

Actualización del ENS

Retos

Pilar en nube

*I Encuentro del ENS.
Tendencias y Políticas de Seguridad*

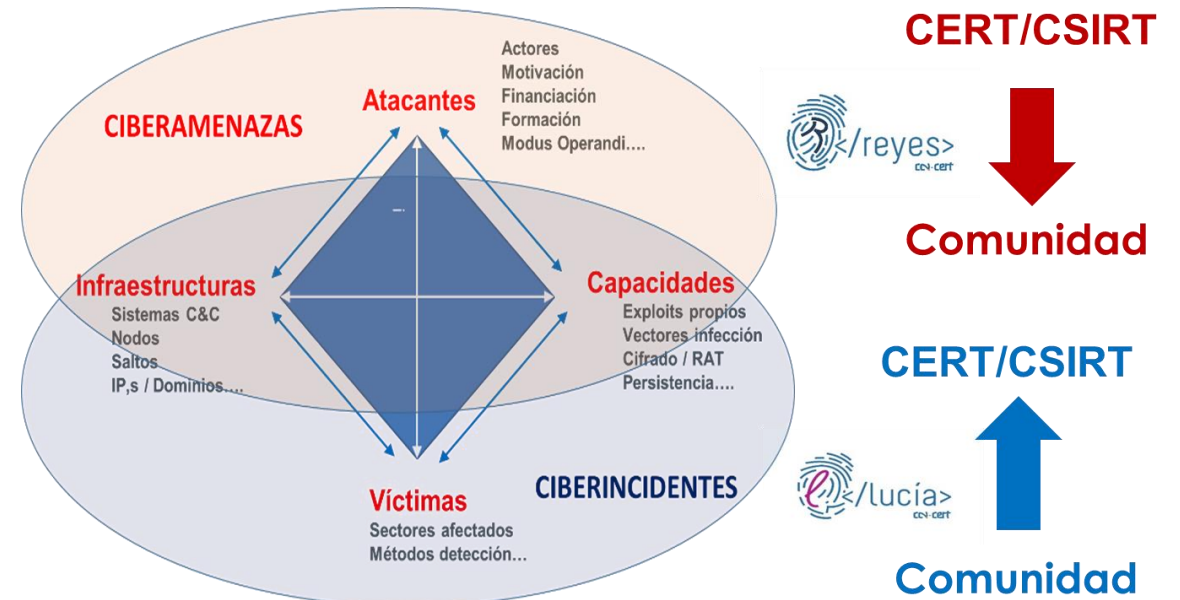


Índice

1. Cumplimiento del ENS. Retos

2. Nuevo PILAR CLOUD

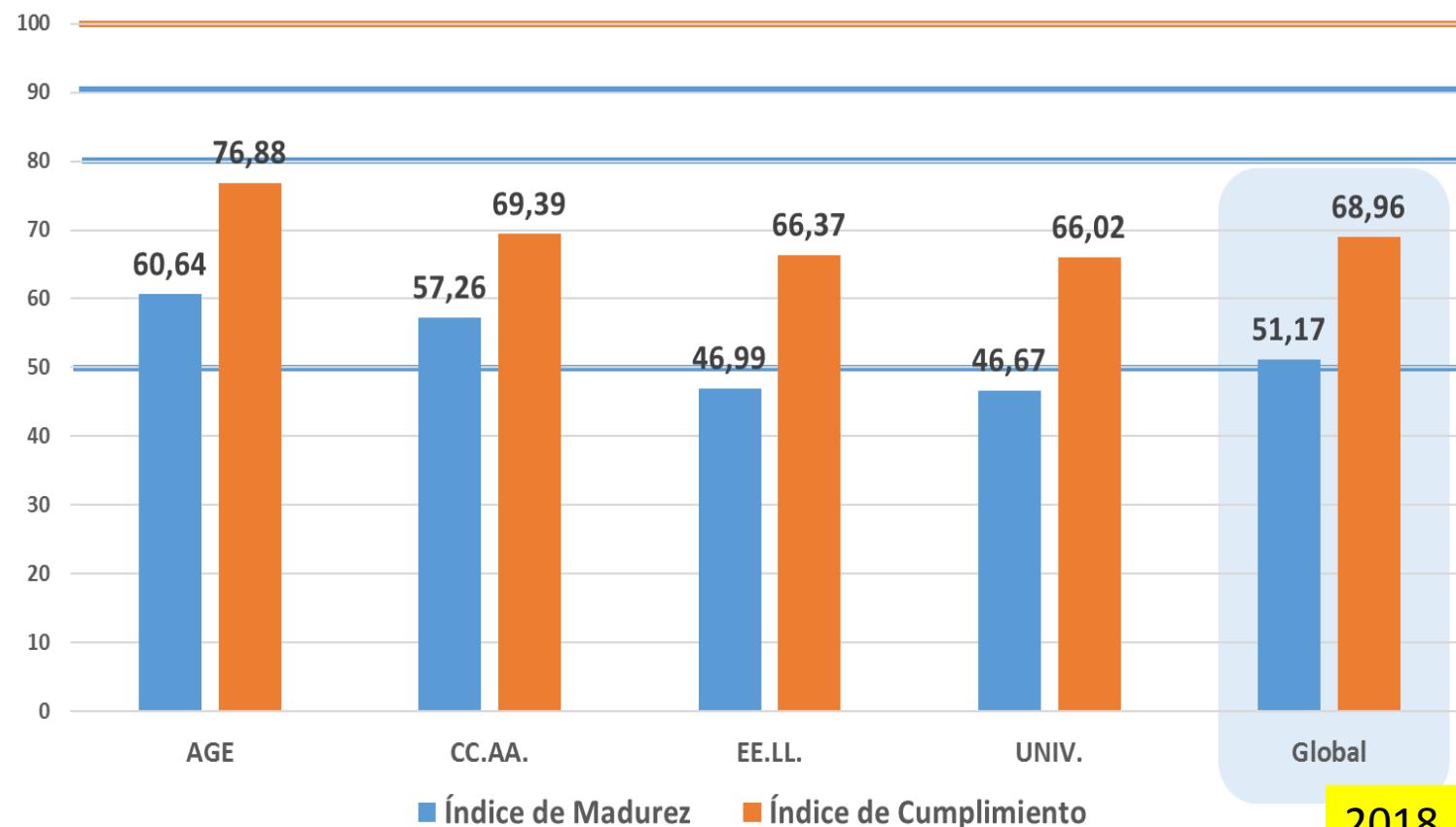
3. Conclusiones



El nivel de madurez sigue siendo **BAJO**



Prevención



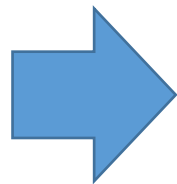
**Sistemas de
Organismos públicos
Certificados (34)**

2017----- 9 / 37

2018----- 28 / 101

2019----- 34 / 136

2018



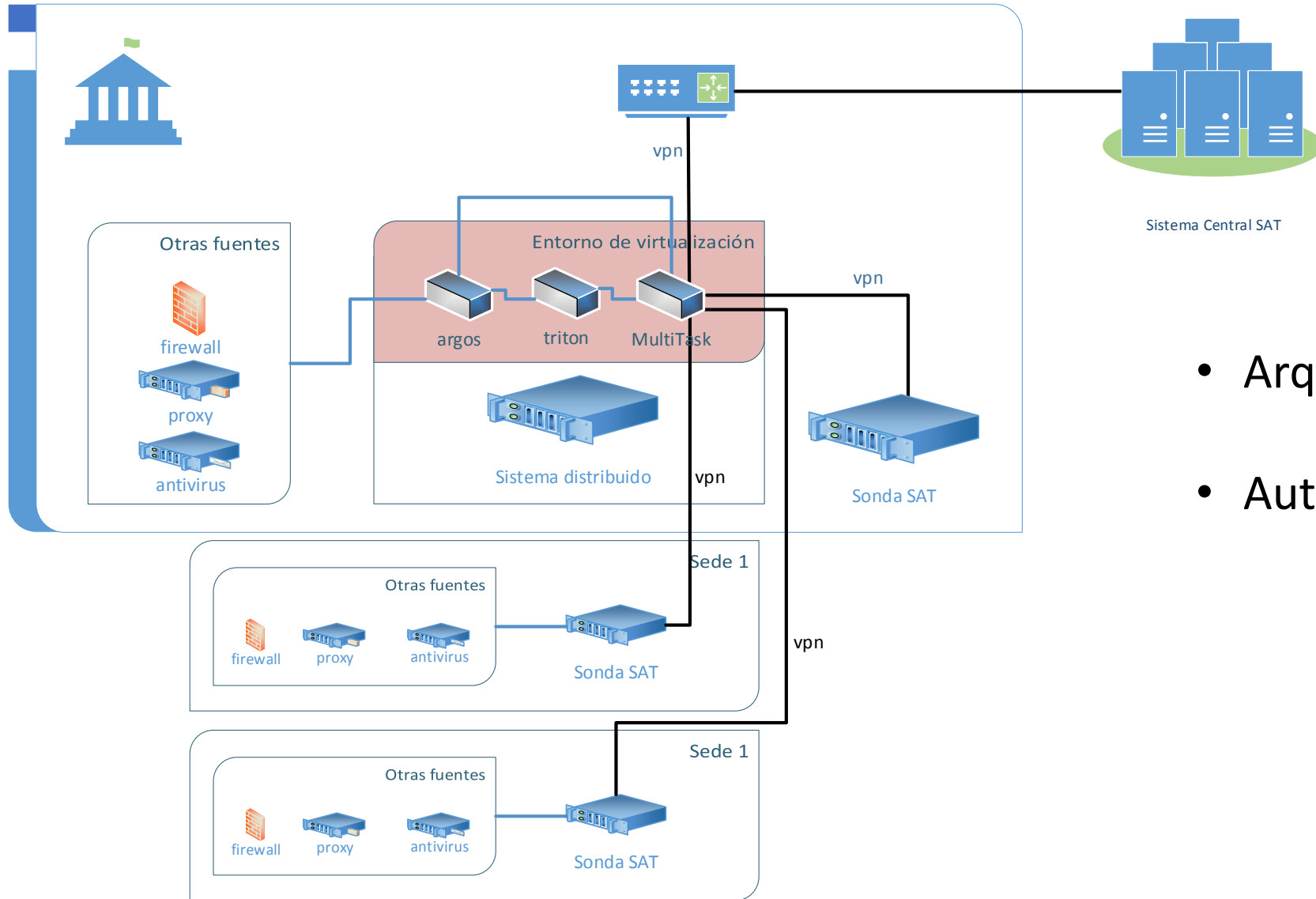
Detección



| | |
|------------|-----|
| LUCIA 2016 | 5% |
| LUCIA 2017 | 21% |
| LUCIA 2018 | 27% |
| LUCIA 2019 | 33% |
| OBJETIVO | ??% |

- Disponer de un SIEM no es una opción
- Vigilar Perímetro y Red interna
- Basados en reglas y anomalías
- El punto final no es una opción



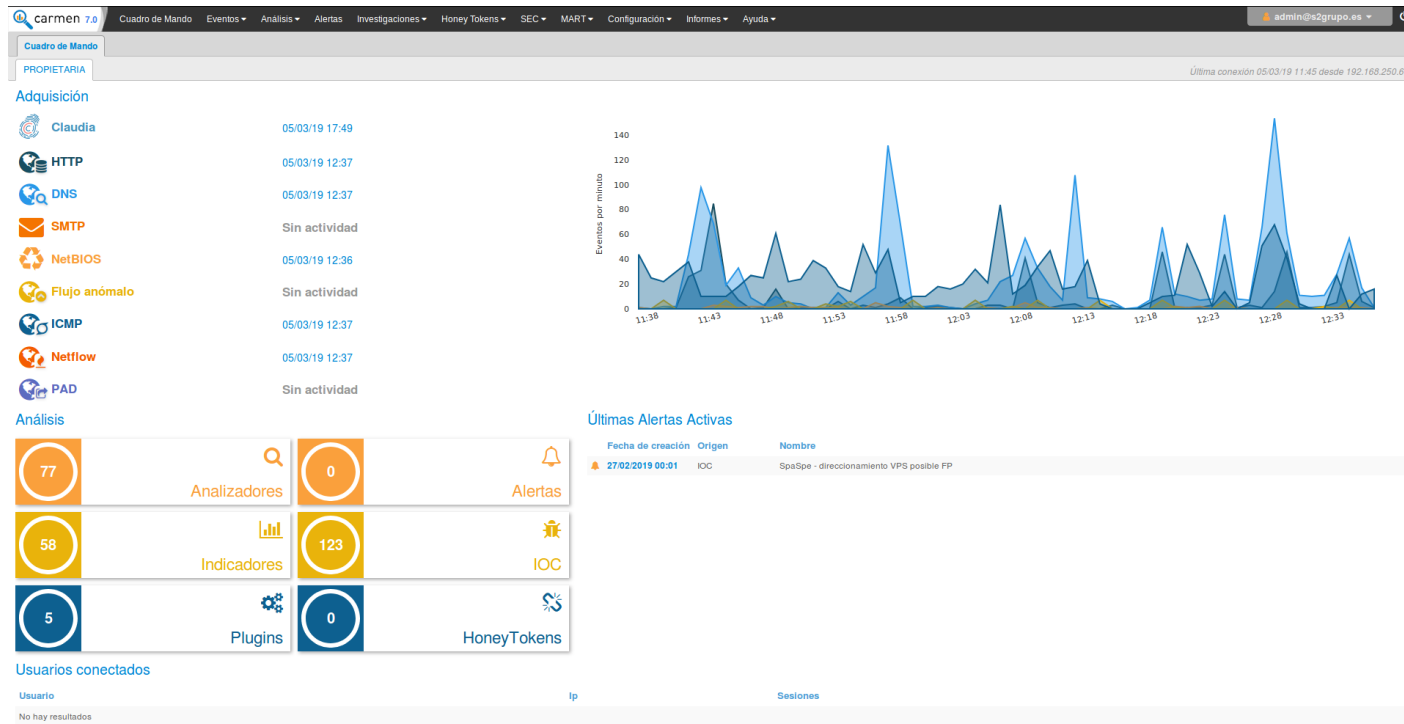


- Arquitectura distribuida
- Automatización

Detección basada en Anomalías

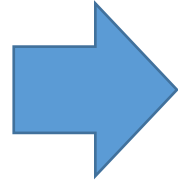


Detección



- Uso de *machine learning* para la búsqueda de anomalías
- Conexiones VPN. Movimientos laterales dentro de la red
- Comunicaciones mediante UDP
- Monitorización Punto final

COCS AGE



vSOC



- Debemos de disponer de capacidad de vigilancia y respuesta propia o subcontratada
- CCN Colabora / apoya otros organismos ---- LUCIA (incidentes complejos)
- **Aplicar regla de las 2 personas RSEG / CISO con equipos dedicados**
- Herramientas integradas nos proporcionan mayor eficiencia
- **DETECCIÓN Y RESPUESTA DEBEN ESTAR DESCENTRALIZADAS EN LOS ORGANISMOS**



Índice

1. Cumplimiento del ENS.Retos

2. Nuevo PILAR CLOUD

3. Conclusiones



2. Nuevo PILAR CLOUD

Un entorno CLOUD sencillo y actualizado



- 1) **Interfaz más intuitiva.**
- 2) **Nuevo entorno web multiplataforma**
- 3) **Más movilidad y disponibilidad**
- 4) **Gestión de Análisis de Riesgos centralizada en la Nube**
- 5) **Orientado a Entidades Locales y organismos pequeños.... SOC VIRTUALES**

2. Nuevo PILAR CLOUD



1. Acceso individualizado mediante **usuario y contraseña**
2. Diferentes **roles y permisos**
3. **Gestión centralizada** de los Análisis de Riesgos del organismo.



Username

Password

☐ Recordar

Entrar

Funcionalidades básicas:

- Análisis de Riesgos.
- Declaración aplicabilidad
- Medidas compensatorias
- EIPD
- Informes

Despliegue en:

- En plataforma CCN-CERT como complemento a INES.
- SOC VIRTUALES
- SOC,s empresas privadas



2019

CCN

Análisis R1

NUEVO PROYECTO

1. Servicios e Información

2. Plataforma de Soporte

3. Valoración de los Servicios

4. Medidas de Seguridad ENS

4.1. Aprobación

4.2. Resultados análisis ENS

4.3. Gráficos

5. Aplicabilidad

5.1. Medidas no aplica

5.2. Medidas compensatorias

6. Informes ENS

7. Evaluación de Impacto

7.1. Contexto

7.2. RGPD

7.3. Aprobación

7.4. Resultados EIPD

7.5. Plan de acción

PLATAFORMA DE SOPORTE

Progreso de esta sección - / -



FAQ

Activos de soporte

[D] Datos / Información

[files] Ficheros de datos



Si



No

[e-files] Ficheros cifrados



Si



No

[backup] Copias de respaldo



Si



No

[conf] Datos de configuración



Si



No

[int] Datos de gestión interna



Si



No

[password] Credenciales (ej. contraseñas)



Si



No

[auth] Datos de validación de credenciales



Si



No

[acl] Datos de control de acceso



Si



No



2019

CCN

Análisis R1

NUEVO PROYECTO

1. Servicios e Información

2. Infraestructura de soporte

3. Valoración de los Servicios

4. Medidas de Seguridad ENS

4.1. Aprobación

4.2. Resultados análisis ENS

4.3. Gráficos

5. Aplicabilidad

5.1. Medidas no aplica

5.2. Medidas compensatorias

6. Informes ENS

7. Evaluación de Impacto

7.1. Contexto

7.2. RGPD

7.3. Aprobación

7.4. Resultados EIPD

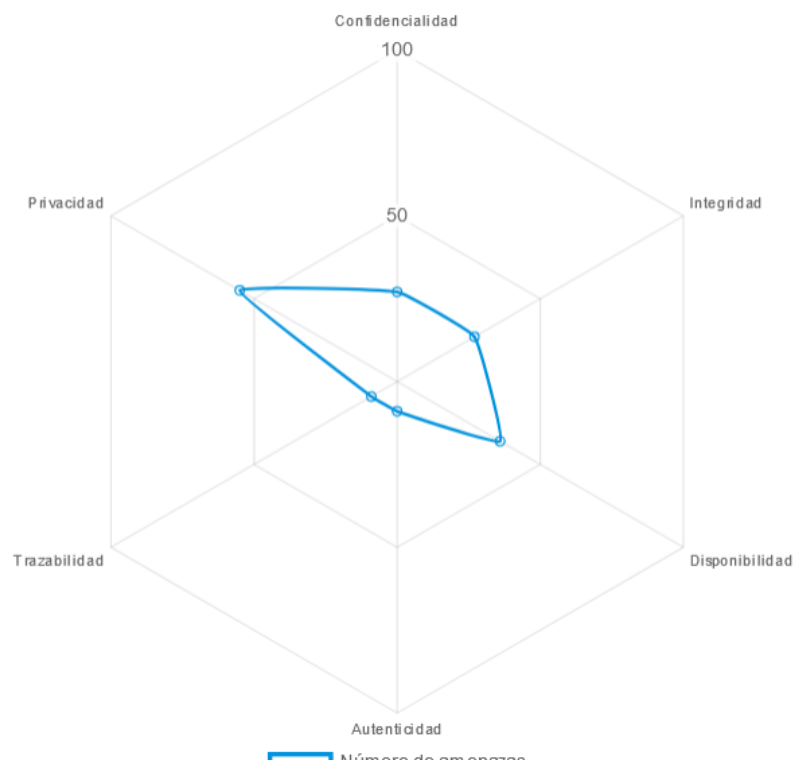
GRÁFICOS

Progreso de esta sección - / -

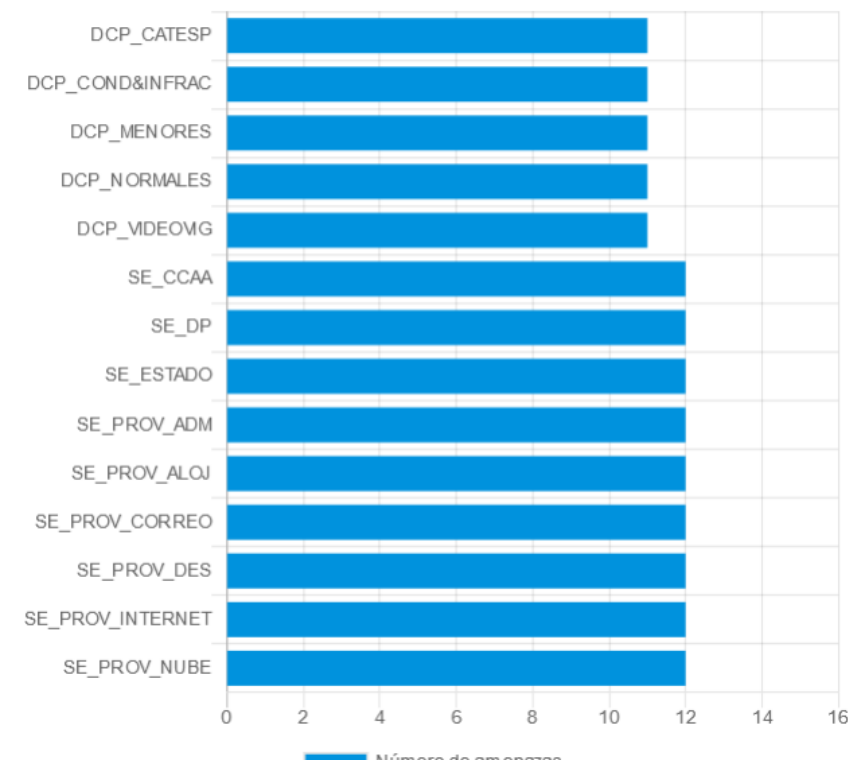


FAQ

Amenazas por dimensión



Amenazas por asset





2019

CSA

ANÁLISIS AR5

NUEVO PROYECTO

1. Servicios e Información
2. Infraestructura de Soporte
3. Valoración de los Servicios
4. Medidas de Seguridad ENS
 - 4.1. Aprobación
 - 4.2. Resultados análisis ENS
 - 4.3. Gráficos
5. Aplicabilidad
 - 5.1. Medidas no aplica
 - 5.2. Medidas compensatorias
6. Informes ENS
7. Evaluación de Impacto
 - 7.1. Contexto

MEDIDAS COMPENSATORIAS

Progreso de esta sección - / -



FAQ



Todas las medidas estan compensadas.

MEDIDAS COMPENSATORIAS

Filtros:

NUEVA MEDIDA

| NOMBRE | ÁMBITO DE APLICACIÓN | |
|---------------------------|----------------------|--|
| Medida Compensatoria Org1 | org.1 | |
| Media comp. org 1_4 | org.1.4 / org.4 | |
| sds | org.1.3 | |

Índice

1. Cumplimiento del ENS

2. Nuevo PILAR CLOUD

3. Conclusiones

3. Conclusiones

- ✓ SOC VIRTUALES. servicio horizontal y escalable
 - Servicios de Salud
 - Diputaciones / Cabildos / CCAA.....
- ✓ PILAR EN LA NUBE. Facilitar cumplimiento del ENS y RGPD.
- ✓ Mayor intercambio de ciberamenazas, ciberincidentes y vulnerabilidades.



EGC group

Análisis dinámico de malware



Análisis estático. 32 antivirus



Gestión de Incidentes



carmen



© Adaptive Defense 360



Ataques complejos. Detección basada en anomalías

(+ 270 sondas)

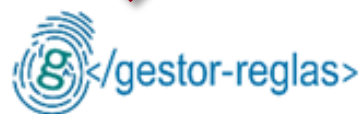


SAT

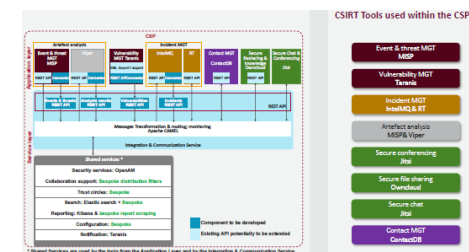
COCS AGE

vSOC

Gestión de Reglas



EGC group



Muchas gracias

