

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



CASO DE ÉXITO:

IMPLANTACIÓN DE PILAR PARA LA
ADECUACIÓN AL RGPD EN LA CONSEJERÍA
DE SANIDAD DE LA COMUNIDAD DE
MADRID



○ Jose Manuel Laperal González

○ CISO SERVICIO MADRILEÑO DE SALUD (SERMAS)

OFICINA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN (OSSI)
DIRECCIÓN GENERAL DE SISTEMAS DE INFORMACIÓN SANITARIA
(DGSIS)
CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID (CSCM)

○ jose.manuel.laperal@madrid.org

Índice

1. Presentación de la OSSI.
2. Introducción.
3. Proyecto: Implantación de la herramienta PILAR para la adecuación al RGPD en la CSCM.
4. Objetivos alcanzados.
5. Próximos pasos.

Presentación de la OSSI

Oficina de Seguridad de Sistemas de Información (OSSI)

Da soporte a los organismos del Servicio Madrileño de Salud (SERMAS), tanto a nivel técnico como legal.

Cumplimiento legal y normativo.

Asesoría y auditoría de controles de seguridad de TI.

SERVICIO SOC. Monitorización y correlación de eventos de seguridad.

Análisis de software, hardware, malware y análisis forense.

Comunicación y formación en seguridad de la información.

Gestión documental.



Introducción

Retos

RETOS

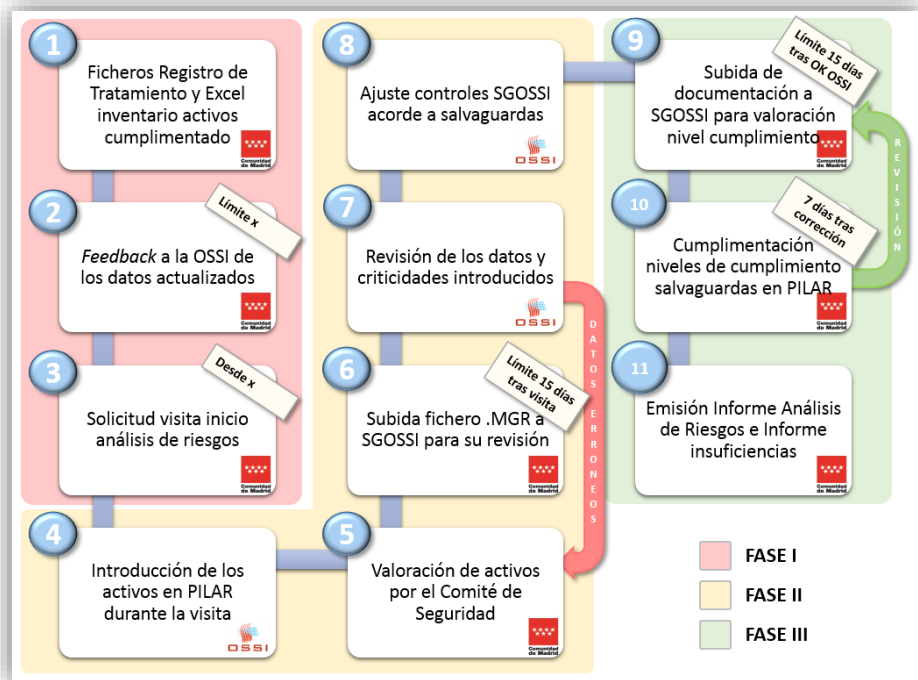
- Evitar soluciones dispersas, divergentes a los mismos problemas.
- Evitar duplicidades, máximo aprovechamiento de recursos.
- No aprovechamiento buenas prácticas.

VISIÓN

- Proveer la seguridad como un servicio.
- Gestionar de forma homogénea y con criterios unificados.
- Provisionar un servicio altamente especializado. Adaptable a las distintas realidades de los centros y enriquecido con sus experiencias.

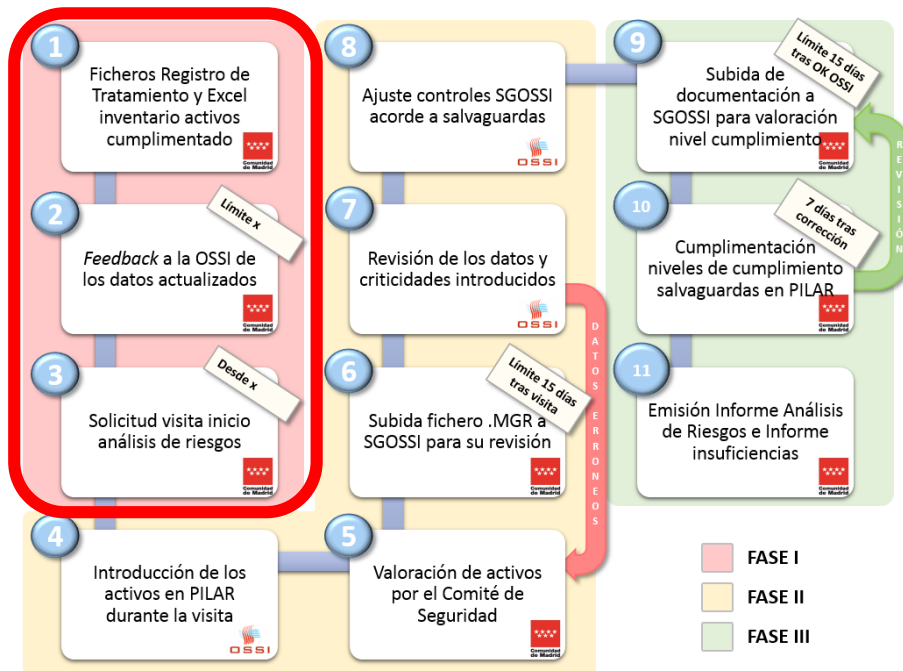
Implantación de PILAR para la adecuación al RGPD en la CSCM

Fases



Implantación de PILAR para la adecuación al RGPD en la CSCM

Fases

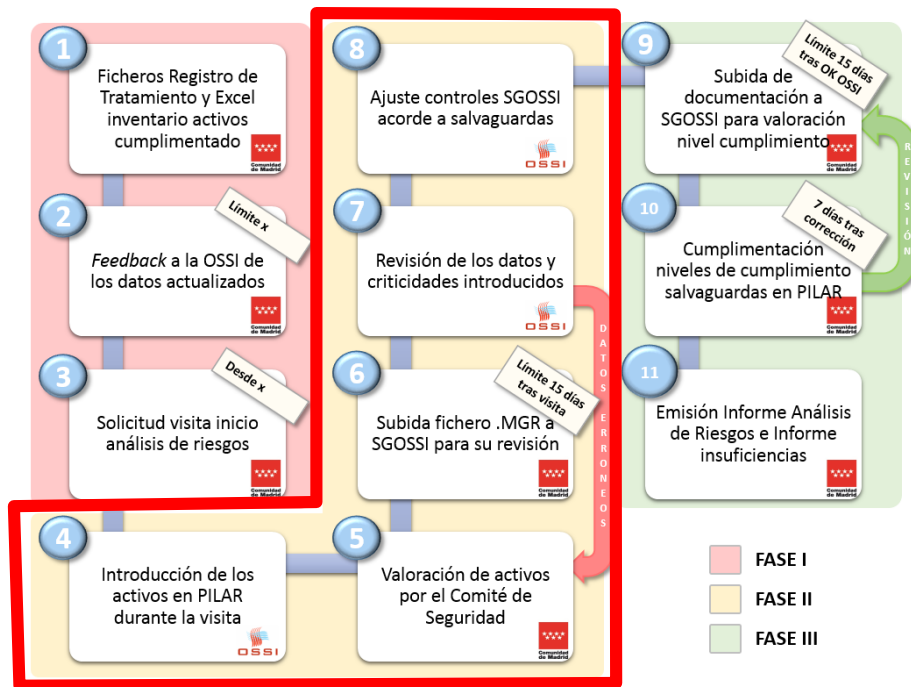


Recopilación de información de los centros sanitarios en base a los **Diagnósticos de Seguridad y auditorías de LOPD** realizados en años anteriores.

Con dicha información se han realizado plantillas para obtener un **inventario de activos** a medida para cada centro y a su vez diseñar el **modelo de dependencias**.

Implantación de PILAR para la adecuación al RGPD en la CSCM

Fases



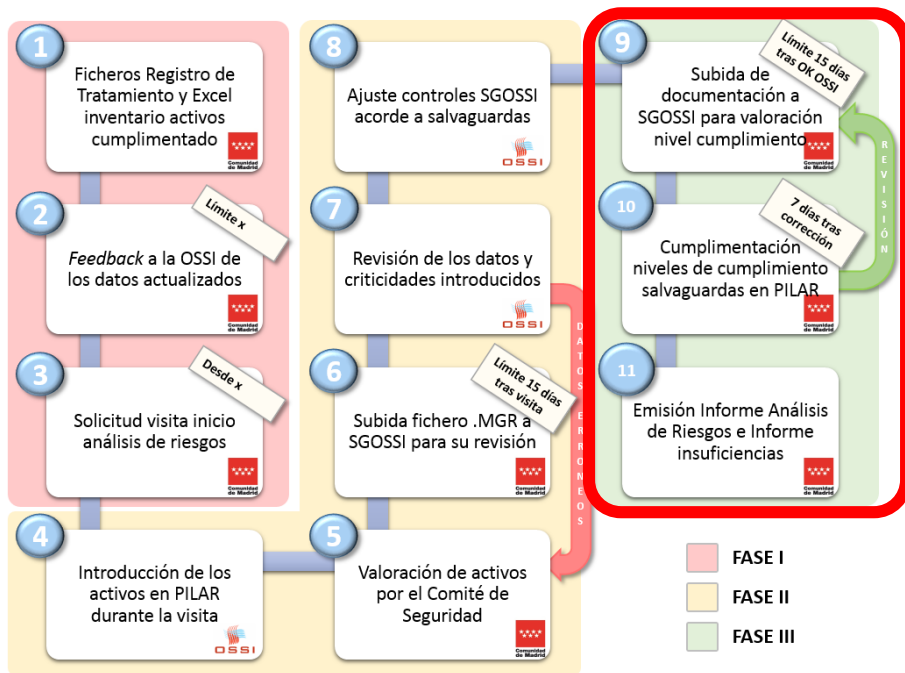
Formación de PILAR para los centros.

Introducción de los activos y dependencias en el proyecto.

Valoración de los activos por el Comité de Seguridad de los centros (Apoyo Comité del SERMAS).

Implantación de PILAR para la adecuación al RGPD en la CSCM

Fases



Asignación de niveles de las salvaguardas.

Resultado del informe del análisis de riesgos.

Plan de tratamiento de riesgos.

Implantación de PILAR para la adecuación al RGPD en la CSCM

Fase I

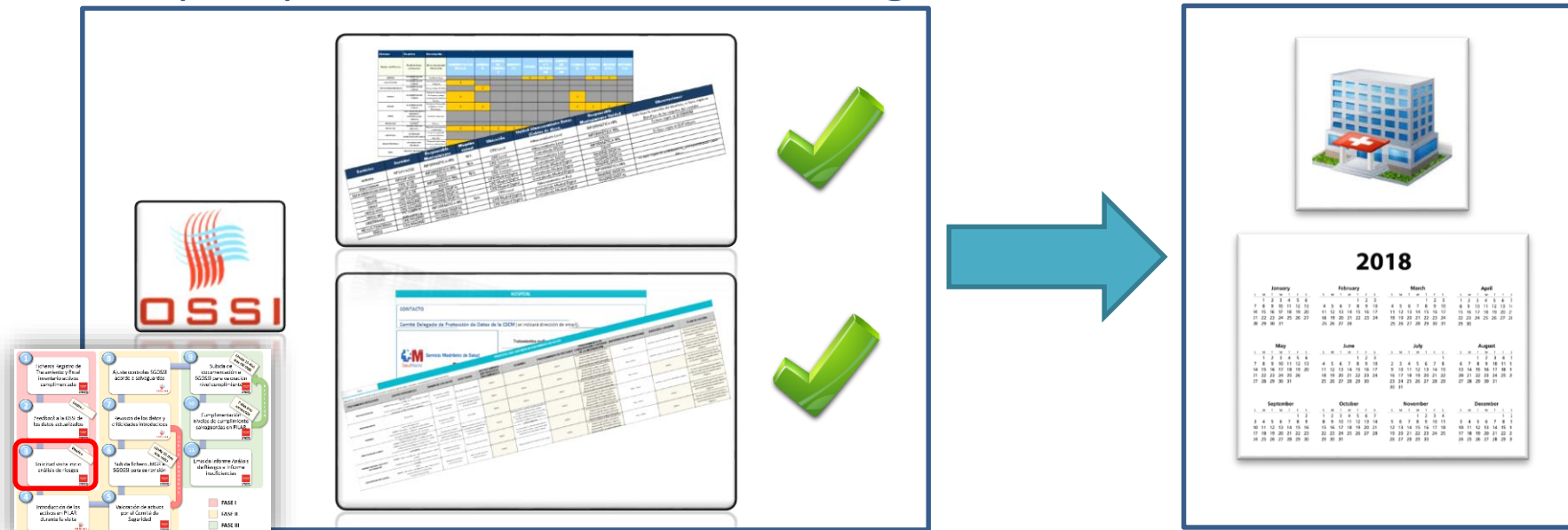
- Hito II:** el centro remite los ficheros a la OSSI para su validación.



Implantación de PILAR para la adecuación al RGPD en la CSCM

Fase I

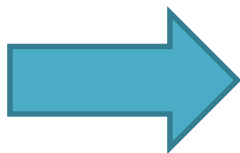
- **Hito III:** una vez validados los ficheros, se concierta una visita con el hospital para iniciar el análisis de riesgo.



Implantación de PILAR para la adecuación al RGPD en la CSCM

Fase 2

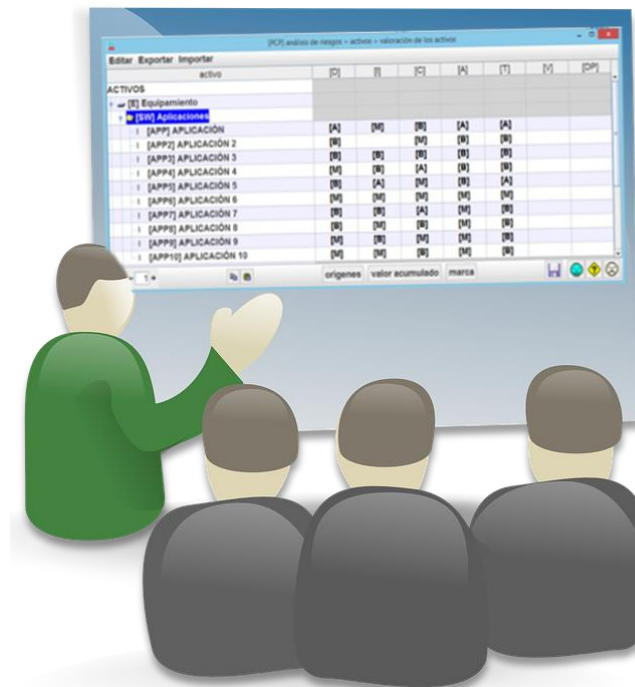
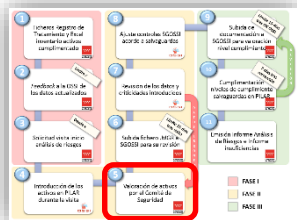
- **Hito IV:** el equipo de la OSSI lleva a cabo una formación en el uso de PILAR y presta apoyo en la introducción de activos, así como en el establecimiento de dependencias.



Implantación de PILAR para la adecuación al RGPD en la CSCM

Fase 2

- **Hito V:** la valoración de los activos se establece por el Comité de Seguridad atendiendo al impacto real que este tiene sobre el servicio del centro.

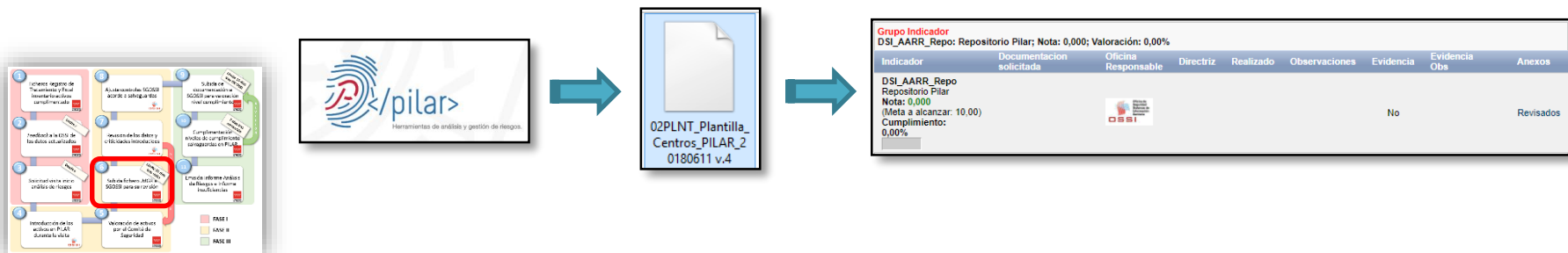


Implantación de PILAR para la adecuación al RGPD en la CSCM

Fase 2

La OSSI cuenta con un Sistema de Gestión (SGOSSI), utilizado para la evaluación, seguimiento y control de las exigencias en el ámbito de seguridad de la información de los centros dependientes de la CSCM.

- **Hito VI:** el centro anexa en la herramienta SGOSSI el fichero .MGR del proyecto de PILAR actualizado con la valoración de los activos realizada por el Comité de Seguridad para su revisión.

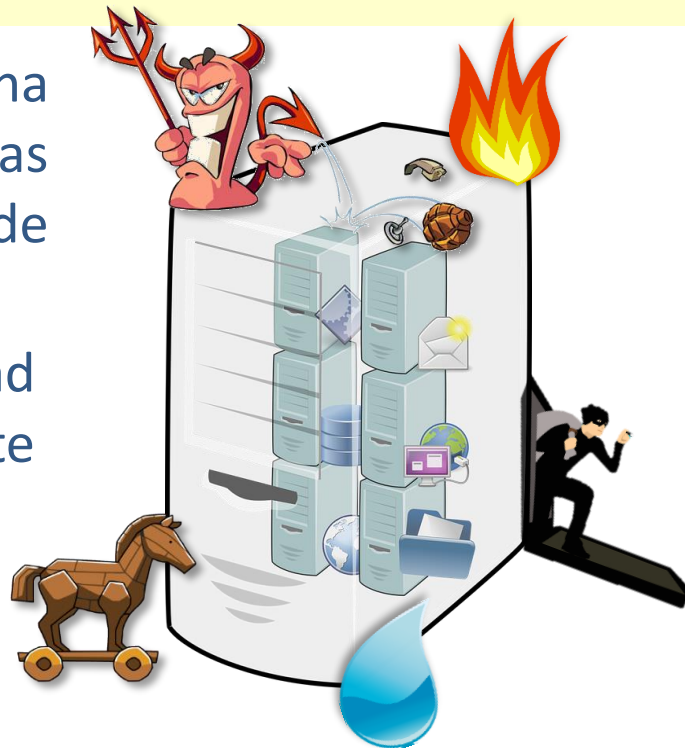
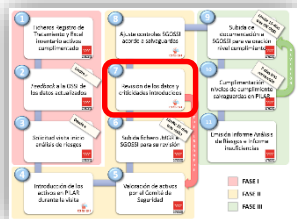


Implantación de PILAR para la adecuación al RGPD en la CSCM

Fase 2

- **Hito VII.b:** la OSSI facilita a los centros una plantilla basada en el ENS, de las amenazas asociadas acorde al tipo de activos.

Estas amenazas así como su probabilidad de ocurrencia se cargan automáticamente dependiendo del tipo de activo.



Implantación de PILAR para la adecuación al RGPD en la CSCM

Fase 3

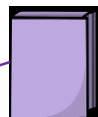
- Hito VIII:** desde la OSSI se indican las evidencias que los centros tienen que proporcionar como salvaguardas.

[OSSI] análisis de riesgos > salvaguardas > Eficacia de la

Editar Expandir Exportar Importar Estadísticas

[base] Ejemplo OSSI Fuentes de información

	asp...	tdp	salvaguarda	dudas
			SALVAGUARDAS	
☐	G	EL	13 [IA] Identificación y autenticación	
☐	G	EL	13 [IA.3] Identificación de los usuarios	
☐	G	EL	13 [IA.4] Gestión de la identificación y autenticación de usuario	
☐	G	EL	13 [IA.5] Cuentas especiales (administración)	
☐	G	PR	13 [IA.7] (ver) Factores de autenticación que se requieren.	
☐	T	EL	13 [AC] Control de acceso lógico	
☐	T	PR	13 [AC.1] Gestión de privilegios	
☐	T	EL	13 [AC.2] Imposición del control de acceso	
☐	T	IM	13 [AC.3] Separación de tareas	
☐	G	PR	13 [D] Protección de la Información	
☐	G	AD	13 [D.1] Se dispone de un inventario de activos de información	
☐	G	std	13 [D.2] Normativa	
☐	G	PR	13 [D.4] Protección de la confidencialidad	
☐	G	RC	13 [D.backup] Copias de seguridad (backups)	
☐	T	EL	13 [D.DS] Uso de firmas electrónicas	
☐	G	IM	13 [D.TSI] Uso de servicios de fechado electrónico (time stamping)	
☐	G	EL	13 [K] Protección de claves criptográficas	
☐	G	PR	13 [S] Protección de los Servicios	
☐	G	PR	13 [SW] Protección de las Aplicaciones Informáticas (SW)	
☐	G	PR	13 [SW.1] Administración	
☐	G	EL	13 [SW.backup] Copias de seguridad (backup) (SW)	



Procedimiento de identificación y autenticación de usuarios.



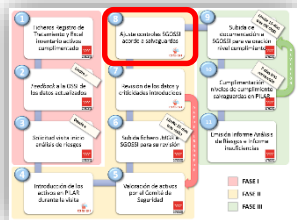
Procedimiento de control de acceso lógico.



Procedimiento de protección de la información.



Procedimiento de protección de las claves criptográficas.

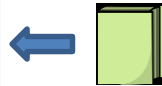
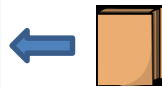
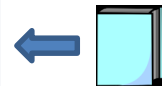
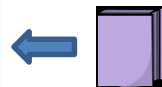
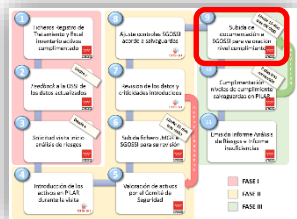


Implantación de PILAR para la adecuación al RGPD en la CSCM

Fase 3

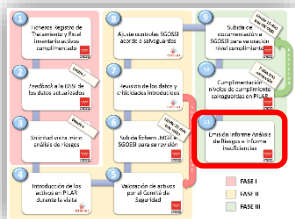
- Hito IX:** la OSSI revisa las evidencias mediante la herramienta SGOSSI e indica el nivel de cumplimiento que tiene en cada salvaguarda.

Grupo Indicador							
DSL_AARR_IA: Identificación y autenticación; Nota: 0,000; Valoración: 0,00%							
Indicador	Documentación solicitada	Oficina Responsable	Diseñador	Realizado	Observaciones	Evidencia	Anexos
DSL_AARR_IA.1 Se dispone de normativa de identificación y autenticación Nota: 0,000 (Meta a alcanzar: 5,00) Cumplimiento: 0,00%	Procedimiento de autenticación		No	0		No	No existen Anexos
DSL_AARR_IA.2 Se dispone de procedimientos para las tareas de identificación y autenticación Nota: 0,000 (Meta a alcanzar: 5,00) Cumplimiento: 0,00%	Procedimiento de gestión de usuarios		No	0		No	No existen Anexos
DSL_AARR_IA.3 Identificación de los usuarios Nota: 0,000 (Meta a alcanzar: 5,00) Cumplimiento: 0,00%	Procedimiento de gestión de usuarios		No	0		No	No existen Anexos
DSL_AARR_IA.4 Gestión de la identificación y autenticación de usuario Nota: 0,000 (Meta a alcanzar: 5,00) Cumplimiento: 0,00%	Procedimiento de gestión de usuarios		No	0		No	No existen Anexos



Fase 3

- **Hito XI:** el centro procede a la emisión del Informe de Análisis de Riesgos.



PILAR [OSSI] Ejemplo OSSI

Proyecto Fichero Db Editar Nivel Ayuda

CONFIDENCIAL

Análisis cualitativo

- D. Proyecto
- A. Análisis de riesgos
- R. Informes
 - R.tpl. por patrón
 - R.T. textuales
 - Resumen de riesgos
 - Modelo de valor (corto)
 - Modelo de valor (largo)
 - Informe de amenazas
 - Evaluación de las salvaguardas
 - Informe de insuficiencias (< Lx)
 - Informe de insuficiencias (< objetivo)
 - Análisis de impacto
 - Análisis de riesgos
 - Perfil de seguridad
 - R.g. gráficas
 - R.sql. Db
 - INÉS: Informe Anual del ENS
- E. Perfiles de seguridad

02FICH_PILAR_OSSI v2..



CDSII Ejemplo CDSII

Análisis de riesgos

5. Riesgo acumulado

5.1. Fase: [INICIAL] Estado Inicial Ejemplo CDSII

[E] Equipamiento

	[E]	[I]	[D]	[A]	[M]	[A]	[M]	[D]	[I]
01	Aplicaciones	(4,3)	(3,9)	(3,9)	(3,9)	(3,9)	(3,9)	(3,9)	(3,9)
02	Computadores	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
03	Impresoras	(0,7)	(2,9)	(2,9)	(2,9)	(2,9)	(2,9)	(2,9)	(2,9)
04	Software	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
05	Redes	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
06	Perif. de salida	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
07	Perif. de entrada	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
08	Perif. de almacenamiento	(4,3)	(3,9)	(3,9)	(3,9)	(3,9)	(3,9)	(3,9)	(3,9)
09	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
10	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
11	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
12	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
13	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
14	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
15	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
16	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
17	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
18	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
19	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
20	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
21	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
22	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
23	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
24	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
25	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
26	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
27	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
28	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
29	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
30	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
31	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
32	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
33	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
34	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
35	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
36	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
37	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
38	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
39	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
40	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
41	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
42	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
43	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
44	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
45	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
46	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
47	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
48	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
49	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
50	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
51	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
52	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
53	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
54	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
55	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
56	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
57	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
58	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
59	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
60	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
61	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
62	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
63	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
64	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
65	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
66	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
67	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
68	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
69	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
70	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
71	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
72	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
73	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
74	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
75	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
76	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
77	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
78	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
79	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
80	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
81	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
82	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
83	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
84	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
85	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
86	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
87	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
88	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
89	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
90	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
91	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
92	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
93	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
94	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
95	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
96	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
97	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
98	Perif. de almacenamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
99	Perif. de comunicación	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
100	Perif. de procesamiento	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)

[R] Registro de Tratamiento

	[E]	[I]	[D]	[A]	[M]	[A]	[M]	[D]	[I]
01	Registros de Tratamiento	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
02	Documentación técnica	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
03	Documentación Regulatoria, Oficial	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
04	Asesoramiento Técnico y Formación	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
05	Formación y Recurso	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
06	Formación de Recursos Humanos y Prevención de Riesgos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
07	Formación	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
08	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
09	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
10	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
11	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
12	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
13	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
14	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
15	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
16	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
17	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
18	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
19	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
20	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
21	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
22	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
23	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
24	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
25	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
26	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
27	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
28	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
29	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
30	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
31	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
32	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
33	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
34	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
35	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
36	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
37	Formación y Gestión de Accesos	(0,0)	(0,0)	(0,0)	(0,0)	(			

Objetivos alcanzados

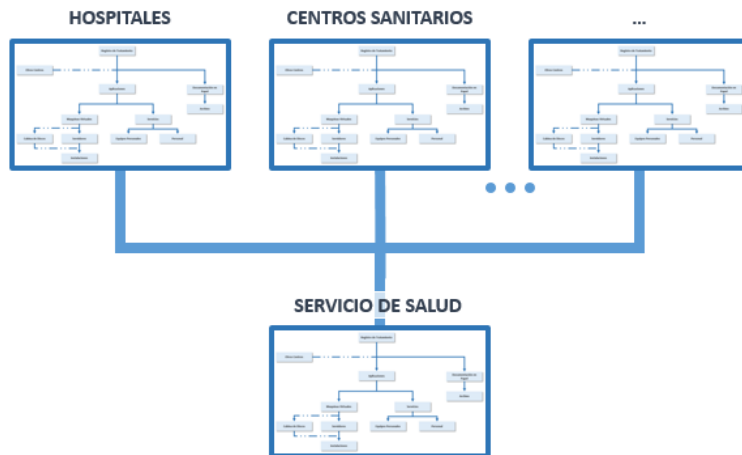


- ✓ Realizar una gestión de riesgos adecuada.
- ✓ Establecer una estrategia homogénea para toda la Consejería de Sanidad de la Comunidad de Madrid.
- ✓ Definir líneas de trabajo, claras y concretas, que les dan a los centros una guía sencilla y clara a seguir.
- ✓ Aunar el cumplimiento de normativa diversa (ENS y RGPD) con una misma herramienta informática.
- ✓ Mantener un control del proceso de adecuación mediante una retroalimentación y seguimiento de la estrategia desplegada.

Próximos pasos

Entornos multicentros para proyectos de PILAR en SERMAS

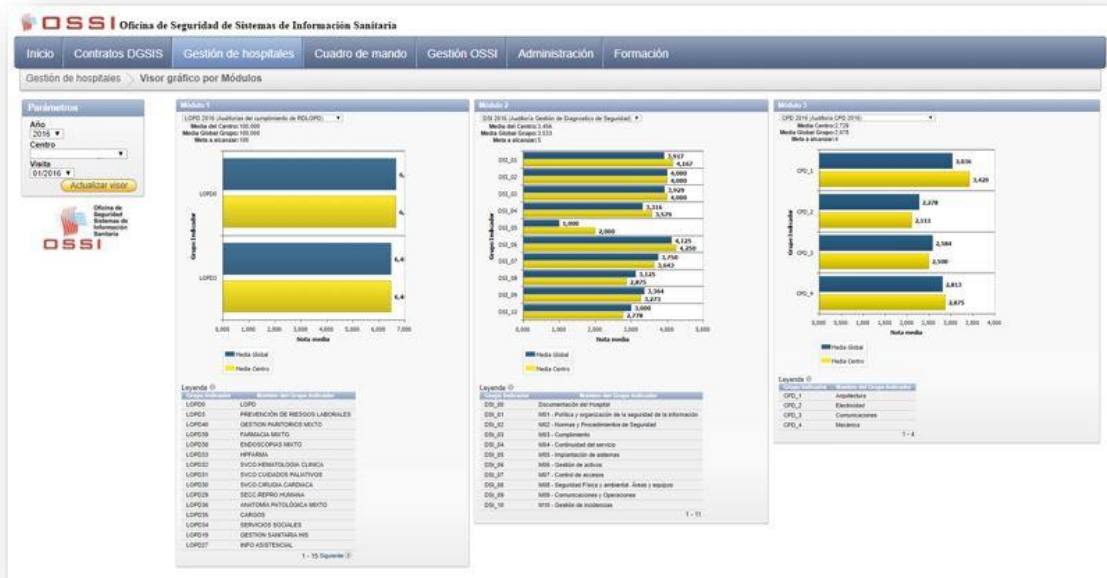
Enriquecimiento de las capacidades de la herramienta PILAR hacia un entorno multicentro que permita obtener una visión global del estado del riesgo de la Consejería de Sanidad de la Comunidad de Madrid.



Próximos pasos

Integración herramienta Sistema de Gestión OSSI con PILAR

Implementar en nuestro SGOSSI un módulo de integración de proyectos de PILAR para el control centralizado del cumplimiento normativo por parte de los centros.



Ventaja: No es un software cerrado

Próximos pasos

Integración herramienta Sistema de Gestión OSSI con PILAR

Objetivo: obtener una **visión global** del estado del **riesgo de los centros**, unificando la información registrada en sus respectivos ficheros de **PILAR** en una base de datos única para ser explotada por la OSSI.



Próximos pasos

Integración herramienta Sistema de Gestión OSSI con PILAR

Los **centros y otras entidades** envían periódicamente sus datos de **PILAR**

La OSSI procesa los ficheros recibidos y **consolida la información** en la herramienta de gestión SGOSSI

Un **nuevo módulo de explotación de datos** permite extraer informes y gráficos de control y seguimiento

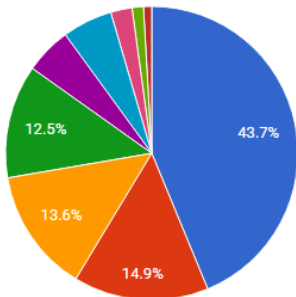
Próximos pasos

Integración herramienta Sistema de Gestión OSSI con PILAR

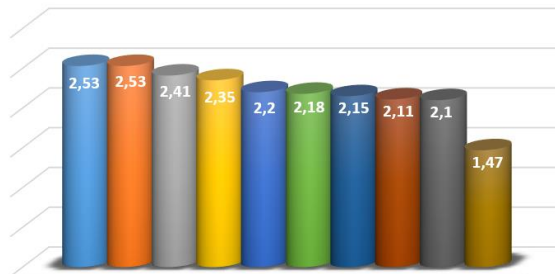


Próximos pasos

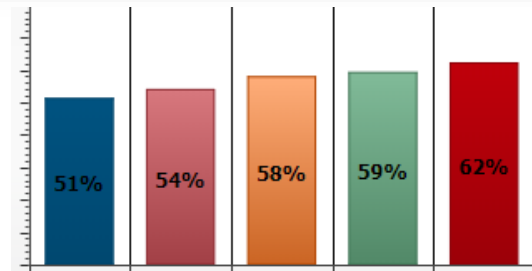
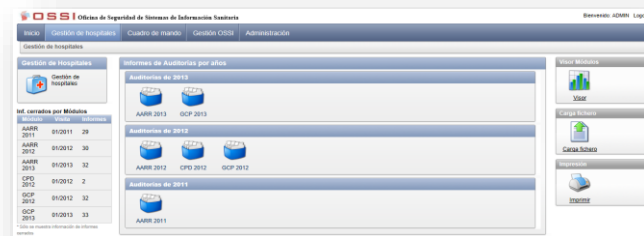
Integración herramienta Sistema de Gestión OSSI con PILAR



TOP 10 de activos con mayor riesgo (a nivel global).



TOP 10 de activos con mayor riesgo (a nivel de centro).



Hospital por grupo y su nivel de riesgo.

Próximos pasos

Integración herramienta Sistema de Gestión OSSI con PILAR

VISIÓN

- ✓ Proveer la seguridad como un servicio.
- ✓ Gestionar de forma homogénea y con criterios unificados.
- ✓ Provisionar un servicio altamente especializado. Adaptable a las distintas realidades de los centros y enriquecido con sus experiencias.



oficina.seguridad@salud.madrid.org

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- oc.ccn.cni.es

➤ Síguenos en

