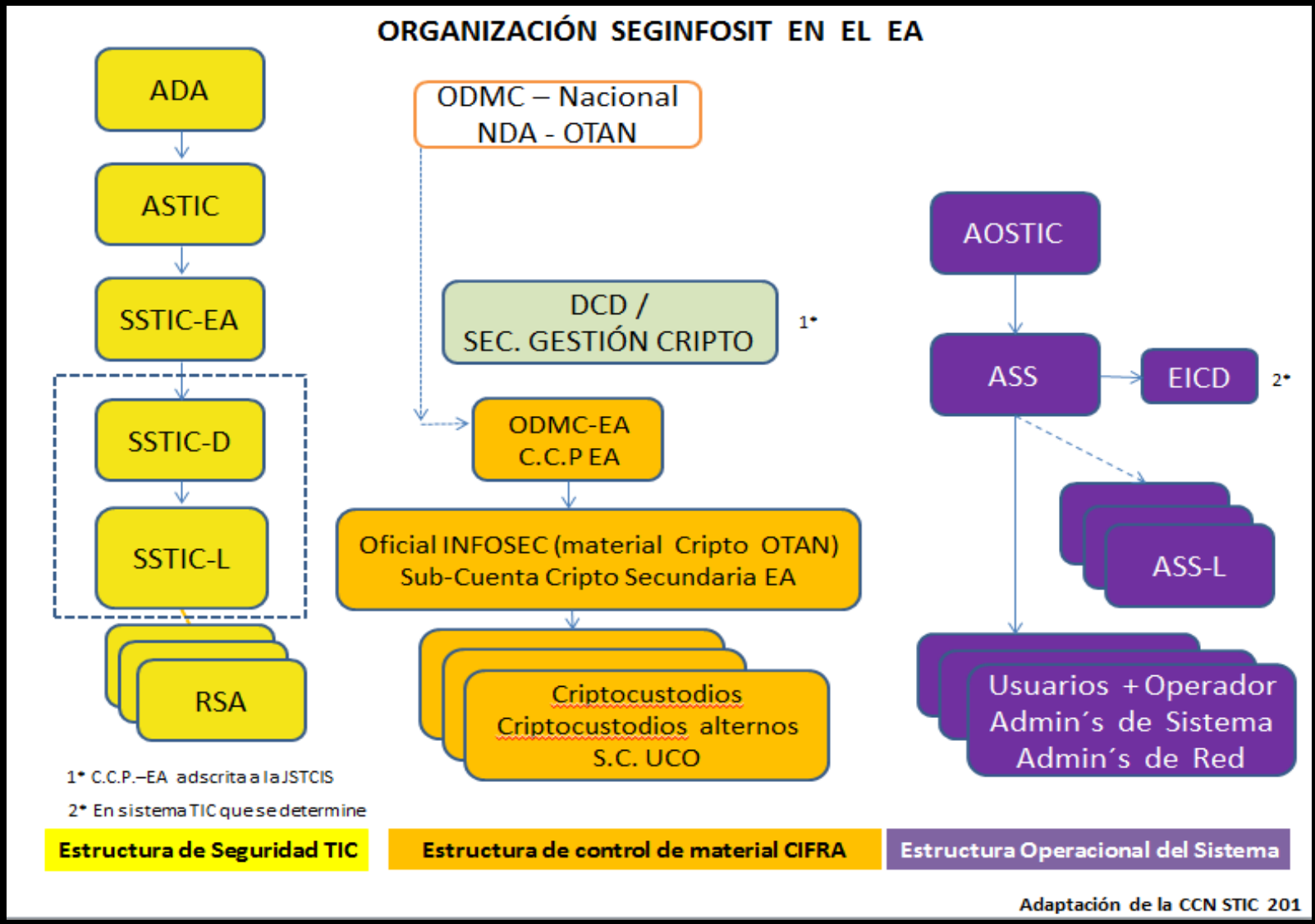
# CENTRO DE OPERACIONES DE SEGURIDAD DEL E.A.


SALAMANCA, MAYO 2018

# Estructuras



# Situación


ESTRATEGIA DE SEGURIDAD NACIONAL
2017
UN PROYECTO COMPARTIDO
DE TODOS Y PARA TODOS


El ciberespacio y su seguridad
Riesgos y Amenazas a la Ciberseguridad Nacional
ESTADOS EXTRANJEROS
CAUSAS TÉCNICAS
FENÓMENOS NATURALES
HACKING
CONFLICTOS
CRIMEN ORGANIZADO
AMENAZAS INTERNAS
CIBERESPACIO
TERRORISMO
SABOTAJE
HACKTIVISTAS
INDIVIDUOS AISLADOS
DELINCUENCIA
ESPIONAJE
ORGANIZACIONES TERRORISTAS
ESTRATEGIA DE CIBERSEGURIDAD NACIONAL
2013

# Metodología ABCD

- **A**CTUALIZACIÓN
- **B**ASTIONADO
- **C**ONCIENCIACIÓN

→ SEGURIDAD ESTÁTICA TRADICIONAL

- **D**EFENSA ACTIVA

## PREGUNTAS BÁSICAS DE LA DEFENSA ACTIVA

- ¿SE HA ACTUADO A TIEMPO?
- ¿SE SABE LO QUE HA OCURRIDO?
- ¿SE HE MEJORADO LA SEGURIDAD TRAS EL EVENTO O INCIDENTE?
- ¿SE HAN EVITADO ATAQUES SIMILARES O IDÉNTICOS EN EL FUTURO?

# Defensa Activa

## EVOLUCIÓN EN LA AMENAZA Y EN LA DEFENSA LÓGICA

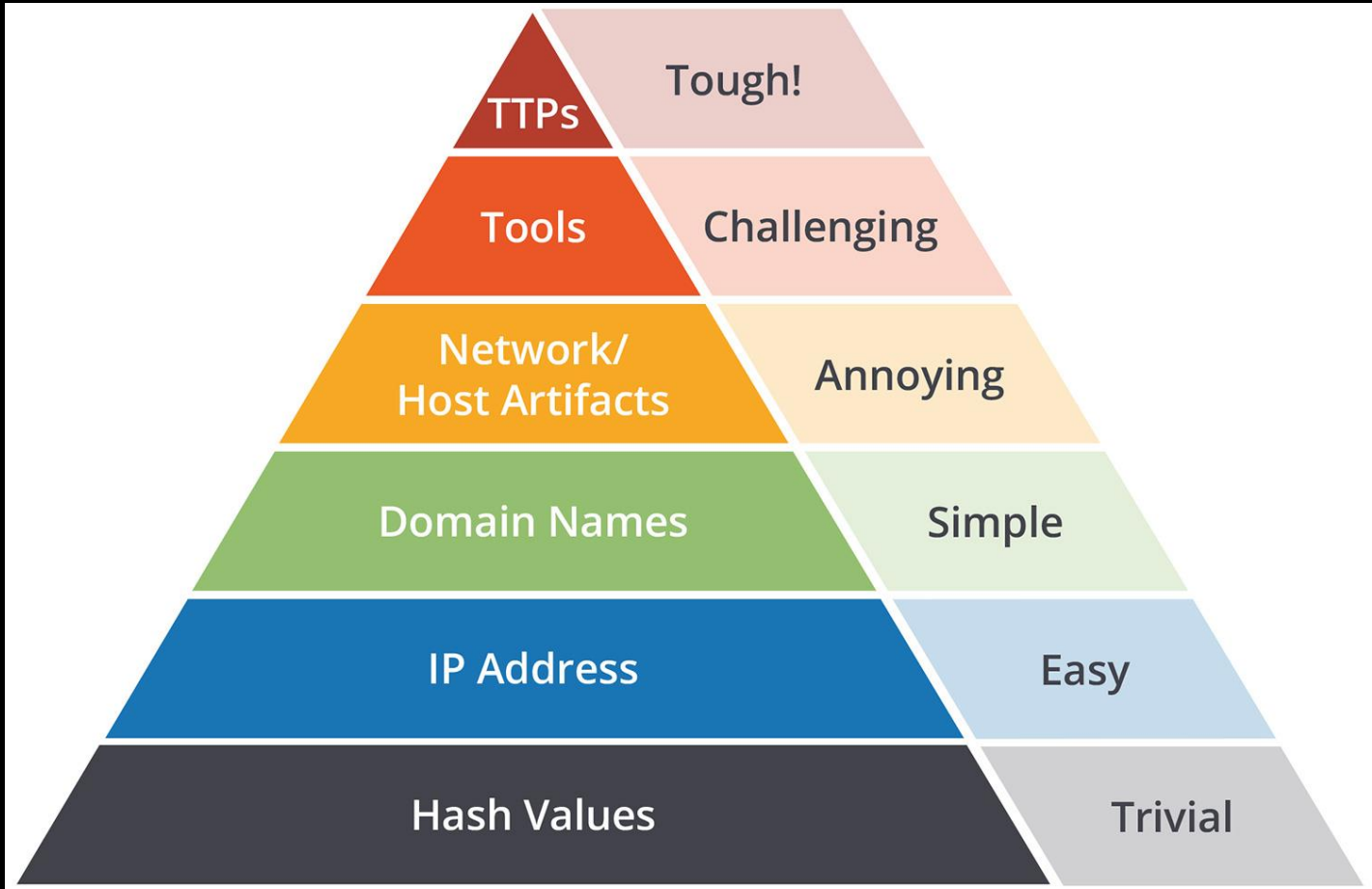
- COMSEC / TRANSEC (NECESIDAD OPERATIVA BÁSICA).
- SEGINFO / SEGINFOSIT (MALWARE / CIBERESPIONAJE) - > 2009.
- CIBERSEGURIDAD/CIBERDEFENSA (APT / CIBERTERRORISMO)- > 2012.
- OPERACIONES MILITARES EN EL CIBERESPACIO (AMENAZA HÍBRIDA/ZONA GRIS).

## NUEVO ENFOQUE DE LA SEGURIDAD

- BASADA EN CIBERINTELIGENCIA ACTUABLE.
- DEBE GESTIONAR EVENTOS (IOA) E INCIDENTES (IOC).
- TIENE QUE CONVERTIR LA AMENAZA DESCONOCIDA EN CONOCIDA (ARTEFACTOS, TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS, HERRAMIENTAS, ETC).
- ARTICULADA EN LA “PIRÁMIDE DEL DOLOR” PLUS.

# Pirámide del dolor

## INTERACCIÓN CON EL ATACANTE




*Source: David J. Bianco, personal blog*

# COS-EA

## COS-EA (IG 10-2 + Directiva 35/15 JEMA)

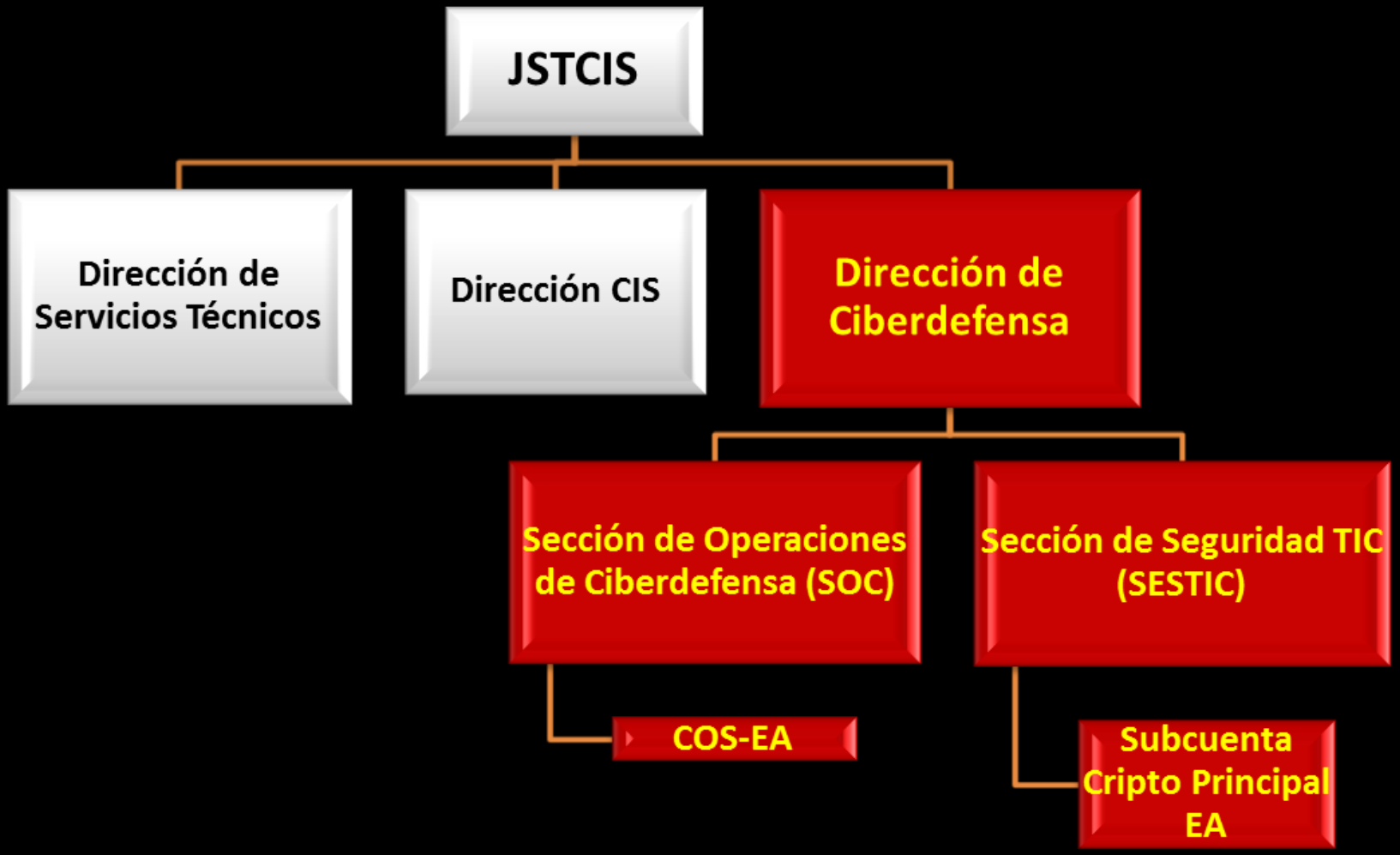
**MISIÓN:**
Proporcionar servicios a las Autoridades Operacionales de los Sistemas TIC (AOSTIC) para permitirles implementar una adecuada seguridad lógica.

**Cometidos defensivos:**

**a) Prevención**
**b) Detección**
**c) Análisis**
**d) Contención y Resiliencia**
**e) Gestión incidentes**
**f) Ciberinteligencia**

**IOC - 31 MAR 2016**
**FOC - 30 SEP 2016**

# Orgánica


JSTCIS
Dirección de Servicios Técnicos
Dirección CIS
Dirección de Ciberdefensa
Sección de Operaciones de Ciberdefensa (SOC)
Sección de Seguridad TIC (SESTIC)
COS-EA
Subcuenta Cripto Principal EA

# Servicios del COS-EA

(1) Servicio de monitorización de seguridad.
(2) Servicio de test de penetración en sistemas y análisis de vulnerabilidades.
(3) Servicio de alertas, documentación y concienciación de seguridad.
(4) Servicio de test de configuración y aplicación de plantillas de seguridad.
(5) Servicio de inspecciones de seguridad y análisis de riesgos.
(6) Servicio de análisis de malware.
(7) Servicio de análisis forense.
(8) Servicio de auditoría y apoyo de seguridad al código fuente.
(9) Servicio de mitigación y contramedidas.
(10) Servicio de gestión y coordinación de incidentes.
(11) Servicio de asesoría de seguridad en sistemas y redes.
(12) Servicio de apoyo a la actualización de sistemas.
(13) Servicio de detección de intrusos.
(14) Servicio de recuperación ante un desastre.

ÁREAS:

Forense

Inspecciones

Gestión

(15) Servicio de detección de la Obsolescencia

# Servicios del COS-EA

**CONTENIDO DE LOS SERVICIOS**

- PERSONAL (APTITUD Y ACTITUD).
- MATERIAL (SOFTWARE + HARDWARE).
- FORMACIÓN.
- PROCEDIMIENTOS.
- INFRAESTRUCTURA

**RETOS:**

- CAPTACIÓN Y RETENCIÓN DEL PERSONAL.
- FORMACIÓN DEL PERSONAL.
- MANTENER EL HARDWARE Y SOFTWARE DEL COS-EA.
- ATENDER LA SEGURIDAD LÓGICA DE SISTEMAS DE ARMAS Y PLATAFORMAS.
- CAPACIDAD DE ADAPTACIÓN A LAS NUEVAS AMENAZAS.

# PREGUNTAS