GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
sgtic S.G. DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

UN BUEN SOC PARA LA AGE

Miguel Ángel Rodríguez Ramos
Subdirector General Adjunto de Tecnologías
de la Información y de las Comunicaciones
Ministerio de Energía, Turismo y Agenda Digital

SOC INFO Ciberseguridad

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
sgtic S.G. DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

Un buen SOC para la AGE
Contenidos

- El SOC de la AGE.
- Ciberseguridad en el MINETAD.
- Un buen SOC para la AGE.
- El futuro de la ciberseguridad en el MINETAD.
- ProtAAPP – Protege las Administraciones Públicas.

CORA Reforma de las AAPP

Infraestructuras comunes.

Herramientas de productividad y puesto de trabajo.

Aplicaciones comunes.

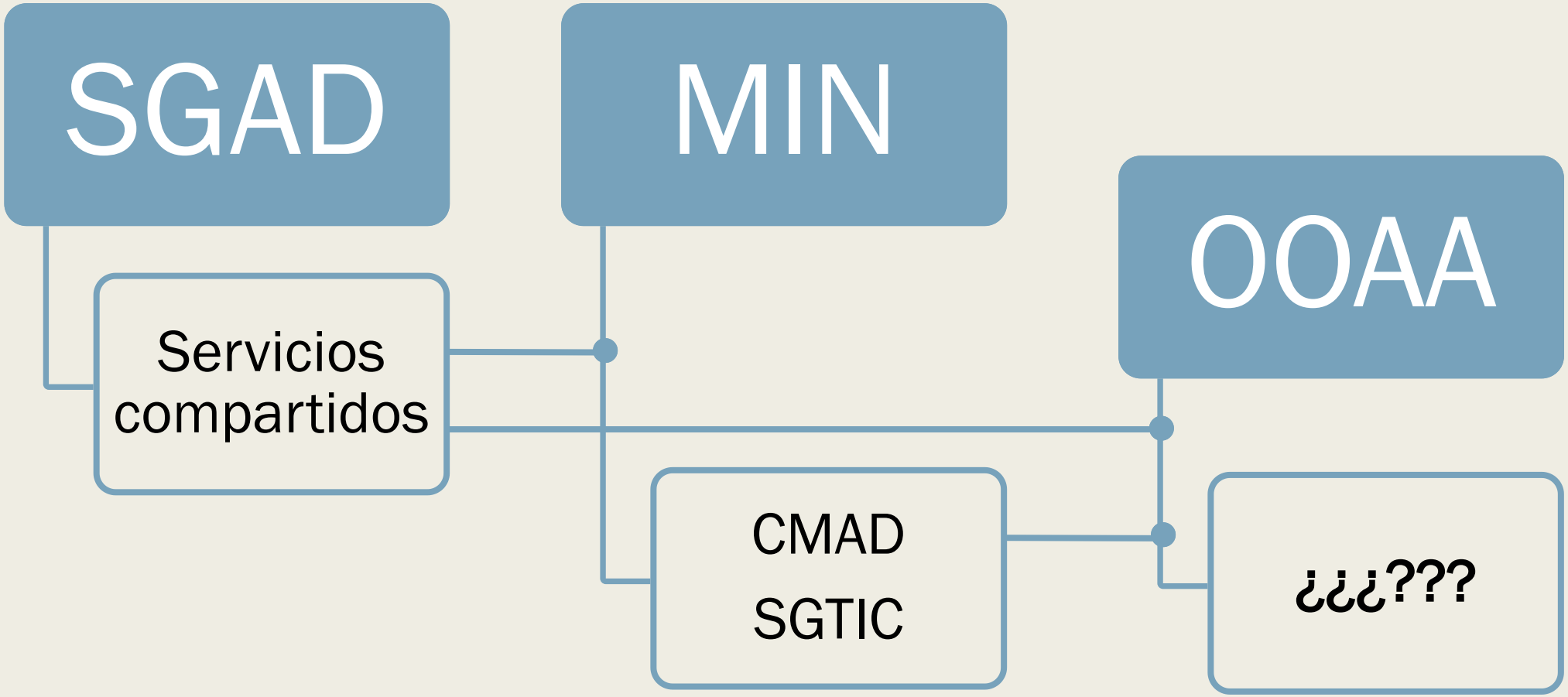
Infraestructuras sectoriales.

Aplicaciones sectoriales.

Gobernanza TIC en la AGE

13 Ministerios

80 Organismos Autónomos, Agencias y otros organismos



Catálogo de Servicios compartidos

- Telecomunicaciones
- **Seguridad gestionada**
- Alojamiento de infraestructuras TIC
- Nube híbrida (Nube SARA)
- Correo electrónico unificado
- Atención al ciudadano multicanal
- Gestión del registro
- Gestión de notificaciones
- Gestión de nómina
- Gestión de personal integral
- Gestión económico-presupuestaria
- Generación y validación de firmas electrónicas
- Gestión de expediente y documento electrónico
- Gestión de archivo electrónico

SOC de la AGE - Seguridad gestionada

SGAD + CCN-CERT

Administración General del Estado (AGE) y sus organismos públicos

- **Operación**, monitorización y actualización de dispositivos de defensa perimetrales.
- **Detección**, respuesta coordinada, investigación de ciberataques y ciberamenazas y resolución de incidentes de seguridad.
- **Servicio de Alerta Temprana** (SAT) en las conexiones a Internet, a redes interadministrativas comunes y, bajo petición, a redes corporativas de las entidades.
- **Análisis de vulnerabilidades** de aplicaciones y servicios.
- Servicios **anti-abuso** de identidad digital.

Valor añadido

NO viene a **sustituir** o reemplazar funciones o responsabilidades existentes.

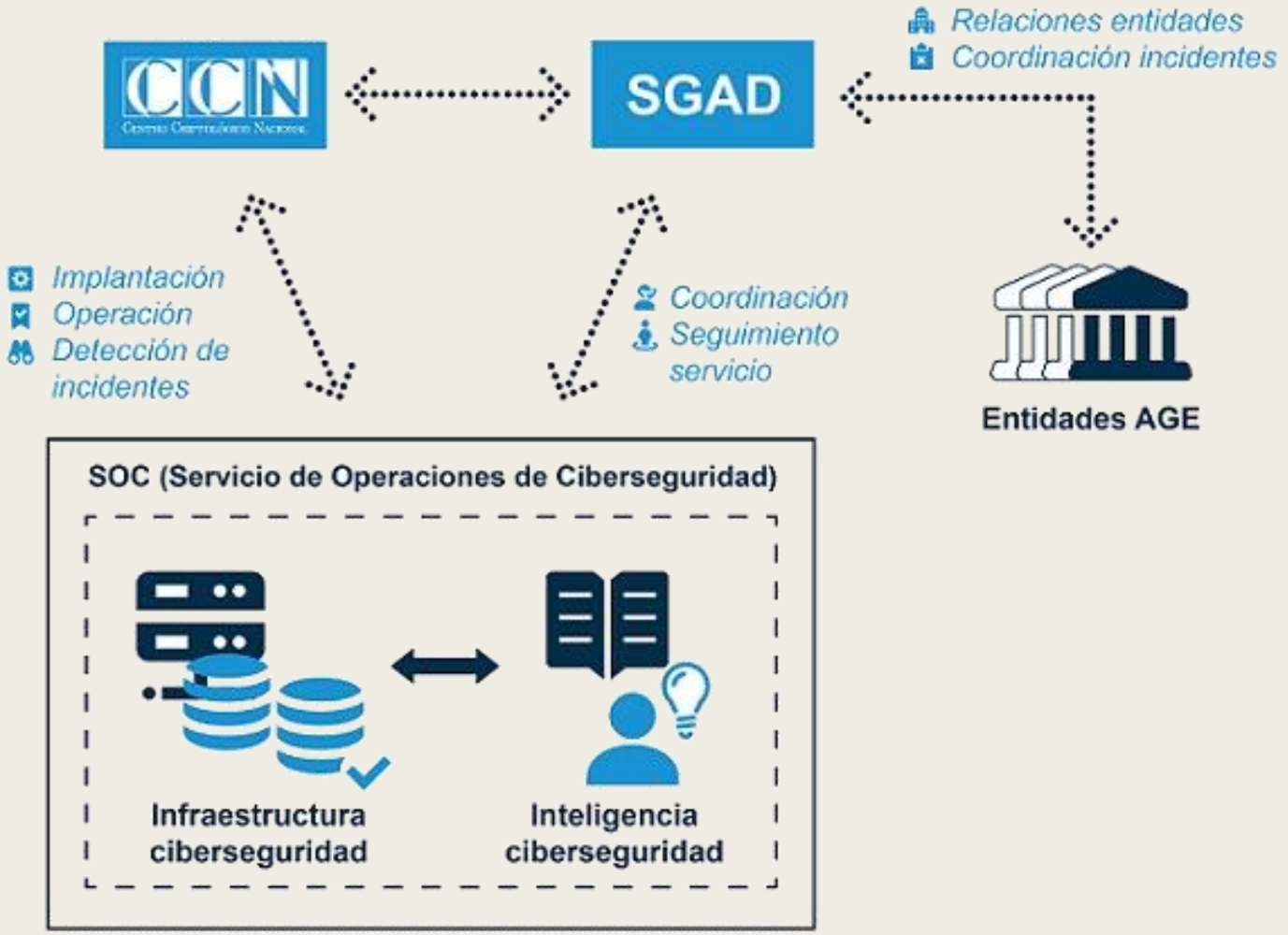
Monitorizar de manera **continua** las medidas de seguridad.

Actuar de manera proactiva incrementando y ampliando las capacidades de detección, vigilancia, protección y reacción ante incidentes.

Equipo de **expertos**: Investigación de incidentes de seguridad, análisis forense, análisis de código, análisis manuales e ingeniería inversa de binarios, asistencia in-situ para la contención y resolución de incidentes críticos y cibervigilancia en redes sociales e Internet.

SOC de la AGE

Seguridad gestionada



Ciberseguridad en el MINETAD

- Equipo de seguridad **común** para MINETAD, Turespaña, Instituto del Carbón y Centro Español de Metrología.
- Formación y **concienciación** de los usuarios.
- Gestión del **cumplimiento** normativo – buenos resultados en el informe INÉS.
- **Prevención** – Gestión de inventario, vulnerabilidades y parches.
- **Auditoría** continua.
- Respuesta a **incidentes**:
  - *NGFW, Sandboxing, Endpoint → Correlación.*
  - *CCN-CERT Pack (LUCÍA, CARMEN, SAT-INET, …).*

Un buen SOC para la AGE

¿Enfoque de máximos o mínimos?

- Un SOC de **mínimos** va orientado a lo operativo sin aportar valor estratégico para la transformación digital.
- Recoger el **máximo** catálogo de servicios comunes de seguridad gestionada para ofrecerlo con las máximas capacidades y garantías.
- **SÍ** debería **reemplazar** funciones existentes.
  - *En Organismos que ya tengan la función desarrollada,* ***liberaría recursos****.*
  - *En Organismos que no tengan la función, la tendrían cubierta como servicio.*
- Al igual que en otros servicios compartidos, una vez elegido el enfoque de máximos, deben redefinirse las funciones de los clientes del servicio que dejan de hacer unas funciones para pasar a hacer otras.

Un buen SOC para la AGE

Servicios adicionales a los previstos (1)
Vigilancia digital ampliada

- Gestión de **vulnerabilidades** continua en entornos internos, red SARA e Internet. Establecer líneas base de configuración segura o de actualización de parches mínima para las diversas arquitecturas de producción de los organismos.

- **Auditoría** automatizada continua o pentesting continuo de aplicaciones.

- Servicio de auditoría de **código fuente** o de security testing para los desarrollos seguros de aplicaciones Web.

- **Vigilancia digital** con capacidad de análisis de webs, foros y redes sociales y correlación con fuentes de inteligencia para la detección previa de las posibles campañas o ataques dirigidos a la AGE

Un buen SOC para la AGE

Servicios adicionales a los previstos (2)
Consultoría y apoyo técnico

- Consultoría de **gestión** para tener un sistema de gestión mínimo que permita a pequeños organismos que tienen carencias en seguridad disponer de un plan mínimo de adecuación al ENS.

- Servicios **técnicos** de bastionado de equipos o adecuación a las guías CCN-STIC.

- Respuesta a **incidentes in-situ** para apoyar la mitigación del impacto de incidentes críticos que puedan expandirse a otros Organismos.

Un buen SOC para la AGE

Servicios adicionales a los previstos (3)
Formación y concienciación

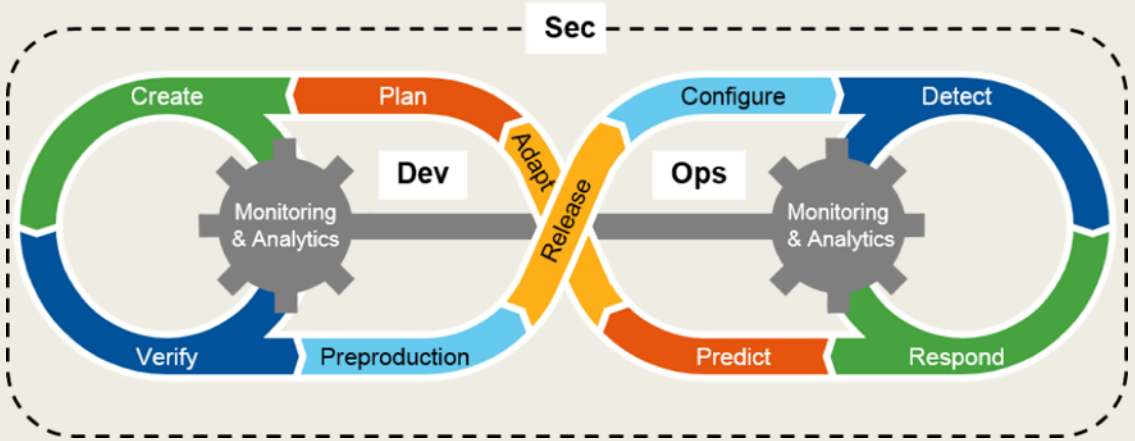
- Formación **técnica** dirigida a los equipos de respuesta a incidentes de los organismos para disponer de unas capacidades de interlocución mínimas y entender el enfoque y procedimientos de escalado del servicio.
- Concienciación a **usuarios finales** con material para uso extensivo en toda la AGE, con formatos “píldora”, en tono formal e informal, etc.
- Concienciación específica dirigida a los **altos cargos** mediante sesiones breves para que conozcan el escenario de ciberseguridad en el que nos encontramos y puedan comprender las medidas de seguridad que se implantan que van orientadas a proteger su información y minimizar riesgos. En este caso es fundamental contar con los empleados públicos de cada Ministerio y, a ser posible, utilizar las estructuras de los Comités definidos en las políticas de seguridad.

Ciberseguridad en el MINETAD

Escenario futuro

Seguridad vertical / Seguridad de negocio

- Orientación a la **seguridad de la información** (Menos ciber y más negocio).
- Integración en el ciclo de vida de desarrollo y creación de servicios → Pasar de modelos DevOps a **DevSecOps**
- Seguridad desde el **diseño** / Privacidad desde el diseño.
- Plan de **continuidad** de negocio.
- Medidas de protección específicas para **aplicaciones y tratamientos** (Apps y Datos).



GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

sgtic
S.G. DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

Muchas gracias

Miguel Ángel Rodríguez Ramos

Subdirector General Adjunto de Tecnologías de la Información y de las Comunicaciones

Ministerio de Energía, Turismo y Agenda Digital

SOC INFO Ciberseguridad

PROTAAPP

Protege las Administraciones Públicas

Tu comunidad de ciberseguridad en el sector público

Comparte

Comparte ideas y experiencias sobre ciberseguridad en el sector público en un foro informal

Conoce

Conoce a gente con tus mismas inquietudes y amplía tu red social

Aprende

Actualiza tus conocimientos a través de la comunidad

Únete en https://groups.google.com/d/forum/protaapp