Guía de Seguridad de las TIC
CCN-STIC 201

ORGANIZACIÓN Y GESTIÓN PARA LA SEGURIDAD DE LAS TIC

Enero 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.01.18 20:02:37 +01'00'

NIPO: 076-09-055-7

Fecha de Edición: enero de 2021

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Precisamente el Real Decreto 3/2010 de 8 de enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte del CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional , tanto en lo referido a la Ley 9/1968, de 5 de abril, sobre secretos oficiales (LSO), como a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Enero de 2021

ÍNDICE

1. INTRODUCCIÓN

De conformidad con la Ley 9/1968, de 5 de abril, sobre secretos oficiales (LSO), la información clasificada que es manejada por un sistema de información debe protegerse contra la pérdida de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, ya sea de forma accidental o intencionada. Como garantía de protección, dichos sistemas deben acreditarse según lo establecido en la Política de Seguridad de las TIC[1], señalada en la Ley 11/2002 de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI) y en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN).

Por otro lado, desde que se promulgó el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), sus modificaciones y su normativa derivada, las organizaciones del sector público, junto a las del sector privado que les aportan soluciones o les prestan servicios, en el ámbito del ENS, también están sujetas al cumplimiento de este conjunto normativo.

Este documento persigue entroncar la gobernanza de la seguridad de una organización con el concepto de ciberseguridad actual, que puede afectar a determinadas organizaciones públicas o privadas, y que exige la armonización y unificación de roles y comités con el objetivo de clarificar y simplificar las estructuras y gestión de la ciberseguridad asociada.

2. OBJETO

Esta guía establece unas pautas de carácter general que son aplicables a todas las entidades del sector público y del sector privado que les aportan soluciones o les prestan servicios, sin entrar en casuísticas particulares. En este sentido, se espera que cada organización las particularice para adaptarlas a su ámbito, naturaleza, competencias y entorno singular.

El objeto de esta guía es desarrollar un marco de referencia que establezca las responsabilidades generales en la gobernanza y gestión de la seguridad de los sistemas de información de las organizaciones que manejan información clasificada, presentando las figuras o roles más significativos que asuman dichas responsabilidades.

Con este propósito, cada entidad debe establecer y aprobar su propia organización de seguridad, de acuerdo con su naturaleza, estructura, dimensión y recursos disponibles, que deberá estar recogida en la Política de Seguridad de la Información de la entidad y,

[1] Tecnologías de la Información y la Comunicación.

cuando se traten datos de carácter personal, también en la Política de Privacidad o Protección de Datos.

3. ALCANCE

Esta guía se orienta a determinar las autoridades y responsables relacionados con la gobernanza de la ciberseguridad de sus sistemas a lo largo de su ciclo de vida (determinación de la necesidad, diseño, desarrollo, implantación, operación, mantenimiento y retirada).

Dichas autoridades tendrán en cuenta los requisitos de seguridad de las TIC a implementar en las diferentes fases del ciclo de vida, debiendo constar y estar presentes en la documentación de seguridad del sistema.

Esta guía está alineada con lo dispuesto en la Guía *CCN-STIC 801, sobre el ESQUEMA NACIONAL DE SEGURIDAD - RESPONSABILIDADES Y FUNCIONES*.

4. ACLARACIÓN TERMINOLÓGICA

Con relación a la terminología utilizada en esta guía, es especialmente relevante hacer una matización en lo que respecta a los términos de información clasificada[2] e información calificada[3] de cara al doble significado que se le otorga históricamente al término 'acreditación', que no debe llevar a confusión.

4.1 Sistemas que manejan información clasificada de cualquier grado

En este contexto, se entiende por **acreditación** a la autorización otorgada a un sistema para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de seguridad, con arreglo a su Concepto de Operación (CO).

Dicha acreditación tiene en cuenta múltiples aspectos, como son la seguridad de su entorno de operación con afectación a personas e instalaciones físicas además de la seguridad de los documentos (evaluado por la ONS[4]), seguridad de las emanaciones electromagnéticas (evaluada según la norma TEMPEST – CCN-STIC 210) y seguridad criptológica (evaluado por el CCN-PYTEC[5]), y la inspección de Seguridad de las TIC (evaluado por el CCN-CERT). En consecuencia, para conceder dicha acreditación global a un sistema intervienen equipos diferenciados, especializados en las diferentes actividades y fases necesarias para poder evaluar los referidos aspectos.

[2] Según la legislación vigente en materia de secretos oficiales y normativa derivada.
[3] Según el control "Calificación de la información - mp.info.2" del Anexo II del ENS.
[4] Oficina Nacional de Seguridad.
[5] PYTEC: Departamento de Productos y Tecnologías del CCN.

Cada equipo emite una declaración de conformidad del ámbito competencial que le corresponde, siendo finalmente la Oficina Nacional de Seguridad (ONS) quien propone la acreditación al Secretario de Estado Director del CNI como Autoridad de Acreditación (AA), tras la validación positiva de todas las declaraciones implicadas.

En el caso de información clasificada nacional, la acreditación la podrá conceder el Ministerio respectivo, que puede delegar -en cada ámbito de su competencia- en la Autoridad de Acreditación Delegada (AA-D) correspondiente.

4.2 Sistemas que manejan información clasificada hasta el grado de DIFUSIÓN LIMITADA (DL) y/o CUALIFICADA respecto al Esquema Nacional de Seguridad (ENS)

En las tres (3) categorías de seguridad que determina el Esquema Nacional de Seguridad (ALTA, MEDIA y BÁSICA), así como en sistemas que manejan información clasificada hasta el grado de DIFUSIÓN LIMITADA (DL), el término acreditación denota un concepto adicional distinto, además del anteriormente referido que sigue siendo válido.

La razón radica en que en el ENS y en sistemas que manejan información clasificada únicamente del grado de DL, las inspecciones STIC[6] se delegan a organizaciones que suelen pertenecer al sector privado denominadas Entidades de Certificación (EC). Dichas EC para poder realizar evaluaciones STIC requieren superar un proceso de autorización previa, denominado **acreditación**, en el que deben evidenciar su compromiso y competencia técnica, que les permita demostrar que pueden desempeñar su labor inspectora en el ámbito STIC.

En el caso de sistemas que manejan información clasificada del grado DL, la acreditación a las EC la otorga el CCN-CERT actuando en este caso como Entidad de Acreditación (EA), mientras que en el caso del Esquema Nacional de Seguridad interviene habitualmente en el proceso de acreditar a las EC la Entidad Nacional de Acreditación (ENAC) de forma adicional al propio CCN-CERT, salvo que dicha EC pertenezca al sector público, en cuyo caso la acreditación podrá concederla también el CCN-CERT.

En resumen, para acreditar los sistemas que manejan información clasificada hasta el grado de DL, se requiere el habitual proceso de acreditación a través de la ONS, aunque una de sus fases - la inspección STIC, en concreto- la puede realizar una Entidad de Certificación (EC), convenientemente acreditada por el CCN-CERT actuando

[6] Seguridad de las TIC.

éste en calidad de Entidad de Acreditación (EA), que certificará el resultado positivo o negativo de su fase dentro del proceso completo de acreditación.

5. ESTRUCTURA DE ACREDITACIÓN E INSPECCIÓN DE LA SEGURIDAD

5.1 Autoridad de Acreditación (AA)

La Autoridad de Acreditación (AA) es la autoridad responsable de conceder la autorización a un determinado sistema para manejar información hasta un grado determinado o en unas determinadas condiciones de seguridad, con arreglo a su concepto de operación (CO).

Para los sistemas nacionales que manejan información clasificada de ámbito internacional (OTAN, UE, EDA, etc.) corresponde este rol al Secretario de Estado Director del Centro Nacional de Inteligencia (CNI), cuyo órgano de trabajo, en lo referente a la protección de información clasificada, es la Oficina Nacional de Seguridad (ONS).

Para los sistemas que manejan información clasificada nacional, la AA recae en el ministro respectivo.

5.1.1 Funciones

Entre las funciones de la Autoridad de Acreditación (AA), se señalan:

- Establecer la Política STIC y velar por su aplicación en el sector público español y en el sector privado que le aporta soluciones o le presta servicios.
- Realizar los procesos de acreditación de los sistemas que le correspondan.
- Verificar el cumplimiento de los procesos de acreditación para sistemas que manejan información clasificada hasta el grado de DL, realizados por las Entidades de Certificación (EC).
- Elaborar y/o aprobar los Procedimientos, Normas, Instrucciones Técnicas y Guías que emanen de la Política STIC de aplicación a su ámbito competencial de entidades, públicas o privadas.

5.2 Autoridad de Certificación Criptológica (ACC)

Corresponde este rol al Secretario de Estado Director del Centro Nacional de Inteligencia (CNI), que se materializa por medio del CCN-PYTEC, adscrito al Centro Criptológico Nacional (CCN).

5.2.1 Funciones

Entre las funciones de la Autoridad de Certificación Criptológica (ACC), se señalan:

- Seleccionar los criptosistemas adecuados para cada organización y entorno de operación.
- Definir y publicar normas para el correcto empleo de los criptosistemas.
- Establecer los procedimientos de control del material de cifra y de las claves utilizadas.
- Formar al personal especialista necesario.

5.3 Entidad de Acreditación (EA)

Corresponde al CCN-CERT acreditar a las Entidades de Certificación (EC) que evidencien su compromiso y competencia técnica para que éstas puedan realizar inspecciones STIC en aquellos sistemas que manejen información clasificada hasta el grado de DIFUSIÓN LIMITADA (DL).

5.3.1 Funciones

Entre las funciones de la Entidad de Acreditación (EA), se señalan:

- Definir los criterios necesarios que debe cumplir una Entidad de Certificación (EC) para que ésta pueda certificar la parte que le corresponda de un sistema.
- Definir los criterios y procedimientos de evaluación que deberán seguir las EC en el ejercicio de sus inspecciones.
- Realizar la evaluación de las EC, concediéndoles o denegándoles la correspondiente acreditación.
- Supervisar y coordinar a las EC en el desempeño de sus funciones, solicitándoles cuantas evidencias estime necesario.

5.4 Entidad de Certificación (EC)

Corresponde este rol a aquellas entidades capacitadas para la realización de inspecciones STIC de sistemas que manejen información clasificada hasta el grado de DL, que previamente hubieren sido acreditadas por el CCN-CERT actuando éste en calidad de Entidad de Acreditación (EA).

5.4.1 Funciones

Entre las funciones de las Entidades de Certificación (EC), se señalan:

- Evaluar y certificar, en el ámbito de sus competencias, la parte que les corresponde de los sistemas que manejan información clasificada hasta el grado de DL, tras haber sido contratados sus servicios y manteniendo vigente su acreditación, que habrá sido otorgada por el CCN-CERT.
- Evaluar y certificar los sistemas de cualquier categoría en el ámbito del ENS, tras haber sido contratados sus servicios y manteniendo vigente su acreditación otorgada por ENAC bajo el reconocimiento del CCN-CERT.

6. ESTRUCTURA DE SEGURIDAD EN LAS ORGANIZACIONES

La gobernanza de la seguridad en una organización se articula a través de un **Comité de Seguridad TIC** y se implementa mediante **Centros de Operaciones de Ciberseguridad (CoCS)** que velan por la operación y correcta implementación de la seguridad mediante una vigilancia continua de los sistemas bajo su responsabilidad, junto a otros roles que se detallan a continuación.

6.1 Comité de Seguridad TIC (CSEGTIC)

Se constituye como un órgano colegiado, algunos de cuyos miembros ostentarán roles especializados dentro de la organización de la seguridad que se definirán en detalle en la presente guía.

Es la máxima autoridad en la organización respecto a las decisiones de seguridad que afecten a los sistemas que manejan información o prestan algún servicio.

6.1.1 Funciones generales del Comité de Seguridad TIC

Serán funciones habituales del Comité de Seguridad (CSEGTIC) las siguientes:

- Elaborar la Política de Seguridad Corporativa que deberá ser aprobada por la Dirección de la entidad.
- Aprobar el marco normativo y medidas técnicas a implementar de acuerdo al Plan de Implantación de la seguridad de las TIC en la organización.
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad con los objetivos de la organización.
- Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban ser activados.

- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose de gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Recibir las inquietudes en materia de seguridad de la Dirección de la entidad y transmitirlas a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.
- Recabar, a través del Responsable de Seguridad de las TIC (CISO), informes regulares del estado de la seguridad de la organización y de los posibles incidentes, para poder adoptar las decisiones oportunas. Estos informes, se consolidan y resumen para su comunicación a la Dirección de la entidad.
- Coordinar y dar respuesta a las inquietudes de los diferentes Administradores del Sistema/Administradores Especialistas en Seguridad (AS/AES), transmitidas habitualmente a través del Responsable de Seguridad de las TIC (CISO) o del Responsable del Sistema (RSIS).
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevándolo a la Dirección en aquellos casos en los que no tenga suficiente autoridad para decidir.

6.1.2 Funciones relacionadas con la seguridad de la información

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos, en materia de seguridad de la información.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información (SGSI).
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Revisar regularmente la Política de Seguridad de la Información, para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y cualificación de responsables, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Supervisar y aprobar la gestión de riesgos de seguridad de la información, el Plan de Tratamiento de Riesgos (PTR) y los principales riesgos residuales asumidos por la organización, recomendando a la Dirección posibles actuaciones.
- A través del Responsable de Seguridad de las TIC (CISO), monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos 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 TIC.

6.1.3 Integrantes del Comité de Seguridad TIC

Dentro del Comité de Seguridad TIC se integrarán roles operacionales, administrativos, legales, de seguridad lógica y de protección física. Cada organización establecerá la composición en función de sus competencias, estructura y circunstancias, pudiendo constar:

- Responsable de Seguridad Física (RSF).

- Responsable de Seguridad de las TIC (CISO).
- Responsable del Sistema (RSIS).
- Autoridad de Control de Material de Cifra (ACMC), si procede.
- Representante del propietario o del depositario de la información clasificada.
- El Delegado de Protección de Datos.
- Responsable de cumplimiento legal.

A la totalidad o a parte de sus reuniones, tanto ordinarias como extraordinarias, podrá invitarse a otras personas cuya opinión se considere necesaria o conveniente, en función de los asuntos a tratar.

En consecuencia, el Comité de Seguridad TIC puede constituirse en base a unos miembros fijos y otros opcionales, en función del orden del día. En cualquier caso, todos los asistentes deberán disponer de la habilitación personal de seguridad (HPS), o equivalente, acorde con la información compartida.

6.2 Responsable de Seguridad de las TIC (CISO)[7]

Corresponde a este rol la responsabilidad directa respecto a la seguridad de las TIC que le delegue el Comité de Seguridad TIC, del que formará parte y hará las funciones de secretario del mismo.

El Responsable de Seguridad de las TIC (CISO) debe ser una persona o autoridad diferente al Responsable de Seguridad Física (RSF) y al Responsable del Sistema (RSIS).

En síntesis, se encargará de la supervisión de la ejecución de medidas y procedimientos de seguridad de los sistemas de la organización, incluyendo la seguridad de las operaciones criptográficas.

En organizaciones complejas, podrán nombrarse los CISO delegados (CISO-D) que se consideren necesarios, estando coordinados por el CISO principal de la organización.

6.2.1 Funciones atribuidas al CISO

El CISO dispondrá de diferentes competencias de coordinación y supervisión de la seguridad, delegadas por el Comité de Seguridad TIC, entre las que se encontrarán:

[7] Este Rol es equiparable a la conjunción de los anteriormente designados como Autoridad de Seguridad de las TIC (ASTIC) y Supervisor de Seguridad de las TIC (SSTIC).

- Proponer al Comité de Seguridad TIC para su aprobación, la política de seguridad de la información y el plan de implantación (marco normativo y medidas técnicas) que lo desarrolla.
- Velar por el cumplimiento de la normativa vigente dentro de la organización, inspeccionando, verificando o analizando la seguridad de las TIC de los sistemas que la integran.
- Aprobar, en coordinación con el Responsable del Sistema (RSIS), el Concepto de Operación (CO) de cada sistema en sus aspectos de Seguridad de las TIC.
- Solicitar la acreditación de cada sistema que maneje información clasificada y, en su caso, su renovación.
- Promover y/o impartir la formación y concienciación STIC que se considere necesaria, dentro de su ámbito de competencia.
- Elaborar las normas y procedimientos de seguridad de los sistemas (marco normativo), en su ámbito de su actuación, consensuando con el Responsable del Sistema (RSIS) las medidas de seguridad más adecuadas para los sistemas concernidos.
- Verificar que las medidas de seguridad establecidas en la documentación de seguridad sean adecuadas para la protección de la información que se va a manejar en el sistema, satisfaciendo, además, los requisitos de protección establecidos por la normativa vigente.
- Analizar y completar toda la documentación relacionada con la seguridad del sistema: Declaración de Aplicabilidad (DA), Procedimientos Operativos de Seguridad (POS), análisis de riesgos y seguridad criptológica.
- Verificar y comprobar la implementación de los Procedimientos Operativos de Seguridad (POS) y de las funciones de seguridad de los sistemas, mediante la realización de verificaciones de seguridad periódicas.
- Realizar el seguimiento, en conjunción con el Centro de Operaciones de Ciberseguridad (CoCS), del estado de seguridad de los sistemas proporcionado por las herramientas de monitorización, gestión de eventos de seguridad y otros posibles mecanismos de vigilancia implementados en el sistema.
- Diseñar los planes de respuesta ante incidentes de seguridad.

- Dirigir, coordinar y apoyar, a través del CoCS y del ERI[8], la investigación de posibles incidentes de seguridad e informar de los mismos al Comité de Seguridad TIC o al que este determine.
- Supervisar, junto al Responsable del Sistema (RSIS) que la adición de nuevos componentes al sistema, se aplique con los criterios de bastionado necesarios, bajo el principio de seguridad por defecto, apoyándose en el catálogo de productos[9] aprobados, en el caso de manejar información clasificada, o cualificados, caso de manejar información sensible calificada por el ENS.
- Supervisar a los proveedores en los que se han externalizado servicios, en base a los informes facilitados por éstos.
- Coordinar y, en su caso, elaborar informes sobre métricas e indicadores relacionados con la seguridad.
- Participar en la realización y sucesivas revisiones periódicas del Análisis de Impacto (BIA)[10], al menos anualmente, y siempre que se desarrollen o incorporen servicios nuevos que manejen la información clasificada.
- Ordenar la realización de análisis forenses, que serán efectuados por el CoCS o el ERI, con el apoyo de los Administradores del Sistema/Administradores Especialistas en Seguridad (AS/AES), reflexionar sobre las lecciones aprendidas, definir planes de acción y hacer seguimiento de su aplicación.
- Convocar al Comité de Seguridad TIC (CSEGTIC) siempre que las circunstancias así lo requieran.

6.3 La Oficina de Seguridad TIC (OSTIC)

Dentro de la estructura del Comité de Seguridad TIC (CSEGTIC), y como elemento operativo, se constituye una Oficina de Seguridad TIC (OSTIC) cuyas competencias estarán relacionadas con las siguientes áreas de trabajo:

- Marco normativo y análisis y gestión de riesgos.
- Seguridad en las interconexiones y conectividad.
- Vigilancia y determinación de superficie de exposición.
- Monitorización y gestión de incidentes.

[8] Equipo de Respuesta a Incidentes de Seguridad.
[9] https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html
[10] BIA: Business Impact-Analysis o análisis de impacto del negocio.

- Observatorio digital y cibervigilancia.
- Otras funciones conexas o concordantes.

La Oficina de Seguridad TIC estará conformada por:

- El Director de la Oficina como Responsable de Seguridad de las TIC (CISO).
- El Directorio de CISO delegados (CISO-D).
- El Directorio de Administradores Especialistas en Seguridad (AES).

6.3.1 Funciones atribuidas a la OSTIC

Las funciones de la Oficina de Seguridad TIC serán, entre otras que les puedan ser encomendadas por el CSEG:

- Órgano de trabajo en apoyo de la labor del CISO.
- Gestión operativa del Plan de Implantación de seguridad, explotación y mantenimiento.
- Análisis y debate de las cuestiones relacionadas con la seguridad de los sistemas de información dentro de su ámbito de competencia.
- Redacción y presentación de propuestas al CSEG.

El director de la Oficina de Seguridad TIC convocará las reuniones de trabajo de sus miembros y recabará los acuerdos alcanzados, de los que dará cuenta al CSEG, para su aprobación, en su caso.

Se reunirá con una periodicidad determinada y siempre antes de las celebraciones del CSEG.

6.4 Centro de Operaciones de Ciberseguridad (CoCS)

Bajo la responsabilidad y dirección del Responsable de Seguridad de las TIC (CISO) como Director de la Oficina de Seguridad TIC del organismo, el Centro de Operaciones de Ciberseguridad (CoCS) presta servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, especialmente los que manejan información clasificada, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

El CoCS será único en la organización, aunque puedan existir varios emplazamientos físicos diferentes, todos los cuales operan bajo la dirección centralizada del Responsable de Seguridad de las TIC (CISO).

Asimismo, en función de la naturaleza y dimensiones de la organización, el CoCS puede ser interno o estar externalizado, en cuyo caso actuará remotamente a través de canales establecidos en coordinación con el Responsable de Seguridad de las TIC (CISO).

6.4.1 Funciones

El Centro de Operaciones de Ciberseguridad (CoCS) puede llevar a cabo las siguientes funciones:

- Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.
- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Operación y actualización de los dispositivos de defensa.
- Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad (ERI).
- Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.
- Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.
- Análisis forense digital y de seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

6.5 Equipo de Respuesta a Incidentes de Seguridad (ERI)

Este equipo se encarga de gestionar los incidentes de seguridad bajo las directrices marcadas por el Comité de Seguridad TIC y funcionales del Responsable de Seguridad de las TIC (CISO) y posibles alertas recibidas del Centro de Operaciones de Ciberseguridad (CoCS).

Está compuesto por un equipo con capacidades de atención inmediata denominado primer nivel de atención (L1) y por un grupo de especialistas para aquellos incidentes no resueltos por el primer nivel que requieran un mayor grado de especialización.

6.5.1 Funciones del ERI

Entre sus funciones se destacan las siguientes:

- Aplicación de inteligencia para la detección, respuesta coordinada, investigación de ciberataques y ciberamenazas y resolución de incidentes de seguridad, siempre en coordinación con el CoCS y el Responsable de Seguridad de las TIC (CISO).
- Llevar a cabo el registro, seguimiento y resolución de los incidentes de seguridad en los sistemas bajo su responsabilidad.
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- Realizar análisis forense digital y de seguridad cuando la complejidad del incidente así lo requiera, en coordinación con el Responsable de Seguridad de las TIC (CISO).
- Proponer al CISO acciones inmediatas a corto plazo si se detecta un comprometimiento de la información que pudiera tener consecuencias graves.
- Asegurar los elementos críticos del sistema, si se ha visto comprometida la seguridad del mismo.
- Determinar, hasta donde sea posible, el modo, los medios, los motivos y el origen del incidente, colaborando con el Responsable de Seguridad de las TIC (CISO) en la obtención de conclusiones y aprendizaje del mismo, de modo que se posibilite la prevención de incidentes similares en el futuro.

6.6 Responsable de Seguridad Física (RSF)[11]

Este rol asume la responsabilidad sobre la seguridad física de la organización, pudiendo designarse más de uno en organizaciones con Zonas de Acceso Restringido (ZAR) en emplazamientos distribuidos geográficamente; en ese caso, se nombrará un coordinador de entre todos ellos.

6.6.1 Funciones

Las funciones del Responsable de Seguridad Física (RSF) podrán ser las siguientes:

- Supervisar los emplazamientos y especialmente de las Zonas de Acceso Restringido (ZAR), en lo que respecta a sus medidas de seguridad física y al control de acceso de personas y equipamiento.

[11] Este Rol asume las funciones del anteriormente designado como Responsable de Seguridad del Área (RSA).

- Mantenimiento actualizado de la lista de usuarios autorizados a acceder a las diferentes áreas y verificación de su adecuación comparándola con el registro de entradas y salidas de personas.
- Comprobar regularmente el estado de seguridad en dependencias, emplazamientos y especialmente Zonas de Acceso Restringido (ZAR).
- Supervisión de todas las acciones que se lleven a cabo sobre el equipamiento del área (instalación, modificación, retirada, etc.), junto al control y registro de sus entradas y salidas. Se comprobará previamente que las acciones están autorizadas y que, durante el desarrollo de las mismas, la seguridad del sistema no se vea comprometida.

6.7 Autoridad de Control de Material de Cifra (ACMC)

Si se emplea material criptológico para la protección de la información clasificada, corresponde a esta figura el registro, contabilidad y seguimiento de todo el material de cifra.

6.7.1 Funciones

Las funciones de la Autoridad de Control de Material de Cifra (ACMC) son:

- Definir y actualizar la estructura criptológica de la organización, donde figurarán los Criptocustodios y los Criptocustodios alternativos.
- Establecimiento de los procedimientos adecuados en todo lo relacionado con el material de cifra empleado para la protección de la información clasificada.

6.8 Órganos de Distribución de Material de Cifra (ODMC)

Si se emplea material criptológico para la protección de la información clasificada, esta figura estará adscrita al Responsable de Seguridad de las TIC (CISO), pudiendo haber más de una en función de los sistemas de la organización y su distribución geográfica.

6.8.1 Funciones

Las funciones de los Órganos de Distribución de Material de Cifra (ODMC) son:

- Gestionar, distribuir, transportar y controlar el material de cifra.
- Establecer períodos de vigencia de las claves.
- Generar y confeccionar las claves según procedimientos aprobados por la ACC[12].

[12] Autoridad de Certificación Criptológica.

- Gestionar las claves según la normativa vigente.
- Controlar los procesos de introducción, utilización y destrucción del material de cifra, en coordinación con la Autoridad de Control de Material de Cifra (ACMC).

6.9 Criptocustodio

Será responsable de la recepción, protección, control y, cuando sea necesario, destrucción de todo el material de cifra bajo su custodia, en coordinación con la Autoridad de Control de Material de Cifra (ACMC).

Habitualmente, se delega en el Criptocustodio la responsabilidad de la seguridad de todo el material de cifra y en el Responsable de Seguridad de las TIC (CISO) la responsabilidad de la seguridad de las operaciones criptográficas.

6.9.1 Funciones

Las funciones del Criptocustodio son:

- Recepcionar, proteger y controlar el material de cifra.
- Realizar el inventario del material de cifra.
- Confeccionar y mantener las listas de claves y fechas de cambio.
- Proporcionar seguridad física del material de cifra, informes y compromisos.
- Destruir el material de cifra bajo su custodia, cuando sea necesario.

7. ESTRUCTURA OPERACIONAL DEL SISTEMA EN LAS ORGANIZACIONES

7.1 Responsable del Sistema (RSIS)[13]

Aunque habitualmente se trata de un rol individual, puede haber más de un RSIS, en función de los diferentes sistemas de la organización. Es designado por el propietario del sistema.

El Responsable del Sistema (RSIS) debe ser una persona o autoridad diferente al Responsable de Seguridad de las TIC (CISO).

En determinados sistemas 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 del RSIS, cada organización podrá designar cuantos Responsables

[13] Este Rol equivale al anteriormente designado como Autoridad Operativa del Sistema de las TIC (AOSTIC).

del Sistema Delegados (RSIS-D) considere necesarios, estando coordinados por el RSIS principal.

Los RSIS-D serán responsables, en su ámbito, de todas aquellas acciones que delegue el RSIS principal relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema. Cada RSIS-D tendrá una dependencia funcional directa del RSIS principal, que es quien tiene la responsabilidad sobre la totalidad del sistema.

7.1.1 Funciones

Las funciones del Responsable del Sistema (RSIS), especialmente las más relacionadas con la seguridad, son:

- Desarrollo, operación y mantenimiento del sistema durante su ciclo de vida, de sus especificaciones, de su instalación y de la verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del sistema, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de nuevos equipos y usuarios en el sistema.
- Aprobar, coordinado con el Responsable de Seguridad de las TIC (CISO), los cambios que afecten a la seguridad del modo de operación del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Conforme a las directrices del Responsable de Seguridad de las TIC (CISO) y en coordinación con él, la implantación y control de las medidas específicas de seguridad del sistema y de que éstas se integren adecuadamente dentro del marco general de seguridad, incluyendo la determinación e implementación de las configuraciones autorizadas de hardware y software a utilizar en el sistema y sus modificaciones.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el sistema, resultado del mismo es la Declaración de Requisitos de Seguridad (DRES), también designada como Declaración de Aplicabilidad (DA), para su aprobación por el CISO.
- Elaboración de la documentación de seguridad del sistema para su aprobación por el CISO.

- Elaboración de los Procedimientos Operativos de Seguridad (POS), cuando se haya delegado su elaboración.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Velar por el cumplimiento de las obligaciones asignadas a los Administradores del Sistema (AS), si los hubiere.
- En el caso de sistemas que manejen información clasificada, informará al CISO en todas aquellas circunstancias que este determine y especialmente cuando:
  - Se desarrolle o adquiera un sistema cuyo Concepto de Operación no haya sido aprobado.
  - Se lleven a cabo modificaciones en los sistemas y/o instalaciones en las que éstos se encuentren y que conlleven una reacreditación.
  - Exista la necesidad de manejar información de mayor grado de clasificación que la autorizada para ese sistema.
- Apoyar al CISO en la investigación de los incidentes de seguridad que afecten al sistema.
- Mantener y recuperar la información almacenada por el sistema y sus servicios asociados.

7.2 Administrador del Sistema (AS)

Su función es realizar las tareas de administración en el sistema, delegadas por parte del Responsable del Sistema (RSIS), para facilitar la operativa diaria.

Puede haber varios administradores en función de su especialización y del tamaño, complejidad y localización de los sistemas[14].

7.2.1 Administrador Especialista en Seguridad (AES)[15]

Dependiendo del Responsable del Sistema (RSIS), se encarga de implementar la seguridad de acuerdo a las directrices del Responsable de Seguridad de las TIC (CISO). Es designado por el propietario del sistema a propuesta del RSIS.

[14] En el MINISDEF, estarían incluidos en este rol los actuales OPERADORES; personal externo subcontratado que realiza tareas de administración de los sistemas.
[15] Este rol equivale al anteriormente designado como Administrador de Seguridad del Sistema (ASS).

En emplazamientos donde se encuentren ubicados varios sistemas, la función del Administrador Especialista en Seguridad de cada uno de ellos podría recaer en la misma persona.

En determinados sistemas 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 administración, se podrán designar diferentes Administradores Especialistas en Seguridad.

Las funciones del Administrador Especialista en Seguridad son:

- Elaborar, cuando así lo determinen el RSIS y el CISO, la aplicación y la gestión de los Procedimientos Operativos de Seguridad (POS).
- Gestionar, configurar y actualizar, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema.
- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema.
- Informar al RSIS de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Aprobar los procedimientos locales de control de cambios en la configuración vigente del sistema.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Mantener un inventario y un diagrama actualizado de la localización de los equipos.
- Verificar que todo el hardware está perfectamente etiquetado de acuerdo con la máxima clasificación de la información que soporta.
- Asegurar que los controles para empleo de software autorizado en el sistema son cumplidos estrictamente y que no se usa software no autorizado.
- Llevar a cabo regulares comprobaciones de presencia de código malicioso en el sistema, recepcionando los informes de las medidas de protección implementadas al respecto.
- Asegurar que los procedimientos aprobados para desclasificación, borrado y destrucción de documentación y elementos susceptibles de su manejo son aplicados.
- Asegurar que la trazabilidad, evidencias de auditoría y otros registros de seguridad son frecuentemente analizados, de acuerdo con la política de

seguridad establecida por la organización, y de forma coordinada con el Centro de Operaciones de Ciberseguridad (CoCS).

- Asegurar que tienen lugar efectivos procedimientos de copia de respaldo de la información almacenada, así como la custodia de los soportes de almacenamiento resultantes con medidas de seguridad equivalentes.
- Establecer procedimientos de seguimiento y reacción ante alarmas y situaciones imprevistas.
- Iniciar el proceso de respuesta ante los incidentes que se produzcan en el sistema bajo su responsabilidad, en coordinación con el ERI y el CoCS, informando y colaborando con el Responsable de Seguridad de las TIC (CISO) en la investigación de los mismos.
- Establecer o supervisar los planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

7.2.2 Administrador Especialista en la Red (AER)

Su función es realizar tareas delegadas de administración de la red, para facilitar la operativa diaria, por parte del Responsable del Sistema (RSIS).

Las funciones del Administrador Especialista en la Red, son:

- Proporcionar servicios de soporte para la interconexión de elementos/dispositivos en la red.
- Asegurarse de que la red sea utilizada eficientemente respecto al tráfico, incorporando criterios y objetivos de calidad de servicio.
- Garantizar la seguridad de la red, apoyándose en el Centro de Operaciones de Ciberseguridad (CoCS) y en el Administrador Especialista en Seguridad.
- Configurar los elementos que constituyen la red, como son los concentradores, enrutadores, etc. atendiendo a cuestiones funcionales y de seguridad.

7.3 Usuarios del sistema (USR)

Los constituye el personal autorizado por el Responsable del Sistema (RSIS) para acceder a determinados servicios, de los que ofrece el sistema, y la información tratada a través de ellos.

Entre sus responsabilidades figuran estar informados de sus obligaciones, conocer las normas de la entidad y actuar bajo sus directrices de cara a evitar la mala praxis en el desarrollo de sus funciones.

8. ESTRUCTURA DE GOBIERNO DE LA INFORMACIÓN

Existen determinados roles que no se han contemplado en esta guía orientada a la gobernanza de la ciberseguridad en entidades que disponen de sistemas que manejan información clasificada y que deben ser tenidos en cuenta.

8.1 Propietario de la Información (o Depositario de la Información)

Partiendo de las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, concretamente la norma NS/04 sobre SEGURIDAD DE LA INFORMACIÓN, que en su apartado 1.2. Propiedad de la información, señala: "*La información tendrá un originador, bajo cuya autoridad o tutela la información es producida, dentro del ámbito de una organización internacional, estado u organismo subordinado. El originador define quién ostenta la propiedad inicial de la información clasificada*. (...) *El **propietario de la información** es el que define las reglas por las que se rige su manejo, en línea con la normativa aplicable, y define los criterios para que pueda producirse una transferencia de la propiedad, si admite esa posibilidad*. (...) *La propiedad de la información puede ser transferida. No debe confundirse con la distribución o la cesión de información, que no implica un cambio de propietario de la misma, sino únicamente de custodio*".

Asimismo, se señala en el apartado 1.5. Custodia de la información clasificada: "*La información clasificada, a lo largo de todo su ciclo de vida, siempre estará asignada a un **responsable (órgano o persona) de su custodia**, quien podrá variar, pero nunca dejar de existir. Dicho custodio manejará y cederá la información bajo su custodia conforme a la normativa establecida por el propietario de la información, o acordada con el mismo. Cuando el custodio sea también quien almacena la información, podrá recibir el nombre de **depositario***". El órgano depositario de la información, en materias clasificadas, es el Subregistro o Punto de Control de materias clasificadas que corresponda.

En consecuencia, podríamos equiparar el **Responsable de la Información del ENS** con el **Propietario de la Información Clasificada** o, desde el punto de vista de una organización concreta a la que ha sido confiada su custodia y almacenamiento, podría equiparase también al **depositario**.

8.2 Responsable del Servicio

En sistemas que manejan información clasificada, se puede afirmar que la responsabilidad última y las medidas de seguridad asociadas vienen determinadas por el grado de la información manejada y custodiada. Luego los servicios que la tratan,

soportados por determinados sistemas, atenderán a las reglas establecidas por los **Propietarios de la Información** que éstos manejan, en determinados casos delegada en el **depositario**.

Por tanto, no siempre cabe hablar en este entorno de Responsable del Servicio en el sentido que establece el Esquema Nacional de Seguridad. Incluso para el ENS, ambos roles (Responsable de la Información y Responsable del Servicio) pueden converger en la misma persona física o entidad.

En consecuencia, se considera que para los sistemas que manejan o custodian información clasificada, únicamente se considerará al **propietario de la información** o, en su caso, al **depositario** de la misma.

9. ANEXOS

9.1 Transición en la designación de roles para sistemas que manejan información clasificada

Para facilitar la transición a la nueva organización, seguidamente se incluye una tabla que relaciona la designación correspondiente al nuevo modelo con la anterior, marcándose en color amarillo los roles que varían significativamente.

Asimismo, en cada uno de los roles y comités que se designan de modo distinto, se ha añadido a lo largo del texto de esta guía una referencia a la designación anterior.

DESIGNACIÓN ACTUAL		DESIGNACIÓN ANTERIOR	
ESTRUCTURA DE ACREDITACIÓN E INSPECCIÓN DE LA SEGURIDAD			
Propietario de la Información	-----	Propietario de la Información	-----
Responsable de su custodia / Depositario	-----	Responsable de su custodia / Depositario	-----
Autoridad de Acreditación	AA	Autoridad de Acreditación	AA
Autoridad de Certificación Criptológica	ACC	Autoridad de Certificación Criptológica	ACC
Entidad de Acreditación	EA	Entidad de Acreditación	EA
Entidad de Certificación	EC	Entidad de Certificación	EC
ESTRUCTURA DE SEGURIDAD EN LAS ORGANIZACIONES			
Comité de Seguridad TIC	CSEGTIC	Autoridad de Acreditación Delegada	AA-D
Responsable de Seguridad de las TIC	CISO	Autoridad de Seguridad de las TIC Supervisor de Seguridad de las TIC	ASTIC SSTIC
Centro de Operaciones de Ciberseguridad	CoCS	Centro de Operaciones de Ciberseguridad	CoCS
Equipo Respuesta a Incidentes de Seguridad	ERI	Equipo Respuesta a Incidentes de Seguridad	ERI

Responsable de Seguridad Física	RSF	Responsable de Seguridad del Área	RSA
Autoridad de Control de Material de Cifra	ACMC	Autoridad de Control de Material de Cifra	ACMC
Órganos de Distribución de Material de Cifra	ODMC	Órganos de Distribución de Material de Cifra	ODMC
Criptocustodio	CC	Criptocustodio	CC
ESTRUCTURA OPERACIONAL DEL SISTEMA EN LAS ORGANIZACIONES			
Responsable del Sistema	RSIS	Autoridad Operativa del Sistema de las TIC	AOSTIC
Responsable del Sistema Delegado	RSIS-D	Autoridad Operativa del Sistema de las TIC Delegada	AOSTIC-D
Administrador del Sistema Administrador Especialista en Seguridad Administrador Especialista en Red	AS AES AER	Administrador del Sistema Administrador de Seguridad del Sistema Administrador de Red	AS ASS -----
Usuarios del sistema	USR	Usuarios del sistema	USR

9.2 Equivalencia designación de roles UE[16]

En el siguiente cuadro se establecen las equivalencias entre la estructura STIC de la Unión Europea y la propuesta en esta guía.

ESTRUCTURA UE	EQUIVALENCIA
Autoridad de Acreditación de Seguridad (AAS)	AA AA-D
Autoridad de Seguridad de la Información (ASI/IAA[17])	CISO
Autoridad Operacional de Garantía de la Información (AOGI)	RSIS
Agente de Seguridad de la Información	CISO/AES

9.3 Equivalencia designación de roles OTAN[18]

En el siguiente cuadro se establecen las equivalencias entre la estructura STIC de la OTAN y la propuesta en esta guía. Las equivalencias no son exactas, pudiendo existir duplicidades en algunas de las funciones.

ESTRUCTURA OTAN	EQUIVALENCIA
Security Acreditation Authority	AA
Major NATO Commands	CSEG
NATO Military and Civil Agencies	

[16] 20013/468/EU Decisión del Consejo sobre las normas de seguridad para la protección de la información clasificada de la UE.
[17] Acrónimo Information Assurance Authority
[18] C-M(2002)49 Security within NATO y AD 70-1 ACE Security Directive

National Security Authorities	
• Security Acreditation Authority (SAA)	
• Local SAA	
INFOSEC Authority	CISO
CIS Operating Authority of System/LAN	
CIS INFOSEC Planning & Implementation Authority	
ADP Authority	
CIS Operational Authority of System/LAN	RSIS
ADP System Operational Authority	
System Administrator of System/LAN	AS/USR* *El AS puede delegar en los usuarios estas tareas
CIS INFOSEC Officer	CISO
CIS System Security Officer	AES
ADP Site Security Officer	AES/AER
ADP System Security Officer	
ADP Network Security Officer	*En sistemas pequeños los puede desempeñar la misma autoridad
COMSEC Officer	CC
HQ Security Officer	RSF
Terminal Area Security Officer (TASO)	AS/AS-Delegados