

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Un SOC para la AGE



- Miguel Ángel Amutio
- SGAD/MINHAFP
- miguel.amutio@correo.gob.es
- Pablo López
- Centro Criptológico Nacional
- ccn@cni.es

Índice

1. **Aproximación Práctica a la Ciberseguridad**
2. **Incidentes 2017. Lecciones Aprendidas**
3. **Centro de Operaciones de Ciberseguridad (SOC)**
4. **SOC-AGE. Esquema de Prestación del Servicio**
5. **SOC-AGE. Operación y Servicios a Prestar**
6. **Conclusiones. SOC-AGE como Respuesta a la Ciberamenaza**

Aproximación práctica a la Ciberseguridad



2006-2016

DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD NACIONAL

Defensa frente a Ciberataques



66.000

Ciberincidentes gestionados desde 2007 en AAPP y empresas de interés estratégico para el país



1,5

Incidentes al día, críticos o muy altos (peligrosidad) APT con exfiltración de información DoS distribuido (denegación de servicio) Ataques dirigidos Código dañino específico



8.000

Troyanos cada año



2

Secuestros informáticos diarios (ransomware)



2.500.000

Eventos de seguridad recibidos diariamente



135

Auditorías de seguridad y páginas web



+80.000

Reglas de detección propias



17

Herramientas propias: detección, análisis, auditoría e intercambio de información

Sector Público y Empresas de Interés Estratégico más seguras



115

Organismos adscritos al Sistema de Alerta Temprana Internet

Administración General del Estado
Entidades públicas (Puertos, Confederaciones Hidrográficas, Agencias, etc.)
Comunidades Autónomas
Entidades locales
Universidades
Empresas de interés estratégico



135

Sondas de Alerta Temprana

54

Áreas de conexión Red-SARA

Sonda AGE

Representante español en Organismos y Grupos Internacionales



16

Grupos de trabajo (UE, OTAN, Inteligencia, Empresas, etc.)

+65

Acuerdos internacionales

Cooperación diaria en la gestión de incidentes (chat, intercambio de información, ...)

Formación personal



6.130

Alumnos presenciales



19.500

Alumnos en cursos online



180

Cursos presenciales



9

Cursos online

Guías y estándares de seguridad propios



268

Guías CCN-STC actualizadas permanentemente



852

Informes de Seguridad
Informes de Amenazas
Informes de Código Dañino
Informes Técnicos
Buenas prácticas

Comunicación



7.197

Usuarios registrados portal CCN-CERT



12.645

Solicitudes de registro



2.105

Seguidores Twitter



3.050

Seguidores LinkedIn



13.125

Visualizaciones en Youtube



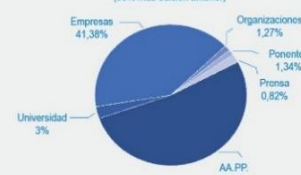
107.230

Promedio de vistas mensuales

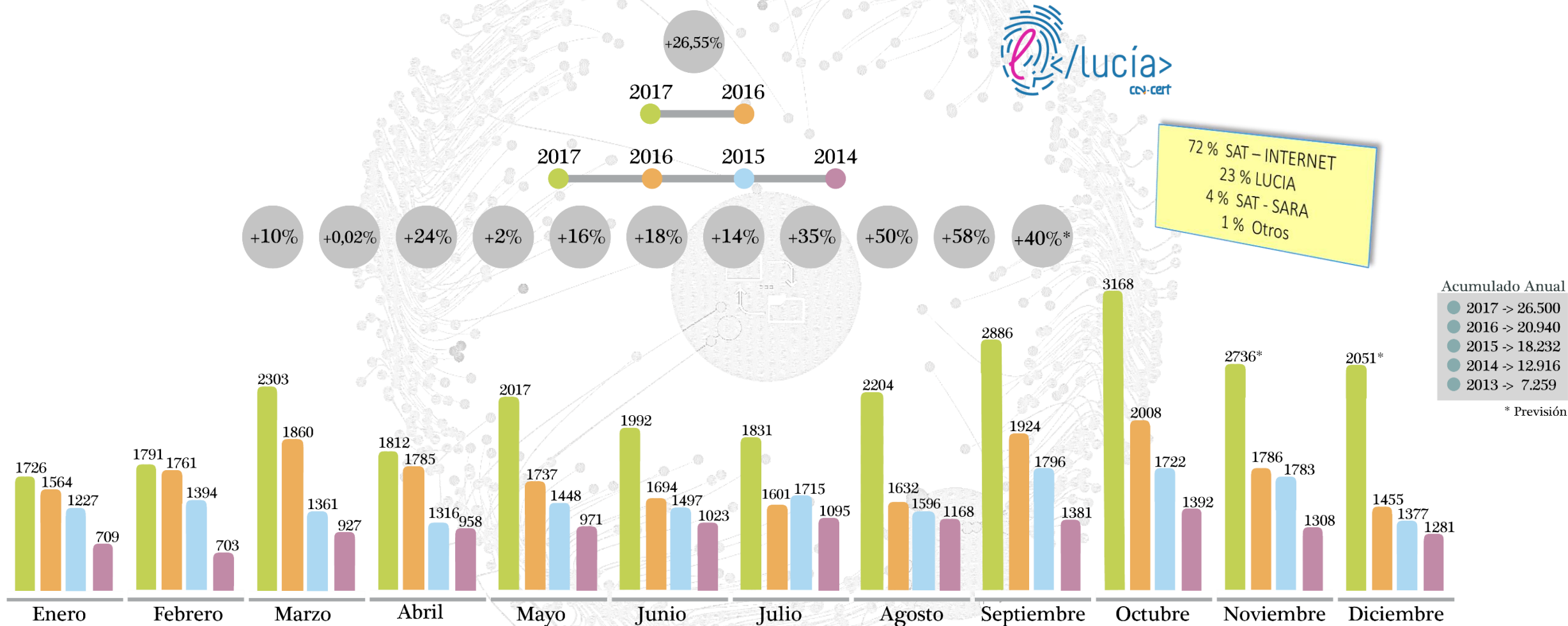
Edición anterior Jornadas STIC CCN-CERT Principal encuentro de ciberseguridad en España

1.421

Personas inscritas (30% más edición anterior)

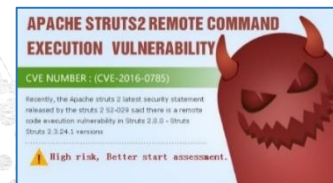


Incidentes 2017



Lecciones Aprendidas

- **Evitar el pánico.** Sensibilizar a la alta Dirección.
- **Establecer canales de comunicación alternativos.**
 - Blogs
 - Chats
 - Mensajería instantánea.
- **Boletines de alerta de vulnerabilidades.**
 - Tiempos mínimos de actualización.
- **Reevaluación de las medidas de seguridad.** Auditorías de seguridad.
- **Incrementar y ampliar las capacidades de vigilancia y respuesta.** Centro de Operaciones de Ciberseguridad (SOC).
- **Mejorar notificación de incidentes e intercambio información sobre amenazas.**
 - Plataforma Común. (Notificación Incidentes)
 - Inteligencia de seguridad. (Gestión Incidentes)



Centro de Operaciones de Ciberseguridad

Se crea el Centro de Operaciones de Ciberseguridad (SOC) como instrumento de la Administración General del Estado y sus organismos públicos vinculados o dependientes para la consolidación del Servicio Compartido de Seguridad Gestionada

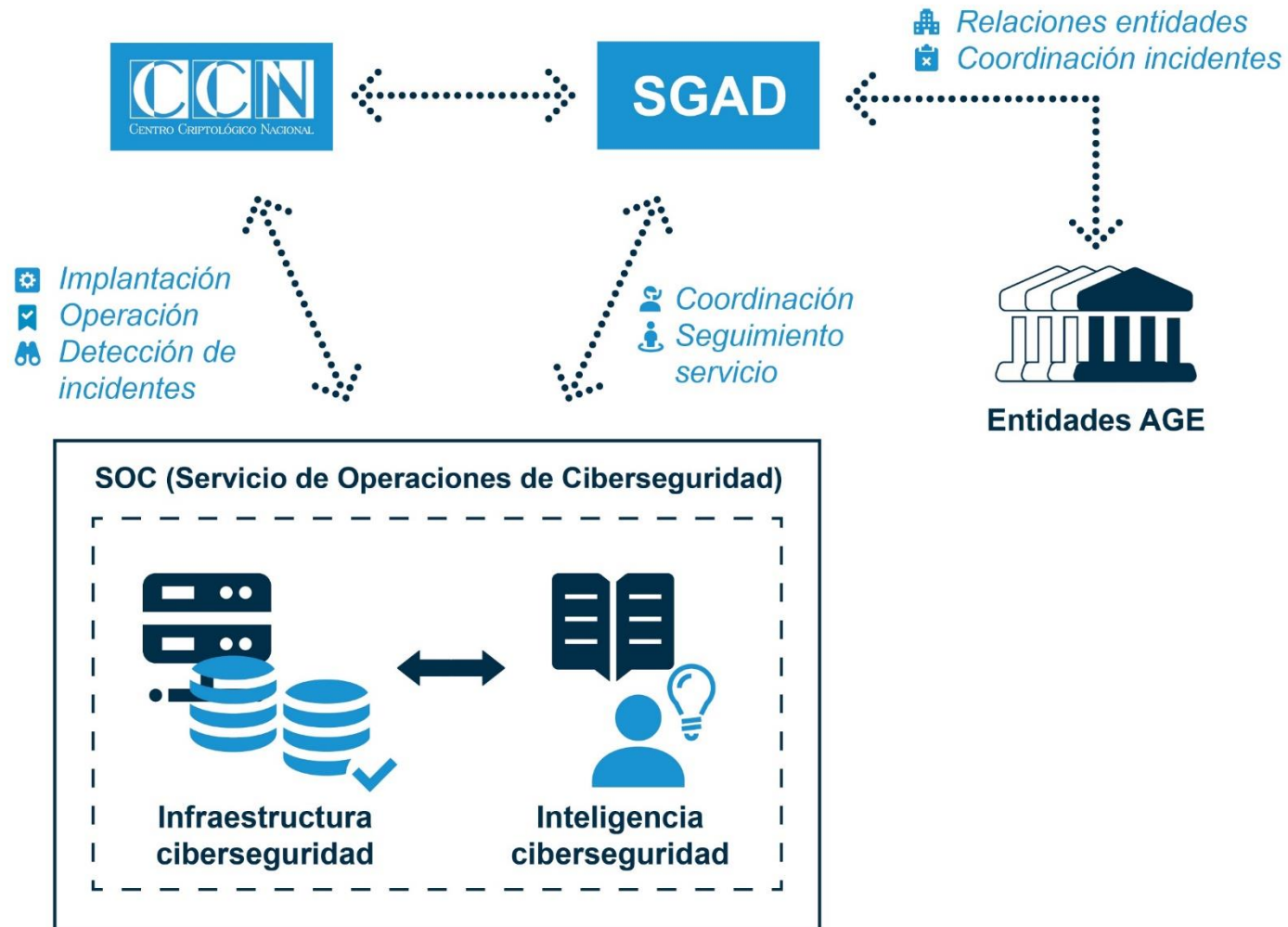
- Prestación de **servicios horizontales de ciberseguridad**
- **Centralizar servicios, eliminar duplicidades**, conseguir un alto grado de **especialización** y **reducir los costes** individuales en todos los organismos adheridos.
- **Aumentar la capacidad de vigilancia y detección de amenazas** en la **operación diaria** de los sistemas de información y comunicaciones de la Administración
- La **mejora de su capacidad de respuesta** ante cualquier ataque.



La **responsabilidad** sobre el Centro de Operaciones de Ciberseguridad corresponde a la **Secretaría General de Administración Digital (SGAD)**

La **operación del servicio** del Centro de Operaciones de Ciberseguridad correrá a cargo del **CCN-CERT**

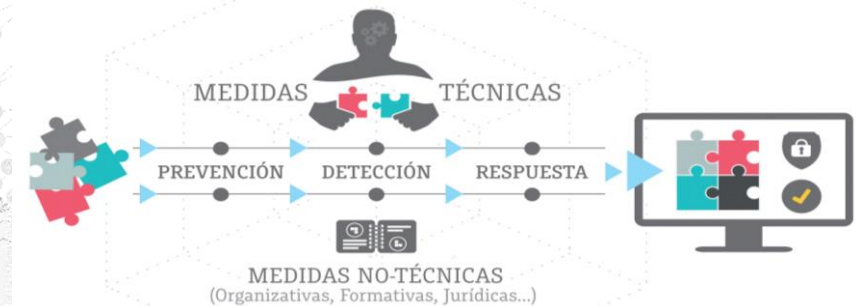
Centro de Operaciones de Ciberseguridad (esquema prestación del servicio)



Centro de Operaciones de Ciberseguridad (servicios)

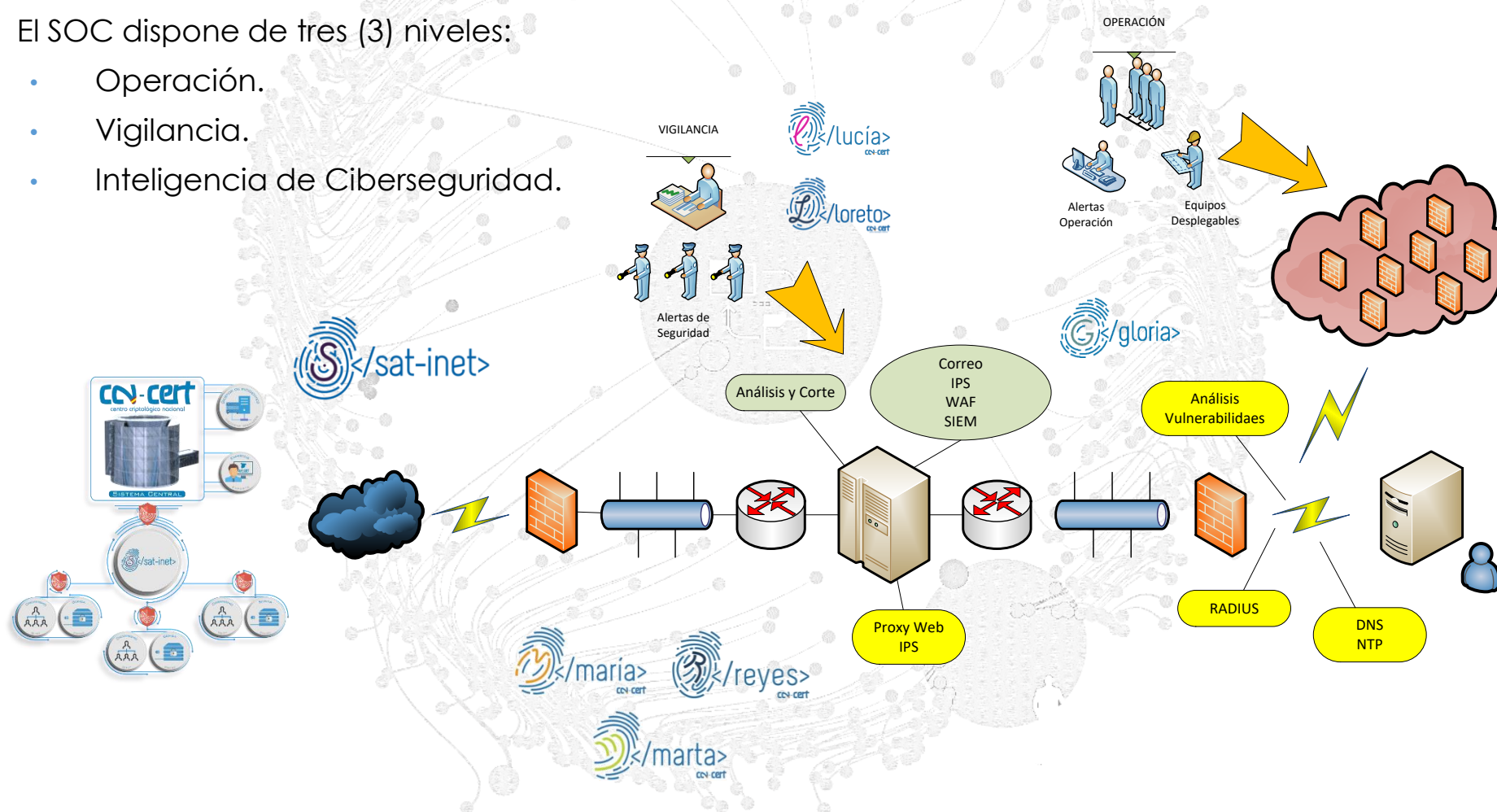
El SOC tiene por objeto proporcionar **protección de manera centralizada** mediante la dotación de una **infraestructura global y única** que incluye el **equipamiento** necesario, así como su **configuración**, **puesta en marcha**, **mantenimiento**, **monitorización** y **gestión de incidentes** de ciberseguridad.

- **Servicio de Alerta Temprana (SAT).**
- **Detección, respuesta coordinada y soporte a la resolución de incidentes de seguridad.**
- **Soporte a la investigación de ciberataques y ciberamenazas.**
- **Operación, monitorización y actualización de dispositivos de defensa perimetrales**
 - Cortafuegos de nueva generación (NGFW).
 - Acceso remoto por Red Privada Virtual (VPN).
 - Servicio anti SPAM
 - Cortafuegos de aplicaciones Web (WAF).
 - Resolución segura de nombres de dominio (DNS).
 - Sistema de base común de tiempos (NTP).
 - Gestión y correlación de eventos de seguridad (SIEM).
- **Análisis de vulnerabilidades de aplicaciones y servicios.**
- **Servicios anti-abuso de identidad digital.**



Centro de Operaciones de Ciberseguridad (idea de actuación)

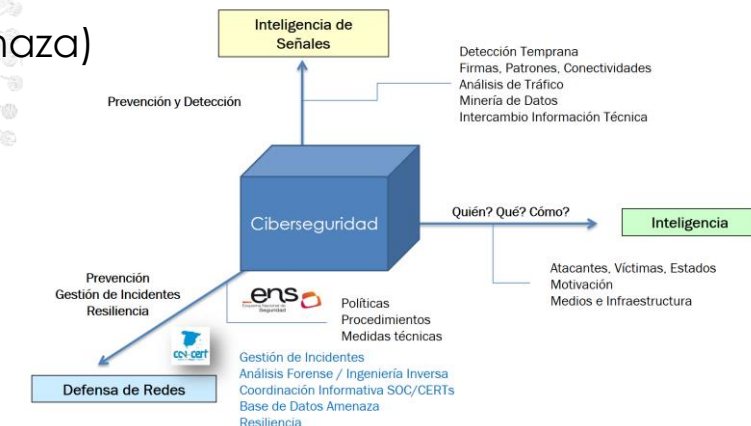
- El SOC dispone de tres (3) niveles:
 - Operación.
 - Vigilancia.
 - Inteligencia de Ciberseguridad.



Centro de Operaciones de Ciberseguridad (valor añadido)

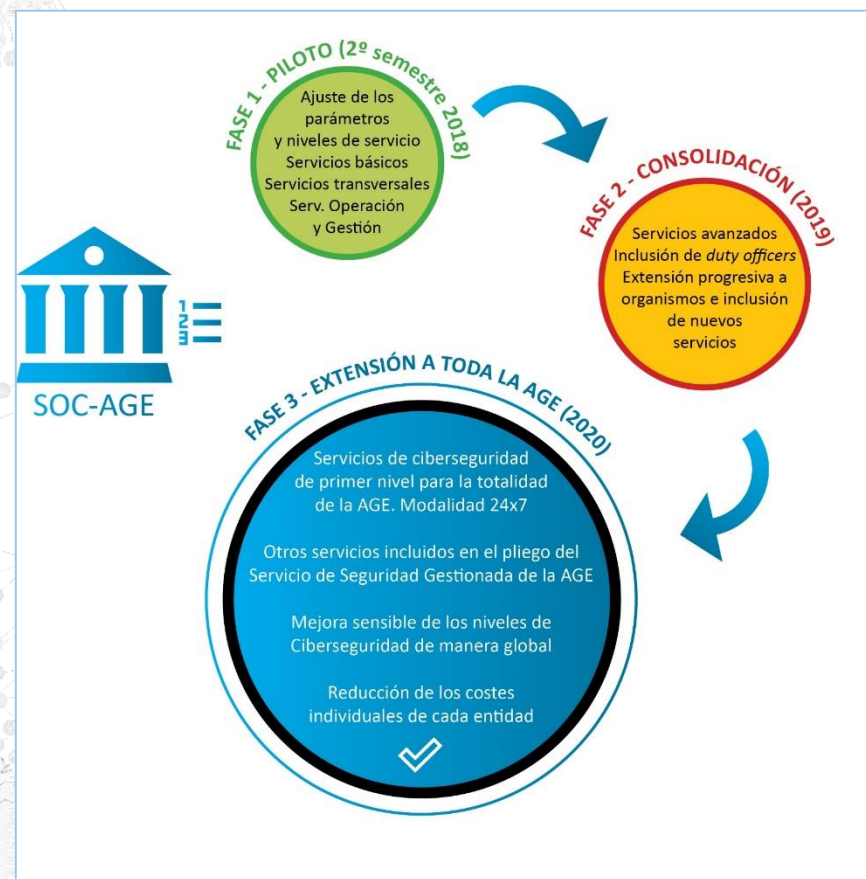
La **responsabilidad** de la seguridad de la información **para cada organismo** seguirá correspondiendo a su **Responsable de Seguridad**. No obstante, **la SGAD coordinará la respuesta ante incidentes** de seguridad entre los diferentes agentes afectados

- El dimensionamiento o inclusión del servicio será **según presupuesto y recursos disponibles**.
- El servicio persigue la **protección de la seguridad perimetral** de la Administración General del Estado y sus Organismos Públicos frente a amenazas externas.
- Modelo integral que favorezca la **coordinación en la respuesta** permitiendo a cada entidad establecer sus propias políticas de seguridad y facilitando el intercambio de información.
- **Verificaciones/Revisiones** de seguridad.
- **Asesoramiento** en ciberseguridad. (asegurar implementación de seguridad)
- Servicios de **inteligencia de ciberseguridad**. (intercambio sobre la amenaza)
- Capacidades de **respuesta en el punto final**.
- **Vigilancia digital**.
- **Consultoría legal** en ciberseguridad.



Centro de Operaciones de Ciberseguridad (situación actual y futura)

- **Finales de octubre 2017.**
 - Diseño conceptual de las comunicaciones.
- **Finales de diciembre 2017.**
 - Diseño conceptual del SOC.
- **Fase 1 (1º semestre 2018).**
 - Determinación de tecnologías para los diferentes dispositivos del SOC.
 - Definición de los parámetros y niveles de servicio.
- **Fase 1 (2º semestre). Inicio de la instalación del equipamiento.**
 - Adquisición e instalación de la infraestructura técnica.
 - Implantación de servicios básicos de ciberseguridad.
 - Incorporación de primeros entidades.
- **Fase 2 (durante 2019). Extensión del servicio.**
 - Extensión del servicio a todo el ámbito de aplicación del ACM.
 - Inclusión de nuevos servicios avanzados de ciberseguridad.
- **Fase 3 (años posteriores a 2019). Mantenimiento y mejora del servicio.**



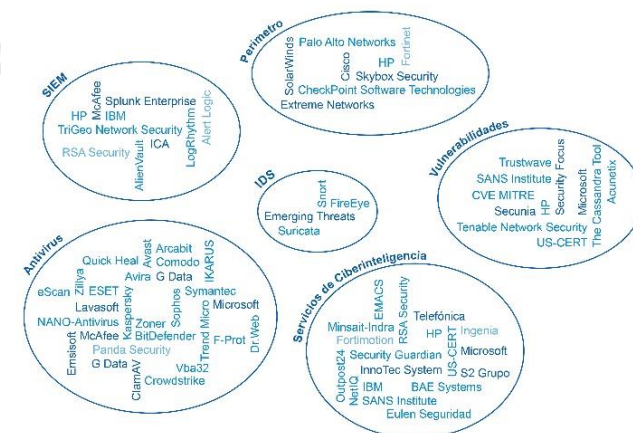
E-Mail

soc.age@correo.gob.es

Centro de Operaciones de Ciberseguridad (respuesta a la ciberamenaza)

Mientras que los **autores de ciberataques**, tanto estatales como no estatales, **solo temen al fracaso**, carecerán de motivos para dejar de intentarlo.

- Una **respuesta más eficaz**, centrada en la **detección**, la **trazabilidad** y el emprendimiento de **acciones penales** contra los ciberdelincuentes, es fundamental **para fomentar una disuasión efectiva**.
 - Colaboración con las **Fuerzas y Cuerpos de Seguridad del Estado**.
- Una **disuasión efectiva** significa poner en marcha un **marco de medidas** que sean a la vez **creíbles** y **disuasorias** para posibles ciberdelincuentes y ciberatacantes.
 - **Identificar** a los actores maliciosos.
 - Reforzar la **respuesta policial**.
 - **Cooperación** de sectores público y privado contra ciberdelincuencia.
 - Reforzar la **respuesta política**.
 - Aumentar la disuasión a través de la **capacidad de defensa**.



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

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

➤ Síguenos en

