GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN
CENTRO CRIPTOLÓGICO NACIONAL

PROCEDIMIENTO DE SEGURIDAD DE LAS TIC
CCN-STIC 101

ACREDITACIÓN DE SISTEMAS DE LAS TIC QUE MANEJAN INFORMACIÓN CLASIFICADA

Diciembre 2016

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

NIPO: 002-16-020-7
Fecha de Edición: diciembre de 2016

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.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado 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 de 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 y 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.

Diciembre de 2016

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 5
2. OBJETO 5
3. ALCANCE 5
4. RESPONSABILIDADES 6
5. CONDICIONES PARA UNA ACREDITACIÓN 6
5.1 DOCUMENTACIÓN DE SEGURIDAD 6
5.2 SEGURIDAD DEL ENTORNO DE OPERACIÓN 7
5.2.1 SEGURIDAD LIGADA AL PERSONAL 7
5.2.2 SEGURIDAD FÍSICA 8
5.2.3 SEGURIDAD DE LOS DOCUMENTOS 8
5.3 SEGURIDAD DE LAS EMANACIONES 8
5.4 SEGURIDAD CRIPTOLÓGICA 8
5.5 SEGURIDAD DE LAS TIC 9
5.6 EVALUACIÓN DE SEGURIDAD DE LAS TIC 9
6. PROCESO DE ACREDITACIÓN 10
7. ACREDITACIÓN DE LAS INTERCONEXIONES 11
7.1 DOCUMENTACIÓN DE SEGURIDAD DE LA INTERCONEXIÓN 12
8. SITUACIONES POSIBLES DE LA ACREDITACIÓN 12
9. VALIDEZ DE LA ACREDITACIÓN 14
10. PERÍODO ENTRE EVALUACIONES DE SEGURIDAD DE LAS TIC 14
11. REACREDITACIÓN 14
12. INFORMES A REMITIR ENTRE ACREDITACIONES 15
13. REGISTRO DE SISTEMAS ACREDITADOS 15
ANEXO A: PROCESO DE ACREDITACIÓN 16
ANEXO B: AUDITORÍAS/INSPECCIONES DE SEGURIDAD DE LAS TIC 18
ANEXO C: DOCUMENTO DE CONFORMIDAD 19
ANEXO D: COMUNICACIÓN DE SITUACIÓN DE ACREDITACIÓN STIC 20
ANEXO E: GLOSARIO DE TÉRMINOS Y ABREVIATURAS 21

1. INTRODUCCIÓN

1. La información clasificada manejada en un Sistema debe protegerse contra la pérdida de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, sea accidental o intencionada, y debe impedirse la pérdida de integridad y disponibilidad de los propios sistemas que sustentan dicha información.
2. Al objeto de conseguir la protección de seguridad adecuada se deberán aplicar un conjunto equilibrado de medidas de seguridad de distinta naturaleza que permitan la creación de un entorno seguro en el que opere el Sistema.
3. Como desarrollo de la Ley 11/2002 de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI) y del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN), se establece una Política de Seguridad de las TIC (CCN-STIC-001) donde se recoge la necesidad de la Acreditación de los sistemas que manejan información clasificada.
4. 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 integridad o disponibilidad, con arreglo a su Concepto de Operación (CO).

2. OBJETO

5. Definir el procedimiento de acreditación de los sistemas que manejen información clasificada, según lo establecido en la Política de Seguridad de las TIC.
6. A los sistemas de la Administración que manejen información sin clasificar les será de aplicación lo establecido en el Esquema Nacional de Seguridad (ENS), según establecen la Ley 39/2015, de 1 octubre, de Procedimiento Administrativo Común a las Administraciones Públicas y la Ley 40/2015, de 1 octubre, de Régimen Jurídico del Sector Público.

3. ALCANCE

7. Este Procedimiento establece un marco común para la ejecución de los procesos de acreditación de los sistemas que manejen información clasificada, y por tanto es de obligado cumplimiento para todos los sistemas que manejen información clasificada en la Administración.
8. Las Autoridades responsables de la acreditación podrán determinar su aplicación a sistemas que manejen otro tipo de información, dentro de su ámbito de competencia.

4. RESPONSABILIDADES

9. El Secretario de Estado Director del Centro Nacional de Inteligencia en virtud del artículo 4, apartados e y f, de la Ley 11/2002, de 6 de mayo, es Autoridad de Acreditación de Seguridad (AAS).

10. La ejecución del procedimiento de acreditación será llevado a cabo bajo la dirección de la AAS o por la AAS-D del ámbito correspondiente en la que la Autoridad de Acreditación de Seguridad haya delegado.

11. La AAS/AAS-D, en adelante AAS, podrá disponer de un organismo de acreditación o de la organización de seguridad adecuada para apoyo en la ejecución de este procedimiento.

12. La acreditación de los sistemas de la Administración que manejen información clasificada procedente de OTAN, UE o de otros países u organizaciones con los que se hayan establecido acuerdos internacionales, será realizada por la Autoridad Nacional de Seguridad Delegada (ANS-D), que corresponde al Secretario de Estado Director del Centro Nacional de Inteligencia.

5. CONDICIONES PARA UNA ACREDITACIÓN

13. Como condición previa a la concesión de la autorización para manejar información clasificada, la AAS deberá someter a todos los sistemas de su ámbito de responsabilidad, que requieran manejar este tipo de información, a un proceso de acreditación que garantice el adecuado nivel de protección y su posterior mantenimiento.

14. Para que el proceso se considere completo, se deberán satisfacer los requisitos especificados en los siguientes apartados.

5.1 DOCUMENTACIÓN DE SEGURIDAD

15. Todo Sistema que maneje información clasificada deberá tener actualizada la documentación de seguridad que se relaciona en este procedimiento o en la norma específica correspondiente al acuerdo de protección suscrito. Esta documentación será revisada y validada según lo establecido en el apartado 6 de este procedimiento.

	SECRETO/ RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Concepto de Operación (CO)	SI	SI	SI
Análisis o Valoración de Riesgos	FORMAL	FORMAL	NO FORMAL
Declaración de Requisitos de Seguridad (DRS)	SI	SI	OPCIONAL

Procedimientos Operativos de Seguridad (POS)	SI	SI	SI
Declaración de Acreditación de Seguridad	SI	SI	SI

Tabla 1.- Documentación de Seguridad de los Sistemas

- **Concepto de Operación.** Declaración expresa que se realiza sobre el objeto o función de un Sistema o de una interconexión, 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. Se trata de un documento de alto nivel, en el que no se debe explicar con exceso de detalle las características de los elementos que componen el Sistema.

  Es responsabilidad de la Autoridad Operativa del Sistema de las Tecnologías de la Información (AOSTIC).

- **Análisis o Valoración de Riesgos.** Proceso sistemático para estimar la magnitud del riesgo a que está expuesto un Sistema de acuerdo a su Concepto de Operación.

- **Declaración de Requisitos de Seguridad (DRS).** Documento base para la acreditación. Consiste en una 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 en base a la política de seguridad vigente.

- **Procedimientos Operativos de Seguridad (POS).** Descripción precisa de la aplicación de los requisitos específicos 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.

16. La documentación de seguridad que se indica en este apartado, se elaborará conforme a las guías CCN-STIC correspondientes.

17. Como parte del proceso de acreditación, la AAS podrá pedir las evidencias que considere oportunas de la adecuada implementación de las medidas de seguridad (informes técnicos asociados a las herramientas de seguridad que se determinen).

5.2 SEGURIDAD DEL ENTORNO DE OPERACIÓN

5.2.1 SEGURIDAD LIGADA AL PERSONAL

18. La necesidad de una autorización para acceder a información nacional clasificada está establecida en el Decreto 242/1969, de 20 de febrero, por el

que se desarrolla la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, modificada por la ley 48/1978, de 7 de octubre.

19. El Jefe del Organismo propietario de la información clasificada determinará la necesidad de conocer para acceder a este tipo de información.

20. La relación de personas autorizadas a acceder al Sistema y a la información en él contenida, deberá figurar como anexo adjunto a la documentación de seguridad (Procedimiento Operativo de Seguridad), detallando los derechos y permisos de las mismas, conforme a lo establecido en las Normas de Seguridad (NS) de la Autoridad Nacional para la protección de la Información Clasificada.

5.2.2 SEGURIDAD FÍSICA

21. Aquellas áreas desde dónde se pueda acceder a información clasificada mediante un Sistema, deberán estar certificadas de acuerdo al nivel de clasificación de la información manejada y a los requisitos de seguridad requeridos conforme a lo establecido en las Normas de Seguridad (NS) de la Autoridad Nacional para la protección de la Información Clasificada.

5.2.3 SEGURIDAD DE LOS DOCUMENTOS

22. Los documentos que contienen información clasificada, así como sus soportes informáticos, serán protegidos de acuerdo con lo establecido en las Normas de Seguridad (NS) de la Autoridad Nacional para la protección de la Información Clasificada.

5.3 SEGURIDAD DE LAS EMANACIONES

23. La seguridad de las emanaciones es el conjunto de medidas destinadas a evitar fugas de información derivadas de emisiones electromagnéticas no deseadas de equipos electrónicos.

24. Para la protección de la información clasificada CONFIDENCIAL o superior, se aplicará la normativa establecida por el Centro Criptológico Nacional (CCN) en relación con la seguridad de las emanaciones.

25. En la documentación de seguridad del Sistema deberán figurar los certificados de las áreas donde se ubiquen los elementos del Sistema y, en su caso, los certificados TEMPEST de estos últimos.

5.4 SEGURIDAD CRIPTOLÓGICA

26. En aquellos sistemas que manejen información clasificada DIFUSIÓN LIMITADA o superior y empleen medios o procedimientos de cifra, será obligatorio el cumplimiento de la correspondiente normativa, y el empleo de productos con certificación criptológica del CCN o autorizados por este Organismo.

27. El personal responsable de la gestión de claves dispondrá de la Habilitación Personal de Seguridad CRIPTO pertinente.

5.5 SEGURIDAD DE LAS TIC

28. Todos los sistemas que manejen información clasificada deberán disponer de un conjunto equilibrado de servicios de seguridad que permita alcanzar los objetivos de seguridad requeridos.

29. Estos servicios de seguridad permitirán, cuando sea apropiado, lo siguiente:

    a. Identificar y autenticar a las personas y controlar su acceso a la información manejada por el Sistema o a los recursos del mismo.

    b. Proporcionar confidencialidad a la información manejada por el Sistema.

    c. Proporcionar integridad a la información manejada por el Sistema o a los recursos del mismo.

    d. Mantener la disponibilidad de la información manejada por el Sistema o de los recursos del mismo.

    e. Emplear productos de seguridad que haya sido revisados, evaluados, recomendados y/o certificados por el Organismo de Certificación competente.

    f. Mantener la trazabilidad y autenticidad de las actuaciones realizadas.

    g. Garantizar y verificar el funcionamiento de los mecanismos de seguridad del Sistema.

    h. Registrar y auditar la actividad de los usuarios del Sistema.

    i. Controlar las conexiones y los enlaces de los sistemas.

    j. Prevenir, detectar y corregir los impactos o incidentes que afecten a la confidencialidad, integridad y disponibilidad de la información o la integridad y disponibilidad del Sistema que la maneja.

30. La AAS tendrá en cuenta que se deben satisfacer dichos requisitos en las diferentes fases del ciclo de vida del Sistema y que los mismos quedarán reflejados en la documentación de seguridad de éste.

5.6 EVALUACIÓN DE SEGURIDAD DE LAS TIC

31. Antes de conceder la autorización a un Sistema, la AAS deberá llevar a cabo las auditorías/inspecciones de seguridad correspondientes bajo las directrices expresadas en este procedimiento y en la normativa que se desarrolle al efecto.

32. Su objeto es verificar el cumplimiento de las condiciones de acreditación, así como los requisitos de seguridad descritos en la documentación de seguridad y la correcta implementación de los servicios de seguridad expresados en el punto anterior.

6. PROCESO DE ACREDITACIÓN

33. El proceso de acreditación a seguir está recogido en la Tabla 1 del Anexo A de este Procedimiento. En la siguiente figura puede observarse una representación gráfica del mismo.

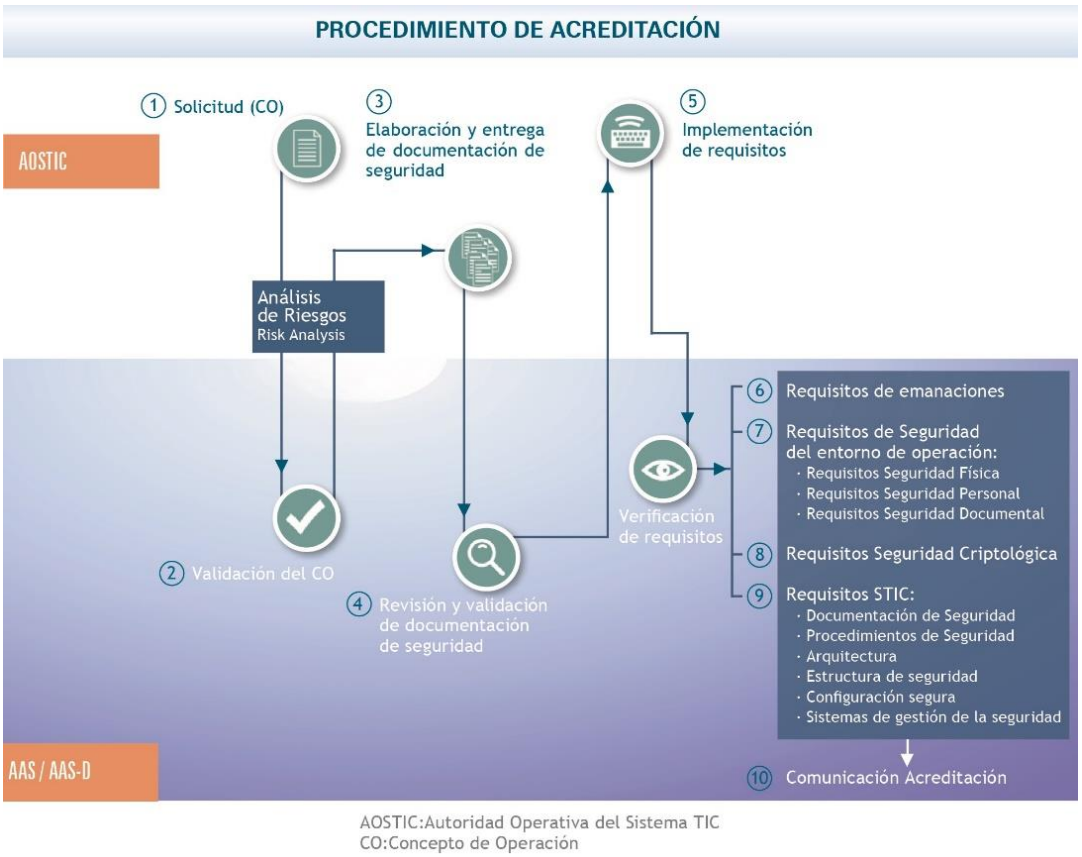

Figura 1.- Representación gráfica del proceso de acreditación para CONFIDENCIAL, o superior

34. Este proceso se basa en la documentación de seguridad, requisitos STIC, TEMPEST, Seguridad Criptológica y demás requisitos de seguridad a tener en cuenta (personal, física y documental).

35. Los sistemas a acreditar para manejar información DIFUSIÓN LIMITADA o equivalente siguen un procedimiento específico que se desarrolla en la Tabla 2 del Anexo A de este Procedimiento.

36. La verificación STIC de todos los procesos se realizará conforme a lo reflejado en el Anexo B de este procedimiento según indica la guía CCN-STIC-303. Se recomienda el nivel 3 de auditoría/inspección para superar un proceso de acreditación.

Figura 2.- Representación gráfica del proceso de acreditación para DIFUSIÓN LIMITADA, o equivalente

7. ACREDITACIÓN DE LAS INTERCONEXIONES

37. A los efectos de este procedimiento, se produce una conexión, cuando se proveen los medios físicos y lógicos de transmisión adecuados (por ejemplo enlace satélite, fibra óptica, etc.), susceptibles de ser empleados para el intercambio de información.

38. Se produce una "interconexión" entre sistemas cuando existe una conexión, se habilitan flujos de información y además puedan existir:

    - Diferentes políticas de seguridad.
    - Diferentes niveles de confianza/grado de clasificación.
    - Diferentes AOSTIC.
    - Una combinación de las anteriores.

39. Todos los sistemas que manejen información clasificada, como paso previo a la solicitud de acreditación de su interconexión a otro Sistema, o redes públicas o similares, deben estar acreditados al grado correspondiente de la información que manejen.

40. La acreditación de la interconexión de sistemas ya acreditados es responsabilidad de la Autoridad/es que haya/n acreditado dichos sistemas.

41. La acreditación de la interconexión de un Sistema acreditado a otro sin acreditar, a Internet o a redes públicas similares es responsabilidad de la Autoridad que haya acreditado dicho Sistema.

42. La acreditación de la interconexión en al ámbito de varias Autoridades podrá ser responsabilidad del comité/panel de acreditación que determinen las mismas.

7.1 DOCUMENTACIÓN DE SEGURIDAD DE LA INTERCONEXIÓN

43. La acreditación será realizada mediante la validación de la correspondiente documentación de seguridad y la evaluación STIC que verifique el cumplimiento de los requisitos establecidos en la citada documentación y la normativa correspondiente. El proceso a seguir es similar al descrito en las Tablas 1 y 2 del Anexo A de este Procedimiento.

44. La documentación de seguridad a elaborar para la interconexión vendrá determinada por el mayor grado de clasificación de la información manejada por los sistemas a interconectar, de acuerdo con la siguiente tabla:

	SECRETO/ RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Concepto de Operación (CO)	SI	SI	SI
Análisis o Valoración de Riesgos	FORMAL	FORMAL	NO FORMAL
Declaración de Requisitos de Seguridad (DRS)	SI	SI	OPCIONAL
Procedimientos Operativos de Seguridad (POS)	SI	SI	SI
Declaración de Acreditación de Seguridad	SI	SI	SI

Tabla 2.- Documentación de Seguridad de las Interconexiones

8. SITUACIONES POSIBLES DE LA ACREDITACIÓN

45. En el proceso de acreditación se podrán dar las siguientes situaciones:

- **Autorización para Pruebas (AP).** Esta situación se utilizará como paso previo a acreditación para manejar información clasificada con objeto de realizar las pertinentes pruebas técnicas (funcionales y de seguridad), de comunicaciones e intercambio de información. Es necesario que esté redactada la documentación de seguridad. En la concesión de la AP se aprobará la máxima clasificación de la información a intercambiar en las pruebas, el plan de pruebas a ejecutar y el período de las mismas.
- **Autorización Provisional de Seguridad (APS).** Esta situación se utilizará para sistemas o interconexiones en proceso de acreditación que no hayan

superado completamente éste (pendiente de la resolución de deficiencias) o como paso previo para la concesión de la acreditación definitiva.

En esta situación cada uno de los elementos del Sistema, incluidas las interconexiones, pueden intercambiar información clasificada. Es necesario que esté redactada la documentación de seguridad. La declaración identificará las condiciones de uso (incluidas posibles medidas de mitigación de riesgo o reducción de determinadas funcionalidades), las acciones a desarrollar para completar el proceso y el marco temporal de validez.

- **Acreditación de Seguridad (AS).** Situación alcanzada por los sistemas e interconexiones que hayan superado con éxito el proceso de acreditación. La Declaración de Cumplimiento estará apoyada por los resultados de la evaluación de seguridad correspondiente y establecerá las condiciones que permiten que mantenga la validez hasta la fecha límite. El periodo máximo de validez de la misma está fijado en el apartado 9 de este procedimiento.
- **Denegación.** Situación en la que el Sistema no dispone de acreditación. Se comunicaran las deficiencias encontradas y las acciones correctivas para solucionarlas.
- **Cancelación.** Situación en la que se deja en suspenso o se revoca permanentemente la acreditación de que ya disponía ese Sistema. Se comunicarán las deficiencias encontradas y las acciones correctivas para solucionarlas.

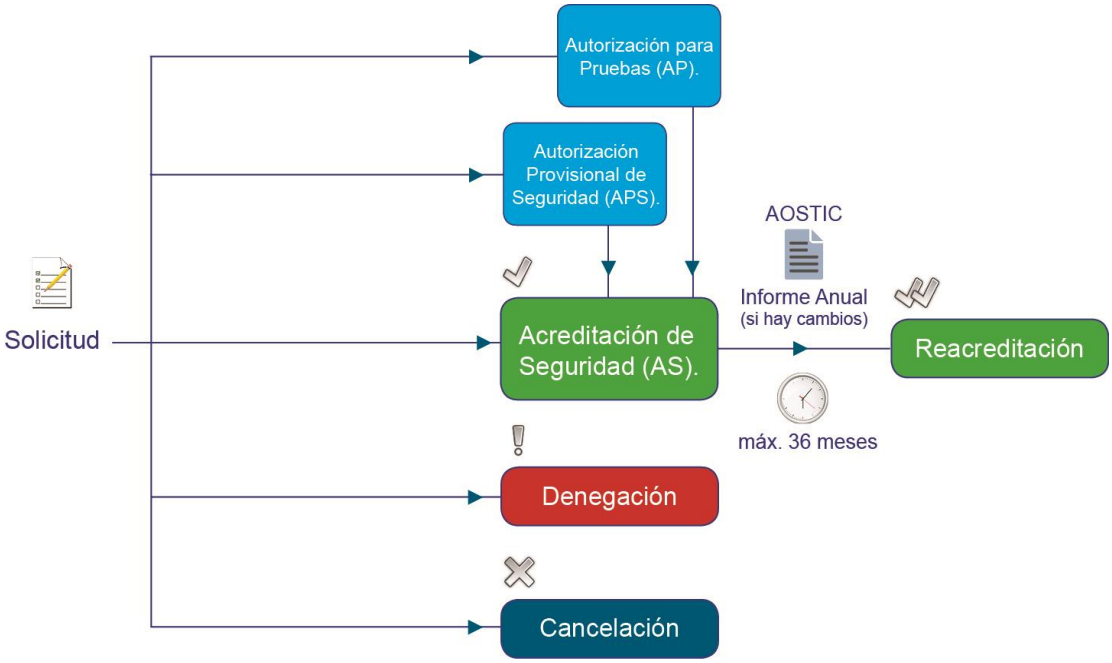

Figura 3.- Situaciones posibles tras la solicitud de acreditación

9. VALIDEZ DE LA ACREDITACIÓN

46. Se establece un período máximo de la validez de las acreditaciones de todos los sistemas de treinta y seis (36) meses, independientemente del grado de clasificación de la información que manejen. Para los sistemas tácticos/desplegables, el período máximo de validez puede establecerse en doce (12) meses cuando se determinen circunstancias de seguridad que así lo aconsejen según la normativa vigente.

47. La vigencia de la acreditación para una interconexión de sistemas vendrá determinado por el período máximo de validez de la acreditación del Sistema interconectado que finalice antes.

10. PERÍODO ENTRE EVALUACIONES DE SEGURIDAD DE LAS TIC

48. Bajo la responsabilidad de la AAS deberán llevarse a cabo evaluaciones de seguridad de las TIC de los sistemas e interconexiones acreditadas para verificar el mantenimiento de las condiciones de acreditación.

49. El período máximo entre evaluaciones para los diferentes sistemas acreditados es de dieciocho (18) meses, independientemente del grado de clasificación de la información que manejen.

50. El período máximo entre evaluaciones para las interconexiones de sistemas vendrá determinado por la del Sistema interconectado que finalice antes.

51. La AAS establecerá el calendario de evaluaciones, siempre dentro de los plazos máximos establecidos.

52. La continuidad de la acreditación otorgada dependerá del resultado de las evaluaciones. La AAS podrá requerir de la AOSTIC la implantación de una serie de medidas correctivas así como un plazo para implementarlas.

53. La no implementación de las medidas correctivas en el plazo requerido podrá ocasionar la pérdida de la acreditación, lo que implicará la eliminación de la información clasificada según el proceso que establezca la AAS.

54. El resultado de una evaluación de la seguridad de las TIC puede, en algunos casos, establecer la necesidad de reacreditar el Sistema/Interconexión.

55. La AAS, en su misión de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada, podrá comprobar la seguridad de los sistemas o de sus interconexiones, previa comunicación y coordinación con la AAS-D correspondiente.

11. REACREDITACIÓN

56. La reacreditación es la renovación de la autorización para manejar información clasificada en función de la autorización concedida previamente.

57. El proceso de reacreditación puede ser ocasionado también por un cambio significativo de la configuración hardware y/o software, de ubicación del Sistema, del tipo o del grado de clasificación de la información manejada u otras circunstancias que lo aconsejen.

58. La AOSTIC valorará las implicaciones de seguridad de todos los cambios sufridos por el Sistema durante su ciclo de vida. Los cambios que afecten a las características de seguridad deberán ser aprobados previamente por él mismo y acreditados por la AAS/AAS-D de su ámbito.

59. En el proceso de reacreditación, solo será necesario remitir el Concepto de Operación cuando haya modificaciones que le afecten.

12. INFORMES A REMITIR ENTRE ACREDITACIONES

60. Una vez concedida la acreditación, y al menos con carácter anual, la AOSTIC deberá remitir un informe a la AAS en el que se expresen las vicisitudes ocurridas en el Sistema que afecten a la acreditación durante dicho período.

61. En el primer trimestre del año, las AOSTIC de los sistemas que manejen información clasificada CONFIDENCIAL, o superior, remitirán por los canales autorizados a la AAS un informe con:

    - Las altas y bajas de personal responsable de la seguridad del Sistema.
    - Modificaciones de hardware, software o de la ubicación previstas durante el año que impliquen aspectos de seguridad.
    - Estado de cumplimiento de los DRS y POS.
    - Resumen de los incidentes que hayan afectado o comprometido la seguridad del Sistema, toda vez que los incidentes de un impacto significativo se comunicarán de acuerdo con la normativa vigente.

62. Cualquier cambio significativo que sufra el Sistema (de emplazamiento, de configuración hardware/software o de las condiciones de seguridad), estuviera o no previsto en el informe remitido en el año, será comunicado por parte de la AOSTIC a la AAS por los canales autorizados para iniciar, en su caso, el proceso de reacreditación.

63. Para los sistemas que procesen información DIFUSIÓN LIMITADA, o inferior, la AAS definirá los informes a remitir y la periodicidad de los mismos.

13. REGISTRO DE SISTEMAS ACREDITADOS

64. La AAS/AAS-D llevará un Registro de los sistemas acreditados.

65. Las AAS-D deberán comunicar mediante escrito a la AAS los procesos de acreditación finalizados, así como cualquier incidencia que se produzca en los sistemas de su responsabilidad durante el tiempo de validez de la acreditación.

ANEXO A: PROCESO DE ACREDITACIÓN

ACCIÓN	OBSERVACIONES	RESPONSABLE
Envío de la solicitud de acreditación y CO.	La AOSTIC remitirá por los canales autorizados el CO del Sistema anexado a la solicitud de acreditación	AOSTIC
Validación del CO e inicio del proceso.	La AAS/AAS-D, una vez validado el CO, comunicará a la AOSTIC el inicio del proceso de acreditación.	AAS/AAS-D
Entrega de la documentación de seguridad.	La AOSTIC elaborará la documentación de seguridad del Sistema según el apartado 5.1 de este procedimiento y la remitirá por los canales autorizados a la AAS/AAS-D.	AOSTIC
Revisión y validación de la documentación de seguridad.	Como acción previa a la evaluación STIC, es necesaria la validación de la documentación de seguridad por parte de la AAS/AAS-D.	AAS/AAS-D
Implementación de requisitos.	La AOSTIC, previo a la evaluación STIC, debe implementar todos los requisitos reflejados en la documentación del Sistema.	AOSTIC
Verificación del cumplimiento de los requisitos de emanaciones.	La AAS/AAS-D verificará que se cumplen los requisitos de seguridad de emanaciones. Para ello, la AOSTIC remitirá por los canales autorizados el correspondiente certificado.	AAS/AAS-D
Verificación del cumplimiento de los requisitos de seguridad del entorno de operación.	Se deben cumplir los requisitos del entorno de operación (seguridad física, documental y del personal). Para ello la AOSTIC dispondrá de los correspondientes certificados.	AAS/AAS-D
Verificación del cumplimiento de los requisitos de seguridad criptológica.	La AAS/AAS-D verificará que se cumplen los requisitos de seguridad criptológica para los sistemas que requieran manejar información clasificada DIFUSIÓN LIMITADA, o superior.	AAS/AAS-D
Verificación del cumplimiento de los requisitos STIC.	La verificación de requisitos STIC se realizará mediante la correspondiente evaluación STIC por la AAS/AAS-D, o por quién ésta haya establecido. En concreto se verificará: a) La implementación de los requisitos STIC declarados en la documentación de seguridad. b) Los procedimientos de seguridad del Sistema descritos en la documentación de seguridad. c) La arquitectura del Sistema, los equipos conectados y las interconexiones del mismo de acuerdo con la documentación de seguridad. d) La estructura de seguridad (responsables de seguridad) que soporta el Sistema es la descrita en la documentación de seguridad. e) Las configuraciones de los elementos del Sistema, verificando que implementan la configuración segura establecida en la correspondiente normativa. La AAS/AAS-D remitirá por los canales autorizados a la AOSTIC el resultado de la evaluación STIC mediante un informe técnico donde se reflejen las deficiencias detectadas.	AAS/AAS-D
Comunicación de la acreditación.	Si el Sistema cumple con lo expresado en la documentación de seguridad validada, la Autoridad responsable de la acreditación emitirá el certificado de acreditación (Anexo B).	AAS/AAS-D

Tabla 1.- Tabla del proceso de acreditación para CONFIDENCIAL, o superior

ACCIÓN	OBSERVACIONES	RESPONSABLE
Identificación del Auditor de Seguridad.	La AOSTIC determinará la entidad auditora de seguridad: a) Entre entidades certificadoras acreditadas por la Entidad Nacional de Acreditación (ENAC) para la certificación de sistemas del ámbito de aplicación del Esquema Nacional de Seguridad conforme a la norma UNE-EN ISO/IEC 17065:2012 que dispongan de Habilitación de Seguridad de Empresa (HSEM) en vigor. b) Entre aquellas entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad. c) O bien, excepcionalmente, entre aquellas empresas validadas por el CCN que hayan demostrado la capacidad técnica suficiente para llevar a cabo auditorías/inspecciones STIC sobre sistemas que manejan información clasificada. El Centro Criptológico Nacional mantendrá en su sede electrónica una relación actualizada de las entidades acreditadas o en vías de acreditación.	AOSTIC
Confección de la documentación de seguridad.	La AOSTIC, o la entidad auditora en nombre de ésta, elaborará la documentación de seguridad del Sistema de acuerdo al apartado 5.1 de este procedimiento y la remitirá por los canales autorizados a la AAS/AAS-D.	AOSTIC
Implementación de requisitos.	La AOSTIC, o la entidad auditora en nombre de ésta, previo a la evaluación de seguridad debe implementar todos los requisitos reflejados en la documentación de seguridad del Sistema.	AOSTIC
Verificación del cumplimiento de los requisitos STIC.	La entidad auditora verificará el cumplimiento de los requisitos y normativa de seguridad vigente por medio de una auditoría/inspección de seguridad (evaluación STIC) y remitirá por los canales autorizados a la AAS/AAS-D el resultado mediante un informe técnico junto con las evidencias resultantes donde se reflejen las posibles deficiencias detectadas. En concreto se verificará: a) La implementación de los requisitos STIC declarados en la documentación de seguridad. b) Los procedimientos de seguridad del Sistema descritos en la documentación de seguridad. c) La arquitectura del Sistema, los equipos conectados y las interconexiones del mismo de acuerdo con la documentación de seguridad. d) La estructura de seguridad (responsables de seguridad) que soporta el Sistema es la descrita en la documentación de seguridad. Las configuraciones de los elementos del Sistema, verificando que implementan la configuración segura establecida en la correspondiente normativa.	Entidad Auditora
Verificación del cumplimiento de los requisitos de seguridad criptológica.	La AAS/AAS-D verificará que se cumplen los requisitos de seguridad criptológica para los sistemas que requieran manejar información clasificada DIFUSIÓN LIMITADA, o equivalente.	AAS/AAS-D
Revisión y validación de la documentación de seguridad.	EL CCN validará la documentación de seguridad y revisará las evidencias de la auditoría/inspección aportadas comunicando su conformidad o disconformidad con las mismas a la AAS/AAS-D.	CCN
Comunicación de la acreditación.	Si el Sistema cumple con lo expresado en la documentación de seguridad validada, la AAS/AAS-D emitirá el certificado de acreditación (Anexo B).	AAS/AAS-D

Tabla 2.- Tabla del proceso de acreditación para DIFUSIÓN LIMITADA, o equivalente

ANEXO B: AUDITORÍAS/INSPECCIONES DE SEGURIDAD DE LAS TIC

	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
ÁMBITO	Elemento (producto, servicio, dispositivo, aplicación,…) y Sistema.	Elemento (producto, servicio, dispositivo, aplicación,…) y Sistema.	Elemento (producto, servicio, dispositivo, aplicación,…), Sistema e Interconexión.	Elemento (producto, servicio, dispositivo, aplicación,…), Sistema e Interconexión.	Elemento (producto, servicio, dispositivo, aplicación,…), Sistema e Interconexión.
OBJETIVO	Determinación de los servicios proporcionados y arquitectura del Sistema.	Análisis de riesgos para determinar las propiedades y funciones de seguridad del Sistema.	Búsqueda de vulnerabilidades para llegar a conocer las propiedades y funciones de seguridad del Sistema.	Determinar el nivel de seguridad de un Sistema y su grado de cumplimiento con la política de seguridad.	Determinar el nivel de seguridad de un Sistema y su grado de cumplimiento con la política de seguridad.
ACTIVIDADES	- Análisis.	- Análisis. - Verificación Manual.	- Análisis. - Verificación Manual. - Verificación Automática.	- Análisis. - Verificación Manual. - Verificación Automática. - Prueba Intrusión Caja Blanca.	- Análisis. - Verificación Manual. - Verificación Automática. - Prueba Intrusión Caja Negra.
MEDIOS Y TÉCNICAS	- Revisión Documentación.	- Revisión Documentación. - Gestión Configuración. - Cuestionarios (ST&E Plan[1]). - Entrevistas.	- Revisión Documentación. - Gestión Configuración. - Cuestionarios (ST&E Plan[1]). - Entrevistas. - Herramientas Seguridad.	Herramientas y técnicas de explotación de vulnerabilidades.	Herramientas y técnicas de explotación de vulnerabilidades.
REALIZACIÓN	Continua, especialmente tras la adición de un nuevo componente al Sistema.	Periódica y acorde con el Procedimiento de Acreditación.	Periódica y acorde con el Procedimiento de Acreditación. Se considera como el Nivel recomendado para superar un proceso de acreditación.	Con carácter excepcional dependiendo de la sensibilidad del Sistema.	Con carácter excepcional dependiendo de la sensibilidad del Sistema.
RESULTADO	Mejora en la gestión “global” de la seguridad.	Mejora en la gestión “global” de la seguridad.	Conocimiento “real” del riesgo del Sistema.	Reconocimiento objetivo de que el Sistema opera dentro del marco de seguridad definido.	Reconocimiento objetivo de que el Sistema opera dentro del marco de seguridad definido.

Tabla 1.- Tabla de Niveles de Auditorías/Inspecciones de Seguridad de las TI

[1] Security Test and Evaluation Plan

ANEXO C: DOCUMENTO DE CONFORMIDAD

DESCRIPCIÓN DEL SISTEMA / SYSTEM DESCRIPTION	
Nombre del Sistema:	**Tipo de Sistema / Clasificación:**
Referencia del Escrito de Solicitud:	**Referencia del Análisis de Riesgos:**
Referencia de la DRS:	**Referencia de los POS:**

PROCESO DE ACREDITACIÓN / SECURITY APPROVAL PROCESS			
Asunto / Subject	**Actividad / Activity**	**Estado / Status**	**Cumplimiento / Compliance**
Revisión y Val. del Análisis de Riesgos Review and Assessment of Risk Analysis	(Revisión / Valoración) (Review / Assessment)	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Revisión y Aprobación de la DRES Review and Approval of SSRS	(Revisión / Aprobación) (Review / Approval)	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Revisión y Aprobación de los POS Review and Approval of SecOPs	(Revisión / Aprobación) (Review / Approval)	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
(Valoración / Pruebas de seguridad / Análisis de vulnerabilidad) (Assessment / Security Tests / Vulnerability Analysis)	EVALUACIÓN STIC INFOSEC Inspection	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Revisión y Aprobación de evidencias Review and Approval of evidences	(Revisión / Aprobación) (Review / Approval)	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Conformidad Seguridad Criptológica Conformance of crypto security	(Valoración / Inspección) (Assessment / Site Inspection)	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Requisitos TEMPEST TEMPEST Requirements	(Instalación de equipos / Medición ZONING) acorde con normativa.	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Fecha y Firma			

Asunto / Subject	**Actividad / Activity**	**Estado / Status**	**Cumplimiento / Compliance**
Conformidad Seguridad Física Conformance of Physical Security	(Valoración / Inspección) (Assessment / Site Inspection)	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Conformidad Seguridad Personal Conformance of Personnel Security	(Valoración / Inspección) (Assessment / Site Inspection)	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Conformidad Seguridad Documentos Conformance of Security of Info.	(Valoración / Inspección) (Assessment / Site Inspection)	(Pendiente/Completada/NA - fecha) (Pending / Completed / NA - date)	Sí / No Yes / No
Fecha y Firma			

ANEXO D: COMUNICACIÓN DE SITUACIÓN DE ACREDITACIÓN STIC

DESCRIPCIÓN DEL SISTEMA	
Nombre del Sistema:	**Tipo de Sistema / Clasificación:**
(Nombre con el que se designa al Sistema)	[Red de área local / Ordenadores aislados]
Referencia del Escrito de Solicitud:	**Referencia del Análisis de Riesgos:**
(Referencia del escrito en el que se solicita la acreditación del Sistema)	(Referencia del documento con el análisis o valoración de riesgos)
Referencia de la DRS:	**Referencia de los POS:**
(Referencia del documento con la declaración de requisitos de seguridad)	(Referencia del documento con los procedimientos operativos de seguridad)
DECLARACIÓN DE SITUACIÓN DEL SISTEMA	
Se da una Autorización para Pruebas (AP) / Autorización Provisional de Seguridad (APS) / Acredita hasta [(fecha)] al Sistema [(nombre del Sistema)] a manejar información clasificada hasta el grado de clasificación [_____] y en el modo seguro de operación [_____] de acuerdo a las condiciones establecidas en la documentación de referencia antes mencionada.	
Nº de registro de la Acreditación:	**Fecha, Firma y Nombre de la Autoridad:**

ANEXO E: GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Acreditación de Seguridad	Autorización otorgada por la Autoridad responsable de la acreditación, para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su 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.
Autenticidad	Aseguramiento de la identidad u origen.
Autoridad de Acreditación de Seguridad	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 de Certificación TEMPEST	Autoridad responsable de la evaluación y certificación de equipos e instalaciones que deban cumplir requisitos TEMPEST.
Autoridad de Acreditación de Seguridad Delegada	Autoridad responsable en su ámbito, de la aplicación de la Política STIC y de las competencias que delegue la AAS.
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.
Autorización para Pruebas	Situación del sistema previa a manejar información clasificada con objeto de realizar las pertinentes pruebas técnicas (funcionales y de seguridad), de comunicaciones e intercambio de información sin clasificar. Es necesario que este redactada la documentación de seguridad
Autorización Provisional de Seguridad	Situación de sistemas o interconexiones en proceso de acreditación que no hayan superado completamente éste (pendiente de la resolución de deficiencias) o como paso previo para la concesión de la acreditación definitiva. En esta situación cada uno de los elementos del Sistema, incluidas las interconexiones, pueden intercambiar información clasificada. Es necesario que esté redactada la documentación de seguridad.
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.
Conexión	Se produce una conexión, cuando se proveen los medios físicos y lógicos de transmisión adecuados (por ejemplo enlace satélite, fibra óptica, etc.) susceptibles de ser empleados para el intercambio de información entre sistemas.
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.
Habilitación Personal de Seguridad (HPS)	Documento que acredita que una persona determinada cumple los criterios necesarios para acceder a Información Clasificada. Esta habilitación la concede, deniega o retira la Autoridad Delegada.
Habilitación de Seguridad de Empresa (HSEM)	La determinación positiva por la que la Autoridad Nacional reconoce formalmente la capacidad y fiabilidad de un contratista para generar y acceder a Información Clasificada hasta un determinado grado, sin que pueda manejarla o almacenarla en sus propias instalaciones
Habilitación de Seguridad de Establecimiento (HSES)	La determinación positiva por la que la Autoridad Nacional reconoce formalmente la capacidad y fiabilidad de un contratista poseedor de una HSEM para manejar y almacenar Información Clasificada hasta un determinado grado en aquellas de sus propias instalaciones habilitadas al efecto
Manejar Información	Presentar, elaborar, almacenar, procesar, transportar o destruir información.
Necesidad de conocer	Determinación positiva por la que se confirma que un posible destinatario requiere el acceso a, el conocimiento de, o la posesión de la información para desempeñar servicios, tareas o cometidos oficiales.
Oficina Nacional de Seguridad (ONS)	Órgano de trabajo del Director del CNI para auxiliarle en el cumplimiento de sus cometidos relacionados con la protección de la Información Clasificada. Tiene por misión fundamental la de velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de Tratados o Acuerdos internacionales suscritos por España (artículo 4 f de la Ley 11/2002, de 6 de mayo, Reguladora del CNI).
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 Emanaciones o Seguridad	Conjunto de medidas destinadas a evitar fugas de información derivadas de emisiones electromagnéticas no deseadas de equipos electrónicos.

TEMPEST **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.
Sistema táctico/desplegable	Sistema, normalmente de las Fuerzas Armadas, desplegado en teatro/zona de operaciones.
TEMPEST	Término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.
ZONING	Término que hace referencia a la clasificación de zona de los locales y plataformas donde se ubican equipos TEMPEST.
AAS	Autoridad de Acreditación de Seguridad
AAS-D	Autoridad de Acreditación de Seguridad Delegada
ANS-D	Autoridad Nacional de Seguridad Delegada
AOSTIC	Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones
AP	Autorización para Pruebas
APS	Autorización Provisional de Seguridad
AS	Acreditación de Seguridad
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
ENAC	Entidad Nacional de Acreditación
ENS	Esquema Nacional de Seguridad
INFOSEC	Information Security
OTAN	Organización del Tratado del Atlántico Norte
NS	Normas de Seguridad
POS	Procedimientos Operativos de Seguridad
Sistema	Sistema de las Tecnologías de la Información y las Comunicaciones
SPP	Sistema de Protección de Perímetro
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones

ST&E Plan	Security Test and Evaluation Plan
TIC	Tecnologías de la Información y las Comunicaciones
UE	Unión Europea.