recuperación objetivo** para cada activo que forme parte del sistema de información con el que se preste un servicio.
- Nótese que, en el caso de que se haya llevado a cabo la gestión de riesgos mediante la mejora del grado de madurez de las salvaguardas, se deberán acometer las acciones de mejora pertinentes para dicho grado de madurez (**BCM: business continuity management**)
- Estas acciones reducen el impacto y el riegos ante incidentes disruptivos.
- Si un incidentes llegase a materializarse, los RTOs marcan los tiempos de recuperación para que el impacto sea mínimo.
- Asimismo, estos RTOs marcan la **estrategia de continuidad**.

Análisis de Impacto del Negocio

¿Cómo lo hacemos? Pasos del proceso



5. Estrategia de respaldo frente a desastres

Una vez conocidos los escalones de interrupción aceptables, se diseñará la estrategia de respaldo.

Análisis de Impacto del Negocio

¿Cómo lo hacemos? Tipos de estrategia de respaldo

FUENTE: INCIBE

Análisis de Impacto del Negocio

¿Cómo lo hacemos? Tipos de estrategia de respaldo

A continuación se muestran los tipos de centro de respaldo en relación al coste, equipamiento y telecomunicaciones:

TIPO DE CENTRO DE RESPALDO	COSTE	EQUIPAMIENTO HARDWARE	TELECOMUNICACIONES	UBICACIÓN
COLD SITE	BAJO	Ninguno	Ninguno	Fija
WARM SITE	MEDIO	Parcial	Parcial / Completo	Fija
HOT SITE	MEDIO/ALTO	Completo	Completo	Fija

Análisis de Impacto del Negocio

¿Cómo lo hacemos? Tipos de estrategia de respaldo vs RTOs

TIEMPO DE INDISPONIBILIDAD PERMITIDO (RTO)	TIPO DE CENTRO DE RESPALDO NECESARIO
Menos de 4 horas	HOT SITE
Entre 1 y 5 días	WARM SITE
Más de 5 días	COLD SITE

Análisis de Impacto del Negocio

Modelo de BIA para la Junta de Andalucía

SEDIAN pone a disposición de los organismos un modelo de BIA en pilar, junto con una guía de uso.

EAR/PILAR

</pilar>

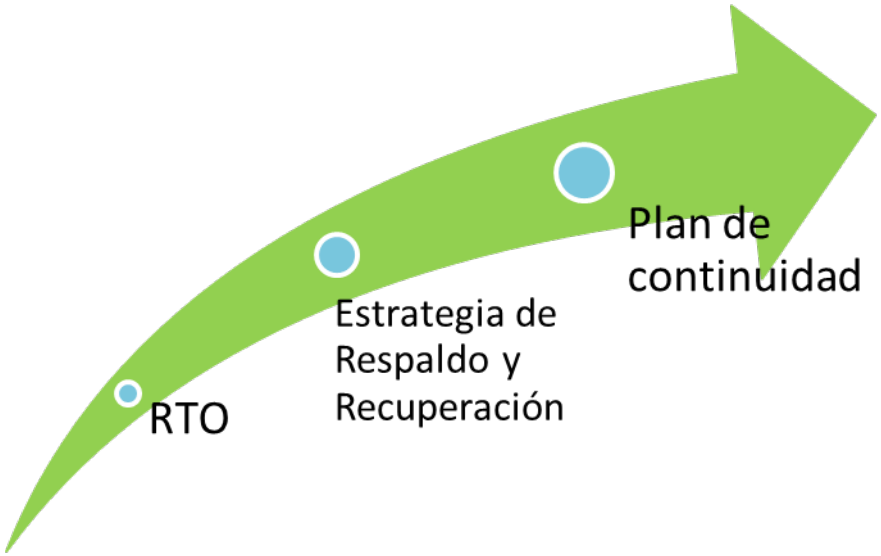
Herramientas de análisis y gestión de riesgos.

ccn-cert

Índice de contenidos

Otras actividades de continuidad

El desarrollo del plan de continuidad



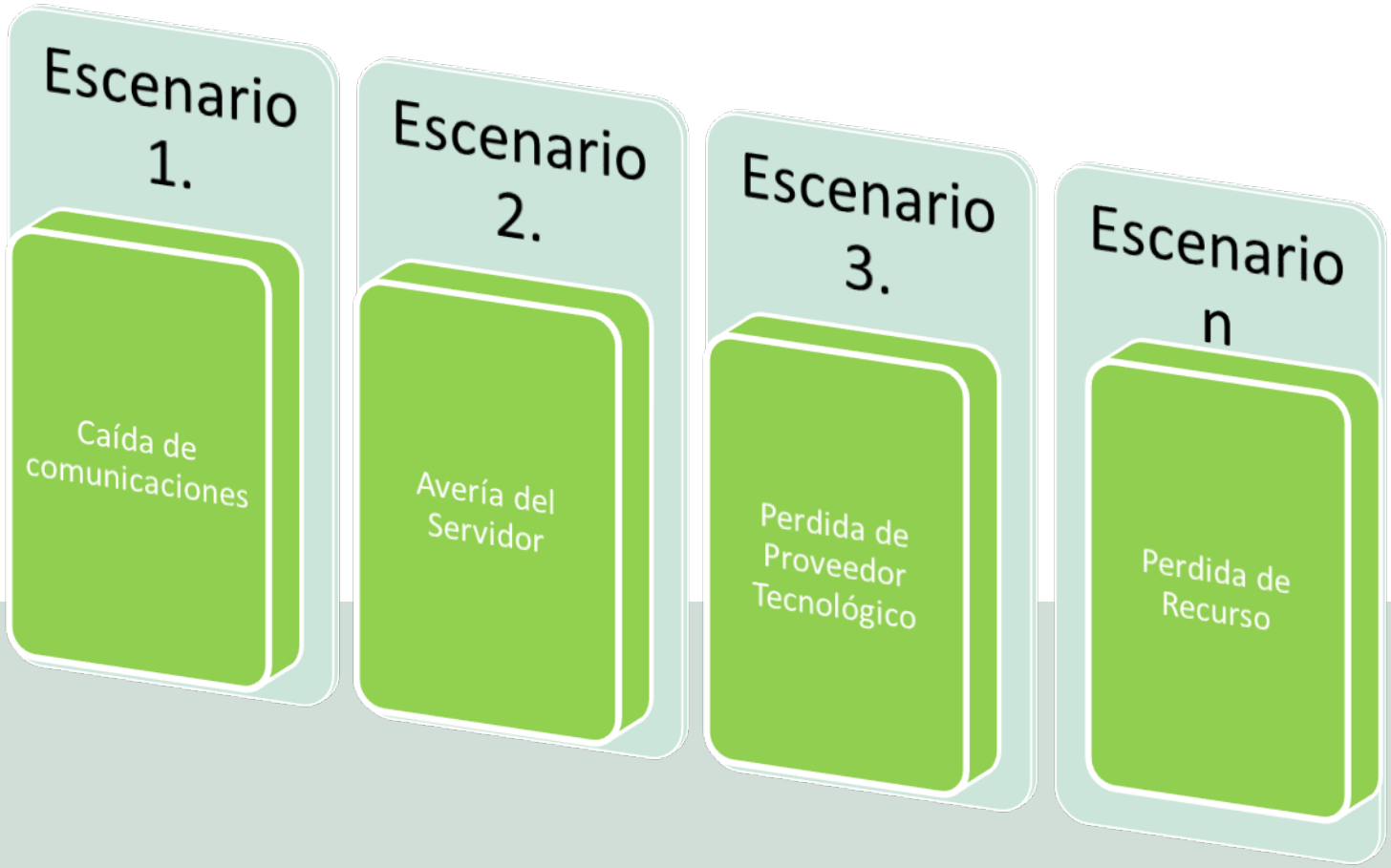
FUENTE: INCIBE

- El plan de continuidad debería incluir tanto las acciones de mejora para la gestión de la continuidad en el BCM como los planes de recuperación tras un incidente disruptivo (DRP: disaster recovery plan) conforme a la estrategia de respaldo

Otras actividades de continuidad

El desarrollo del plan de continuidad.

Escenarios de contingencias : incidentes disruptivos



Otras actividades de continuidad

El desarrollo del plan de continuidad.

Plan de continuidad de Alto nivel

Para cada escenario y con las estrategias definidas, se deberán documentar las acciones de alto nivel para llevarlas a cabo.

Otras actividades de continuidad

El desarrollo del plan de continuidad.

Plan de continuidad de detalle

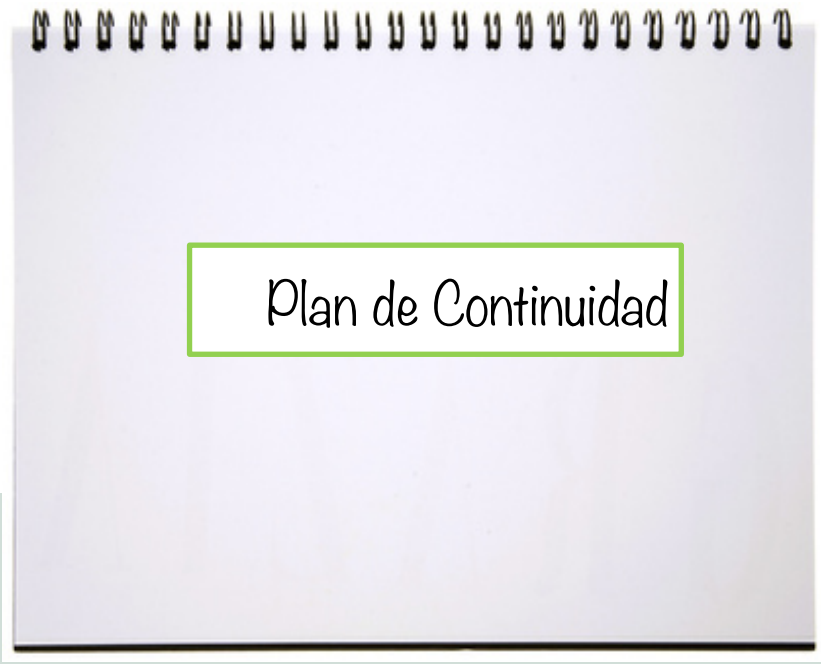
Plan Técnico: instrucciones técnicas de detalle.

Plan Administrativo: responsabilidades, árboles de llamadas, comités.

Otras actividades de continuidad

El desarrollo del plan de continuidad.

Plan de continuidad



Otras actividades de continuidad

La explotación del plan de continuidad.

Pruebas, simulacros, revisión y formación

FUENTE: INCIBE

Índice de contenidos

Normativa de referencia

ISO 22301

Esta norma define los requisitos para implantar un sistema de gestión de la continuidad del negocio y certificarlo (por alguna entidad de certificación).

FUENTE: INCIBE

Índice de contenidos

Conclusiones

- El BIA como requisito para definir las estrategias de continuidad
- Sirve para definir los tiempos de recuperación.
- Obligatorio para el ENS (categoría MEDIA o superior) (op.cont.1)

sedian Seguridad Digital de Andalucía