Grado de Informática
Universidad de Almería

Análisis de riesgos mediante la metodología MAGERIT y planes de seguridad

Miguel Santiago Cervilla
Juan Soler Márquez

Fiabilidad y Gestión de Riesgos
Grupo Práticas

Departamento de Matemáticas

Índice

1. Contexto del Sistema de Información

Para el desarrollo de esta sesión hemos elegido el Banco Cajamar, cuya sede principal se encuentra en Almería. Nos parece una apuesta interesante ya que una entidad bancaria puede presentar un análisis de riesgos muy interesante, ya que su servicio es de extrema delicadeza.

Como banco de crédito, sus activos principales son los datos de las cuentas de los clientes, balances, extractos, etc. Así como la disponibilidad del banco para que el cliente pueda hacer uso de su dinero en cualquier momento.

Además, debe poder realizar la operativa desde cualquier punto del planeta, por lo que la operativa se vuelve más compleja. Debiendo contar con un sistema de información consistente, integral y con una serie de medidas que permitan un 99,9 % de operatividad.

2. Activos del Sistema de Información

2.1. Activos Esenciales y No Esenciales

Como activos esenciales nos debemos centrar en el uso de los datos internos de la empresa, junto con los datos de los clientes de la mismas, que son de carácter muy sensible.

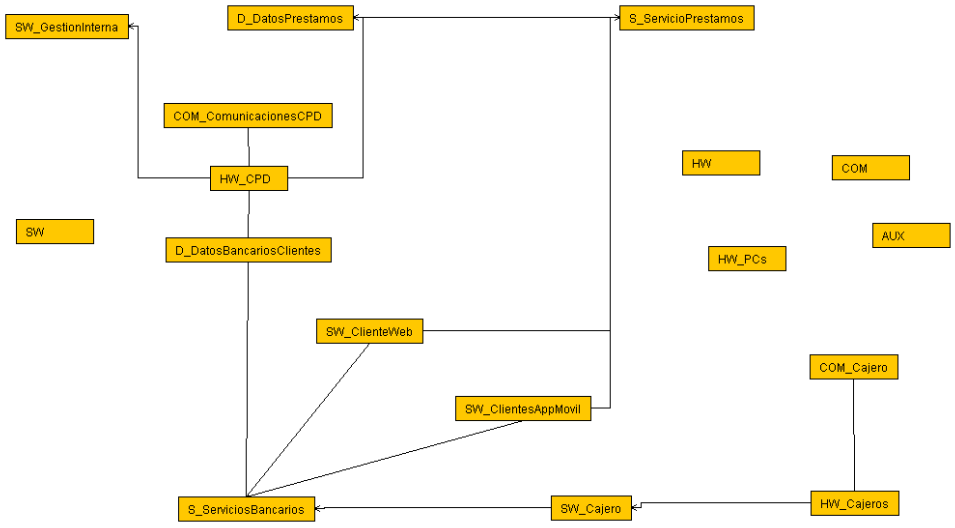
Hemos elegido estos activos esenciales ya que nos parecen los más esenciales del entorno, destacando que no se trata de un análisis exhaustivo de la entidad, pero a nuestro parecer, son los más esenciales de la empresa. Un fallo en dichos activos pueden ocasionar problemas de gran gravedad.

Para activos no esenciales hemos seleccionado los que creemos más adecuados y a su vez son los más significativos. Aunque se trate de activos no esenciales, un fallo en los mismos ocasiona una pérdidad de operatividad de la empresa grave.

Si no paramos detenidamente a observar cada uno de los activos esenciales, podemos llegar a la conclusión, que dentro de los activos no esenciales, tienen mayor prioridad frente a todos los activos no esenciales que pueden completar el análisis, ya que dichos activos proporcionan el servicio de nuestra empresa.

2.2. Dependencia entre Activos

Para las dependencias entre los activos, hemos representado el siguiente gráfico:



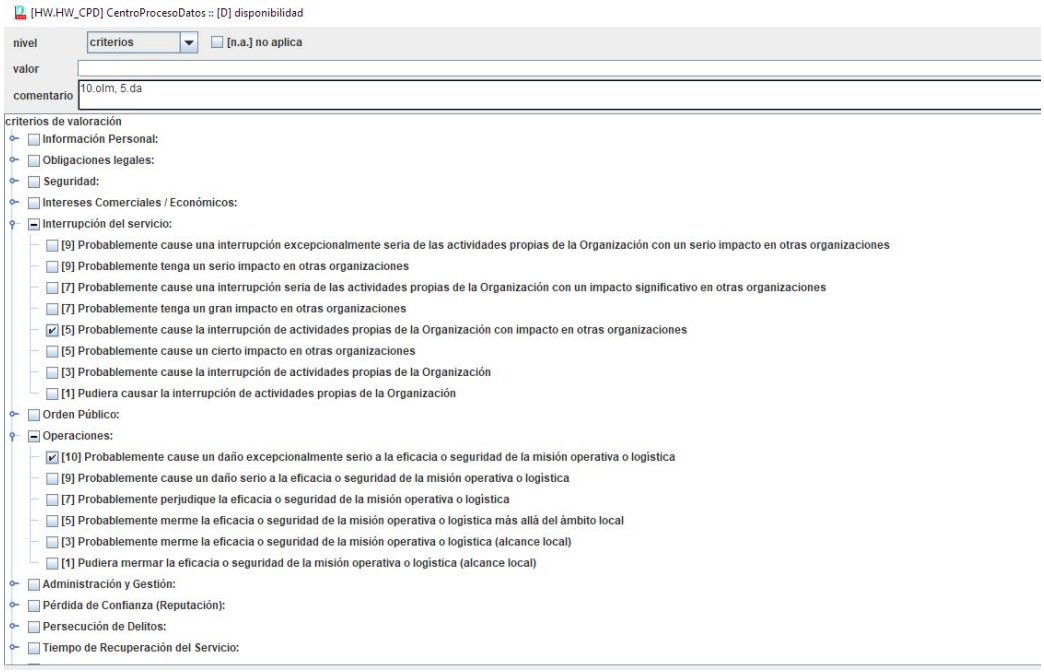
Si nos paramos detenidamente a observar el gráfico representado, podemos observar que el HW_CPD es de gran importancia, ya que sin su operatividad no podríamos dar el servicio necesario. También podemos observar que para el servicio de cajero, los datos a los cuales vamos a tener acceso sólo van a ser los datos bancarios del cliente. Dentro de un cajero no se podrán realizar operaciones de préstamo.

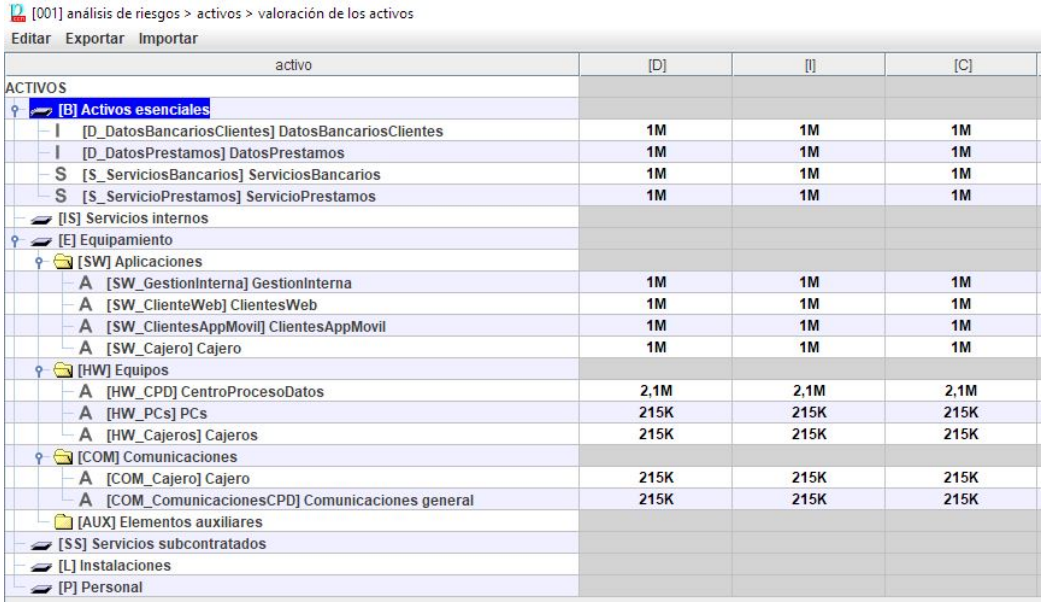
2.3. Valoración de los Activos

Para la valoración de los activos, vamos a tener en cuenta tres campos: Disponibilidad, Integridad y Confidencialidad. Para ello vamos a realizar una tabla en la que vamos a incluir cada una de las valoraciones que creemos que son adecuadas para cada campo antes citado. La tabla realizada es la siguiente:

Activo	Datos	Integridad	Confidencialidad
S_bancario	7.da,9.cei.c,6.pi1,6.p2, 9.lg.a	7.da,9.cei.c,6.pi1,6.p2, 9.lg.a	7.da,9.cei.c,6.pi1,6.p2, 9.lro, 9.lg.a
S_prestamo	7.da,9.cei.c,6.pi1,6.p2, 9.lg.a	7.da,9.cei.c,6.pi1,6.p2, 9.lg.a	7.da,9.cei.c,6.pi1,6.p2, 9.lro, 9.lg.a
D_clientes	7.da,9.cei.c,6.pi1,6.p2, 9.lg.a	7.da,9.cei.c,6.pi1,6.p2, 9.lg.a	7.da,9.cei.c,6.pi1,6.p2, 9.lro, 9.lg.a
D_prestamos	7.da,9.cei.c,6.pi1,6.p2, 9.lg.a	7.da,9.cei.c,6.pi1,6.p2, 9.lg.a	7.da,9.cei.c,6.pi1,6.p2, 9.lro, 9.lg.a
COM_CPD	7.da, 3.po		
COM_Cajero	7.da, 3.po		
SW_Web	7.da,9.cei.c,6.pi1,6.p2	7.da,9.cei.c,6.pi1,6.p2	7.da,9.cei.c,6.pi1,6.p2, 9.lro
SW_App	7.da,9.cei.c,6.pi1,6.p2	7.da,9.cei.c,6.pi1,6.p2	7.da,9.cei.c,6.pi1,6.p2, 9.lro
SW_Interno	7.da,9.cei.c,6.pi1,6.p2	7.da,9.cei.c,6.pi1,6.p2	7.da,9.cei.c,6.pi1,6.p2, 9.lro
SW_Cajero			7.da,9.cei.c,6.pi1,6.p2, 9.lro
HW_Cajero	7.olm, 3.da	7.olm, 3.da	7.olm, 3.da
HW_PC	7.olm, 5.da	7.olm, 5.da	7.olm, 5.da
HW_CPD	10.olm, 5.da	10.olm, 5.da	10.olm, 5.da

Una vez realizada esta tabla, procedemos a pasar dichos datos a PILAR con los campos que nos proporciona la herramienta:



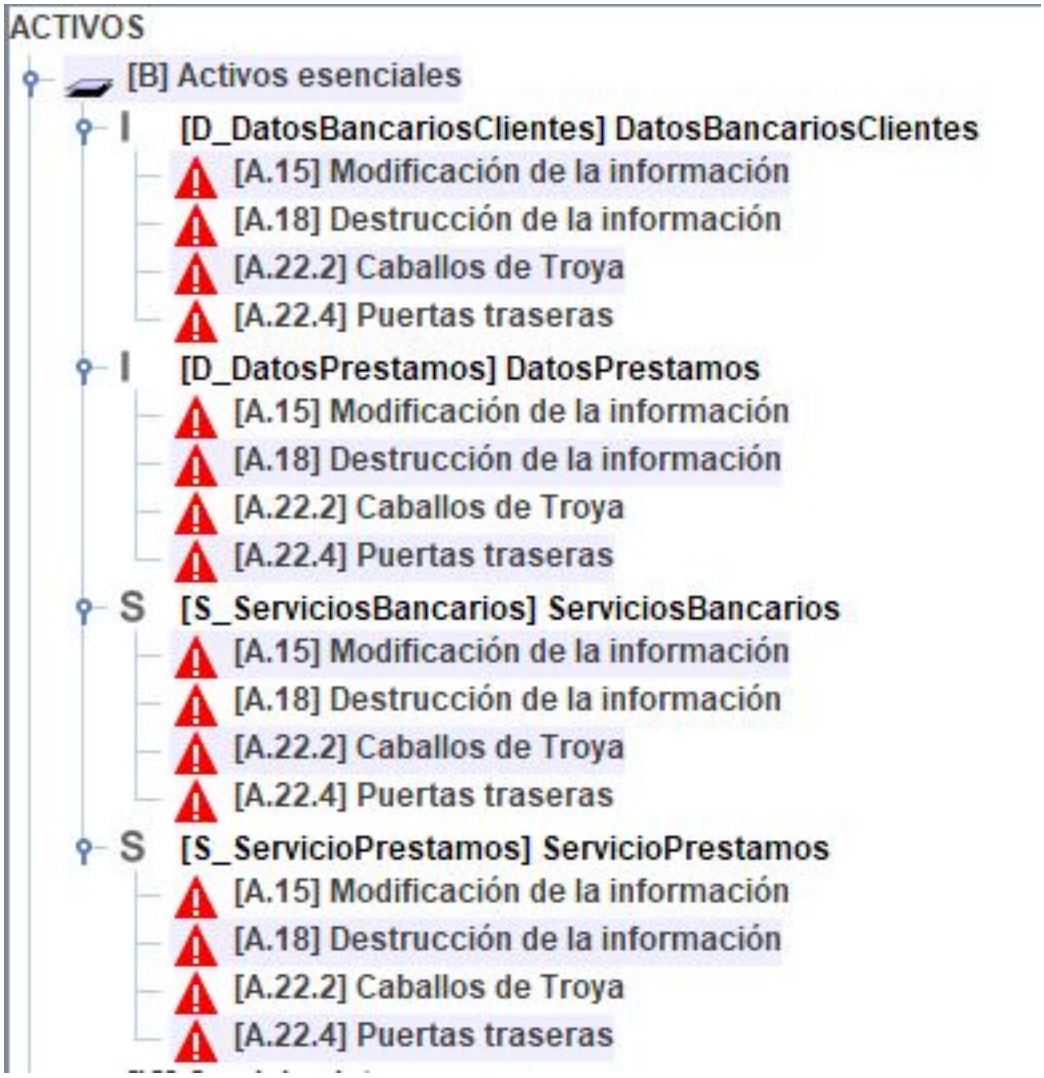


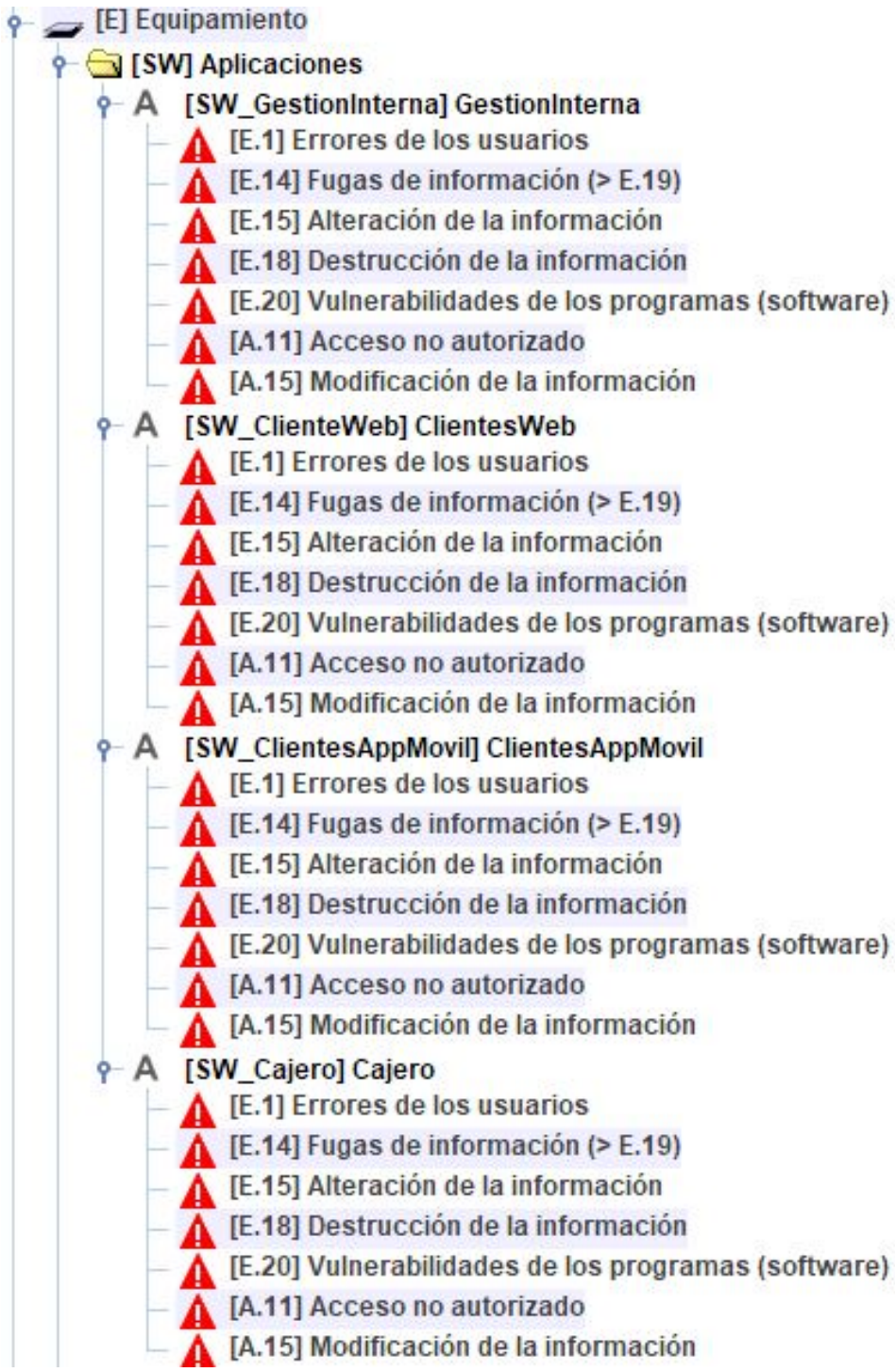
activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
I [D_DatosBancariosClientes] DatosBancariosClientes	1M	1M	1M
I [D_DatosPrestamos] DatosPrestamos	1M	1M	1M
S [S_ServiciosBancarios] ServiciosBancarios	1M	1M	1M
S [S_ServicioPrestamos] ServicioPrestamos	1M	1M	1M
[IS] Servicios internos			
[E] Equipamiento			
[SW] Aplicaciones			
A [SW_GestionInterna] GestionInterna	1M	1M	1M
A [SW_ClienteWeb] ClientesWeb	1M	1M	1M
A [SW_ClientesAppMovil] ClientesAppMovil	1M	1M	1M
A [SW_Cajero] Cajero	1M	1M	1M
[HW] Equipos			
A [HW_CPD] CentroProcesoDatos	2,1M	2,1M	2,1M
A [HW_PCs] PCs	215K	215K	215K
A [HW_Cajeros] Cajeros	215K	215K	215K
[COM] Comunicaciones			
A [COM_Cajero] Cajero	215K	215K	215K
A [COM_ComunicacionesCPD] Comunicaciones general	215K	215K	215K
[AUX] Elementos auxiliares			
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			

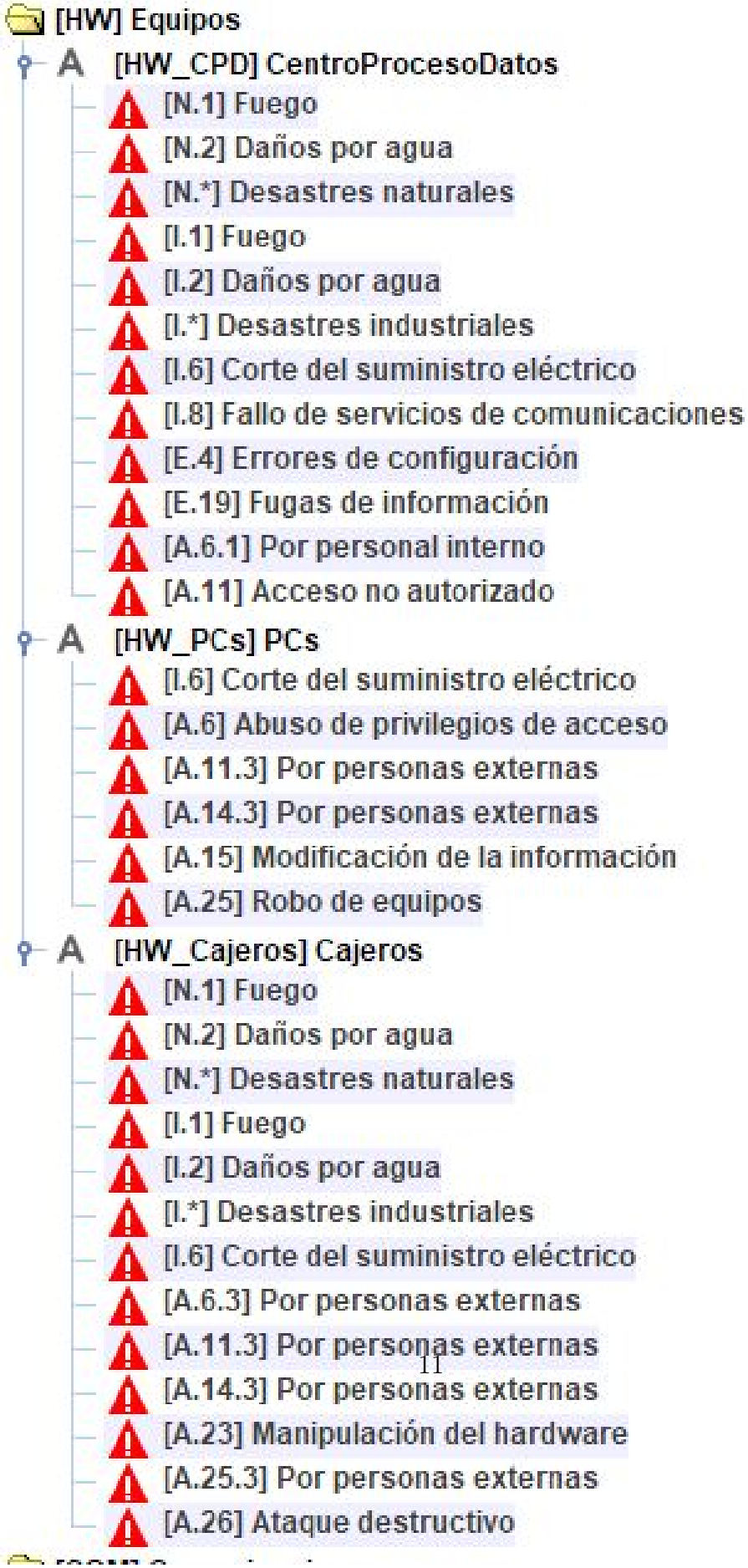
Como podemos observar, dentro de los activos esenciales, tanto en valoraciones de Disponibilidad,Integridad y Confidencialidad, un fallo en los mismos ocasionaría problemas muy graves para la entidad.

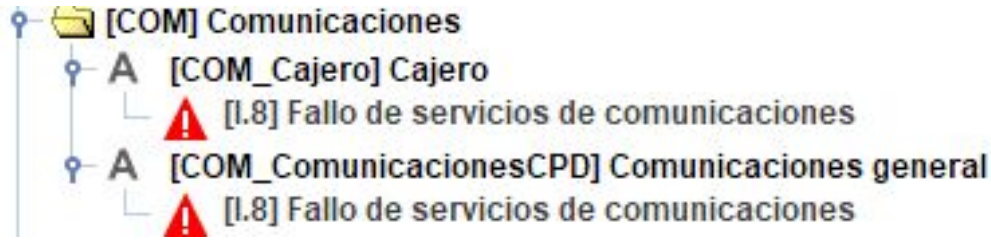
3. Amenazas del Sistema de Información

Para las amenazas vamos a elegir las apropiadas para nuestro sistema de información:




[E] Equipamiento
[SW] Aplicaciones
[SW_GestionInterna] GestionInterna
[E.1] Errores de los usuarios
[E.14] Fugas de información (> E.19)
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.20] Vulnerabilidades de los programas (software)
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[SW_ClienteWeb] ClientesWeb
[E.1] Errores de los usuarios
[E.14] Fugas de información (> E.19)
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.20] Vulnerabilidades de los programas (software)
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[SW_ClientesAppMovil] ClientesAppMovil
[E.1] Errores de los usuarios
[E.14] Fugas de información (> E.19)
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.20] Vulnerabilidades de los programas (software)
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[SW_Cajero] Cajero
[E.1] Errores de los usuarios
[E.14] Fugas de información (> E.19)
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.20] Vulnerabilidades de los programas (software)
[A.11] Acceso no autorizado
[A.15] Modificación de la información


[HW] Equipos
A [HW_CPD] CentroProcesoDatos
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.6] Corte del suministro eléctrico
[I.8] Fallo de servicios de comunicaciones
[E.4] Errores de configuración
[E.19] Fugas de información
[A.6.1] Por personal interno
[A.11] Acceso no autorizado
A [HW_PCs] PCs
[I.6] Corte del suministro eléctrico
[A.6] Abuso de privilegios de acceso
[A.11.3] Por personas externas
[A.14.3] Por personas externas
[A.15] Modificación de la información
[A.25] Robo de equipos
A [HW_Cajeros] Cajeros
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.6] Corte del suministro eléctrico
[A.6.3] Por personas externas
[A.11.3] Por personas externas
[A.14.3] Por personas externas
[A.23] Manipulación del hardware
[A.25.3] Por personas externas
[A.26] Ataque destructivo



Dentro de las amenazas para los activos esenciales, vamos a tener todas las relacionadas con la información, manejo de la información y robo de la misma.

Para los servicios que disponen de Hardware debemos destacar los errores de dichos hardware junto con desastres naturales.

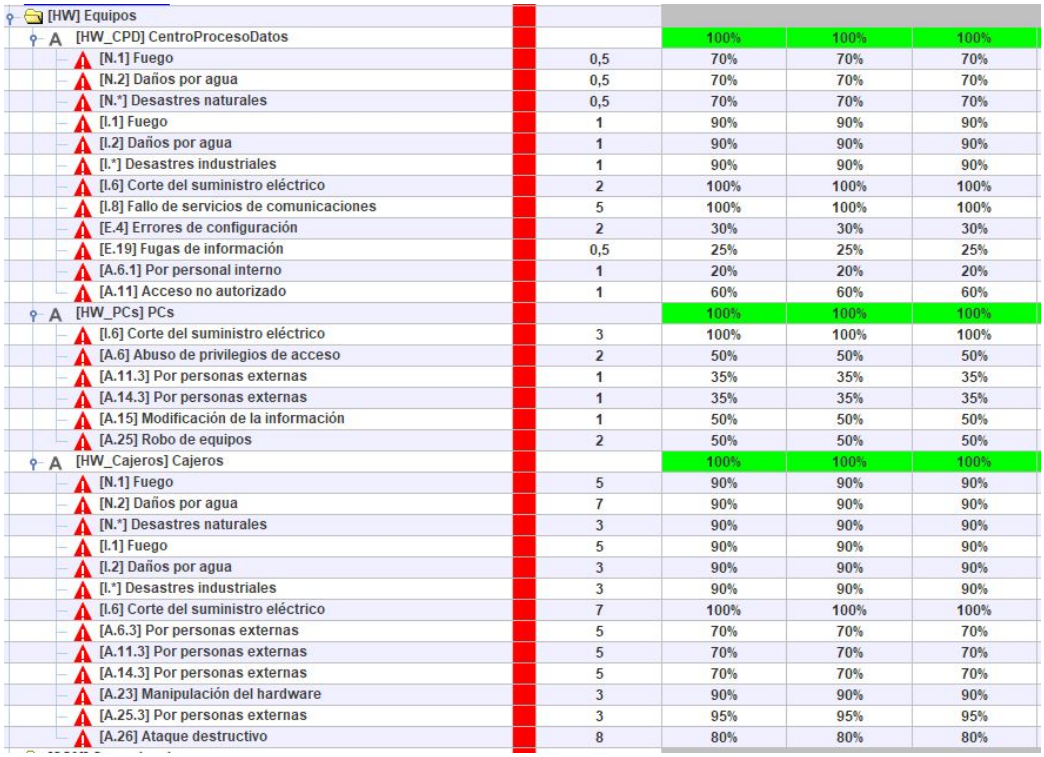
3.1. Valoración de las Amenazas

Una vez realizado el paso anterior de análisis de las amenazas, vamos a proceder a su valoración dentro de nuestra aplicación PILAR.

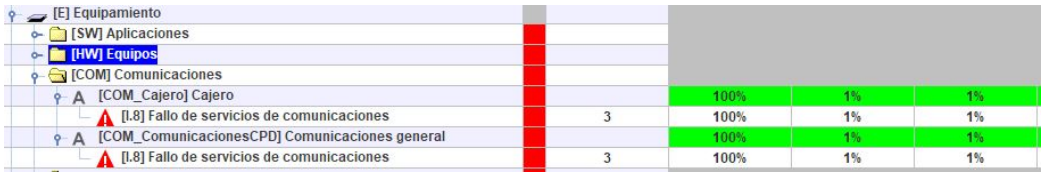
En las siguientes imágenes podemos observar la valoración de las amenzas.

ACTIVOS					
[B] Activos esenciales					
I [D_DatosBancariosClientes] DatosBancariosClientes			10%	30%	50%
[A.15] Modificación de la información		3	10%	30%	50%
[A.18] Destrucción de la información		1	10%	30%	50%
[A.22.2] Caballos de Troya		1	10%	30%	50%
[A.22.4] Puertas traseras		1	10%	30%	50%
I [D_DatosPrestamos] DatosPrestamos			10%	30%	50%
[A.15] Modificación de la información		3	10%	30%	50%
[A.18] Destrucción de la información		1	10%	30%	50%
[A.22.2] Caballos de Troya		1	10%	30%	50%
[A.22.4] Puertas traseras		1	10%	30%	50%
S [S_ServiciosBancarios] ServiciosBancarios			40%	70%	40%
[A.15] Modificación de la información		3	40%	60%	40%
[A.18] Destrucción de la información		1	40%	60%	40%
[A.22.2] Caballos de Troya		1	30%	70%	30%
[A.22.4] Puertas traseras		1	25%	70%	25%
S [S_ServicioPrestamos] ServicioPrestamos			40%	70%	40%
[A.15] Modificación de la información		3	40%	60%	40%
[A.18] Destrucción de la información		1	40%	60%	40%
[A.22.2] Caballos de Troya		1	30%	70%	30%
[A.22.4] Puertas traseras		1	25%	70%	25%

[E] Equipamiento				
[SW] Aplicaciones				
[SW_GestionInterna] GestionInterna			15%	15%	20%
[E.1] Errores de los usuarios		7	5%	10%	20%
[E.14] Fugas de información (> E.19)		0,5	1%	5%	20%
[E.15] Alteración de la información		1	3%	10%	20%
[E.18] Destrucción de la información		1	1%	15%	20%
[E.20] Vulnerabilidades de los programas (software)		1	5%	5%	20%
[A.11] Acceso no autorizado		2	10%	10%	20%
[A.15] Modificación de la información		3	15%	15%	20%
[SW_ClienteWeb] ClientesWeb			15%	15%	20%
[E.1] Errores de los usuarios		7	5%	10%	20%
[E.14] Fugas de información (> E.19)		0,5	1%	5%	20%
[E.15] Alteración de la información		1	3%	10%	20%
[E.18] Destrucción de la información		1	1%	15%	20%
[E.20] Vulnerabilidades de los programas (software)		1	5%	5%	20%
[A.11] Acceso no autorizado		2	10%	10%	20%
[A.15] Modificación de la información		3	15%	15%	20%
[SW_ClientesAppMovil] ClientesAppMovil			15%	15%	20%
[E.1] Errores de los usuarios		7	5%	10%	20%
[E.14] Fugas de información (> E.19)		0,5	1%	5%	20%
[E.15] Alteración de la información		1	3%	10%	20%
[E.18] Destrucción de la información		1	1%	15%	20%
[E.20] Vulnerabilidades de los programas (software)		1	5%	5%	20%
[A.11] Acceso no autorizado		2	10%	10%	20%
[A.15] Modificación de la información		3	15%	15%	20%
[SW_Cajero] Cajero			15%	15%	20%
[E.1] Errores de los usuarios		7	5%	10%	20%
[E.14] Fugas de información (> E.19)		0,5	1%	5%	20%
[E.15] Alteración de la información		1	3%	10%	20%
[E.18] Destrucción de la información		1	1%	15%	20%
[E.20] Vulnerabilidades de los programas (software)		1	5%	5%	20%
[A.11] Acceso no autorizado		2	10%	10%	20%
[A.15] Modificación de la información		3	15%	15%	20%



[HW] Equipos				
[HW_CPD] CentroProcesoDatos		100%	100%	100%
[N.1] Fuego	0,5	70%	70%	70%
[N.2] Daños por agua	0,5	70%	70%	70%
[N.*] Desastres naturales	0,5	70%	70%	70%
[I.1] Fuego	1	90%	90%	90%
[I.2] Daños por agua	1	90%	90%	90%
[I.*] Desastres industriales	1	90%	90%	90%
[I.6] Corte del suministro eléctrico	2	100%	100%	100%
[I.8] Fallo de servicios de comunicaciones	5	100%	100%	100%
[E.4] Errores de configuración	2	30%	30%	30%
[E.19] Fugas de información	0,5	25%	25%	25%
[A.6.1] Por personal interno	1	20%	20%	20%
[A.11] Acceso no autorizado	1	60%	60%	60%
[HW_PCs] PCs		100%	100%	100%
[I.6] Corte del suministro eléctrico	3	100%	100%	100%
[A.6] Abuso de privilegios de acceso	2	50%	50%	50%
[A.11.3] Por personas externas	1	35%	35%	35%
[A.14.3] Por personas externas	1	35%	35%	35%
[A.15] Modificación de la información	1	50%	50%	50%
[A.25] Robo de equipos	2	50%	50%	50%
[HW_Cajeros] Cajeros		100%	100%	100%
[N.1] Fuego	5	90%	90%	90%
[N.2] Daños por agua	7	90%	90%	90%
[N.*] Desastres naturales	3	90%	90%	90%
[I.1] Fuego	5	90%	90%	90%
[I.2] Daños por agua	3	90%	90%	90%
[I.*] Desastres industriales	3	90%	90%	90%
[I.6] Corte del suministro eléctrico	7	100%	100%	100%
[A.6.3] Por personas externas	5	70%	70%	70%
[A.11.3] Por personas externas	5	70%	70%	70%
[A.14.3] Por personas externas	5	70%	70%	70%
[A.23] Manipulación del hardware	3	90%	90%	90%
[A.25.3] Por personas externas	3	95%	95%	95%
[A.26] Ataque destructivo	8	80%	80%	80%



[E] Equipamiento				
[SW] Aplicaciones				
[HW] Equipos				
[COM] Comunicaciones				
[COM_Cajero] Cajero		100%	1%	1%
[I.8] Fallo de servicios de comunicaciones	3	100%	1%	1%
[COM_ComunicacionesCPD] Comunicaciones general		100%	1%	1%
[I.8] Fallo de servicios de comunicaciones	3	100%	1%	1%

4. Salvaguardas del Sistema de Información

En este apartado vamos a tratar las salvaguardas de nuestro sistema dentro de la herramienta PILAR. En el apartado de salvaguardas, vamos a seleccionar aquellas que son de vital importancia en nuestro sistema. Las salvaguardas propuestas para nuestro sistema son las siguientes:

[base] Base

	aspecto	tdp	salvaguarda	dudas	fuente	come...	recom.	on / off	aplica
			SALVAGUARDAS						
	G	EL	[IA] Identificación y autenticación			(*)	8		
	T	EL	[AC] Control de acceso lógico			(*)	7		
	G	PR	[D] Protección de la Información			(*)	6		
	G	EL	[K] Protección de claves criptográficas						
	G	PR	[S] Protección de los Servicios						
	G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7		
	G	PR	[HW] Protección de los Equipos Informáticos (HW)				7		
	G	PR	[COM] Protección de las Comunicaciones				7		
	G	PR	[IP] Sistema de protección de frontera lógica						
	G	PR	[MP] Protección de los Soportes de Información						...
	G	PR	[AUX] Elementos Auxiliares				5		...
	F	EL	[HW_0049] Protección física del equipamiento				6		n.a.
	F	PR	[L] Protección de las Instalaciones						...
	F	EL	[PPS] Protección del perímetro físico						...
	P	PR	[PS] Gestión del Personal						...
	G	PR	[PDS] Servicios potencialmente peligrosos						...
	G	CR	[IR] Gestión de incidentes				6		...
	T	PR	[tools] Herramientas de seguridad				6		...
	G	CR	[V] Gestión de vulnerabilidades				6		
	T	MN	[A] Registro y auditoría						...
	G	RC	[BC] Continuidad del negocio				5		...
	G	AD	[G] Organización				5		...
	G	AD	[E] Relaciones Externas				6		
	G	AD	[NEW] Adquisición / desarrollo				5		...

Una vez visto las salvaguardas de nuestro sistema, vamos a proceder a su valoración.

4.1. Valoración de las Salvaguardas

Para la valoración de las salvaguardas nos centramos en dos campos: Target y Current. Current se corresponde con el nivel de salvaguarda a día de hoy mientras que Target se corresponde con el nivel inicial de la salvaguarda. Como podemos observar en la anterior figura, al ser nuestro sistema de información un sistema que maneja datos y servicios de vital importancia, no sólo a nivel de empresa, sino que repercute en diferentes organizaciones, las medidas de las salvaguardas están la gran mayoría al máximo para así poder garantizar una estabilidad en su funcionamiento.

[base] Base — Fuentes de información

	aspecto	tdp	salvaguarda	dudas	fuente	come...	reco...		current	target	PILAR
			SALVAGUARDAS								
	G	EL	[IA] Identificación y autenticación			(*)	8		L3	L5	L2-L5
	T	EL	[AC] Control de acceso lógico			(*)	7		L3	L5	L2-L4
	G	PR	[D] Protección de la Información			(*)	6		L3	L5	L2-L4
	G	EL	[K] Protección de claves criptográficas						L3	L5	n.a.
	G	PR	[S] Protección de los Servicios						L3	L5	n.a.
	G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7		_L5	_L5	L2-L4
	G	PR	[HW] Protección de los Equipos Informáticos (HW)				7		L2	L5	L2-L4
	G	PR	[COM] Protección de las Comunicaciones				7		L4	L5	L2-L4
	G	PR	[IP] Sistema de protección de frontera lógica						L3	L5	n.a.
	G	PR	[MP] Protección de los Soportes de Información						L4	L5	n.a.
	G	PR	[AUX] Elementos Auxiliares				5		L3	L5	L2-L3
	F	PR	[L] Protección de las Instalaciones						L4	L5	n.a.
	F	EL	[PPS] Protección del perímetro físico						L4	L5	n.a.
	P	PR	[PS] Gestión del Personal						L4	L5	n.a.
	G	PR	[PDS] Servicios potencialmente peligrosos						L4	L5	n.a.
	G	CR	[IR] Gestión de incidentes				6		L4	L5	L2-L3
	T	PR	[tools] Herramientas de seguridad				6		L3	L5	n.a.
	G	CR	[V] Gestión de vulnerabilidades				6		L4	L5	L2-L4
	T	MN	[A] Registro y auditoría						L4	L5	n.a.
	G	RC	[BC] Continuidad del negocio				5		L4	L5	L2-L3
	G	AD	[G] Organización				5		L2	L5	L2-L3
	G	AD	[E] Relaciones Externas				6		L3	L5	L2-L4
	G	AD	[NEW] Adquisición / desarrollo				5		L4	L5	L2-L3

4.2. Análisis de riesgos residual

Una vez realizado la valoraciń de las salvaguardas, podemos calcular el riesgo residual entre el estado actual y su objetivo.

potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS	141K	238K	264K
[B] Activos esenciales	23K	64K	53K
[D_DatosBancariosClientes] DatosBancariosClientes	1,4K	4K	6,8K
[D_DatosPrestamos] DatosPrestamos	1,6K	23K	26K
[S_ServiciosBancarios] ServiciosBancarios	11K	20K	11K
[S_ServicioPrestamos] ServicioPrestamos	9,2K	16K	9,2K
[IS] Servicios internos	0	0	0
[E] Equipamiento	118K	174K	211K
[SW] Aplicaciones	11K	31K	67K
[SW_GestionInterna] GestionInterna	5,3K	16K	34K
[SW_ClienteWeb] ClientesWeb	1,6K	4,3K	9,4K
[SW_ClientesAppMovil] ClientesAppMovil	1,6K	4,3K	9,4K
[SW_Cajero] Cajero	2,3K	6,3K	14K
[HW] Equipos	108K	143K	143K
[HW_CPD] CentroProcesoDatos	56K	79K	79K
[HW_PCs] PCs	3,4K	3,4K	3,5K
[HW_Cajeros] Cajeros	47K	62K	62K
[COM] Comunicaciones	574	5,5	5,6
[COM_Cajero] Cajero	251	2,8	2,8
[COM_ComunicacionesCPD] Comunicaciones general	323	2,7	2,8
[SS] Servicios subcontratados	0	0	0
[L] Instalaciones	0	0	0
[P] Personal	0	0	0

potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[D_DatosBancariosClientes] DatosBancariosClientes			
[D_DatosPrestamos] DatosPrestamos			
[S_ServiciosBancarios] ServiciosBancarios			
[S_ServicioPrestamos] ServicioPrestamos			
[IS] Servicios internos	0	0	0
[E] Equipamiento			
[SW] Aplicaciones	2K	6,3K	15K
[SW_GestionInterna] GestionInterna	1K	3,4K	7,7K
[SW_ClienteWeb] ClientesWeb	297	828	2K
[SW_ClientesAppMovil] ClientesAppMovil	297	828	2K
[SW_Cajero] Cajero	425	1,3K	3,1K
[HW] Equipos			
[HW_CPD] CentroProcesoDatos			
[HW_PCs] PCs			
[HW_Cajeros] Cajeros			
[COM] Comunicaciones			
[COM_Cajero] Cajero			
[COM_ComunicacionesCPD] Comunicaciones general			
[SS] Servicios subcontratados	0	0	0
[L] Instalaciones	0	0	0
[P] Personal	0	0	0

4.3. Plan de seguridad

El plan de seguridad se adjunta en fichero pdf.