GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-205)

ACTIVIDADES DE SEGURIDAD EN EL CICLO DE VIDA DE LOS SISTEMAS TIC

DICIEMBRE 2007

Edita:

NIPO: 076-07-236-6

Tirada: 1000 ejemplares
Fecha de Edición: diciembre de 2007
José Antonio Mañas ha participado en la elaboración y modificación del presente documento y sus anexos.

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.

Diciembre de 2007

Alberto Sáiz
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

1. Los Sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) son un componente básico para conseguir los niveles de calidad y productividad actuales. Pero al tiempo son una vía que puede ser utilizada, voluntaria o inadvertidamente, en detrimento de la seguridad de la información que manejan o de los servicios que prestan.
2. Es posible, e imperativo, incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la Organización. Es un hecho reconocido que tomar en consideración la seguridad del sistema antes y durante su desarrollo es más efectivo y económico que tomarla en consideración a posteriori. La seguridad debe estar embebida en el sistema desde su primera concepción.
3. Los responsables de planificación, tanto técnica como económica, deberán tener en cuenta la seguridad en todas las fases del ciclo de desarrollo, de forma que haya cobertura técnica, temporal y presupuestaria para implantar las medidas de protección identificadas.
4. Se pueden identificar dos tipos de actividades diferenciadas:
   - SSI: actividades relacionadas con la propia seguridad del sistema de información producido.
   - SPD: actividades que velan por la seguridad del proceso de desarrollo del sistema de información.
5. La mayor parte de la guía se centra en la seguridad del sistema de información producido. La sección 11 se centra en la seguridad del entorno de desarrollo.

2. OBJETO

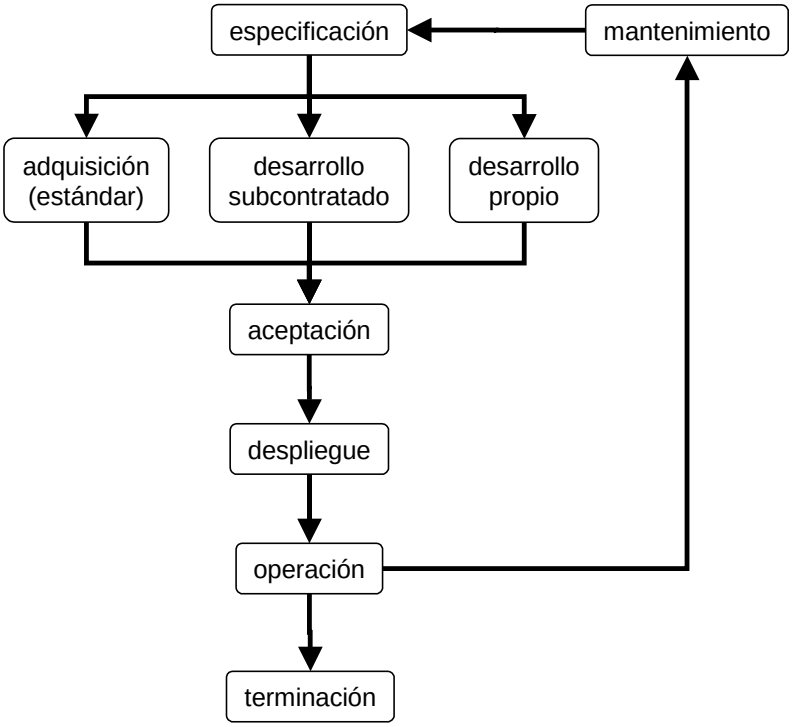
6. Es objeto de esta guía describir el tratamiento de los requisitos de seguridad durante el ciclo de vida de sistemas de información.
7. Es también requisito de esta guía describir la gestión de los riesgos en el entorno de desarrollo.

3. ALCANCE

8. La arquitectura de desarrollo propuesta sirve como guía, pudiendo ser la implantación final diferente en cada Organización. No obstante, las actividades identificadas en esta guía deben ser cubiertas sea cual fuere la implantación final adoptada.

4. CICLO DE VIDA

9. Típicamente, un sistema sigue un ciclo de vida a través de varias fases:



10. **Especificación.** En esta fase se determinan los requisitos que debe satisfacer el sistema y se elabora un plan para las siguientes fases. Se puede distinguir entre algunas subfases:
    - iniciación: donde se identifica la necesidad de servicio o de negocio
    - concepto: donde
        - se especifica el servicio necesitado
        - se identifica la aproximación que se va a seguir para resolver el problema a nivel de borrador o grandes líneas
    - requisitos: donde se concreta lo que se quiere:
        - niveles de seguridad de la información manejada
        - niveles de calidad de servicio
        - instrucciones para su adquisición o desarrollo
        - criterios de aceptación
    - entorno de seguridad: donde se perfilan las condiciones de operación del sistema
11. **Adquisición o desarrollo.** Para traducir una especificación en una realidad, se puede adquirir un producto, o se puede desarrollar, bien en casa, bien por subcontratación externa. Si hay un desarrollo, se pueden distinguir algunas subfases:
    - **diseño:** de alto nivel (arquitectónico) y de bajo nivel (componentes) que identifican los componentes a desarrollar
    - **estructura de la información:** donde se identifica cómo se almacena la información y cómo se va a hacer accesible

- **construcción:** donde
  - se desarrolla y/o integra el código de la aplicación software
  - se desarrollan y/o integran los componentes hardware, incluidos los componentes de comunicaciones
  - se desarrollan y/o integran servicios externos

12. **Aceptación.** Tanto si es un sistema nuevo como si es modificación de un sistema anterior, nunca un sistema debe entrar en operación sin haber sido formalmente aceptado.
    - Pruebas de aceptación
    - Validación de la documentación
    - Formación de administradores, operadores y usuarios
13. La aceptación puede incluir elementos que garanticen la seguridad del sistema:
    - **Certificación de la seguridad.** Una tercera parte, independiente, examina las salvaguardas dispuestas emitiendo un dictamen acerca de su idoneidad para los objetivos de seguridad propuestos, y el riesgo residual remanente.
    - **Acreditación para operar.** Se recaba la autorización formal para entrar en operación, aceptando el riesgo residual.
14. **Despliegue.** Consistente en
    - instalación del sistema,
    - integración en su entorno, incluyendo planes de continuidad,
    - configuración y
    - carga de datos iniciales
15. **Operación.** Los usuarios usan el sistema, siendo atendidos los incidentes por parte de los administradores y/o los operadores. Los operadores y administradores se encargan de la configuración, mantenimiento y gestión de los registros de actividad.
16. **Mantenimiento.** Bien porque aparecen nuevos requisitos, bien porque se ha detectado un fallo, el sistema puede requerir un mantenimiento que obligue a regresar a cualquiera de las etapas anteriores, en última instancia a la especificación básica.
    - Pruebas de regresión.
    - Revisión de documentación y procedimientos operativos
    - Revisión de planes de continuidad
    - Re-acreditación.
17. **Terminación.** Eventualmente un sistema será retirado del servicio. Esta terminación debe ser ordenada, siguiendo una política que determine qué debe conservarse, qué debe destruirse concienzudamente y que puede ser simplemente desechado.

5. ROLES

18. La guía CCN-STIC-201, "Organización y Gestión de para la Seguridad de las TIC", establece tres tipos de estructuras dentro de cada Organización STIC:
    - Estructura de Seguridad de las TIC de la Organización: responsable de establecer y aprobar los requisitos de seguridad del 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.
19. La Estructura de Seguridad aparece en la fase de aceptación, siendo la Autoridad de Acreditación (AA) o en quien esta delegue (ADA) la responsable de la acreditación del sistema e incluso de la solicitud de certificaciones si fuera pertinente.
20. La Estructura de Control de Material de Cifra aparece en las fases de despliegue (generación de material de cifra), operación (uso del material) y terminación (destrucción del material). No se profundizará más en esta estructura siendo de plena aplicación lo establecido en la guía 201.
21. Por último, la Estructura Operacional estará presente a lo largo de todo el ciclo de vida.
22. Sin perjuicio de que se aplique en su totalidad lo establecido en dicho documento, los siguientes roles son especialmente significativos en el desarrollo de sistemas.
23. **Autoridad de acreditación (AA) o en quien esta delegue (ADA)** – Aprueba formalmente la capacidad para pasar a producción.
24. **Autoridad de Seguridad TIC (ASTIC)** – Responsable de las especificaciones y decisiones tomadas a lo largo del ciclo de vida.
25. **Supervisor de Seguridad TIC (SSTIC)** – Responsable de la supervisión de las medidas y procedimientos de seguridad de los sistemas a su cargo. Depende del ASTIC.
26. **Responsable Seguridad del Área (RSA)** – A cargo de los aspectos de seguridad física de las instalaciones relacionadas con el sistema. Depende del ASTIC.
27. **Autoridad Operativa de Seguridad TIC (AOSTIC)** – Responsable de la operación del sistema.
28. **Administrador de Seguridad del Sistema (ASS)** – Responsable de la ejecución de las medidas de seguridad. Depende del AOSTIC.
29. **Equipo de Respuesta a Incidentes de Seguridad (ERIS)** – Responsable de la gestión de incidencias de operación. Depende del AOSTIC.
30. Otros roles son relevantes en proceso de desarrollo; pero no se profundizará en ellos al tratarse de elementos paralelos a las necesidades de seguridad:
    - Responsable(s) del establecimiento de los requisitos funcionales del sistema.
    - Arquitecto técnico – Establece la arquitectura funcional del sistema.
    - Desarrolladores – Se encargan del desarrollo de aplicaciones según especificaciones.

- Integradores – Integran las diferentes piezas, propias y subcontratadas.

6. PRINCIPIOS GENERALES

31. El desarrollo metódico y riguroso es una manera eficaz de gestionar los riesgos del sistema: analizándolos y tratándolos sistemáticamente.
32. Los requisitos de seguridad deben determinarse a la par que los requisitos funcionales.
33. Los costes de las medidas de seguridad deben ser parte de los elementos de decisión entre diferentes arquitecturas del sistema.
34. Cuando existan productos en el mercado (COTS), se preferirán a desarrollos específicos.
    a. El principio se aplica tanto a sistemas completos como a subsistemas o componentes de sistemas.
    b. El principio es especialmente importante cuando se refiere a dispositivos criptográficos, preferentemente certificados y acreditados para una cierta función.
    c. Debe analizarse la opción de adaptar los requisitos del sistema a las posibilidades de sistemas o componentes ya existentes antes que desarrollar nuevos sistemas específicos.
    d. El uso extendido de un sistema es garantía de mantenimiento y mejora continua.
35. Las medidas de protección aprobadas deben incorporarse durante la fase de adquisición / desarrollo, formando parte integral del sistema que se presenta para su aceptación.
36. Las fases a través de las cuales se gestiona el ciclo de vida de un sistema deben ser identificadas claramente, planificadas y ejecutadas bajo un sistema de gestión que se adapte a los requisitos de la organización beneficiaria del sistema. El orden exacto de las fases y su desarrollo en detalle quedan fuera del alcance esta guía, pueden ser específicos de cada organización e incluso variar para adaptarse a los diferentes tipos de sistemas. En cualquier caso, las fases se documentarán y aprobarán adecuadamente.
37. Las fases del ciclo de vida serán objeto de un sistema de gestión adecuado que permita conocer el grado de avance, detectar desviaciones, reubicar dinámicamente recursos y adecuar la planificación para adaptarse a las incidencias que pudieran surgir.

7. ANÁLISIS DE RIESGOS

38. El análisis de riesgos es una actividad fundamental de soporte de un sistema de información por cuanto analiza los bienes a proteger, identifica las amenazas a las que pudieran estar expuestos y ayuda a identificar y calificar las salvaguardas pertinentes.
39. El análisis de riesgos debe verse como un método de análisis del sistema que informa en todo momento de la posición de riesgo y permite tomar decisiones alineadas con el riesgo residual aceptado.
40. El modelo de riesgos debe correr parejo con el sistema de información, recogiendo su evolución propia (activos y salvaguardas) y la del entorno en el que opera (amenazas). Igual que del sistema conocemos al principio sus líneas generales y luego sus detalles, en el análisis de riesgos analizaremos primero las amenazas generales y luego las amenazas en detalle sobre los componentes que lo soportan.

7.1. DURANTE LA ESPECIFICACIÓN

41. Activos de información. Se identifica y valora la información manejada por el sistema, tanto la información final o de negocio como la información subsidiaria: claves criptográficas, identificación de usuarios, caracterización de usuarios y repositorios de datos, etc.
42. En la valoración de la información de negocio, se adoptará la opinión del responsable de la información. La información subsidiaria no tendrá más valor que el imputado como soporte de la información de negocio.
43. Activos de servicio. Se identifican y valoran los servicios proporcionados por el sistema a sus usuarios y los servicios existentes o por desarrollar que se utilizarán como soporte.
44. En la valoración de los servicios prestados, se adoptará la opinión del responsable del servicio y se combinará con la valoración de la información manejada. Los servicios subcontratados tendrán la valoración imputada por los activos que los empleen.
45. Se inicia el Plan de Continuidad. En particular se determinan los indicadores
    a. RTO (*Recovery Time Objective*) – tiempo de recuperación del servicio
    b. RPO (*Recovery Point Objective*) – margen tolerable de pérdida de datos
46. Amenazas: se identifican y valoran amenazas generales, independientes de la solución tecnológica que se adopte más adelante.
47. En la identificación se tendrá en cuenta el perfil de los atacantes:
    a. identificación de potenciales atacantes: causas naturales, incidentes o desastres industriales y sujetos internos y externos; en particular hay que considerar los ataques que puedan tener como origen o vía de ataque servicios prestados por otras entidades.
    b. en el caso de amenazas naturales o industriales: características y antecedentes del entorno en el que va a operar el sistema
    c. en el caso de amenazas accidentales: características de los usuarios tales como formación, experiencia, antecedentes, etc.
    d. en el caso de amenazas deliberadas:
        - identificación de las motivación de los atacantes
        - incentivos que pudieran incitar a los atacantes
        - capacidad técnica y económica de los atacantes
48. Las salvaguardas identificadas (ver sección 8) se incorporarán como parte de la especificación del sistema y se transferirá a las fases de desarrollo y aceptación.
49. Algunas salvaguardas pueden tomarse directamente en consideración si ya se encuentran disponibles en el entorno en el que el sistema se desplegará. En este caso se recopilarán y se evaluarán, de forma que los requisitos de seguridad del sistema tengan 2 partes:
    a. base: utilización de salvaguardas disponibles
    b. marginal: nuevas salvaguardas o mejoras de las existentes

7.2. DURANTE LA ADQUISICIÓN / DESARROLLO

50. Activos. El modelo de análisis de riesgos se enriquece paulatinamente con nuevos componentes que heredan su valoración de la de los activos identificados en la fase de especificación.
51. Amenazas. El modelo de análisis de riesgos se enriquece paulatinamente con nuevas amenazas sobre los nuevos componentes. Aparecen nuevas vías de ataque, especializadas en la naturaleza de los activos que se van introduciendo. Para la valoración de las amenazas hay que especializar las facetas técnicas (potencial del ataque) a la naturaleza del componente atacado y la capacidad del atacante.
52. En la identificación se tendrá en cuenta el perfil de exposición de cada activo:
    a. la exposición a amenazas de origen natural o industrial
    b. los posibles mecanismos de ataque
    c. las diferentes vías de ataque
53. En la valoración se tendrá en cuenta:
    a. la caracterización de los posibles atacantes: naturales, industriales y personas
    b. las características del atacante: formación, experiencia, etc
    c. la motivación del atacante: deseo de poseer, deseo de destruir, posibles ganancias económicas
    d. la potencia del atacante (conocimientos, capacidad técnica y económica)
    e. el tiempo requerido para la perpetración del ataque (distinguiendo entre ataques fulgurantes y ataques que requieren tiempo)
54. Las salvaguardas identificadas (ver sección 8) se incorporarán como parte del diseño detallado y se transferirán a la fase de aceptación.
55. Cuando aparecen varias opciones de diseño, se desarrollarán análisis de riesgos paralelos:
    a. uno por opción, con el conjunto de activos que caracterizan cada opción,
    b. procurando la máxima uniformidad en la valoración de las amenazas,
    c. identificando las salvaguardas (ver sección 8) pertinentes en cada caso.
56. Los resultados de los análisis de riesgos paralelos aportan información paralela sobre
    a. las salvaguardas necesarias en uno u otro caso
    b. los niveles residuales de impacto y riesgo
57. Cada modelo paralelo supone unos costes específicos de esfuerzo de desarrollo, operación y mantenimiento.
58. Los análisis paralelos se deben comparar y servir como un criterio de decisión más para optar por una u otra opción.

7.3. DURANTE LA ACEPTACIÓN

59. El análisis de riesgos sirve como índice de las contramedidas que deben ser inspeccionadas. Ver 8.3

7.4. DURANTE LA OPERACIÓN

60. El modelo de análisis de riesgos se utiliza para analizar continuamente el estado de riesgo del sistema, incorporando el mejor conocimiento que en cada momento se tenga de las amenazas posibles:
    a. vulnerabilidades de los componentes, bien reportadas por el fabricante, reportadas por centros de respuesta temprana
    b. incidentes sufridos en el propio sistema o reportados en sistemas similares
    c. variaciones en la motivación de potenciales atacantes (escenarios de alerta)
    d. variaciones en la capacidad del atacante (descubrimiento de nuevas o mejores técnicas de ataque o automatización de técnicas conocidas)
61. La incorporación de un mejor conocimiento del entorno puede llevar a una nueva evaluación del riesgo al que está expuesto el sistema y por tanto a reconsiderar el sistema:
    a. evitando la exposición (por ejemplo, reduciendo el perímetro de ataque, eliminando servicios, eliminando información, etc.); esto incluye la modificación de la configuración segura (fortificación o bastionado) del sistema
    b. aumentando la protección con salvaguardas nuevas o mejores; esto incluye la aplicación de parches de seguridad
62. La variación del perfil de amenaza puede ser desencadenante de un ciclo de mantenimiento.

7.5. EN LOS CICLOS DE MANTENIMIENTO

63. Los ciclos de mantenimiento pueden iniciarse por varios motivos:
    a. cambio de las funcionalidades del sistema: bien por inclusión de nuevas funciones, por modificación de las existentes o por retirada de las mismas
    b. nuevo entorno de servicios subcontratados
    c. nuevos requisitos de seguridad
    d. nuevos perfiles de ataque: cambios en la caracterización de los atacantes o en las vías y mecanismos de ataque
64. En cualquiera de los supuestos citados, se realiza un nuevo ciclo de gestión de riesgos: análisis, evaluación, decisión relativa al tratamiento y, en su caso, implantación de un nuevo sistema de salvaguardas que será objeto de una fase de aceptación previa a la puesta en operación.

7.6. EN SISTEMAS RETIRADOS DE SERVICIO

65. Ver 8.5.

66. Debe realizarse un análisis de riesgos sobre el material retenido teniendo en cuanta el conjunto de información y el equipamiento dispuesto para su custodia. Se identificarán salvaguardas necesarias para garantizar la seguridad de los elementos custodiados.

8. ACTIVIDADES RELACIONADAS CON LA SEGURIDAD

67. A lo largo del ciclo de vida hay una serie de actividades relacionadas con la seguridad del sistema.

8.1. DURANTE LA ESPECIFICACIÓN

68. Ver 7.1.

69. Identificación de quién va a evaluar / certificar / acreditar el sistema, según corresponda.

70. Identificación de los requisitos de evaluación / certificación / acreditación, según corresponda.

71. Planificación de las actividades de evaluación / certificación / acreditación, según corresponda.

8.2. DURANTE LA ADQUISICIÓN / DESARROLLO

72. Ver 7.2.

73. Actualización de la normativa de seguridad en el entorno donde va a desplegarse el nuevo sistema, o creación si no existiera.

74. Actualización de los procedimientos operativos del entorno donde va a desplegarse el nuevo sistema.

75. Creación de los procedimientos operativos del nuevo sistema.

76. Adquisición o desarrollo de las salvaguardas identificadas y aprobadas. Esto incluye los medios de configuración y monitorización.

77. Introducción de mecanismos de registro e indicadores de eficacia y eficiencia.

78. Creación de perfiles de configuración, que pueden ser extensión o particularización de otros perfiles ya existentes.

79. Preparación de las pruebas de aceptación y datos para la ejecución de dichas pruebas.

8.3. DURANTE LA ACEPTACIÓN

80. Ejecución de las pruebas de aceptación aprobadas.

81. Las salvaguardas identificadas en las fases anteriores son inspeccionadas para cerciorarse de que están dispuestas y operativas con la calidad requerida.

82. Deben revisarse:

a. documentación de instalación, configuración, operación y gestión de registros de actividad
b. formación de las personas afectadas en cada aspecto
c. calidad de la implantación
d. registros de actividad
e. generación de alarmas

83. Hay que establecer el marco de seguridad de los servicios externos que se utilicen:
    a. establecer acuerdos de nivel(es) de servicio
    b. acordar las condiciones de inspección de la seguridad de sistemas ajenos
84. Si la política de seguridad lo requiere, se deberá realizar una acreditación formal del sistema previa a su pase a explotación.
85. Se deben realizar pruebas de regresión en el entorno en el que se va a instalar el nuevo sistema de forma que se verifique que no se ven perjudicados otros servicios o información.

8.4. DURANTE LA EXPLOTACIÓN

86. Ver 7.4.
87. Gestión de la configuración. Una configuración determina una forma concreta de operar el sistema, dentro de todas las posibles. La configuración puede variar dinámicamente atendiendo a la evolución del sistema o a las necesidades requeridas en cada momento. La gestión de configuración debe garantizar:
    a. que en todo momento hay una configuración conocida y aprobada
    b. que todo cambio de configuración es debidamente autorizado, incluyendo el impacto en la continuidad de los servicios prestados
    c. que sólo el responsable autorizado puede ejecutar cambios en la configuración del sistema
    d. que tras cada cambio de configuración se aplican las pruebas de regresión aprobadas con el fin de verificar que el sistema mantiene sus funciones y las garantías de seguridad requeridas
    e. que se retienen copias de configuraciones previas a efectos de
        i. retorno en caso de emergencia
        ii. auditoría
88. Mantenimiento y gestión de cambios. Los sistemas evoluciones y están sujetos a cambios en sus componentes: parches, actualizaciones, reemplazo de componentes, incorporación de nuevos componentes y retirada de componentes. El control de cambios es un proceso formal para garantizar:
    a. que en todo momento hay una relación exacta y aprobada de los componentes de un sistema, explicitando su versión

b. que todo cambio de componentes es debidamente autorizado, incluyendo el impacto en la continuidad de los servicios prestados

c. que sólo el responsable autorizado puede ejecutar cambios en la configuración del sistema

d. que tras cada cambio se aplican las pruebas de regresión aprobadas con el fin de verificar que el sistema mantiene sus funciones y las garantías de seguridad requeridas

e. que se retienen copias de los componentes previos a efectos de

i. retorno en caso de emergencia

ii. auditoría

89. Gestión de incidencias. La gestión de incidencias se refiere a las acciones a ejecutar cuando ocurre algo en el sistema fuera de su uso previsto y aprobado. La gestión de incidencias tiene varios objetivos:

a. reacción de emergencia: minimizar el impacto de los incidentes

b. aprender del incidente: analizar el motivo del incidente para prevenir su repetición, optimizar los procedimientos de respuesta o iniciar un proceso de cambio del sistema

c. prevenir incidentes: identificar intentos de ataque, deliberados o accidentales, antes de que sean efectivos

90. La gestión de incidencias es un proceso formal para

a. reportar comportamientos anómalos, reales o supuestos

b. analizar los comportamientos reportados

c. reaccionar con prontitud para devolver el sistema a un estado seguro de operación

d. documentar todas las actuaciones y derivar indicadores de eficacia y eficiencia del sistema

91. Registro de actividad. Es la recopilación del uso que se hace del sistema. Tiene varios objetivos:

a. disuadir a los usuarios de un uso no aprobado

b. permitir el análisis a posteriori de incidentes

c. detectar con antelación usos del sistema no previstos que pudieran ser causa de un incidente

92. El registro de actividad debe ser un proceso formalizado que determina

a. los datos que se registran, que deben reflejar la actividad, pero no la información tratada

b. quienes tienen acceso a los registros, en qué condiciones y con qué trazas

c. el periodo de retención de los datos registrados

d. la destrucción de los registros tras vencer su periodo de retención

93. Auditoría. Actividades de inspección para determinar que el sistema se explota de forma acorde con su función aprobada y de acuerdo a las normas y procedimientos aprobados.

El auditor debe ser persona diferente del usuario y del administrador del sistema. El auditor requiere un perfil específico de "necesidad de conocer" que le centra en los registros de actividad e incidencias, excluyéndole de la información manejada y la participación en los procesos operativos.

8.5. EN LA TERMINACIÓN

94. Durante el proceso de terminación debe identificarse y clasificarse la información según el tratamiento que deba recibir.
95. Se contemplará
    a. la información propiamente dicha,
    b. los registros de actividad o acceso del sistema que se va a retirar,
    c. los programas o aplicaciones para su tratamiento,
    d. la configuración de los sistemas: aplicaciones, equipos informáticos y equipos de comunicaciones,
    e. la documentación del sistema,
    f. los resultados de pruebas y los datos de prueba y
    g. los informes de auditorías / inspecciones / acreditaciones realizadas.
96. La información que deba destruirse se eliminará de forma segura de todos los soportes en los que se encuentre, incluyendo la posible destrucción del soporte si así lo establece la normativa de tratamiento en función de la clasificación de la información.
97. La información que deba retenerse será transferida a los soportes de información que se vayan a emplear para su custodia, etiquetando y protegiendo dichos soportes en función de la clasificación de la información retenida en los mismos.
98. La información desechable sin valor será borrada simplemente. La eliminación debe incluir todas las copias que pudieran existir, en particular copias de seguridad.

9. REQUISITOS DE SEGURIDAD

99. Se relacionan en este apartado una serie de medidas de seguridad que se deben considerar en cada fase a fin de garantizar la seguridad del sistema de información producido.

9.1. DURANTE LA ESPECIFICACIÓN

100. Dimensionado.
101. Perfiles de usuario.
102. Requisitos de identificación y autenticación de usuarios.
103. Garantías o requisitos de confidencialidad.
104. Garantías o requisitos de integridad.
105. Garantías o requisitos de disponibilidad.
106. Requisitos de monitorización (control) y registro (log):

a. de datos de entrada
b. de datos de salida
c. de datos intermedios
d. de acceso a la aplicación
e. de actividad (uso)

9.2. SI SE ADQUIERE SOFTWARE ESTÁNDAR (COTS)

107. Contratos de adquisición y mantenimiento.

9.3. SI SE SUBCONTRATA EL DESARROLLO DE SOFTWARE

108. Ver sección 11.
109. Contratos de adquisición y mantenimiento.
110. Entorno de desarrollo: locales, personas, plataforma y herramientas.
111. Técnicas de programación segura.
112. Gestión de código fuente:
    a. control de acceso y
    b. control de versiones.

9.4. SI SE DESARROLLA SOFTWARE EN CASA

113. Ver sección 11.
114. Condiciones de mantenimiento.
115. Entorno de desarrollo: locales, personas, plataforma y herramientas.
116. Técnicas de programación segura.
117. Gestión de código fuente:
    a. control de acceso y
    b. control de versiones.

9.5. PARA REALIZAR LA ACEPTACIÓN

118. Pruebas de aceptación
    a. inspección de servicios / inspección de código
        i. fugas de información: canales encubiertos, a través de los registros, etc.
        ii. puertas traseras de acceso
        iii. escalado de privilegios
        iv. problemas de desbordamiento de registros (*buffer overflow*)

b. datos de prueba:
    i. si no son reales, deben ser realistas
    ii. si no se puede evitar que sean reales, hay que controlar copias y acceso
c. pruebas funcionales (de los servicios de seguridad)
    i. simulación de ataques
    ii. intrusión controlada (*hacking* ético)
    iii. pruebas en carga

119. Acreditaciones.

9.6. PARA REALIZAR EL DESPLIEGUE

120. Inventario de aplicaciones en operación
121. Gestión de cambios: normativa y procedimientos
122. Establecimiento de claves
123. Formación inicial: administradores, operadores y usuarios

9.7. DURANTE LA OPERACIÓN

124. Normativa y procedimientos de ...
    a. gestión de usuarios
    b. gestión de claves
    c. gestión de registros (*log*)
    d. gestión de incidencias: registro de evidencias, escalado, plan de emergencia y de recuperación
125. Análisis de registros (log): herramientas, criterios, procedimientos, ...
126. Manuales de uso: administradores, operadores y usuarios
127. Formación continua: administradores, operadores y usuarios

9.8. EN LOS CICLOS DE MANTENIMIENTO

128. Normativa y procedimientos de ...
    a. solicitud
    b. aprobación, incluyendo el análisis diferencial de riesgos y, aprobación en su caso de las nuevas medidas
129. Re-certificación del sistema.
130. Re-acreditación del sistema, si procede.

9.9. TERMINACIÓN

131. Destrucción de información
132. Copia y custodia de información
133. Eliminación del código operativo: ejecutable, datos de configuración y cuentas de usuario
134. Eliminación de registros de actividad de sistemas en operación
135. Revisión de las copias de seguridad:
    a. eliminación de información antigua
    b. creación de las copias permitentes para asegurar la información y servicios retenidos
136. Destrucción de soportes de información electrónicos y no electrónicos.

10. DOCUMENTACIÓN DEL SISTEMA

137. La siguiente tabla muestra lo que hay que hacer con los diferentes documentos relativos a la seguridad del sistema a lo largo del ciclo de vida:

Fase	**COS**	**DRES**	**POS**	**análisis de riesgos**
especificación	aprobación	versión inicial, aprobación	identifica procedimientos a desarrollar	versión inicial de alto nivel
Adquisición / desarrollo		actualización incremental, aprobación	desarrollo	elaboración en detalle
Aceptación	se usa como marco de evaluación		verificación aprobación	
Operación			mantenimiento evolutivo	
mantenimiento	se actualiza			
terminación	destrucción o retención según corresponda			

138. La siguiente tabla muestra quién es el responsable de cada actividad relativa a los documentos de seguridad del sistema:

Acción	**COS**	**DRES**	**POS**	**análisis de riesgos**
Elaboración	AOSTIC	AOSTIC	AOSTIC	AOSTIC
Aprobación	AA / ADA	AA / ADA	AA / ADA	AA / ADA
Aplicación	AOSTIC	AOSTIC	AOSTIC	AOSTIC

Acción	COS	DRES	POS	análisis de riesgos
verificación	SSTIC	SSTIC AA / ADA	SSTIC	SSTIC

10.1. ESPECIFICACIÓN

139. Se comienza la documentación de seguridad. En particular se pueden exigir los documentos
    a. DRES – Declaración de Requisitos Específicos del Sistema
    CCN-STIC-202, -204
    b. POS – Relación de Procedimientos de Operación del Sistema
    CCN-STIC-203, -204
    c. COS - Concepto de Operación
    CCN-STIC-207, -204
140. Se comienza el Análisis de los Riesgos
    CCN-STIC-410
141. Se establece el Plan de Calidad (*Quality Assurance Plan*)
142. Se establece el Plan de Auditorías
143. Todos los documentos citados estarán vivos:
    a. sujetos a la evolución del sistema (desarrollo en detalle y ciclos de mantenimiento)
    b. sujetos a un sistema de gestión documental que incluye procesos formales de actualización y aprobación

10.2. ADQUISICIÓN / DESARROLLO

144. Durante esta fase hay que preparar
    a. Plan de aceptación
        - pruebas de aceptación: funcionalidad, carga, robustez, ...
        - pruebas de registro de actividad: normal y ante incidencias
        - pruebas de regresión (si hay servicios previos que pudieran verse afectados)
    b. Plan de formación
        - formación de administradores
        - formación de operadores

- formación de usuarios

c. Plan de configuración y gestión de configuraciones

d. Normativa de seguridad

e. Procedimientos operativos (POS) detallados

10.3. ACEPTACIÓN

145. Informe de aceptación: ejecución de las pruebas.

146. Certificación(es) si procede(n).

147. Acreditación del sistema, si procede.

10.4. DESPLIEGUE

148. Registro de actuaciones:

a. concienciación de los usuarios

b. formación de usuarios, operadores y administradores

c. configuración inicial

d. carga de datos

149. Acuerdos de prestación de servicios con proveedores externos.

10.5. OPERACIÓN

150. Registro de actividad, prestando especial atención a:

a. garantías de integridad frente a manipulaciones

b. garantías de disponibilidad frente a pérdidas, robo y destrucción

c. garantías de control de acceso por "necesidad de conocer"

d. revisión regular de la actividad

151. Registro de incidencias, prestando especial atención a:

a. garantías de completitud: se recogen todos los datos referentes a la identificación, notificación, análisis y actividades de resolución llevadas a cabo

b. garantías de integridad

c. garantías de disponibilidad

d. garantías de control de acceso

152. Informes de auditorías internas

153. Informes de auditorías externas

154. Informes de auditorías realizadas sobre los proveedores externos de servicios

10.6. CICLOS DE MANTENIMIENTO

155. Revisión de la documentación del sistema (ver 10.1)

10.7. TERMINACIÓN

156. Informe de cierre del servicio
157. Informe de retención de datos
158. Análisis de riesgos del sistema de retención de datos
159. Informes de auditoría del sistema de retención de datos

11. EL ENTORNO DE DESARROLLO

160. El propio entorno de desarrollo de sistemas es un sistema de información cuya seguridad debemos garantizar.

11.1. ACTIVOS A CONSIDERAR

161. La información que se maneja
    a. especificaciones y documentación de los sistemas
    b. código fuente
    c. manuales del operador y del usuario
    d. datos de prueba
162. El entorno software de desarrollo:
    a. herramientas de tratamiento de la documentación: generación, publicación, control de documentación, etc.
    b. herramientas de tratamiento del código: generación, compilación, control de versiones, etc.
163. El entorno hardware de desarrollo:
    a. equipos centrales, puestos de trabajo, equipos de archivo, etc.
164. El entorno de comunicaciones de desarrollo
165. Las instalaciones donde se lleva a cabo el desarrollo
166. El personal involucrado:
    a. desarrolladores,
    b. personal de mantenimiento y
    c. usuarios (de pruebas)

11.2. VALORACIÓN DE LOS ACTIVOS

167. Deben considerarse:
    a. integridad del código fuente
    b. confidencialidad del código fuente
    c. autenticidad de las entidades que acceden a la información de desarrollo
    d. trazabilidad de las entidades que acceden a la información de desarrollo
168. Puede ser conveniente considerar
    a. disponibilidad del entorno de desarrollo para atender a incidentes urgentes que exijan revisiones de código fuente o del equipamiento

11.3. AMENAZAS

169. Las habituales que penden sobre los componentes del sistema de desarrollo en busca de dañar los bienes protegidos.
170. Contra la integridad del software producido
    a. software malicioso, en particular troyanos
    b. puertas traseras que eludan el sistema de control de acceso
    c. defectos en el sistema de registro de actividad
    d. bombas lógicas que pudieran causar la destrucción total o parcial del propio software o del sistema en el que trabajan
171. Contra la integridad del sistema producido
    a. inclusión de elementos que faciliten la fuga de información
    b. elementos que pudieran causar la destrucción parcial o total del sistema

11.4. SALVAGUARDAS

172. Las habituales para oponerse a las amenazas sobre el sistema de desarrollo y garantizar su fiabilidad
173. Para garantizar la integridad del software producido
    a. inspecciones de código
    b. certificaciones de seguridad
    c. acuerdos de mantenimiento
174. Para garantizar la integridad del sistema producido
    a. certificaciones de seguridad
    b. acuerdos de mantenimiento

ANEXO A. PRINCIPIOS DE SEGURIDAD

175. Basado en SP800-27 "Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST 2004.

176. **Fundamentos de la seguridad**

177. **Principio P1** – Establezca una política de seguridad sólida como la base para todo diseño.

178. **Principio P2** – Trate la seguridad como parte integral del sistema.

179. **Principio P3** – Delimite claramente la seguridad física y la seguridad lógica, estableciendo la política de seguridad pertinente para cada una de ellas.

180. **Principio P4** – Asegúrese de que los desarrolladores saben desarrollar software seguro.

181. El siguiente gráfico, que se repetirá para los diferentes grupos de principios, permite asociar los principios citados a las fases del ciclo de vida, resaltando
    a. con una marca (√) aquellos puntos donde el principio es digno de ser considerado y
    b. con dos marcas (√√) aquellos puntos donde es fundamental tener en cuanta el principio correspondiente para alcanzar los objetivos seguridad.

	aplicación durante el ciclo de vida				
principio	**iniciación**	**des / adq**	**implemen.**	**oper / mant**	**terminación**
1	√√	√	√	√	√
2	√√	√√	√√	√√	√
3	√√	√√	√	√	
4	√√	√√	√		

182. **Decisiones basadas en el análisis de riesgos**

183. **Principio P5** – Reduzca el riesgo a un nivel aceptable.

184. **Principio P6** – De por seguro que los sistemas externos no son seguros.

185. **Principio P7** – Identifique posibles soluciones de compromiso entre la reducción del riesgo, el aumento de costes y la disminución de la eficacia operativa.

186. **Principio P8** – Aplique medidas de seguridad específicamente orientadas a alcanzar los objetivos de seguridad propuestos por la Dirección.

187. **Principio P9** – Proteja la información mientras se está procesando, mientras está en tránsito, y en sus lugares de almacenamiento.

188. **Principio P10** – Evalúe la necesidad de desarrollar mecanismos de protección propios para alcanzar un nivel adecuado de seguridad.

189. **Principio P11** – Protéjase frente a todos los ataques probables.

	aplicación durante el ciclo de vida				
principio	iniciación	des / adq	implemen.	oper / mant	terminación
5	√√	√√	√√	√√	√√
6	√√	√√	√√	√√	√
7	√√	√√		√√	
8	√	√√	√	√√	√
9	√	√√	√	√√	√
10	√	√√	√	√	
11	√	√√	√√	√	√

190. **Facilidad de uso.**

191. **Principio P12** – Siempre que sea posible, la seguridad de base en estándares abiertos para la interoperabilidad y la portabilidad.

192. **Principio P13** – Use un lenguaje sencillo para expresar los requisitos de seguridad

193. **Principio P14** – Realice un diseño de la seguridad que permita la adopción continua de nuevas tecnologías, habilitando procesos de cambio seguros y lógicos.

194. **Principio P15** – Haga lo imposible por la facilidad de uso.

	aplicación durante el ciclo de vida				
principio	iniciación	des / adq	implemen.	oper / mant	terminación
12	√	√√	√		
13	√√	√√		√√	
14		√√	√	√√	
15	√	√√	√	√√	

195. **Sistemas robustos**

196. **Principio P16** – Implemente la seguridad en varias capas consecutivas. (Asegúrese de que no hay puntos únicos de fallo).

197. **Principio P17** – Diseñe y opere los sistemas TIC de forma que los daños sean limitados y la respuesta flexible pero robusta.

198. **Principio P18** – Ofrezca garantías de que el sistema es seguro frente a las amenazas previstas y sigue siendo robusto cuando se materializan dichas amenazas.

199. **Principio P19** – Limite o mantenga bajo control las vulnerabilidades del sistema.

200. **Principio P20** – Aísle los sistemas de acceso público de los sistemas de misiones críticas.

201. **Principio P21** – Separe los sistemas de tratamiento de información de las infraestructuras de red.

202. **Principio P22** – Diseñe y aplique mecanismos de auditoría para detectar el uso no autorizado y para apoyar la investigación de incidentes.

203. **Principio P23** – Desarrolle y ejercite regularmente los procedimientos de contingencia y de recuperación de desastres para garantizar una adecuada disponibilidad.

	aplicación durante el ciclo de vida				
principio	iniciación	des / adq	implemen.	oper / mant	terminación
16	√	√√	√	√√	√
17	√	√√		√√	
18	√	√√	√	√√	√
19		√√	√	√	
20	√	√√	√	√	
21		√√	√	√√	
22	√	√√	√√	√	
23	√	√	√	√√	

204. **Reduzca las vulnerabilidades**

205. **Principio P24** – Haga lo imposible en pro de la sencillez del sistema..

206. **Principio P25** – Reduzca al mínimo los elementos del sistema en los que hay que confiar.

207. **Principio P26** – Implemente una política de "privilegios, los mínimos necesarios".

208. **Principio P27** – No implemente mecanismos de seguridad innecesarios.

209. **Principio P28** – Asegure la seguridad de la información cuando un proceso termina o un sistema es desmantelado.

210. **Principio P29** – Identifique y prevenga los errores y vulnerabilidades más frecuentes.

	aplicación durante el ciclo de vida				
principio	iniciación	des / adq	implemen.	oper / mant	terminación
24	√	√√	√	√√	
25	√	√√	√	√√	
26	√	√	√	√√	
27	√	√	√	√	√
28		√		√	√√
29		√√	√√	√	

211. **Mientras diseñe la seguridad del sistema, nunca olvide las [redes de] comunicaciones**

212. **Principio P30** – Implemente la seguridad combinando medidas distribuidas física y lógicamente.

213. **Principio P31** – Formule las medidas de seguridad de forma que cubran múltiples dominios de seguridad superpuestos.

214. **Principio P32** – Autentique usuarios y procesos para asegurar las decisiones control de acceso, tanto dentro de un dominio de seguridad, como entre varios.

215. **Principio P33** – Asegúrese de que las identidades se utilizan de forma singular a fin de poder garantizar un conocimiento preciso de quién hizo qué cosa.

	aplicación durante el ciclo de vida				
principio	**iniciación**	**des / adq**	**implemen.**	**oper / mant**	**terminación**
30		√√	√	√	√
31	√	√√	√	√	
32	√	√	√	√√	
33	√	√	√	√√	

ANEXO B. ABREVIATURAS

CCN	Centro Criptológico Nacional
COS	Concepto de Operación del Sistema
COTS	Commercial off-the-Shelf Software
DRES	Declaración de Requisitos Específicos de Seguridad
POS	Procedimientos Operativos de Seguridad
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	System Development Life Cycle
SLC	System Life Cycle
SPD	Seguridad del Proceso de Desarrollo
STIC	Seguridad de las Tecnologías de la Información y Comunicaciones
SSI	Seguridad del Sistema de Información
TIC	Tecnologías de la Información y Comunicaciones

ANEXO C. REFERENCIAS

[Ref.- 1] CCN – Guías STIC, Seguridad en las Tecnologías de Información y Comunicaciones,
https://www.ccn-cert.cni.es/

[Ref.- 2] CCN-STIC-201 Organización y Gestión de la Seguridad TIC

[Ref.- 3] CCN-STIC-202 Estructura y Contenido DRS

[Ref.- 4] CCN-STIC-203 Estructura y Contenido POS

[Ref.- 5] CCN-STIC-204 CO-DRS-POS Formulario

[Ref.- 6] CCN-STIC-204 CO-DRS-POS Pequeñas Redes

[Ref.- 7] CCN-STIC-207 Estructura y Contenido del Concepto Operación de Seguridad (COS)

[Ref.- 8] CCN-STIC-207 Modelo de COS

[Ref.- 9]

[Ref.- 10] NIST Special Publications for security guidance:
http://csrc.nist.gov/publications/nistpubs/

[Ref.- 11] SP 800-64 - Security Considerations in the Information System Development Life Cycle, NIST, Special Publication 800-64 REV. 1, June 2004.

[Ref.- 12] SP 800-27 - Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST, Special Publication 800-27 Rev. A, June 2004.

[Ref.- 13]

[Ref.- 14] AC/35-D/2004 - Primary Directive on Infosec, NATO, 17 June 2002

[Ref.- 15] EPA 2100.5 - System Life Cycle Management Policy, EPA, 2005.

[Ref.- 16]