DISEÑO E IMPLANTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (en el MINISDEF)

Autor: JOSÉ LUIS QUINTERO VILLARROYA
Director/es: IAGO LÓPEZ ROMÁN

I. INTRODUCCIÓN Y CONTEXTO

El crecimiento exponencial de las Tecnologías de la Información y las Comunicaciones en los últimos tiempos genera cantidades ingentes de información que intercambiamos a través de los sistemas de comunicaciones, ofreciéndonos servicios y facilitando nuestro trabajo, creándonos una dependencia de la que no podemos prescindir.

La tecnología se desarrolla a una velocidad tal que difícilmente es comparable con el avance del desarrollo de la seguridad necesaria para protegerla. La protección de la Confidencialidad, Integridad y Disponibilidad de información manejada por las TIC es un gran reto al que se enfrenta las organizaciones.

El Ministerio de Defensa se encuentra en pleno proceso de transformación digital y uno de los principales proyectos del proceso, es la creación de la Infraestructura Integrada de la Información del MINISDEF (I3D), una red privada destinada a los servicios específicos de la defensa y seguridad nacional, dotada de los más altos estándares de calidad y seguridad.

Por todo ello, y como se contempla en la Política CIS/TIC del MINISDEF (O. DEF 2639/2015), "*se presenta la necesidad de consolidar la seguridad en las CIS/TIC, a través del fortalecimiento de las capacidades de prevención, detección y respuesta a ciberataques, en línea con la normativa nacional y de las organizaciones internacionales de las que España forma parte*".

Con este Trabajo de Fin de Master pretendo presentar un proyecto sobre el "Diseño e Implantación de un Centro de Operaciones de Seguridad en el Ministerio de Defensa" (COS) que cubriría estas necesidades de seguridad de las TIC dentro del Ministerio de Defensa, tomando como referencia la normativa nacional y del Ministerio, la taxonomía de OTAN y los estándares nacionales, teniendo en cuenta las buenas prácticas de ITIL v3 y la experiencia propia de los años dedicados a la ciberseguridad dentro del Ministerio de Defensa.

Este COS proporcionará las capacidades operativas en materia de Seguridad de la Información de Prevención, Protección, Detección, Respuesta y Recuperación, generando información sobre el estado de la ciberseguridad de las TIC del Ministerio de Defensa.

Aunque el contenido de este trabajo puede ser aplicado al diseño e implantación de un Centro de Operaciones de Seguridad en cualquier otro Organismo, he querido personalizarlo para el Ministerio de Defensa. Esto implica que se ha tenido como referencia la normativa interna del Ministerio de Defensa, la normativa nacional que afecta a la Seguridad de la Información, la normativa de referencia de OTAN y sus marcos de referencia y por último la organización propia del Ministerio de Defensa y su idiosincrasia por lo que se hace uso de conceptos que son utilizados habitualmente en el funcionamiento diario del Ministerio.

II. DESARROLLO Y RESULTADOS

El trabajo está organizado cubriendo los siguientes puntos:

- **Introducción y Objetivos**. Motivación de la realización de este TFM y los objetivos que se pretenden alcanzar, así como la organización del trabajo.
- **Estado del Arte.** Basado principalmente en la normativa propia del Ministerio de Defensa y la taxonomía C3 de OTAN, la normativa nacional referente a la protección de la información (LOPD, GDPR, ENS, ENI, etc.), la normativa y guías elaboradas por el CCN-CERT y todo ello teniendo en cuenta los estándares nacionales e internacionales y la buenas prácticas de ITIL v3.
- **Introducción sobre los Centros de Operaciones de Seguridad** en general, su necesidad y la necesidad particular de implantarlo en el seno del Ministerio de Defensa, con su misión, ámbito de actuación, objetivos y capacidades.
- **Evaluación del estado actual**. Para ello se realizará un análisis mediante una matriz DAFO (Debilidades-Amenazas-Fortalezas-Oportunidades) y así poder hacer un diagnóstico inicial.
- **Análisis DAFO-CAME**. Una vez realizado el análisis DAFO, aplicamos la matriz CAME (Corregir-Afrontar-Mantener-Explotar) para definir las estrategias a adoptar.
- **Servicios del COS**. En base a la normativa nacional y al modelo de OTAN (C3 Technical Services Taxonomy) se definen los servicios a implementar y la modalidad de servicio propuesta.
- **Relaciones entre los diferentes servicios**. Como se relacionan los diferentes servicios entre sí y las relaciones con otros organismos del Ministerio de organismos externos.
- **Evaluación Coste-Beneficio**. Donde como resultado de la evaluación se priorizarán los diferentes servicios a implementar.
- **Concepto MIRADO**. Realización de un análisis de los diferentes conceptos a estudiar para la implementación del COS. Se hace uso del concepto MIRADO de amplio uso dentro del Ministerio de Defensa en el que se analizan los conceptos de **M**aterial, **I**nfraestructura, **R**ecursos Humanos, **A**diestramiento, **D**octrina y **O**rganización.
- **Procesos y Procedimientos**. Un análisis de los procesos globales dentro de cada una de las áreas definidas en el COS y de los procedimientos a desarrollar dentro de cada una de las áreas en base a los procesos definidos.
- **Documentación**. Los Planes a generar para la puesta en servicio del COS.

- **Implantación del COS**. Tomando como referencia el Modelo de Madurez (CMMI) y definiendo los objetivos a alcanzar en cada una de las fases de implantación.
- **Plan de Implantación del COS**. Dividido en los proyectos de Implantación Física, Implantación Tecnológica y Despliegue del Personal del COS.
- **Capacidades de Seguridad.** La taxonomía de Seguridad CIS/TIC del Ministerio de Defensa.
- **Controles de seguridad.** Controles de seguridad a implantar para su monitorización, desarrollo y seguimiento del COS.
- **Niveles de Alerta**. Los niveles de alerta del COS teniendo en cuenta la gravedad de los incidentes.

III. CONCLUSIONES

Una vez finalizado este trabajo de Fin de Master sobre "Diseño e Implantación de un Centro de Operaciones de Seguridad (en el MINISDEF)" se exponen las conclusiones más interesantes obtenidas que se han alcanzado.

1. La Administración General del Estado y en este caso, el Ministerio de Defensa, se encuentra en fase de transformación digital que comenzó con la creación del Centro de Tecnologías de la Información y las Comunicaciones (CESTIC) en el año 2012. Se avanza hacia una infraestructura común denominada Infraestructura Integrada de la Información para la Defensa (I3D). La I3D será una red privada destinada a los servicios específicos de la defensa y seguridad nacional, para lo que estará dotada de los más altos estándares de calidad y seguridad.
2. El COS proporcionará las capacidades operativas en materia de Seguridad de la Información de Prevención, Protección, Detección, Respuesta y Recuperación, generando información sobre el estado de la ciberseguridad de los CIS/TIC del Ministerio de Defensa
3. La puesta en marcha de un Centro de Operaciones de Seguridad es un proyecto que debe ser planificado minuciosamente, tanto en su Diseño como en su Implantación.
4. El objetivo principal de un COS es la protección de forma centralizada de la Información, para ello debemos basarnos en tres pilares fundamentales, Personas, Procesos y Tecnología de forma equilibrada. Si no se tienen en cuenta estos tres pilares de forma conjunta, no se podrá alcanzar el objetivo.
5. Este trabajo ha supuesto una labor de recolección de información de normativa del Ministerio de Defensa, nacional y OTAN para que todo lo aquí expuesto sea conforme con la estrategia del Ministerio y nacional.
   Se ha hecho uso de metodologías y estándares para el diseño y gestión de servicios CIS/TIC como ITIL, ISO 27000 o la Command, Control and Communications Technical Services Taxonomy de OTAN.
6. Mediante una matriz DAFO (Debilidades-Amenazas-Fortalezas-Oportunidades) hemos podido definir la situación actual y así poder hacer un diagnóstico inicial mostrando cuales son los puntos fuertes y débiles y así poder evaluar el estado final que queremos alcanzar.

Este análisis de la matriz DAFO nos va a permitir conocer las estrategias a adoptar para "Corregir las Amenazas", "Afrontar las Amenazas", "Mantener las Fortalezas" y "Explotar las Oportunidades" (DAFO-CAME).

7. Tomando en cuenta el Plan Estratégico CIS (PECIS) que marca los servicios de ciberseguridad que debe prestar el COS y la Taxonomía C3 (Command, Control and Communications) de OTAN adoptada por el Ministerio de Defensa, ha servido como referencia para la organización de las diferentes áreas y actividades relacionadas.
8. Se han definido 10 áreas que se consideran las mínimas para la puesta en servicio del COS, el resto de las áreas formarán parte de la mejora continua del COS.
   Estas áreas mencionadas no son independientes, están relacionadas unas con otras de tal manera que el intercambio de información entre ellas es fundamental para el correcto funcionamiento del COS. Por otro lado, el COS debe mantener relaciones externas con otros departamentos del Ministerio de Defensa y con entidades externas, tanto públicas como privadas.
9. La priorización de la puesta en marcha de las diferentes áreas es consecuencia de una evaluación de Coste-Beneficio, priorizando aquellas áreas que reportan un mayor beneficio con un menor esfuerzo para así obtener resultados significativos a corto plazo. También se priorizarán aquellas áreas en las que, a pesar de suponer para su implantación un esfuerzo grande, el beneficio aportado es grande y merece la pena el esfuerzo.
10. Para el diseño del COS se ha hecho uso del concepto MIRADO (Material-Infraestructura-Recursos Humanos-Adiestramiento-Doctrina-Organización), de amplio uso en el Ministerio de Defensa, en el que se analizan los diferentes conceptos y las necesidades en cada uno de ellos.
    Especial interés tiene el apartado de los Recursos Humanos, en el que hay que definir claramente los perfiles necesarios para cada uno de los puestos.
11. Los Procesos deben quedar claramente definidos. En este TFM se han expuesto los procesos globales que a su vez se podrán descomponer en otros subprocesos. Estos procesos requieren su desarrollo en Procedimientos de detalle.
12. Para proyecto de la implantación del COS se ha tenido en cuenta la Capability Maturity Model Integration (CMMI) de la Carnaggie Mellon University, asignando actividades a realizar en cada una de las fases Inicial, Desarrollo, Definido, Gestionado y Optimizado.
13. Se debe desarrollar un Plan de Implantación estructurado en tres proyectos principales, Implantación Física, Implantación Tecnológica y Despliegue de Personal, para que de una forma coordinada, se llegue a la puesta en servicio del COS.
    Este plan está realizado sobre la base de disponer de las infraestructuras adecuadas, de los recursos económicos necesarios y los expedientes de contratación de personal y adquisición del equipamiento están en marcha y no van a sufrir retrasos.