NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-201)

ORGANIZACIÓN Y GESTIÓN PARA LA SEGURIDAD DE LAS TIC

ENERO 2009

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.06.26 10:48:38 +02'00'

© Editor y Centro Criptológico Nacional, 2009
NIPO: 076-09-055-7

Tirada: 1000 ejemplares
Fecha de Edición: Enero de 2009

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

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, 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 en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

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 su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Enero de 2009

Alberto Sáiz
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

FIGURAS

1. INTRODUCCIÓN

1. El mantenimiento y gestión de la seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (TIC), en adelante Sistemas, va íntimamente ligada al establecimiento de una Organización de Seguridad.
2. Dicha Organización se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los Sistemas y la implantación de una estructura que las soporte.
3. La Política de Seguridad debe establecer las funciones y responsabilidades, en materia STIC, del personal que constituye las diferentes estructuras de la Organización.

2. OBJETO

4. El objeto de esta norma es crear un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad de los Sistemas, así como proponer unas figuras o roles de seguridad que las implementen, todo ello de acuerdo con la Política de Seguridad de las TIC en la Administración.
5. Es responsabilidad de cada Organismo establecer su propia Organización de Seguridad de acuerdo con sus necesidades y limitaciones.

3. ALCANCE

6. La estructura propuesta en este documento sirve como guía, pudiendo ser la implantación final diferente en cada Organización. No obstante, las funciones y misiones definidas en esta norma deben ser cubiertas sea cual fuere la solución final adoptada.
7. La Autoridad de Acreditación del Sistema (AA) y en su defecto la Autoridad Delegada de Acreditación (ADA) es responsable de la aprobación de cualquier estructura de seguridad que sustente al Sistema y que permita el cumplimiento de los requisitos de seguridad necesarios para manejar la información que soporta.

4. ORGANIZACIÓN DE SEGURIDAD

8. La Organización de la Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) está constituida por las Autoridades responsables del establecimiento y aplicación de los procedimientos y normas STIC en el Sistema.
9. Dentro de cada Organización STIC se establecen tres tipos de estructuras:
   - Estructura de Seguridad de las TIC de la Organización: responsable de establecer y aprobar los requisitos de seguridad para el Sistema además de verificar y supervisar la correcta implementación y mantenimiento de los mismos.
   - Estructura de Control de Material de Cifra: íntimamente ligada a la anterior, que tendrá cabida en todo Sistema que haga uso de material de cifra.
   - Estructura Operacional del Sistema: responsable de la implementación y mantenimiento de los requisitos de seguridad aprobados para el Sistema por la Autoridad de Acreditación.

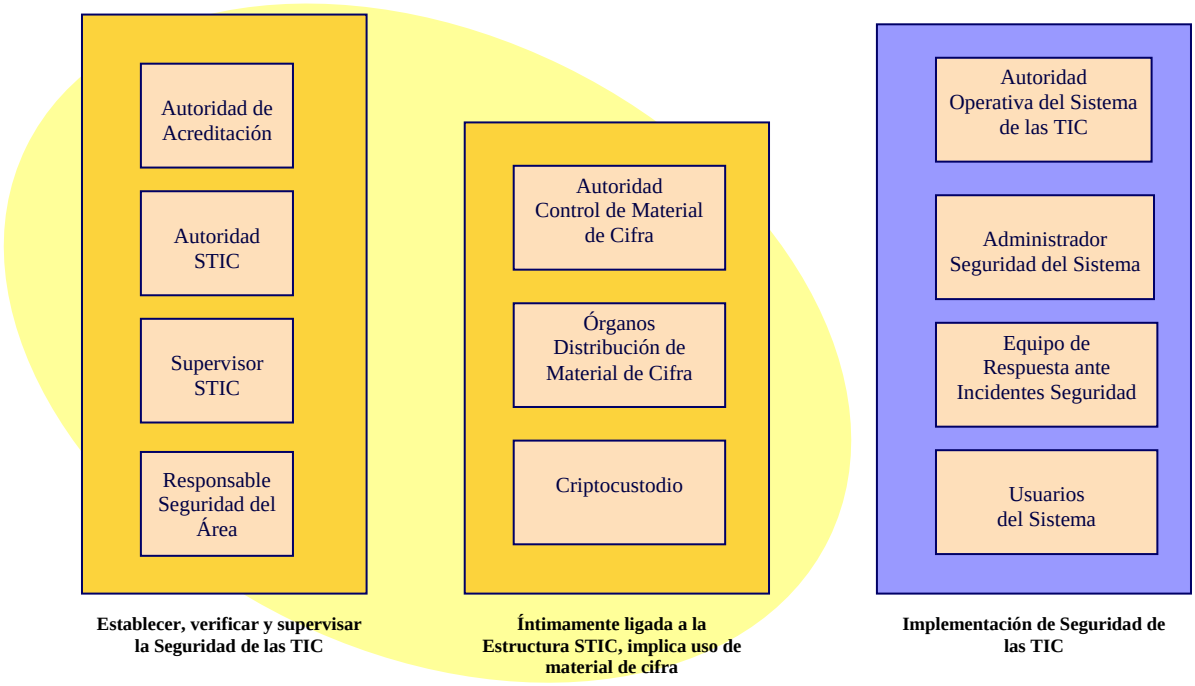

Figura 1.- Estructuras definidas para una Organización de Seguridad

5. ESTRUCTURA STIC DE LA ORGANIZACIÓN

10. Como norma general se encontrarán definidas las figuras que se citan en los siguientes apartados. Hay que tener en cuenta que estas figuras serán un modelo de referencia que servirá de orientación en el desarrollo de la estructura de seguridad de cualquier Organización, donde las necesidades de personal y recursos disponibles son determinantes.

5.1. AUTORIDAD DE ACREDITACIÓN (AA)

11. Autoridad responsable de conceder la autorización a un Sistema para manejar información hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación. Entre sus funciones se señalan:

    a. Establecer y aplicar la Política STIC en la Administración.
    b. Realizar los procesos de acreditación que le correspondan.
    c. Verificar el cumplimiento de los procesos de acreditación para Sistemas que manejan información clasificada realizados por las ADA,s.
    d. Elaborar y/o aprobar los Procedimientos, Normas, Instrucciones Técnicas y Guías que emanen de la Política STIC de aplicación a toda la Administración.

12. La Autoridad de Acreditación (AA), en su ámbito de competencia, podrá nombrar una Autoridad Delegada de Acreditación (ADA) responsable de la seguridad de los Sistemas de su Organización, y por tanto, de la acreditación de aquellos que manejen información clasificada.

13. Como funciones que la ADA puede desempeñar se indican las siguientes:
    a. Mantener la seguridad de la información manejada en los Sistemas de su ámbito de responsabilidad.
    b. Garantizar la realización de inspecciones periódicas que permitan la verificación del cumplimiento de lo expresado en la Política STIC.
    c. Definir y actualizar el organigrama de la estructura STIC correspondiente a su ámbito.
    d. Acreditación, o renovación de la acreditación, de los Sistemas.
    e. Solicitar la certificación de productos y en su caso promover su adquisición.
14. Las autoridades responsables de la acreditación, en apoyo a sus funciones, pueden nombrar cuantas Autoridades de Seguridad de las TIC (ASTIC) consideren necesarias, constituyendo la estructura STIC de la Organización:
    - Autoridad STIC.
    - Supervisor STIC.
    - Responsable de Seguridad del Área.

5.2. AUTORIDAD DE SEGURIDAD DE LAS TIC (ASTIC)

15. La ASTIC es responsable de aquellas funciones que le delegue la ADA, entre las que se pueden encontrar:
    a. Velar por el cumplimiento de la normativa STIC vigente dentro de la Organización inspeccionando, verificando o analizando la seguridad de las TIC de los Sistemas que la integran.
    b. Aprobar el Concepto de Operación (CO) de cada Sistema en sus aspectos STIC.
    c. Solicitar la acreditación de cada Sistema que maneje información clasificada, y en su caso su renovación.
    d. Promover la formación y concienciación STIC que se considere necesaria dentro de su ámbito.
    e. Elaborar y aprobar las guías de seguridad de los Sistemas en su ámbito de actuación.
16. La ASTIC podrá nombrar cuantos Supervisores de Seguridad de las TIC (SSTIC) considere necesarios en apoyo de sus funciones.

5.3. SUPERVISOR DE SEGURIDAD DE LAS TIC (SSTIC)

17. El SSTIC será responsable de la supervisión de la ejecución de las medidas y procedimientos de seguridad de todos los Sistemas a su cargo, especialmente en aspectos técnicos y de implementación.
    a. Verificar que las medidas de seguridad establecidas en la Declaración de Requisitos de Seguridad (DRS) sean adecuadas para la protección de la información que se va a manejar en el Sistema y que además se satisfacen los requisitos de protección establecidos por la normativa vigente.
    b. Analizar, completar y aprobar toda la documentación relacionada con la seguridad del Sistema (DRS y POS), análisis de riesgos y seguridad criptológica.

c. Verificar y comprobar la implementación de los Procedimientos Operativos de Seguridad (POS) y de las funciones de seguridad de los Sistemas bajo su responsabilidad mediante la realización de inspecciones de seguridad periódicas.

d. Monitorizar el estado de seguridad del Sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el Sistema.

e. Apoyar en la investigación de posibles incidentes de seguridad.

18. La persona designada como SSTIC figurará como tal en la documentación de seguridad (DRS y POS) de los Sistemas que tenga bajo su responsabilidad.

19. En aquellos casos en que existan varios Sistemas que por su complejidad, diversidad, distribución, etc… requieran de una mayor dedicación, se podrán nombrar Supervisores de Seguridad de las TIC Delegados (SSTIC-D) con las mismas atribuciones que el SSTIC pero sólo en el ámbito de los Sistemas para los que están designados.

20. Los supervisores delegados (SSTIC-D) tendrán una dependencia funcional del SSTIC, el cuál ejercerá la coordinación de los mismos.

5.4. RESPONSABLE DE SEGURIDAD DEL ÁREA (RSA)

21. En cada emplazamiento o área física de la Organización donde se encuentren Sistemas que manejen información clasificada CONFIDENCIAL o superior, se podrá designar un Responsable de Seguridad del Área (RSA).

22. Sus funciones serán:

a. Supervisión del control de acceso físico al área. Incluye el mantenimiento actualizado de la lista de usuarios autorizados a acceder a dicha área, así como llevar a cabo regulares comprobaciones del estado de seguridad.

b. Supervisión de todas las acciones que se lleven a cabo sobre el hardware (HW) y software (SW) de los sistemas del área (instalación, modificación, retirada, etc.).

c. Comprobará que las acciones desarrolladas en el área están autorizadas y que, durante el desarrollo de las mismas, la seguridad del Sistema no se ha visto comprometida.

6. ESTRUCTURA DE CONTROL DE MATERIAL DE CIFRA

23. En aquellas Organizaciones que se emplee material de cifra para la protección de la información clasificada, deberá crearse una estructura para el control de todo el material de cifra utilizado.

24. La Autoridad STIC establecerá las distintas figuras (autoridades) que constituyen la estructura de control de material de cifra de la Organización dentro de su ámbito de competencia:

- Autoridad de Control de Material de Cifra (ACMC).
- Órganos de Distribución de Material de Cifra (ODMC).
- Criptocustodio.

6.1. AUTORIDAD DE CERTIFICACIÓN CRIPTOLÓGICA (ACC)

25. La Autoridad de Certificación Criptológica (ACC) es el Secretario de Estado Director del Centro Criptológico Nacional.

26. La ACC es responsable:

    a. Selección de los criptosistemas adecuados.
    b. Dar normas para el correcto empleo de los criptosistemas.
    c. Establecer los procedimientos de control del material de cifra y de las claves utilizadas.
    d. Formar al personal especialista.

6.2. AUTORIDAD DE CONTROL DE MATERIAL DE CIFRA (ACMC)

27. La ACMC es responsable del registro, contabilidad y seguimiento de todo el material de cifra utilizado para la protección de la información clasificada en la Organización, estableciendo los procedimientos adecuados.

28. Esta Autoridad definirá y actualizará la estructura criptológica de su Organización donde figurarán los Criptocustodios y los Criptocustodios Alternativos.

6.3. ÓRGANOS DE DISTRIBUCIÓN DE MATERIAL DE CIFRA (ODMC)

29. Los ODMC son Órganos dependientes de la ADA y ASTIC correspondiente.

30. Las responsabilidades son las siguientes dentro de los Sistemas de su competencia o bajo su responsabilidad:

    a. Gestión, distribución, transporte y control del material de cifra.
    b. Establecimiento de períodos de vigencia de las claves.
    c. Generación y confección de claves mediante procedimientos aprobados por la ACC.
    d. Gestión de claves según la normativa vigente.
    e. Control de procesos de introducción, utilización y destrucción del material de cifra.

6.4. CRIPTOCUSTODIO

31. El Criptocustodio será responsable de la recepción, protección, control y, cuando sea necesario, destrucción de todo el material de cifra bajo su custodia.

32. A eso hay que añadir:

    a. Confección y mantenimiento de las listas de claves y fechas de cambio.
    b. Inventario del material de cifra.
    c. Seguridad física del material de cifra e informes relacionados.

33. Normalmente, en el Criptocustodio se delega la responsabilidad de la seguridad de todo el material de cifra y en el Supervisor STIC la responsabilidad de la seguridad de las operaciones criptográficas.

7. ESTRUCTURA OPERACIONAL DEL SISTEMA

7.1. AUTORIDAD OPERATIVA DEL SISTEMA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES (AOSTIC)

34. Autoridad designada por el propietario del Sistema y podrá variar de una persona a otra conforme al ciclo de vida del Sistema.

35. Sus responsabilidades son:

    a. Desarrollo, operación y mantenimiento del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
    b. Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
    c. Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
    d. Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
    e. Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
    f. 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.
    g. Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
    h. Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
    i. Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema, obteniendo como resultado del mismo la Declaración de Requisitos de Seguridad (DRS).
    j. Elaboración de la documentación de seguridad del Sistema.
    k. Aprobación de los Procedimientos Operativos de Seguridad (POS), cuando se haya delegado su elaboración.
    l. Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
    m. Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).
    n. Para Sistemas que manejen información clasificada, informar a las Autoridades responsables de la Seguridad de las TIC, solicitando su intervención en todas aquellas circunstancias que éstas determinen 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.
    o. Investigación de los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación a la ADA o a quién ésta determine.

36. 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 AOSTIC, cada Organización podrá designar cuantas Autoridades Operativas del Sistema Delegadas (AOSTIC-D) considere necesarias.
37. Las AOSTIC-D serán responsables, en su ámbito, de todas aquellas acciones que delegue la AOSTIC relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema.
38. Cada AOSTIC-D tendrá una dependencia funcional directa de la AOSTIC, que es la que tiene la responsabilidad sobre la totalidad del Sistema.
39. La documentación de seguridad del Sistema (DRS y POS) recogerá su identidad en el anexo habilitado a tal efecto.

7.2. ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)

40. El ASS será designado por el propietario del Sistema a propuesta de la AOSTIC, pudiendo variar de una persona a otra conforme al ciclo de vida del Sistema.
41. Su nombramiento figurará en la documentación de seguridad del Sistema (DRS y POS).
42. Entre sus responsabilidades se pueden reseñar:
    a. La elaboración, cuando así lo determine la AOSTIC, aplicación y gestión de los Procedimientos Operativos de Seguridad (POS).
    b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema
    c. Implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema.
    d. Informar al SSTIC y la AOSTIC de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
    e. Aprobar los procedimientos locales de control de cambios en la configuración vigente del Sistema
    f. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida
    g. Mantener un diagrama actualizado de la localización de los equipos.
    h. Verificar que todo el hardware está perfectamente etiquetado de acuerdo con la máxima clasificación de la información que soporta.
    i. Asegurar que los controles para empleo de software autorizado en el Sistema son cumplidos estrictamente y que no se usa software no autorizado.
    j. Llevar a cabo regulares comprobaciones de presencia de software malicioso (virus) en el Sistema.
    k. Asegurar que son aplicados los procedimientos aprobados para desclasificación, borrado y destrucción de documentación y elementos susceptibles de su manejo.
    l. Asegurar que la trazabilidad, auditoría y otros registros de seguridad se llevan a cabo frecuentemente, de acuerdo con la política de seguridad establecida por la Organización.

m. Asegurar que tienen lugar efectivos procedimientos de copia de respaldo de la información almacenada, así como la custodia de los soportes de almacenamiento empleados.

n. Establecer procedimientos de seguimiento y reacción ante alarmas y situaciones imprevistas.

o. Iniciar el proceso de respuesta ante incidentes que se produzcan en el Sistema bajo su responsabilidad, informando y colaborando con el SSTIC en la investigación de los mismos.

P. Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

43. En emplazamientos donde se encuentren ubicados varios Sistemas, la función de ASS de cada uno de ellos podría recaer en la misma persona.

44. 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 ASS, se podrán designar Administradores de Seguridad del Sistema Delegados (ASS-D).

45. 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.

46. El ASS-D será designado a solicitud del ASS, del que dependerá funcionalmente. Su identidad aparecerá reflejada en la documentación de seguridad del Sistema (DRS y POS).

7.3. EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD (ERIS)

47. El Equipo de Respuesta ante Incidentes de Seguridad (ERIS) es un conjunto de medios humanos y materiales encargado de gestionar los incidentes de seguridad, bajo la dependencia técnica y funcional de la AOSTIC.

48. El ERIS está compuesto por un equipo con capacidades de atención inmediata y por un grupo de especialistas para aquellos otros incidentes no resueltos en primera instancia.

49. Entre sus cometidos se indican los siguientes:

a. Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.

b. Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.

c. Tomar decisiones a corto plazo si se ha originado un comprometimiento de la información que pudiera tener consecuencias graves.

d. Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos.

e. Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.

f. Determinar el modo, los medios, los motivos y el origen del incidente.

g. Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.

7.4. USUARIOS DEL SISTEMA

50. En cada Sistema, además tendrán cabida las siguientes figuras:

- **Administrador del Sistema:** tiene por misión realizar las tareas de administración del Sistema, coordinando a los operadores del Sistema.
- **Administrador de Red:** encargado de las tareas de administración de red, siendo responsable de aspectos de seguridad relativos a la infraestructura de red (enrutadores/switches, dispositivos de protección de perímetro, redes privadas virtuales, detección de intrusos, dispositivos trampa, etc…).
- **Operador de Sistema:** responsables de la operación diaria de los servicios del Sistema. Son los primeros receptores de las incidencias que se produzcan, notificadas por los usuarios.

  Resolverán los incidentes que por procedimiento les competan y elevarán al Administrador STIC correspondiente las que les excedan, siempre ajustándose a procedimiento.
- **Usuarios del Sistema:** constituyen el personal autorizado por la AOSTIC para acceder al Sistema utilizando las posibilidades que les ofrece el mismo. Deberán haber leído los Procedimientos Operativos de Seguridad (POS) o un extracto del mismo redactado al efecto por el SSTIC.

51. Los usuarios aparecerán relacionados como Anexo a los POS. Para cada uno figurará como mínimo la siguiente información:
    - Autorización de seguridad.
    - Tipo de usuario.
    - Servicios a los que tiene derecho.
    - Ubicación y teléfono de contacto.
52. Los usuarios juegan un papel fundamental en el mantenimiento de la seguridad del Sistema, por lo tanto, es fundamental su concienciación en la seguridad de las TIC ya que en la mayoría de los casos constituyen voluntariamente o involuntariamente la principal amenaza para el propio Sistema.
53. Los usuarios deben estar debidamente informados de sus obligaciones y responsabilidades, así como haber sido instruidos para la labor que desempeñan.
54. Los usuarios del Sistema son responsables entre otras cosas de:
    a. Conocer los procedimientos que les competen.
    b. Asegurarse de que están preparados adecuadamente para llevar a cabo operaciones en el Sistema, en particular las correspondientes a la gestión de mecanismos de identificación y al procedimiento de gestión de incidentes.
    c. Asegurarse de leer, comprender y seguir los Procedimientos Operativos de Seguridad (POS) relativos a su Sistema.
    d. Informar de cualquier incidente de seguridad o acontecimiento inusual que sea observado durante la operación de su Sistema, tal y como se indica en los POS.

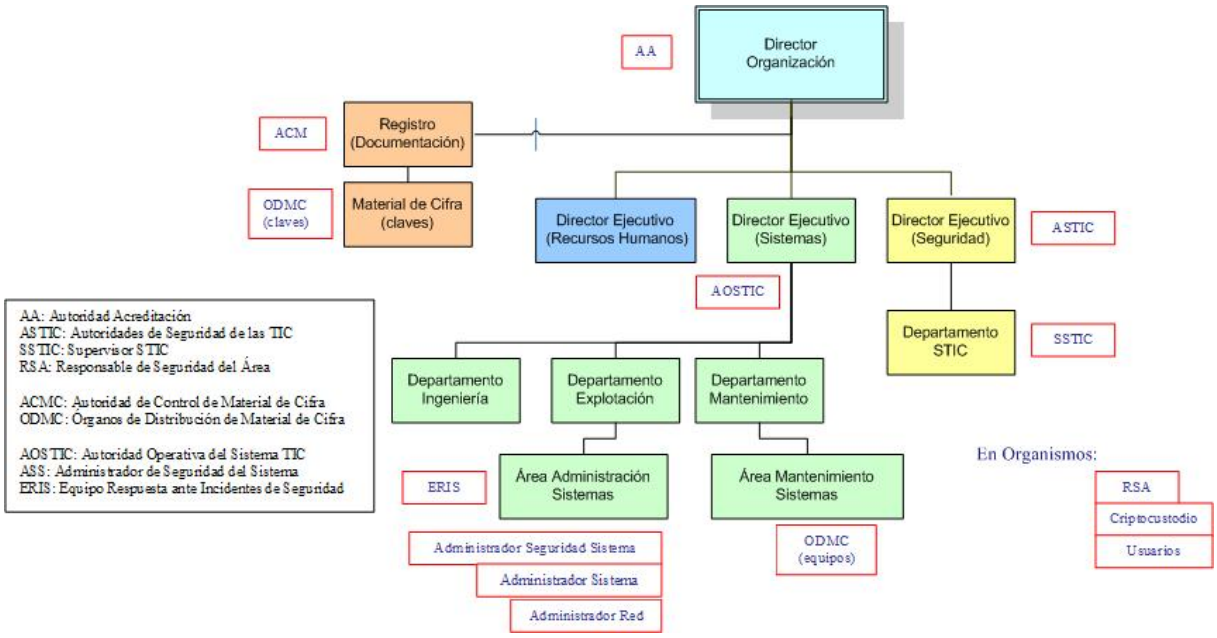

Figura 2.- Modelo de Organización de Seguridad

8. CONCLUSIONES

55. Esta guía sirve de referencia para la implantación de la estructura de seguridad de las TIC en una Organización facilitando de esta manera la gestión de su seguridad. Se considera que las figuras de ADA y AOSTIC son las mínimas necesarias, siendo la Autoridad de acreditación la que establezca de forma clara el resto de las figuras según las limitaciones y particularidades de la Organización.

56. Se considera que cualquier estructura de seguridad que permita el cumplimiento de los requisitos de seguridad y acreditación de un Sistema es válida si es aprobada por la Autoridad responsable de la acreditación.

ANEXO A. EQUIVALENCIAS ENTRE ESTRUCTURAS STIC

1 MINISTERIO DE DEFENSA

En el siguiente cuadro se establecen las equivalencias entre la estructura STIC del Ministerio de Defensa [Ref.- 1] y la propuesta en esta guía:

MINISTERIO DE DEFENSA	EQUIVALENCIA
AUTORIDAD DELEGADA DE ACREDITACIÓN (ADA)	ADA
AUTORIDAD INFOSEC (AI)	ASTIC
AUTORIDAD OPERACIONAL DEL SISTEMA (AOS)	AOSTIC
ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)	ASS
OFICIAL INFOSEC (OI)	SSTIC

Tabla 1. Equivalencias entre la estructura STIC del Ministerio de Defensa y la propuesta

2 UNIÓN EUROPEA

En el siguiente cuadro se establecen las equivalencias entre la estructura STIC de la UE [Ref.- 11] y la propuesta en esta guía:

UNIÓN EUROPEA	EQUIVALENCIA
AUTORIDAD DE ACREDITACIÓN EN MATERIA DE SEGURIDAD (AAS)	AA ADA
AUTORIDAD INFOSEC	ASTIC
AUTORIDAD OPERATIVA DEL SISTEMA DE TECNOLOGÍA DE LA INFORMACIÓN (AOSTI)	AOSTIC
AGENTE DE SEGURIDAD INFOSEC	SSTIC ASS

Tabla 2. Equivalencias entre la estructura STIC de la UE y la propuesta

3 OTAN

En el siguiente cuadro se establecen las equivalencias entre la estructura STIC de la OTAN [Ref.- 12 y Ref.- 13] y la propuesta en esta guía. Las equivalencias no son exactas pudiendo existir duplicidades en algunas funciones.

ESTRUCTURA OTAN	EQUIVALENCIA
SECURITY ACREDITATION AUTHORITY Major NATO Commands NATO Military and Civil Agencies **National Security Authorities** • Security Accreditation Authority (SAA) • Local SAA	AA ADA
INFOSEC AUTHORITY **CIS Operating Authority of the System/LAN** **CIS INFOSEC Planning & Implementation Authority** ***ADP Authority***	ASTIC
CIS Operational Authority of the System/LAN ***ADP System Operational Authority***	AOSTIC
System Administrator of the System/LAN	Usuarios del Sistema/Administrador del Sistema
CIS INFOSEC Officer **CIS System Security Officer** ***ADP Site Security Officer*** ***ADP System Security Officer*** ***ADP Network Security Officer***	SSTIC ASS En sistemas pequeños los puede desempeñar la misma autoridad.
COMSEC Officer	Criptocustodio
HQ Security Officer	RSA
Terminal Area Security Officer (TASO)	ASS-D

Tabla 3. Equivalencias entre la estructura STIC de OTAN y la propuesta

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Acreditación	Autorización otorgada por la Autoridad responsable de la acreditación, para manejar información nacional clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo al concepto de operación.
Amenaza	Evento que puede desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Análisis o valoración de Riesgos	Proceso sistemático para estimar la magnitud del riesgo sobre un Sistema.
Autoridad de Acreditación	Autoridad responsable de la definición y la aplicación de la Política STIC
Autoridad de Certificación Criptológica	Autoridad responsable de la evaluación y certificación de productos y Sistemas (de tecnologías de la información y telecomunicaciones) que incorporen mecanismos criptológicos.
Autoridad Delegada de la Acreditación	Autoridad responsable en su ámbito, de la aplicación de la Política STIC y de las competencias que delegue la AA.
Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones	Autoridad designada por el propietario del Sistema, responsable del desarrollo, la operación y mantenimiento del Sistema durante su ciclo de vida; de sus especificaciones, de su instalación y de la verificación de su correcto funcionamiento.
Concepto de Operación	Declaración expresa que realiza la AOSTIC sobre el objeto o función del Sistema, el tipo de información que va a ser manejada, las condiciones de explotación (perfil de seguridad de los usuarios, clasificación de la información, modo de operación, etc.), y las amenazas a las que estará sometido.
Confidencialidad	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
Declaración de Requisitos de Seguridad	Es el documento base para la acreditación. Consiste en la exposición completa y detallada de los principios de seguridad que deben observarse y de los requisitos de seguridad que se han de implantar conforme al correspondiente análisis de riesgos realizado previamente.
Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
Evaluación de la Seguridad	Proceso de comprobación de que un producto o Sistema satisface las características de seguridad que proclama tener. Dicho proceso consiste en el examen detallado con el fin de encontrar una posible vulnerabilidad y confirmar el nivel de seguridad establecido. El examen se realiza de acuerdo a un procedimiento o metodología determinado y siguiendo unos criterios de evaluación perfectamente definidos y establecidos.
Gestión del Riesgo	Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.
Integridad	Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
Manejar Información	Presentar, elaborar, almacenar, procesar, transportar o destruir información.

Procedimientos Operativos de Seguridad	Descripción precisa de la aplicación de los requisitos de seguridad, detallando las responsabilidades y todas las acciones y procedimientos de seguridad a seguir, con el objetivo de garantizar y mantener la seguridad del Sistema. En su caso será la descripción de la aplicación de la DRS correspondiente.
Riesgo	Estimación del grado de exposición de un Sistema frente a amenazas que pudieran causar daños o perjuicios a la Organización.
Salvaguardas (contramedidas)	Procedimiento o mecanismo tecnológico que reduce el riesgo.
Seguridad de las Tecnologías de la Información y las Comunicaciones	La capacidad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (Sistema) para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, integridad y/o confidencialidad de los datos almacenados o transmitidos y de los servicios que dichos Sistemas ofrecen o hacen accesibles.
Sistema de las Tecnologías de la Información y las Comunicaciones	Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información que está bajo responsabilidad de una única autoridad.

AA	Autoridad de Acreditación
ACC	Autoridad de Certificación Criptológica
ACMC	Autoridad de Control de Material de Cifra
ADA	Autoridad Delegada de Acreditación
AOSTIC	Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones
ASS	Administrador de Seguridad del Sistema
ASTIC	Autoridad de Seguridad de las de las Tecnologías de la Información y las Comunicaciones
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
CO	Concepto de Operación
DRS	Declaración de Requisitos de Seguridad
DRSI	Declaración de Requisitos de Seguridad de la Interconexión
ERIS	Equipo de Respuesta ante Incidentes de Seguridad
O.M.	Orden Ministerial
ODBC	Órgano de Distribución de Material de Cifra
OTAN	Organización del Tratado del Atlántico Norte
POS	Procedimientos Operativos de Seguridad
RSA	Responsable de Seguridad del Área
Sistema	Sistema de las Tecnologías de la Información y las Comunicaciones
SSTIC	Supervisor de Seguridad de las de las Tecnologías de la Información y las Comunicaciones
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones.
TIC	Tecnologías de la Información y las Comunicaciones
UE	Unión Europea.

ANEXO C. REFERENCIAS

[Ref.- 1] Orden Ministerial 76/2002, de 18 de abril, por la que se establece la "Política de Seguridad para la Protección de la Información del Ministerio de Defensa almacenada, procesada o transmitida por Sistemas de información y telecomunicaciones.
[Ref.- 2] Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
[Ref.- 3] Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).
[Ref.- 4] CCN-STIC-001. Seguridad de los Sistemas de las TIC que manejan información nacional clasificada en la Administración.
[Ref.- 5] CCN-STIC-002. Coordinación Criptológica.
[Ref.- 6] CCN-STIC-003. Uso de cifradores certificados para la protección de información nacional clasificada en la Administración.
[Ref.- 7] CCN-STIC-003. Uso de cifradores certificados para la protección de información nacional clasificada en la Administración.
[Ref.- 8] CCN-STIC-202. Estructura y contenido de la Declaración de Requisitos de Seguridad (DRS).
[Ref.- 9] CCN-STIC-203. Estructura y contenido de los Procedimientos Operativos de Seguridad (POS).
[Ref.- 10] UNE 71501-2 IN. Tecnología de la Información (TI). Guía para la Gestión de la Seguridad de TI. Parte 2: Gestión y planificación de la seguridad TI. AENOR. Noviembre 2001.
[Ref.- 11] 2001/264/CE. Decisión del Consejo de 19 de marzo de 2001 por la que se adoptan las normas de seguridad del Consejo.
[Ref.- 12] C-M(2002)49. Security whitin NATO.
[Ref.- 13] AD 70-1 ACE Security Directive.