Servicios Informáticos
Seguridad de la Información

Documentos UCM

Serie: Seguridad

SE0002 Organización de la Seguridad de la Información

Versión del Documento 1.2

04/04/2017

INDICE

1 INTRODUCCIÓN

1.1 Alcance

Para poder responder de forma eficaz y eficiente a los retos de la seguridad de la información en la UCM, se deben organizar y estructurar las responsabilidades y las funciones relacionadas con la seguridad, así como asegurar que no existan lagunas.

El objeto de este documento es describir y documentar la estructura de responsabilidades, competencias y relaciones relativas a la seguridad de la información en la UCM.

1.2 Definiciones, acrónimos y abreviaturas

UCM:	Universidad Complutense de Madrid
ENS:	Esquema Nacional de Seguridad
CSI:	Comité de Seguridad de la Información
ASS:	Administrador de Seguridad del Sistema
API:	Administrador de Protección de la Información

1.3 Referencias

- UNE 71501-1:2001 IN Tecnología de la Información (TI). Guía para la gestión de la seguridad de TI. Parte 1: Conceptos y modelos para la seguridad de TI
- SE0001 Política de seguridad de la información
- Real Decreto 3/2010 del 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Guía de seguridad (CCN-STIC-801) Esquema Nacional de Seguridad, responsabilidades y funciones.
- Guía de seguridad (CCN-STIC-805) Esquema Nacional de Seguridad, política de seguridad de la información.

2 PRINCIPIOS PARA LA ORGANIZACIÓN DE LA SEGURIDAD

Para poder acometer con éxito los objetivos de seguridad se deben definir y asignar responsabilidades y competencias en seguridad de la información.

Una organización correcta en seguridad se debe apoyar sobre varios principios fundamentales:

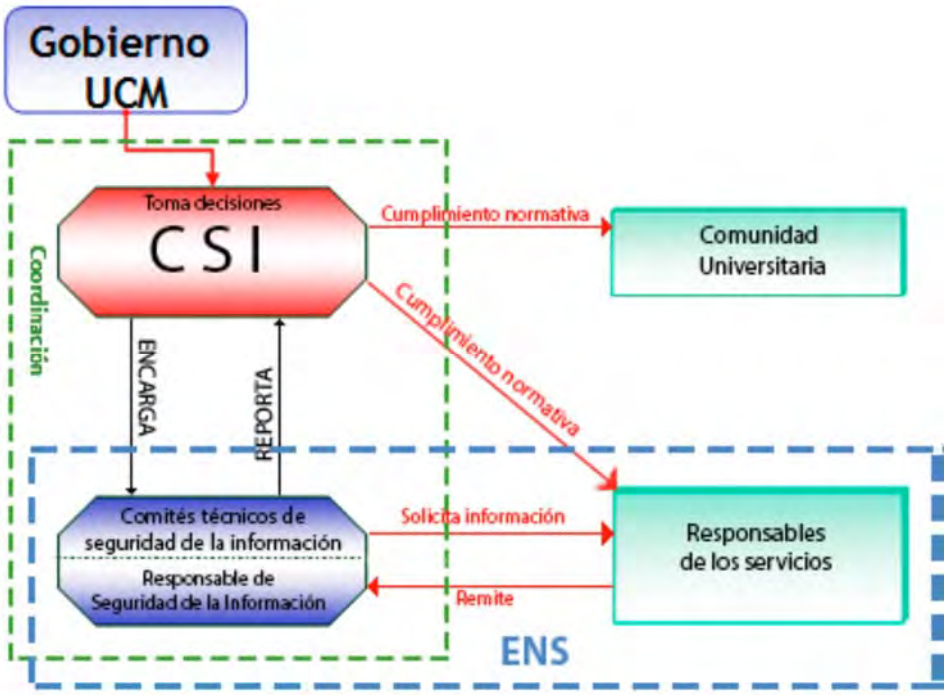
- La seguridad ha de entenderse como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los servicios prestados.
- Un análisis y gestión de riesgos actualizados son una parte esencial del proceso de seguridad.
- Prevención, detección y recuperación: la utilización de todos los tipos de medidas permitirá un enfoque integral de la seguridad, evitando incidencias y reduciendo el impacto de aquellas que finalmente ocurran.
- Los servicios deben estructurarse con diferentes líneas de defensa constituidas por medidas organizativas, físicas y lógicas, de modo que una amenaza que se materialice no pueda desarrollar todo su potencial y se mitigue, rápidamente, el daño producido.
- Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
- Segregación de roles para asegurar la calidad y evitar posibles conflictos de intereses, asegurando la consistencia de la seguridad, mediante actuaciones coordinadas entre todos los actores implicados.
- No dejar lagunas de responsabilidades, asegurando que el ciclo de vida de las medidas de seguridad esté cubierto: definición, implantación/operación, revisión y mejora.
- Permitir la toma de decisiones para hacer frente a los retos, problemas e incidencias relacionados con la seguridad de la información.

3 ESTRUCTURA ORGANIZATIVA DE LA SEGURIDAD

3.1 Estructura

Se crea el Comité de Seguridad de la Información (CSI), quien a su vez creará los Comités Técnicos de Seguridad de la Información necesarios para el ágil funcionamiento de una estructura operativa de seguridad, repartida entre las diferentes áreas de responsabilidad de la UCM.

El diagrama siguiente representa el esquema de decisión y coordinación de la seguridad de la información.



Con esta estructura se pretende:

- Conseguir decisiones con una coordinación fluida y consistencia en las actuaciones de seguridad: Comité de Seguridad de la Información y Comités Técnicos de Seguridad de la Información.
- Responsabilizar a cada área implicada en la operativa de las medidas de seguridad de su competencia.
- Reportar a los distintos responsables.
- Gestionar los riesgos.
- Crear, comunicar y hacer cumplir la normativa de la UCM en materia de seguridad.

3.1.1 Comité de Seguridad de la Información

El Comité de Seguridad de la Información tiene como funciones:

- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el Rector, en los términos establecidos en el artículo 11 del RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Aprobar la normativa interna en el ámbito de la seguridad de la información que sea necesaria.
- Aprobar el Plan de Adecuación al Esquema Nacional de Seguridad y las medidas necesarias para su implantación.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de Tecnología de la Información (TI), desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TI.
- Promover la realización de las auditorías periódicas, que permitan verificar el cumplimiento de las obligaciones en materia de seguridad que establezca la Política de Seguridad y la normativa vigente.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables o entre diferentes áreas de la UCM.
- Recabar de los responsables de los distintos ámbitos de la seguridad informes regulares del estado de la seguridad de la Universidad y de las posibles incidencias que se produzcan.

Este comité está constituido por representantes de distintas áreas de gobierno de la UCM y se reunirá periódicamente al menos trimestralmente, o cuando existan propuestas o eventos que lo justifiquen, y podrá invitar a personas de otras áreas de la UCM, o a especialistas externos cuando lo estime oportuno.

3.1.2 Comités Técnicos de Seguridad de la Información

El CSI creará cuantos **Comités Técnicos de Seguridad de la Información** estime necesarios para coordinar las operaciones de la seguridad de los sistemas de información afectados por el ENS en la UCM entre los diferentes departamentos técnicos responsables de su implantación y seguimiento, con las siguientes funciones:

- **Consensuar y acordar las funciones y tareas específicas de cada área**
- **Acordar métodos y procesos**
- **Implementar y respaldar las iniciativas aprobadas por el CSI**
- **Evaluar y reportar la conformidad con las directrices y los objetivos establecidos**
- **Revisar y reportar las incidencias de seguridad**
- **Revisar y evaluar la documentación**

Estos comités, constituidos por representantes de distintas áreas técnicas de la UCM, **se reunirán periódicamente, y siempre antes que el CSI,** y podrán invitar a personas de otras áreas de la UCM, o a especialistas externos cuando lo estimen oportuno.

3.1.3 Roles, responsabilidades y competencias relacionadas con la Seguridad de la Información

Para asegurar una seguridad consistente, se indica a continuación un resumen de competencias y responsabilidades asignadas a los diferentes roles establecidos. Para ver una información más detallada ver la "Guía de Seguridad CCN-STIC-801 Esquema Nacional de Seguridad responsabilidades y funciones"

3.1.3.1 El Responsable de la Información

Sobre él recae la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección ante un incidente de seguridad.

Establece los requisitos de la información en materia de seguridad: determina los niveles de seguridad en cada dimensión de seguridad que se realizará dentro del marco establecido en el Anexo I del ENS.

Participa junto con el Responsable del Servicio de la aceptación final del riesgo residual.

Los criterios de valoración estarán respaldados por la Política de Seguridad de la UCM en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

3.1.3.2 El responsable del Servicio

Establece los requisitos del servicio en materia de seguridad: determina los niveles de seguridad en cada dimensión de seguridad que debe realizarse dentro del marco establecido en el Anexo I del ENS.

Participa junto con el Responsable de la Información de la aceptación final del riesgo residual.

Los criterios de valoración estarán respaldados por la Política de Seguridad de la UCM en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

La prestación de un servicio siempre debe atender a las necesidades de seguridad de la información que maneja, es decir, hereda sus requisitos de seguridad y el responsable tiene la potestad de añadir otros relacionados con la disponibilidad, accesibilidad, interoperabilidad, etc.

3.1.3.3 El responsable de la Seguridad

Tiene como responsabilidades mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la UCM.

Determinará la categoría del sistema, elaborará la declaración de aplicabilidad y decidirá sobre las medidas de seguridad adicionales.

Elaborará la configuración de seguridad que aplicará el ASS.

Recae bajo su responsabilidad aprobar los procedimientos operativos de seguridad elaborados por el Responsable del Sistema.

Tiene el deber de verificar el estado de la seguridad del sistema monitorizado por el ASS y el API.

Elaborará junto con el Responsable del Sistema los planes de mejora de la seguridad.

Es su deber promover la formación y concienciación, en materia de seguridad de la información, para la Comunidad Universitaria.

Es su responsabilidad la validación de los planes de continuidad elaborados por el Responsable del Sistema.

Recibe los informes sobre el grado de implantación y eficacia de las medidas de seguridad físicas e incidentes sobre las mismas del Responsable de la Seguridad Física.

Debe verificar la seguridad en el ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación y cambios, previo informe del Responsable del Sistema.

DELEGACIÓN DE FUNCIONES

Podrá designar cuantos Responsables de Seguridad delegados considere necesarios, aunque la responsabilidad final sigue recayendo sobre sí mismo.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad.

Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reporta.

3.1.3.4 El responsable del Sistema

Tiene como responsabilidades:

Desarrollar, operar y mantener los sistemas de información afectados por el ENS durante todo su ciclo de vida: especificaciones, instalación y verificación de su correcto funcionamiento.

Definir la topología y sistema de gestión de dichos sistemas de información estableciendo los criterios de uso y los servicios disponibles en los mismos.

Elaborar los procedimientos operativos de seguridad que deberán ser aprobados por el Responsable de Seguridad y aplicados por el API y el ASS.

Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

Elaborar junto con el Responsable de Seguridad los planes de mejora de la seguridad.

Elaborar los planes de continuidad para los sistemas afectados (NIVEL ALTO) y realizar los simulacros correspondientes.

Puede decidir, de manera cautelar, la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Comunicará dichas suspensiones temporales al Responsable de Seguridad y al Responsable del Servicio afectado.

DELEGACIÓN DE FUNCIONES

Podrá designar cuantos Responsables de Sistema delegados considere necesarios, aunque la responsabilidad final sigue recayendo sobre sí mismo.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con el desarrollo, la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. Se podrán encargar de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.

Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, que es a quien reporta.

3.1.3.5 El Administrador de Seguridad del Sistema (ASS)

Será propuesto por el Responsable del Sistema para nombramiento por el Rector y su ámbito de actuación estará determinado por el alcance del ENS en la UCM.

Funciones:

La implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas de información.

La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.

Aprobar los cambios en la configuración vigente de los Sistemas de Información.

Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

Informar al Responsable del Sistema y al API de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Monitorizar el estado de seguridad de los sistemas con las herramientas disponibles de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en dichos sistemas

DELEGACIÓN DE FUNCIONES

En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de ASS, se podrán designar Administradores de Seguridad del Sistema Delegados (ASS-D).

Los ASS-D serán responsables, en su ámbito, de aquellas acciones que delegue el ASS relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información y reportarán cualquier incidencia relacionada con los mismos al ASS.

El ASS-D será designado por el Responsable del Sistema, a solicitud del ASS del que dependerá funcionalmente. Su identidad aparecerá reflejada en la documentación de seguridad del correspondiente sistema de información.

3.1.3.6 El Administrador de Protección de la Información (API)

Será propuesto por el Responsable de seguridad para nombramiento por el Rector y su ámbito de actuación estará determinado por el alcance del ENS en la UCM

Funciones:

La gestión y el análisis de riesgos.

Incorporar y mantener la documentación de seguridad del sistema.

Reportar periódicamente al Responsable de la Seguridad y al Responsable del Sistema:

- Las anomalías, compromisos o vulnerabilidades relacionadas con la seguridad.
- El cumplimento de los Procedimientos Operativos de Seguridad.
- El estado de cumplimiento de los controles de seguridad establecidos conforme a la política de seguridad y análisis de riesgos.
- Que son aplicados los procedimientos aprobados para manejar los sistemas de información.

Monitorizar el estado de seguridad de los sistemas con las herramientas disponibles de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en dichos sistemas.

Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Dependencias

4 ANEXO A

A continuación se relacionan resumidas las tareas y sus responsables para los sistemas dentro del ámbito de aplicación del ENS en la UCM.

En la tabla se usan las siguientes abreviaturas:

RINFO -- Responsable de la Información

RSERV -- Responsable del Servicio

RSEG --- Responsable de la Seguridad

RSIS----- Responsable del Sistema

ASS ----- Administrador de la Seguridad del Sistema

API ----- Administrador de Protección de la Información.

Tarea	**Responsable**
Determinación de los niveles de seguridad requeridos en cada dimensión	CSI
Determinación de la categoría del sistema	RSEG
Análisis y gestión de riesgos	API
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	API
Política de seguridad	elabora: CSI aprueba: Rector
Normativa de seguridad	elabora: API aprueba: CSI
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS + API
Estado de la seguridad del sistema	RSEG monitoriza: ASS + API
Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CSI

Tarea	**Responsable**
Planes de concienciación y formación	elabora: RSEG aprueba: CSI
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: CSI ejercicios: RSIS
Suspensión temporal del servicio	ejecuta: RSIS informa a: RSEG + RSERV
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG