Gestión de la Seguridad de la información manejada en un centro de trabajo

Autor: Martinez Tamargo, Vanesa

Director: Rodelgo Lacruz, Miguel

Contacto: Ministerio de Defensa – Dirección General de Armamento y Material – Subdirección General de Programas – Jefatura de Sistemas Satelitales y Ciberdefensa. Pº Castellana, 109 - Madrid

---

La Jefatura de Sistemas Satelitales y Ciberdefensa se encuadra en la Subdirección General de Programas de la Direccion General de Armamento y Material del Ministerio de Defensa. Se crea en febrero de 2020 con el fin de impulsar, realizar un seguimiento y controlar la gestión, realizada por las Oficinas de Programa (OOPP) y en colaboración con las FAS, de los programas de obtención, de modernización y de sostenimiento común de sistemas satelitales y de ciberdefensa, asegurando su necesaria uniformidad e interoperabilidad. No obstante, dada la transversalidad la Jefatura, surge una nueva necesidad como apoyo al resto de Jefaturas de la SDG PROGRAMAS, y otros organismos que se determinen, en la consideración de aspectos relativos a ciberdefensa en los programas de sus ámbitos de competencia.

Ante la creación de la misma, se hace necesaria la implementación de unos procedimientos de trabajo con el fin de asegurar la trazabilidad de la documentación manejada en el mismo y para securizar dicha información. Mediante el presente Trabajo de Fin de Máster se pretende cubrir este reto.

El centro de trabajo tendrá unos requisitos mínimos de seguridad que se desarrollarán en diferentes entornos de seguridad.

Los entornos de seguridad serán:

- Entorno Global de seguridad del centro de trabajo.
- Entorno Local de seguridad del centro de trabajo
- Entorno Electrónico de seguridad del centro de trabajo.

Además de las medidas de seguridad de un edificio, cada entorno de seguridad tendrá unas medidas particularizadas que se desarrollaran en función de unos riesgos particularizados.

Una vez estos riesgos sean gestionados, se establecerán una serie de procedimientos de seguridad básicos, los cuales podrán ser ampliados según las necesidades tanto de la documentación como del entorno de seguridad en sí mismo.

Los procedimientos básicos que se trataran en este trabajo son los siguientes:

- Procedimiento de alta y baja de usuarios.
- Procedimiento de medidas de seguridad a adoptar por el personal no usuarios del sistema clasificado.
- Procedimiento de seguridad documental del sistema clasificado.
- Procedimiento de seguridad TIC.
- Procedimiento de gestión de incidentes de seguridad.
- Procedimiento de auditoria y gestión interna de la seguridad.

Palabras clave: Seguridad, Información, Riesgos, Incidente, Medidas

---

1. Introducción

En febrero de 2020 se crea la Jefatura de Sistemas Satelitales y Ciberdefensa (JSSAT&CIBER) con un cometido principal que es común a todas las Jefaturas de los Programas de Armamento y Material, enfocado en este caso a los sistemas Satelitales y de Ciberdefensa: “Impulso, seguimiento y control de la gestión, realizada por las Oficinas de Programa (OOPP) y en colaboración con las FAS, de los programas de obtención, de modernización y de sostenimiento común de sistemas satelitales y de ciberdefensa, asegurando su necesaria uniformidad e interoperabilidad”.

No obstante, dada la transversalidad de la Ciberdefensa, se consideró conveniente añadir un segundo cometido, definido como “apoyo al resto de Jefaturas de la SDG de Programas, y otros organismos que se determinen, en la consideración de aspectos relativos a ciberdefensa en los programas de sus ámbitos de competencia”. Señaló, así mismo, que esta segunda misión no estaba oficializada todavía, al no figurar en la Instrucción de Organización de la DGAM.

El objetivo principal de este trabajo es la descripción de los diferentes entornos reales de seguridad en un Centro de Trabajo en el que se maneja información con diferentes grados de clasificación, los requisitos y medidas de seguridad requeridas para su protección.

Por ello se hace necesario establecer una metodología de trabajo además de una serie de procedimientos para el manejo de la información con un nivel determinado de clasificación al tratarse de sistemas de armas, en este caso se generaliza, aunque los sistemas de armas en los que se incluye contenido para la “ciberdefensa” se puede decir que su contenido si cabe se puede clasificar como “altamente sensible”.

Con este fin se proponen los siguientes objetivos específicos:

- Estudio de la normativa actual y su aplicabilidad.
- Análisis de los siguientes condicionantes:

1. Identificación de los requisitos de seguridad necesarios de acuerdo a la normativa aplicable.
2. Identificación de los entornos de seguridad.
3. Identificación de medidas de seguridad a implantar.
4. Identificación y autentificación.
5. Registros.
6. Salvaguarda de la información y datos.
7. Salvaguarda de la integridad y disponibilidad.
8. Salvaguarda sobre el HW y SW.
9. Salvaguarda sobre las comunicaciones.
10. Salvaguarda sobre la reutilización de elementos.
11. Auditorias.
12. Administración de la seguridad.

Estos condicionantes nos dan lugar a la redacción de una serie de procedimientos de acuerdo a cumplir los requisitos específicos de cada uno de ellos, estos serán los siguientes:

- Procedimiento de alta y baja de usuarios.
- Procedimiento de medidas de seguridad a adoptar por el personal no usuarios del sistema clasificado.
- Procedimiento de seguridad documental del sistema clasificado.
- Procedimiento de seguridad TIC.
- Procedimiento de gestión de incidentes de seguridad.
- Procedimiento de auditoria y gestión interna de la seguridad.

2. Desarrollo

El trabajo incluye el análisis de:

- El Centro de Trabajo, el cual estará compuesto tanto de estaciones de trabajo, servidores dedicados, aplicaciones SW, periféricos y equipamiento de red tanto local como externa y WAN-PG, soportada por los sistemas de telecomunicaciones del Ministerio de Defensa.
    - Descripción de los niveles de clasificación de la información.
    - Tipos de usuarios del Centro de Trabajo, estos deberán estar en posesión de la Habilitación Personal Seguridad (HPS) de acuerdo a la información que han de manejar.
    - Requisitos mínimos de seguridad del Centro de Trabajo.
    - Análisis de las posibles amenazas y vulnerabilidades asociadas a diversos factores.
- Los diferentes entornos de seguridad, catalogándolos de acuerdo a la información que se va a manejar y dónde se va archivar.

Como resultado se establecerán:

- Medidas de seguridad del entorno perimetral teniendo en cuenta el control de accesos. En función de los riegos detectados, se decretaran e implantarán distintos controles asociados a dichos riesgos.
- Medidas para identificar y autentificar a los usuarios del sistema de acuerdo a los riesgos identificados.
- Un registro de las acciones derivadas del manejo de la información de acuerdo a los riesgos reconocidos.
- La salvaguarda de la información y datos de acuerdo a los riesgos identificados.
- Una garantía de la integridad y disponibilidad de la información de acuerdo a los riesgos detectados.
- Las salvaguardas adecuadas asociadas a Hw y SW.
- Una serie de salvaguardas de las comunicaciones en los diferentes entornos de seguridad.
- Una serie de salvaguardas sobre la reutilización de elementos.
- Una serie de auditorías periódicas del sistema
- Procedimientos para la administración del sistema.
- Un procedimiento con el fin de controlar la altas y bajas de los usuarios.
- Un procedimiento con el fin de establecer la seguridad documental necesaria para un sistema clasificado.
- Un procedimiento con el fin de asegurar la seguridad de las TIC.
- Un procedimiento de gestión de los posibles incidentes de seguridad.
- Un procedimiento de auditorías tanto internas como externas.

3. Resultados y discusión

Los resultados del presente trabajo se pueden aplicar en cualquier centro de trabajo real que maneje información con diferentes grados de clasificación.

No obstante, cada uno de ellos se particularizará para la Jefatura de Sistemas Satelitales y Ciberdefensa.

De esta manera se cubre el objetivo de asegurar la trazabilidad de la documentación manejada en el mismo y para securizar la información que se maneja en el Centro de trabajo.

Estos procedimientos son los mínimos a aplicar, pudiendo en un futuro ampliarlos conforme sea necesario y requerido.

4. Conclusiones

Con el presente trabajo se cubren los objetivos iniciales que se planteaban:

- Se han identificación de los requisitos de seguridad necesarios de acuerdo a la normativa aplicable.

- Se han identificado y analizado los diferentes entornos de seguridad.
- Se han definido y procedimentado las medidas de seguridad a implantar.
- Se ha definido y procedimentado el proceso de autentificación.
- Se han definido y procedimentado los registros mínimos.
- Se ha definido y procedimentado la salvaguarda de la información y datos.
- Se ha definido y procedimentado la salvaguarda de la integridad y disponibilidad.
- Se ha definido y procedimentado la salvaguarda sobre el HW y SW.
- Se ha definido y procedimentado la salvaguarda sobre las comunicaciones.
- Se ha definido y procedimentado la salvaguarda sobre la reutilización de elementos.
- Se ha definido y procedimentado auditorías.
- Se ha definido y procedimentado como se ha de administrar la seguridad.

De esta manera se han cumplido el objetivo de establecer una metodología de trabajo a partir de una serie de procedimientos para el manejo de la información con un nivel determinado de clasificación asegurando la trazabilidad de la documentación manejada con el fin de securizarla a través de la delimitación los diferentes entornos de seguridad que se pueden dar en un centro de trabajo. Se han identificación de los posibles riesgos que se pueden dar anulándolos o mitigándolos y se han analizado y aplicado la normativa actual vigente.

Agradecimientos

A Miguel Rodelgo por su eterna comprensión al aceptar ser tutor de este trabajo.

A mi familia, por todo el tiempo que no les he dedicado, su paciencia y colaboración aliviando las tareas cotidianas, siempre o casi siempre, con una sonrisa.

Al profesorado del Máster; nos ha tocado vivir un curso inusual debido a esta pandemia, han intentado sacar siempre lo mejor de todo el alumnado, tratando de colaborar y apoyar en situaciones complicadas tanto a nivel personal, laboral o académicas con el mejor talante y dedicación.

A mis compañeros del Máster, hemos hecho de un grupo de gente independiente de muy diversa índole y procedencia, un grupo de amigos..

Referencias

[1] *NORMA CCN-STIC-001 - Seguridad de las Tecnologías de la Información y las Comunicaciones que maneja Información Clasificada en la Administración.*

[2] *NORMA CCN-STIC-152-Evaluación y Clasificación de Zoning Locales (DL) (clasificada).*

[3] *NORMA CCN-STIC-202-Estructura y Contenido Declaración de Requisitos Seguridad.*

[4] *NORMA CCN-STIC-301-Medidas de Seguridad de las TIC a Implementar en Sistemas Clasificados.*

[5] *NORMA CCN-STIC-305-Destrucción y sanitización de soportes informáticos.*

[6] NORMA CCN-STIC-403-Gestión Incidentes de Seguridad."

[7] *NORMA CCN-STIC-404-Control de soportes informáticos.*

[8] *NORMA CCN-STIC-430-Herramientas de Seguridad.*

[9] *Riesgos de los Sistemas de Información (MAGERIT I, II Y III).*