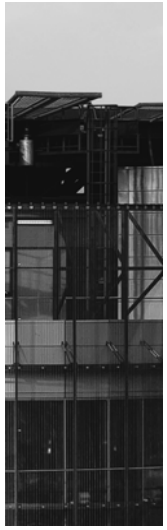


Red Nacional de SOC

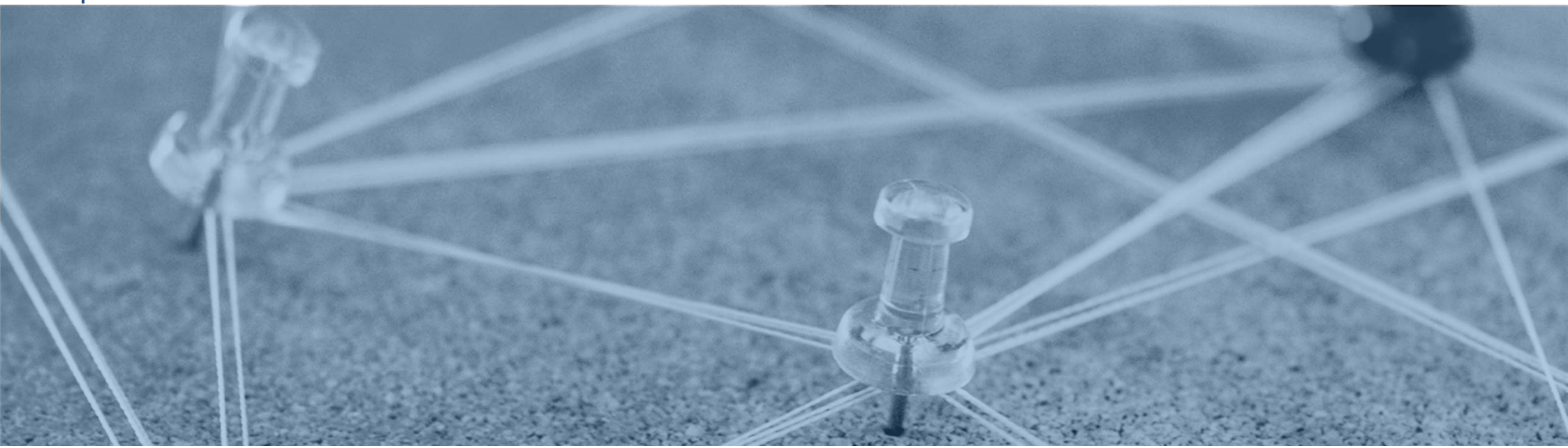
Carlos Córdoba

Jefe del Área de Centros de Operaciones de Ciberseguridad

centro criptológico nacional

Marzo 2022

ÍNDICE



RED NACIONAL DE SOC

¿En qué consiste la RNS?

¿En qué consiste la Red Nacional de SOC?

Mediante la RNS se pretende **mejorar la seguridad colectiva de TODOS los Organismos Públicos, mediante la superposición de las distintas capacidades**.

Por un lado, mediante un **modelo federado**, se coordinarán los flujos de información entre todos los SOC en tres campos:

- ✓ **Notificación de incidentes**: necesaria para la visibilidad de los incidentes en los escalones necesarios según la regulación actual, así como para poder reaccionar a tiempo en el resto de organismos.
- ✓ **Ciberinteligencia**: obtención y compartición de inteligencia para mejora continua de la detección.
- ✓ **Visibilidad**: recepción de los metadatos necesarios para elaborar el mapa de situación de la ciberseguridad a escala nacional.

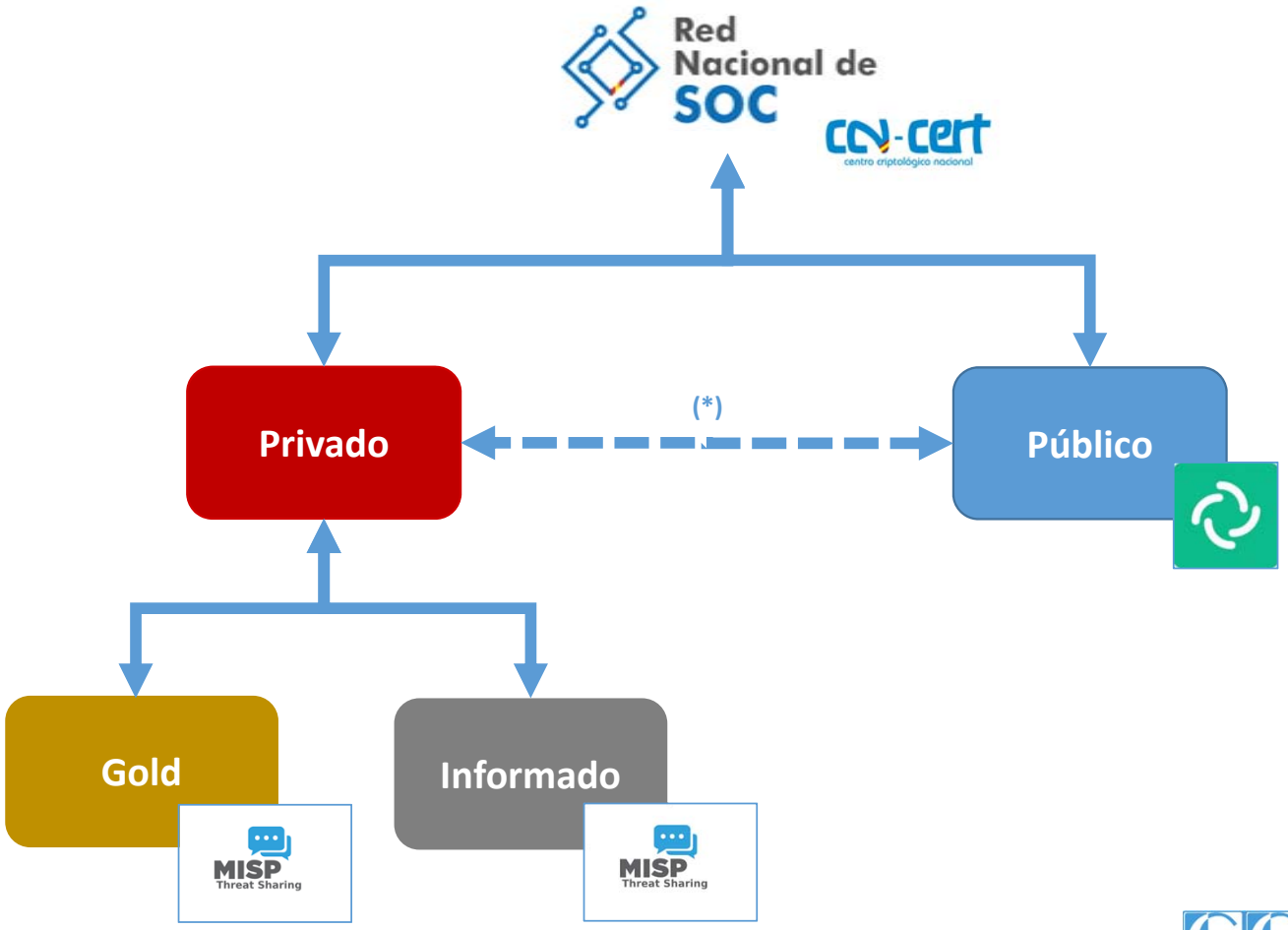
Por otro lado, se coordinarán las empresas privadas que (generalmente) gestionan la ciberseguridad de los organismos públicos mediante el **intercambio activo de indicadores** de ciberincidente, anonimizando a la víctima y antes de que se pueda extender a otros organismos.

CCN
centro criptológico nacional

RNS | Grupos y organización

Para Organizar la información la RNS tiene 2 grupos de pertenencia:

- ***Público***: grupo de todos los SOC de los Organismos Públicos. **Modelo federado**
- ***Privado***: grupo con los Proveedores de Seguridad que gestionan SOC de un Organismo Público. **Roles**:
  - ✓ ***Gold***: Proveedores de alto valor estratégico dentro de los SOC
  - ✓ ***Informado*** : Proveedores dedicados a la seguridad con capacidades de dar servicio de SOC y den Servicio de SOC



(*): El Organismo público exigirá a su Proveedor de Servicios que gestiona su SOC la participación activa en la RNS

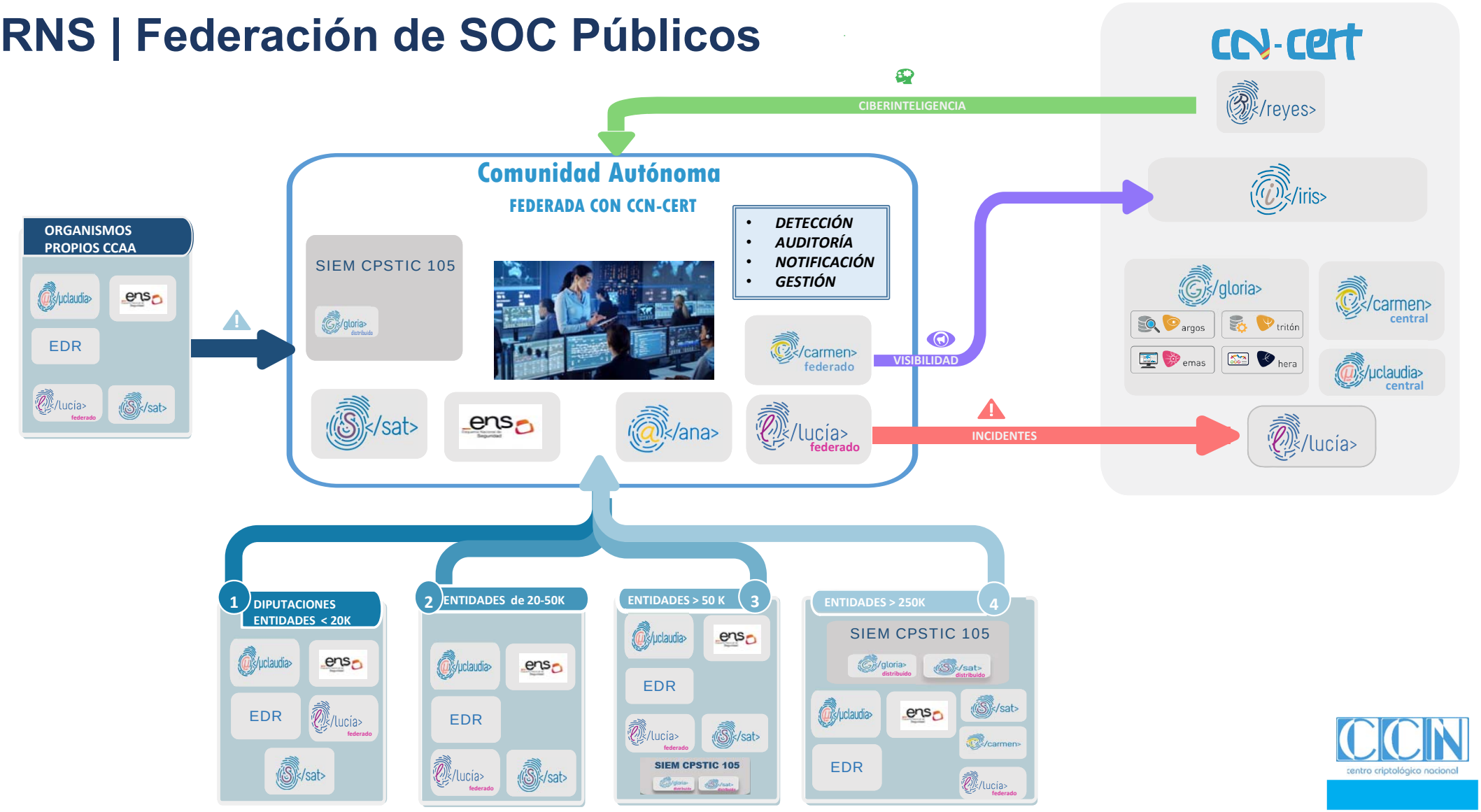
CCN
centro criptológico nacional

RED NACIONAL DE SOC

Público

Modelo federado en la RNS

RNS | Federación de SOC Públicos



RNS – Grupo públicos

GRUPO PÚBLICO | ORGANISMOS PÚBLICOS

Composición:

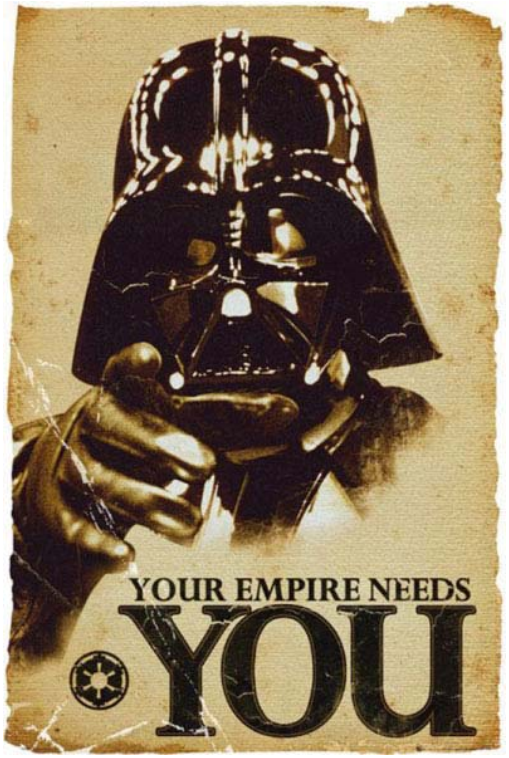
- Organismo público con SOC
- Diputaciones SOC
- Comunidades autónomas SOC
- Ministerios con SOC
- Ayuntamiento con SOC

Requisitos de pertenencia:

- Disponer de un SOC o de servicios de ciberseguridad
- **Participación de personal únicamente público**

Beneficios:

- Recepción de indicadores de ciberataque consolidados
- Compartir información con SOCs del mismo ámbito
- Interactuar con otros organismo públicos



Capacidades desplegadas por la Comunidad Autónoma o Diputación en apoyo a sus propios Organismos

1. **Defensa perimetral**: WAF, IPS, Firewall, Anti SPAM, SAT (Servicio de Alerta Temprana: SAT-INET, SAT-ICS)

2. **EDR:** Gestión centralizada de alerta y despliegue de reglas para dotar de protección a los puestos de trabajo de los usuarios.

3. **AUDITORÍA:** Revisión de sistemas y aplicaciones para conocer su estado de seguridad y representarlo en ANA.

4. **LUCIA federado:** Gestión de incidentes por parte del equipo de seguridad de la Comunidad Autónoma.

5. **microCLAUDIA federado:** Centraliza la conexión de los agentes de microCLAUDIA distribuidos en las entidades.

6. **SIEM:** Instancia completa del SIEM con la capacidad de recolección de logs, normalización y almacenamiento, correlación, gestión de alertas y cuadro de mando. Puede implementarse con la herramienta GLORIA, SIEM del Catálogo CPSTIC 105 o mediante la opción de **SAT Distribuido.**

7. **Sistemas de Backup:** Revisión del sistema de copia de seguridad para conocer alcance y si es efectivo. En caso de no tener ver las posibilidades de proveer uno.

8. **Adecuación al ENS:** Ejecución de las tareas para llevar a termino el cumplimiento del ENS al menos en su categoría Baja e implementarlo en los sistemas.

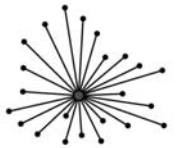
9. **Sistema de detección de anomalías (CARMEN federado):** Centraliza la conexión de las diferentes instancias desplegadas en las entidades, permitiendo la administración de las mismas.

10. **Copiadora de tráfico:** Almacenamiento del trafico al menos durante un mes para mejorar las investigaciones.

(*): En color, las capacidades recomendadas para implantar las Diputaciones en apoyo a los Ayuntamientos de menos de menos de 20.000 hab (recomendado hasta 50.000 hab).

CCN centro criptológico nacional

Servicios ofrecidos por la Comunidad Autónoma o Diputación en apoyo a Entidades Locales



1. **Defensa perimetral:** WAF, IPS, Firewall, Anti SPAM, SAT (Servicio de Alerta Temprana: SAT-INET, SAT-ICS), siempre que haya salidas unificadas o centralizadas a Internet

2. **EDR** Gestión centralizada de alerta y despliegue de reglas para dotar de protección a los puestos de trabajo de los usuarios

3. **AUDITORÍA :** Revisión de sistemas, aplicaciones para conocer su estado de seguridad y representarlo en ANA.

4. **LUCIA federado:** Gestión de incidentes por parte del equipo de seguridad de la Comunidad Autónoma.

5. **microCLAUDIA federado:** Centraliza la conexión de los agentes de microclaudia distribuidos en las entidades.

6. **SIEM**: Instancia completa del SIEM con la capacidad de recolección de logs, normalización y almacenamiento, correlación, gestión de alertas y cuadro de mando. Puede implementarse con la herramienta GLORIA, SIEM del Catálogo CPSTIC 105 o mediante la opción de **SAT Distribuido**

7. **Adecuación al ENS:** Ejecución de las tareas para llevar a termino el cumplimiento del ENS al menos en su categoría Baja e implementarlo en los sistemas.

8. **Sistema de detección de anomalías (CARMEN federado):** Centraliza la conexión de las diferentes instancias desplegadas en las entidades, permitiendo la administración de las mismas.

(*): En color, las capacidades recomendadas para implantar las Diputaciones en apoyo a los Ayuntamientos de menos de menos de 20.000 hab (recomendado hasta 50.000 hab).

Modelo de despliegue de capacidades coordinado

- **Servicio provisto por la propia EELL**
- **Servicio provisto por la Diputación**
- **Servicio federado con la Diputación o la Comunidad Autónoma**

HABITANTES	μclaudia	sat	EDR	Auditoría	carmen	SIEM	lucía	Back-up
Menos 20.000 hab								
Entre 20.000 y 50.000 hab								
Más de 50.000 hab								
Mas de 250.000 hab.								

Dimensionamiento SOC (personas)

Equipos SOC

- **Incidentes**
  - Explotar SIEM y EDR
  - Buscar incidentes de seguridad
- **Auditoría**
  - Revisar estado de seguridad de forma continua
  - Establecer el impacto de alertas o vulnerabilidades
- **Adecuación**
  - Adaptar el ENS
  - Ayudar en la corrección de vulnerabilidades
- **Operación**
  - Gestión de elementos de seguridad perimetral
  - Instalación y mantenimiento de equipos del SOC

CCN
centro criptológico nacional

Dimensionamiento SOC (personas)

Personal ofrecido en modo servicio o presencial

Personal en modo presencial

Dispositivos	Incidentes	Auditoría	Adecuación	Operación
Menos 5.000			 	
Entre 5.000 y 10.000	 		  	
Más de 10.000	 	 	  	 

RED NACIONAL DE SOC

Privado

Roles de los Proveedores de Servicios de Seguridad

RNS – Grupo privados

GRUPO PRIVADOS

NIVEL GOLD

Composición:

- Empresa Privada que gestiona un SOC Público
- Empresa Privada que gestiona un SOC Ministerio
- Empresa Privada que gestiona un SOC CCAA
- Empresa Privada que gestiona un SOC de Dip/EELL
- Empresa Privada que gestiona un SOC Entidad Pública

Requisitos de pertenencia:

- Dar servicio de SOC a un organismo público
- Participación activa*
- **Miembro de CSIRT.es**
- Compartir de información de incidentes a través de **LUCIA** federado

Beneficios:

- Compartición de indicadores de ciberataque en tiempo real
- Colaboración conjunta en investigaciones

NIVEL INFORMADO

Composición:

- Empresa Privada que gestiona un SOC Público
- Empresa Privada que gestiona un SOC Ministerio
- Empresa Privada que gestiona un SOC CCAA
- Empresa Privada que gestiona un SOC de Dip/EELL
- Empresa Privada que gestiona un SOC Entidad Pública

Requisitos de pertenencia:

- Proporcionar servicios de seguridad SOC a cualquier organismo del sector público.
- Compartir de información de incidentes a través de LUCIA federado
- Cumplir con ciertos niveles de servicios de seguridad (Auditorías, forense, implantación ENS, etc.

Beneficios:

- Recepción de indicadores de ciberataque consolidados
- Compartir información con SOCs del mismo ámbito

(*): esta participación se evaluará periódicamente, para revalidar la pertenencia al Nivel GOLD

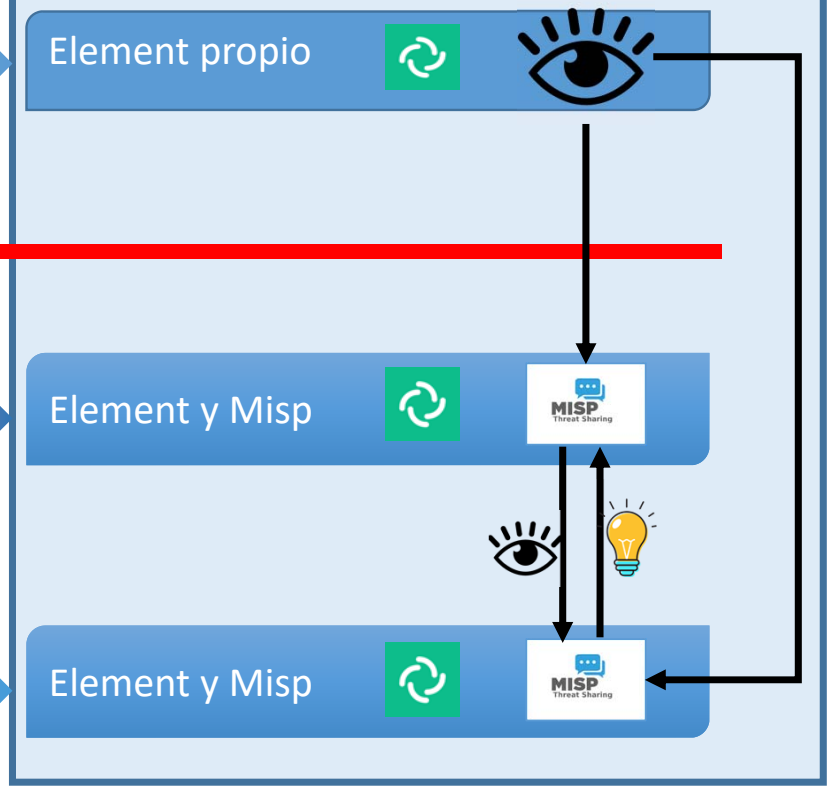
CCN centro criptológico nacional

RNS – Grupos foros

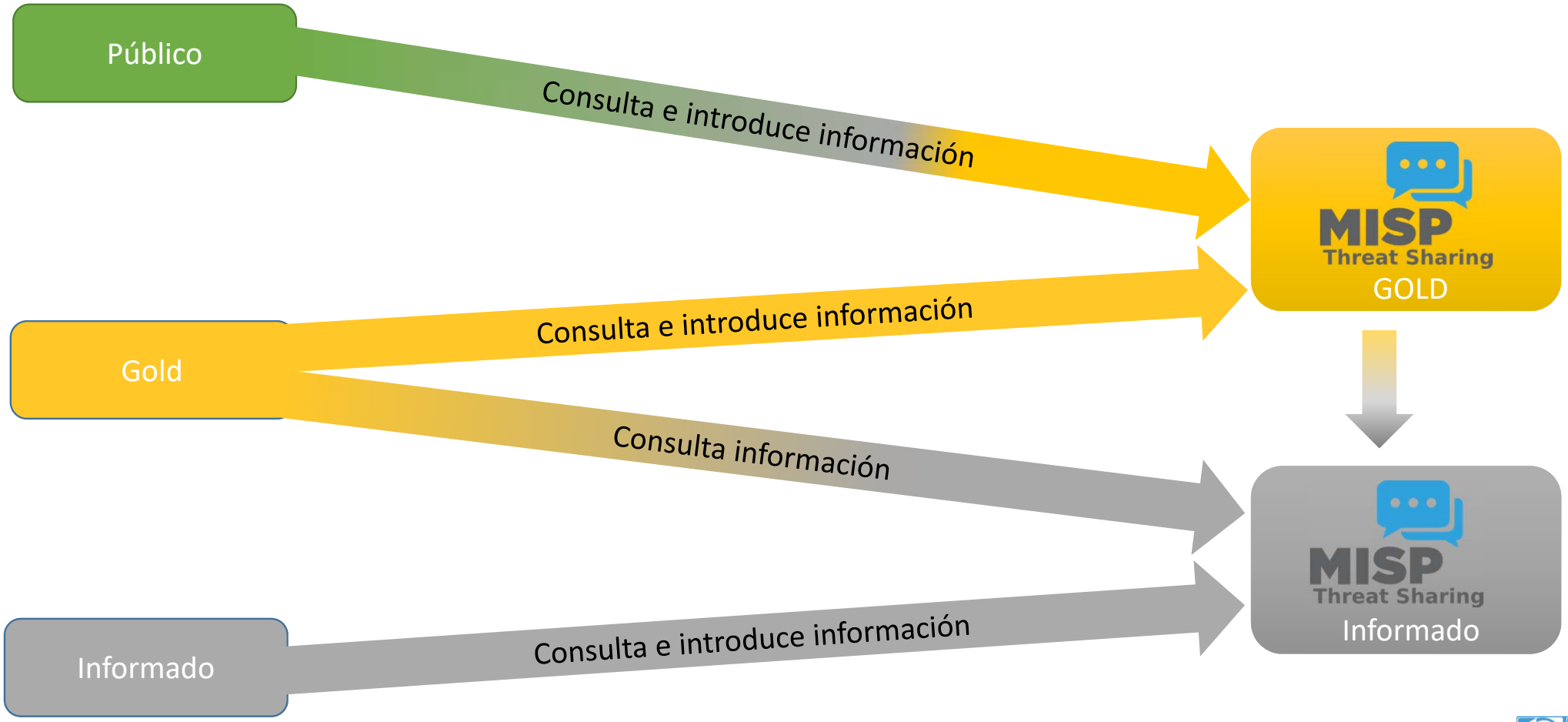
Sector Público (independientemente de su grado de conocimiento)

Proveedores de Seguridad RNS Gold

Proveedores de Seguridad RNS Informado



RNS – Entrada de datos



RNS | Intercambio de información técnica en Red de SOC Públicos y Privados)

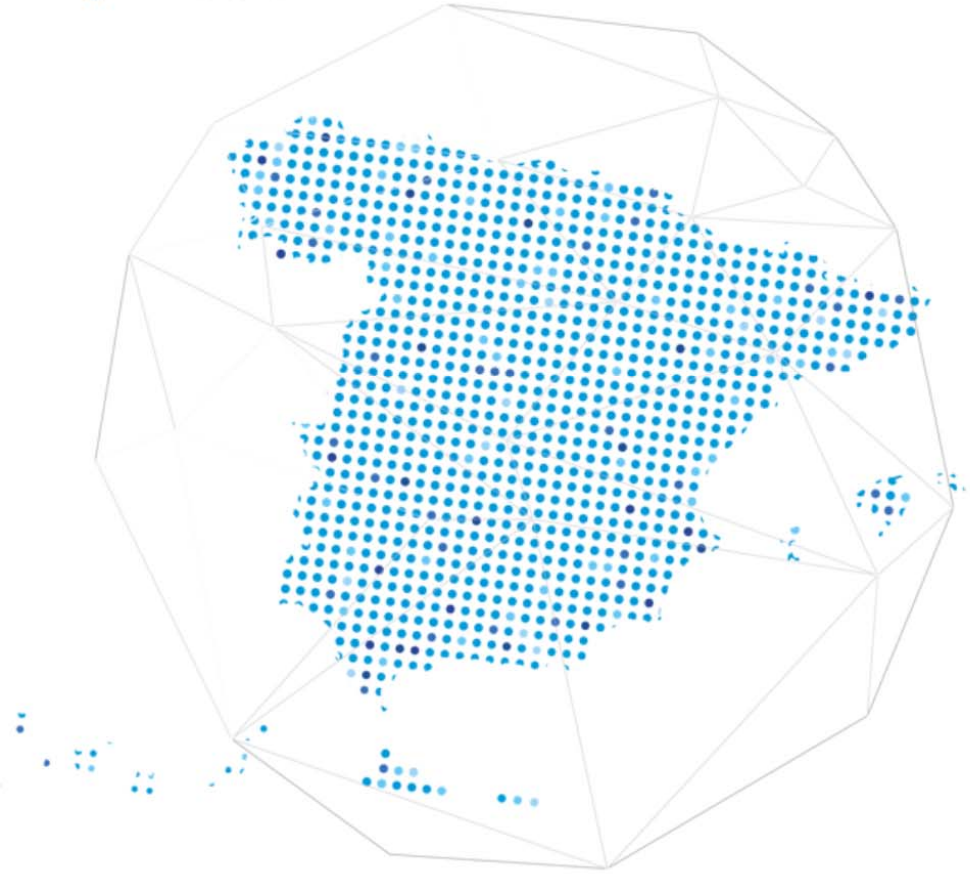
PRINCIPIOS DE INTERCAMBIO

- Compartir Información en el minuto 0 de una anomalía
- **Compartir sin mencionar la victima, anonimizando los datos**
- Tener una mayor eficiencia en activar medidas ante agresores
- Mayor nivel de automatización (Firewall, antispam, EDR,….)

TIPO DE INTERCAMBIO

- Elementos para compartir por ser anómalos
  - 'ATTACK IPs'
  - 'TTP'
  - 'IOA'
  - 'MAILS'
  - 'IOC'
  - 'VALORACIÓN'

Red Nacional de SOC



MUCHAS GRACIAS

jsoc@ccn.cni.es
socccn@ccn-cert.cni.es

CCN
centro criptológico nacional