CENTRO de SISTEMAS y
TECNOLOGÍAS de la INFORMACIÓN
y las COMUNICACIONES
(CESTIC)

La experiencia en el MDEF con el Esquema Nacional de Seguridad

SOCINFO: Ciberseguridad (13)
Esquema Nacional de Seguridad, actualización y temas pendientes

MINISTERIO DE DEFENSA
SECRETARÍA DE ESTADO
CESTIC

24 mayo 2018

La experiencia en el MDEF con el ENS: resumen

MINHAFP (DTIC / SGAD)

Modelo de Gobernanza TIC de la AGE y OOPP

RD 3/2010

Organización TIC de la AGE (RD 806/2014)

Plan de Transformación Digital de la AGE (Estrategia TIC 2015-2020)

Declaración de Servicios Compartidos

Contratos Centralizados

2010

2014

2015

Nuevo Alcance ENS

2016

2017

2018

2020

Ministerio de Defensa

Esfuerzo inicial ENS-MDEF

Política CIS/TIC MDEF

Arquitectura Global

Gobernanza TIC
Infraestructura Única
Racionalización
Centralización Servicios
Interoperabilidad
AGE y OTAN

Esquema Nacional de Seguridad

Plan de Acción para la Transformación Digital del MDEF (1ª parte)

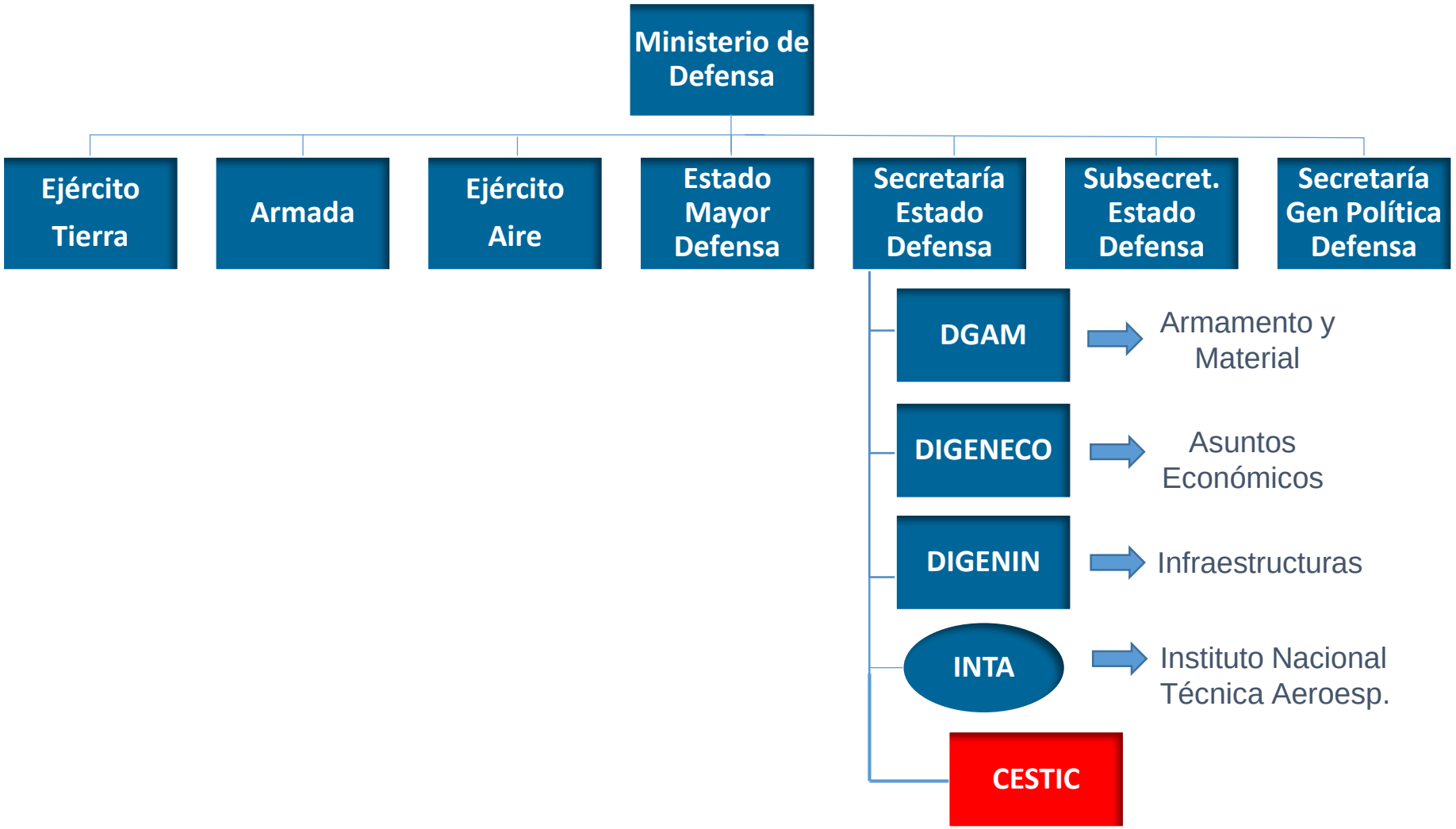
Plan de Actuación de SEGINFO

Plan Estratégico CIS

Ejecución y seguimiento de los tres planes estratégicos 2018-2019-2020

ÍNDICE

El Ministerio de Defensa: organización



Centro de Sistemas y Tecnologías de la Información y las Comunicaciones

(antigua Subdirección General TIC)

El Ministerio de Defensa: responsabilidades del CESTIC

El Ministerio de Defensa: funciones y responsabilidades

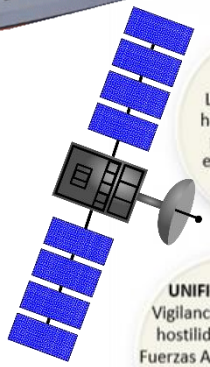
¿Cuales son las funciones del Ministerio de Defensa?

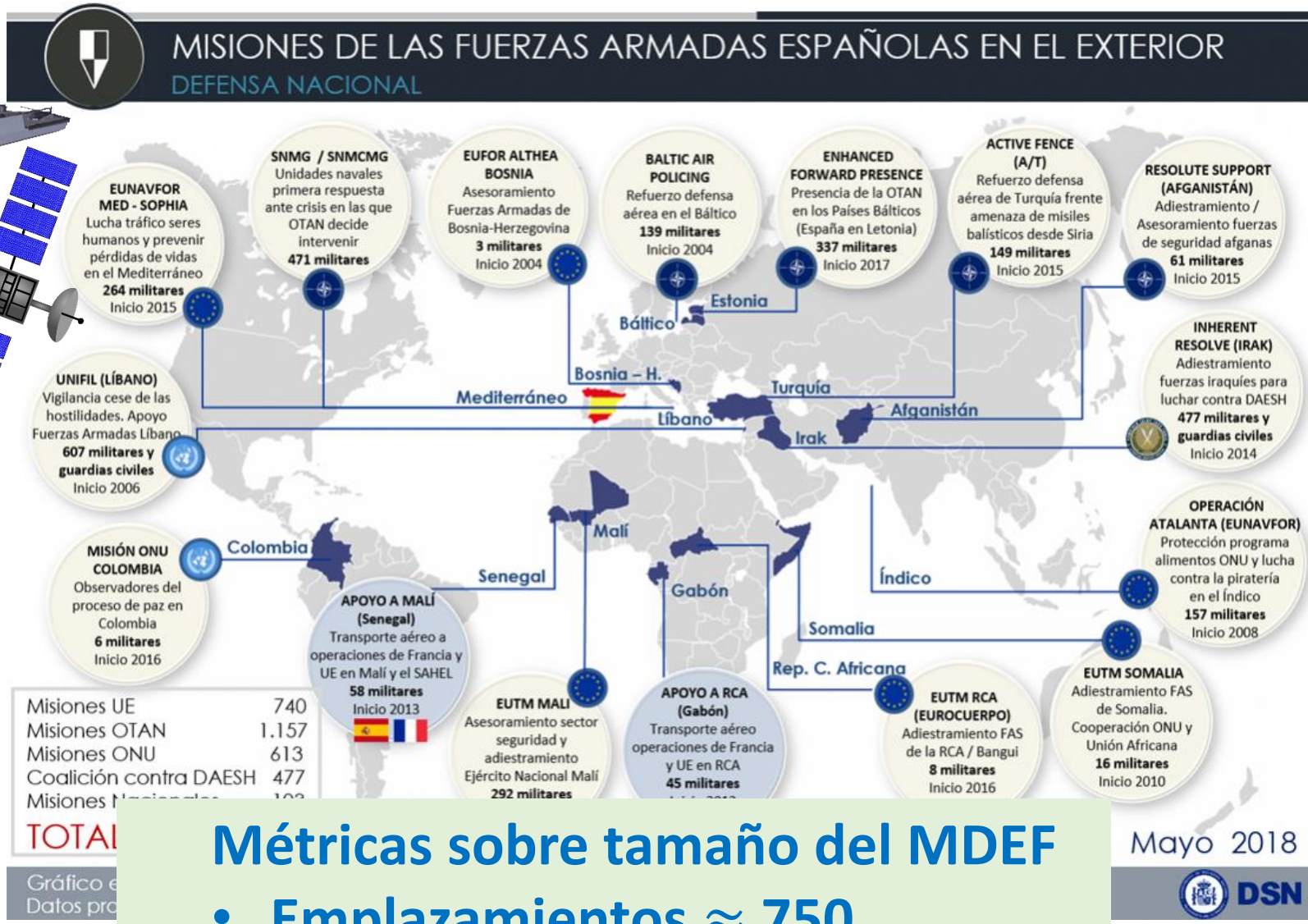
Preparación, desarrollo y ejecución de la política de defensa determinada por el Gobierno y la gestión de la administración militar

Ejemplos:

- Defensa de la integridad territorial (Territorio Nacional)
  - Control Espacio Aéreo y Marítimo
  - Control Ciberespacio
  - Respuesta a desastres y crisis (UME)
- Misiones de paz fuera de Territorio Nacional
- Preparación de la fuerza
- Gestión Logística (vehículos, aeronaves, buques, armas, etc.)
- Gestión de Infraestructuras
- Sanidad: Hospitales propios
- Justicia: Tribunales propios
- Enseñanza: Centros de enseñanza propios
- Sistemas Aeroespaciales
- Diplomacia: Agregadurías de Defensa en el extranjero
- I+D

El Ministerio de Defensa: tamaño y movilidad





Métricas sobre tamaño del MDEF

- Emplazamientos ≈ 750
- Usuarios ≈ 100.000

ÍNDICE

La seguridad de la información en el MDEF

- Ley de Secretos Oficiales de 1968 (modificada en 1978)
  - Materias Clasificadas: SECRETO y RESERVADO
- Primera Política de Seguridad de Sistemas: OM 76/2002
  - Acreditación de sistemas ANTES de manejar informac. CLASIFICADA
  - Autoridades, roles y responsabilidades
  - Materias Clasificadas, Criptología, etc
- Política de Seguridad de la Información global: OM 76/2006
  - Protección de la información del MDEF en todo momento: Personas, Documentos, Instalaciones, Empresas y Sistemas
  - Estructura funcional:
    - Nivel Corporativo: Director de SEGINFO (el SEDEF), Consejo de Dirección de SEGINFO, Responsables Áreas
    - Nivel Específico: responsable de seguridad por cada ámbito
  - SECRETO, RESERVADO: +CONFIDENCIAL, +DIFUSIÓN LIMITADA
- Instrucción 53/2016 del SEDEF
  - Comisión Ejecutiva de SEGINFO
  - Plan de Actuación de SEGINFO

ÍNDICE

ENS, 2010-2015: alcance ley 11/2007

- Esquema Nacional de Seguridad, RD 3/2010
  - Alcance relativo a la ley 11/2007 acceso electrónico ciudadanos…
  - En MDEF: Sedes Electrónicas, Registros Electrónicos y diversas Plataformas de Servicios Web (intermediación)

- Fuera del alcance ENS: sistemas que manejan Inform. CLASIFICADA
  - Estos sistemas deben ser Acreditados (revisión formal e independiente) antes de manejar Información CLASIFICADA
  - Requisitos de seguridad mayores que el ENS
  - Prioritario para el MDEF

- Acciones para adecuar el MDEF al ENS, 2010-2015:
  - Plan de Adecuación al ENS del MDEF (2013)
  - Asignación de Roles, Categorización, Declaración de Aplicabilidad
  - Nuevos procedimientos
  - Auditorías periódicas
  - Implantado con éxito (aunque con alcance limitado)

ÍNDICE

ENS, 2015-2017: nuevo alcance leyes 39 y 40/2015

- Real Decreto 951/2015 (modificación del ENS)
- Leyes 39 y 40/2015 (el medio electrónico por defecto)
- Estrategia TIC 2015-2020 de la AGE (extender ENS a TODOS los sistemas de las AAPP)

- Hasta este momento, ENS en MDEF sólo a Sedes, Registros y Plataformas de Servicios Web para empresas y otras AAPP
- A partir de aquí, ENS a **¿TODOS LOS SISTEMAS?**

- En el caso del MDEF:
  - ¿Cuantos Sistemas de Información existen en el MDEF?
  - Multitud de sistemas "legacy"
  - Sistemas críticos: Operaciones, Logística, Sanidad, etc.
  - Servicios CIS no centralizados

- ¿Tiene sentido aplicar el ENS directamente a TODOS estos sistemas?

- Necesario un cambio de modelo…

ENS, 2015-2017: nuevo alcance leyes 39 y 40/2015

- 2015: La antigua Subdirección General TIC MDEF se transforma en el "Centro de Sistemas y Tecnologías de la Información y las Comunicaciones" (CESTIC)
- 2015: Nueva "Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa" (OM 2639):
  - Planificar, Racionalizar, Adecuar
  - Un único proveedor de servicios CIS para todo el MDEF (CESTIC)
  - Una Infraestructura Única de Comunicaciones (I3D)
- 2016: Arquitectura Global de la I3D (Instr. 58/2016)
  - Centrarse en las capacidades CIS/TIC de las FFAA
  - Normalización/estándares
  - Interoperabilidad AGE/OTAN
  - Modelo de gobierno integral
  - Optimizar y racionalizar los recursos humanos y materiales
- 2017: Plan de Transformación Digital MDEF (1ª parte)
  - Identificados Procesos y Sistemas de Información del MDEF asociados
  - Identificadas acciones para conseguir objetivos de la Estrategia TIC AGE
  - Se eliminan duplicidades, centralización de recursos

ÍNDICE

ENS, 2018-2020: Ejecutar Planes Estratégicos

Los siguientes planes estratégicos incluyen extender el alcance del ENS:

- **Plan de Transformación Digital del MDEF (1ª parte)**
- **Plan de Actuación de Seguridad de la Información del MDEF**
- **Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones**

Una vez definido el nuevo modelo de provisión de servicios y racionalizados los sistemas de información ¿qué queda por hacer en el ENS?

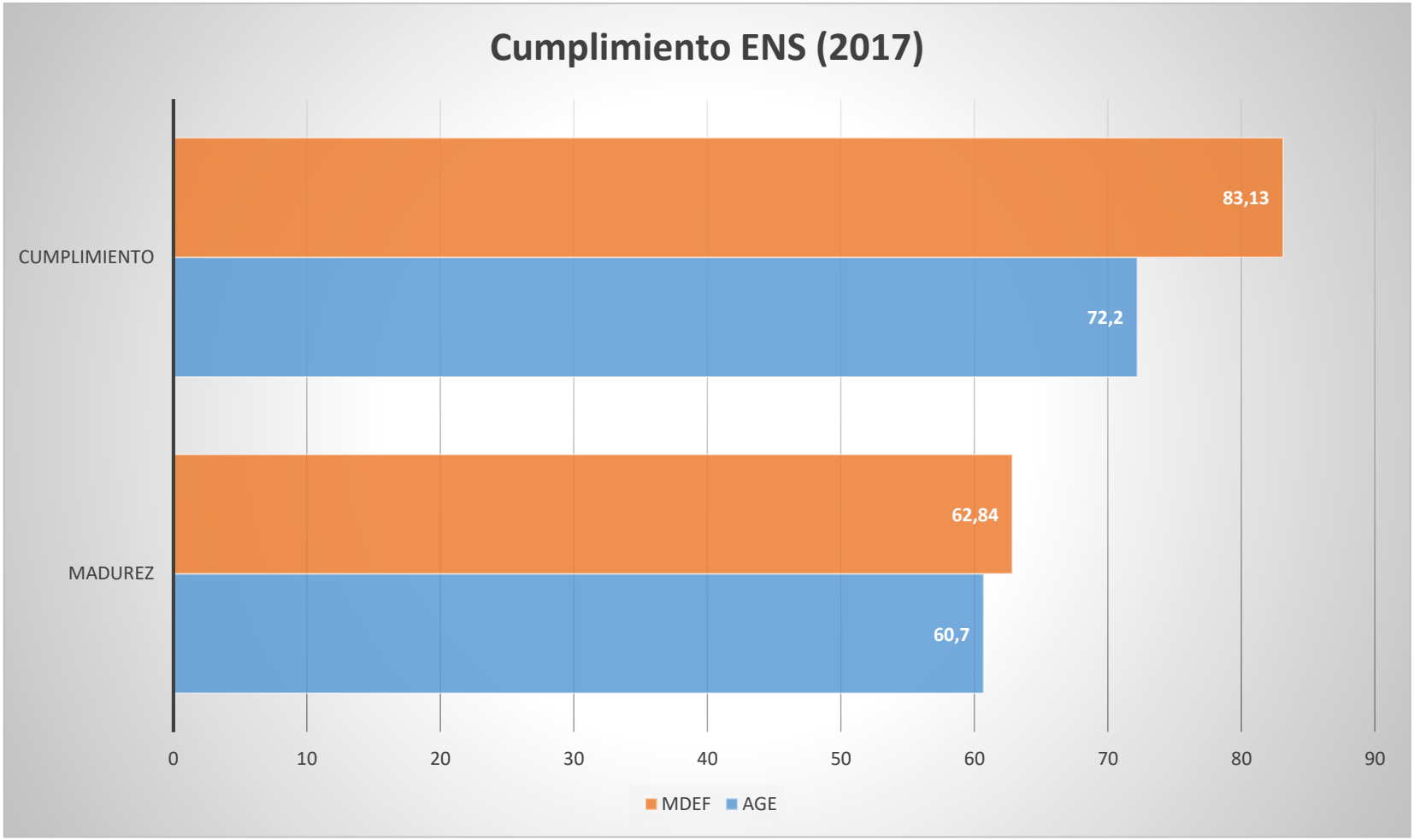
- **Implantar los controles verticales que falten en los sistemas de información definidos en la 1ª parte del Plan de Transformación Digital.**

- **Impulsar auditorías: vulnerabilidades y cumplimiento**

- **Conformidad “oficial” con el ENS, según nueva ITS.**

ÍNDICE

Experiencia en el MDEF



Grado de cumplimiento ¿aceptable? pero….

Con un alcance limitado de sistemas… y además…

Autoevaluación = ¿Autocomplacencia?

Experiencia en el MDEF: puntos fuertes

- Sistemas clasificados (críticos): acreditación formal ANTES de manejar información CLASIFICADA.

- Sistemas en el alcance del ENS:
  - Normativa de seguridad en todas las áreas (Personas, Documentos, Instalaciones, Sistemas y Empresas)
  - Enfoque integrado LOPD + ENS
  - Seguridad perimetral
  - Protección del puesto de trabajo
  - Equipos de auditorías con experiencia (auditorías periódicas y también previo paso a producción)
  - Disponemos de nuestro propia infraestructura para emitir certificados electrónicos y nuestro propio token físico (TEMD)

Experiencia en el MDEF: aspectos a mejorar

Aspectos a mejorar:

- **Captar y retener el "talento"**
- **Agilidad para modificar la normativa vigente**
- **Análisis de Riesgos formal en TODOS los sistemas**
- **Gestión de activos en tiempo real**
- **Auditoría continua (incluso análisis de código desde fases tempranas del desarrollo)**
- **Conformidad "oficial" con el ENS en sistemas nivel medio-alto**

Estrategia para obtener la conformidad "oficial":

- **MDEF tiene órganos propios para inspección y auditorías (los que se ocupan de acreditar sistemas clasificados nacionales).**
- **Manteniendo la prioridad en los sistemas clasificados, destinar recursos a la conformidad con el ENS.**
- **Comenzando con los sistemas que tengan relación con ciudadanos, empresas y otras administraciones públicas.**

Experiencia en el MDEF: proyectos de seguridad en marcha

Proyectos de seguridad en marcha

- Tecnológicos:
  - Control de Acceso a Red
  - Inspección del tráfico cifrado
  - Uso de certificados comerciales para sitios web del MDEF “públicos” + implementación segura HTTPS, en línea con iniciativa CCN-CERT
  - Potenciar el Centro de Operaciones de Seguridad de la I3D (COSI3D)

- Contratación:
  - Potenciar las clausulas de seguridad de la información en TODOS los contratos.
  - Si cedemos datos a contratista, exigir medidas de seguridad ENS (al nivel correspondiente) y reservarse la potestad de realizar auditorías
  - Criterios de valoración de ofertas: “premiar” a prestadores de servicios que dispongan de servicios certificados ENS
  - Potenciar uso de soluciones que estén en el catálogo de productos STIC del CCN (guía CCN-STIC-105)

Experiencia en el MDEF: algunos retos

¿Cómo beneficiarse de la inteligencia de la “nube” para obtener mejores capacidades de seguridad sin poner en riesgo nuestros datos?

¿Cómo fomentar la colaboración y cooperación entre el personal CIS y de seguridad, de las diferentes Administraciones Públicas?

El soldado del futuro ;)

Muchas gracias

José Ángel Álvarez Pérez
Email: jalvpe1@mde.es
Twitter: @joseangel_a76