GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-402)

ORGANIZACIÓN Y GESTIÓN PARA LA SEGURIDAD DE LOS SISTEMAS TIC

DICIEMBRE 2006

Edita:

NIPO: 076-06-216-8

Tirada: 1000 ejemplares
Fecha de Edición: diciembre de 2006
José A. Mañas ha participado en la elaboración y modificación del presente documento y sus anexos.

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

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 2006

Alberto Sáiz
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

1. El mantenimiento y gestión de la seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (TIC), en adelante Sistemas, van íntimamente ligado al establecimiento de una Organización de Seguridad.
2. Dicha Organización queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los Sistemas y la implantación de una estructura que las soporte.

2. OBJETO

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

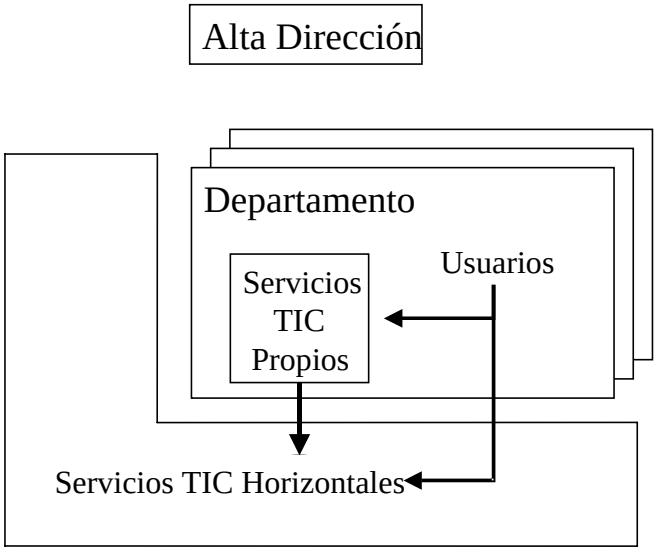
3. ALCANCE

5. La estructura propuesta sirve como guía, pudiendo ser la implantación final diferente en cada Organización. No obstante, las funciones y misiones definidas en esta guía deben ser cubiertas sea cual fuere la implantación final adoptada.
6. La Alta Dirección es responsable de la aprobación de cualquier estructura de seguridad que sustenta al Sistema y que permite el cumplimiento de los requisitos de seguridad necesarios para manejar la información que soporta.

4. ESTRUCTURA TIC DEL SISTEMA

7. Las Organizaciones, públicas o privadas, suelen diferenciar entre una Alta Dirección y una serie de Unidades Operativas o Departamentos[1].

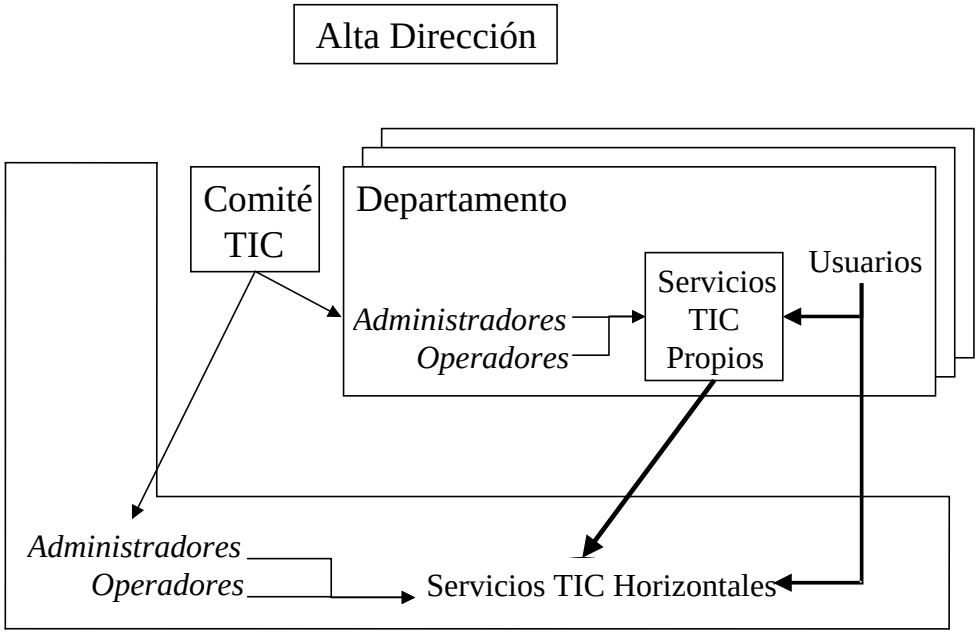
[1] En el ámbito privado es frecuente hablar de “Áreas de Negocio”, mientras en la administración pública se suelen denominar “Servicios”. La terminología puede ser aún mucho más variada en la práctica.



8. Cada Departamento tiene un responsable que informa a la Alta Dirección. Los Departamentos pueden disponer de recursos TIC propios, para sus usuarios, o limitarse a utilizar los servicios TIC horizontales, habitualmente encuadrados en su propio Departamento. Los servicios horizontales son también empleados por los diferentes usuarios.
9. En teoría, los servicios TIC pueden organizarse según un simple esquema donde:
   - Los responsables de los Departamentos imponen las necesidades de la Organización.
   - Los responsables de los Sistemas TIC proporcionan soluciones eficaces y eficientes a las necesidades planteadas.

4.1. COMITÉ TIC

10. En la práctica es muy conveniente coordinar las actividades TIC por medio de un Comité específico en el que:
    - Se coordinan adquisiciones y desarrollos, decidiendo inversiones y controlando el gasto.
    - Se coordinan servicios para evitar disfunciones y maximizar el uso.
    - Este Comité no es técnico, pero recaba del personal técnico de los Departamentos la información pertinente para tomar decisiones.
11. El Comité TIC delega en una red de administradores y operadores TIC las tareas decididas:
    - Los administradores se encargan de la instalación y configuración de aplicaciones, equipos y comunicaciones
    - Los operadores se encargan de la operación continua de los servicios TIC.



5. ORGANIZACIÓN DE SEGURIDAD

12. La Organización de la Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) está constituida por las Autoridades responsables del establecimiento y aplicación de los procedimientos y normas STIC en el Sistema.
13. Dentro de cada Organización STIC se establecen dos tipos fundamentales de estructuras:
    - Estructura de Supervisión: responsable de establecer y aprobar los requisitos de seguridad para el Sistema además de verificar y supervisar la correcta implementación y mantenimiento de los mismos.
    - Estructura de Operación: responsable de la implementación y mantenimiento de los requisitos de seguridad aprobados para el Sistema por la Alta Dirección.

6. ESTRUCTURA DE OPERACIÓN STIC

14. Está formada por
    - Administradores STIC, encargados de la instalación y configuración
    - Operadores STIC, encargados de la operación diaria
    - Usuarios de los sistemas

6.1. ADMINISTRADORES STIC

15. Son los responsables de la implantación, configuración y mantenimiento de los servicios de seguridad relacionados con las TIC.
16. Pudieran ser las mismas personas que cumplen el papel de administradores del sistema o tratarse de personas diferentes.
17. Habrán administradores STIC de servicios horizontales, pudiendo aparecer administradores STIC asignados a áreas que disponen de un Responsable STIC Delegado.

18. En cada Sistema, además tendrán cabida las siguientes figuras:
    - **Administrador del Sistema:** tiene por misión realizar las tareas de administración del Sistema. Son los responsables de la implantación, configuración y mantenimiento de los servicios TIC.
    - **Administrador de bases de datos (DBA):** encargado de las tareas de configuración, mantenimiento y optimización de las bases de datos.
    - **Administrador de Red:** encargado de las tareas de administración de red, siendo responsable de aspectos de seguridad, como enrutamiento y filtrado, relativos a la infraestructura de red (routers / switches, dispositivos de protección de perímetro, redes privadas virtuales, detección de intrusos, dispositivos trampa, etc…).
    - **Administrador de claves criptográficas:** encargado de los procedimientos relacionados con la generación, custodia, explotación y terminación de claves de cifra.
    - Pueden existir otros tipos de administradores encargados de tareas especializadas propias de la organización

19. Ejecutarán los procedimientos que les competan en cuanto a actividad rutinaria.
20. Ejecutarán los procedimientos que les sean asignados en la resolución de incidentes recibidos de los operadores y usuarios.
21. Los administradores deben reportar cualquier inseguridad o debilidad, real o supuesta, que perciban durante la realización de sus tareas. Se informará al Responsable de Seguridad inmediato superior.

6.2. OPERADORES STIC

22. Son los responsables de la operación diaria de los servicios de seguridad relacionados con las TIC.
23. Habrán operadores de servicios horizontales, pudiendo aparecer operadores asignados a áreas que disponen de un Responsable STIC Delegado.
24. Reciben instrucciones e informan a su Responsable de Seguridad inmediato superior.
25. Ejecutarán los procedimientos que les competan en cuanto a actividad rutinaria.
26. Son los primeros receptores de las incidencias que se produzcan, notificadas por usuarios. Resolverán los incidentes que por procedimiento les competan y elevarán al Administrador STIC correspondiente las que les excedan, siempre ajustándose a procedimiento.
27. Los incidentes para las que no exista procedimiento de reacción se trasladarán al Responsable se Seguridad inmediato superior para su tratamiento.
28. Los operadores deben reportar cualquier inseguridad o debilidad, real o supuesta, que perciban durante la realización de sus tareas. Se informará al Responsable de Seguridad inmediato superior.

6.3. USUARIOS

29. Los usuarios se relacionan con los servicios TIC para cumplir sus obligaciones laborales. Son el personal autorizado para acceder al Sistema utilizando las posibilidades que les ofrece el mismo.
30. Los usuarios juegan un papel fundamental en el mantenimiento de la seguridad del Sistema, por lo tanto, es fundamental su concienciación en la seguridad de las TIC ya que en la mayoría de los casos constituyen voluntariamente o involuntariamente la principal amenaza para el propio Sistema.
31. Los usuarios deben estar debidamente informados de sus obligaciones y responsabilidades, así como haber sido instruidos para la labor que desempeñan. En particular deben estar formados en relación a la gestión de mecanismos de identificación y al procedimiento de gestión de incidentes.
32. Los usuarios del Sistema son responsables entre otras cosas de:
    - Conocer los procedimientos que les competen.
    - Informar de cualquier incidente de seguridad o acontecimiento inusual que sea observado durante la operación de su Sistema.

7. ESTRUCTURA DE SUPERVISIÓN STIC

33. La seguridad necesita estar coordinada tanto o más que los servicios TIC.
    - Es conveniente coordinarla para racionalizar el gasto.
    - Es necesario coordinarla para evitar disfunciones que permitan fallas de seguridad al ofrecer el Sistema puntos débiles donde pudieran ocurrir accidentes o se pudieran perpetrar ataques.
34. La Seguridad de las TIC (STIC) debe estar coordinada en un Comité STIC y debe existir un responsable STIC.
35. El Comité STIC no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.
36. El Comité STIC debe estar coordinado con el Comité TIC, siendo lo idóneo que la representación formal de los Departamentos en dichos comités sea la misma persona, sin perjuicio de que la representación real se delegue en especialistas diferentes, que informen a un único representante por Departamento.
37. El Responsable STIC es el Secretario del Comité STIC y como tal:
    - Convoca las reuniones del Comité STIC.
    - Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
    - Es responsable de la ejecución directa o delegada de las decisiones del Comité.

38. Los responsables STIC pueden contar con responsables delegados o intermedios centrados en un Departamento, un aspecto tecnológico o un proyecto concreto, apareciendo:

    – Responsables STIC departamentales.
    – Responsables de la seguridad de determinadas aplicaciones informáticas (bases de datos, sistemas operativos, etc…).
    – Responsables de la seguridad de determinado equipamiento (equipos móviles o sedes remotas).
    – Responsables de la seguridad de las redes de comunicaciones.
    – Responsables de seguridad de un proyecto de adquisición o desarrollo que termina con el proyecto y que luego pasa a los responsables de explotación.
    – Responsables de seguridad en las relaciones con otras Organizaciones.

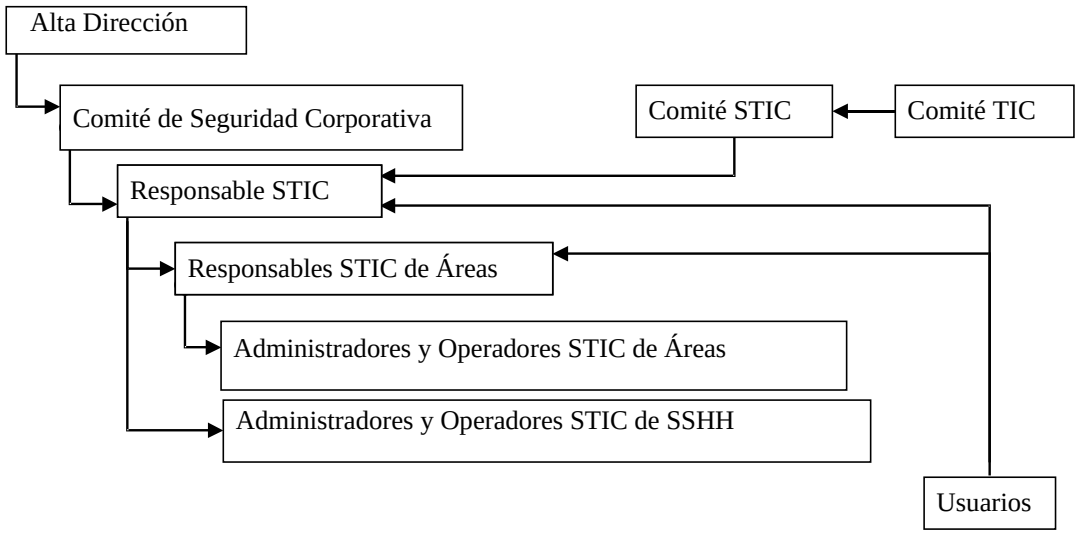
39. En teoría los diferentes roles STIC se limitan a una jerarquía simple: el Comité STIC da instrucciones al Responsable STIC que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la Organización.

40. En la práctica, la situación es menos simple y existe también un flujo inverso en el que administradores, operadores y usuarios transmiten incidencias, debilidades (reales o supuestas) e informes de explotación para que se tomen las medidas preventivas o correctivas que el Comité STIC o el Responsable STIC por delegación, consideren oportunas.

41. El Comité STIC también escuchará las inquietudes de la Alta Dirección y del Comité TIC e informará a todos ellos del estado de seguridad de las TIC.

42. En grandes Organizaciones aparecerán nuevas figuras entre la Alta Dirección y el Comité TIC. Se trata del Comité de Seguridad Corporativa con su propio Secretario, el responsable de seguridad corporativa. El Responsable STIC queda como miembro del Comité de Seguridad Corporativa junto con otros responsables de otras áreas, tales como:

    – Responsables de la seguridad de instalaciones y áreas (seguridad física).
    – Responsables de la seguridad de la información.
    – Responsables de seguridad industrial.
    – Responsables de seguridad operacional.
    – etc.



7.1. ALTA DIRECCIÓN

43. La Alta Dirección es responsable de que la Organización alcance sus objetivos a corto, medio y largo plazo.
44. Debe respaldar explícita y notoriamente las actividades STIC en la Organización.
45. Expresa sus inquietudes al Comité de Seguridad Corporativa a través del Responsable de Seguridad Corporativa.
46. Aprueba la Política de Seguridad de la Organización.
47. Aprueba presupuestos presentados por el Comité de Seguridad Corporativa cuando sobrepasen una cantidad determinada.

7.2. COMITÉ DE SEGURIDAD CORPORATIVA

48. Coordina todas las funciones de seguridad de la Organización.
49. Vela por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
50. Vela por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
51. Es responsable de la elaboración de la Política de Seguridad Corporativa, que será aprobada por la Alta Dirección.
52. Aprueba las políticas de seguridad de las diferentes áreas, que serán presentadas por los correspondientes responsables de seguridad.
53. Coordina y aprueba las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad. Los presupuestos elevados serán transmitidos a la Alta Dirección para su aprobación. Los responsables de seguridad se encargarán de llevar a cabo un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
54. Escucha las inquietudes de la Alta Dirección y las transmite a los Responsables de Seguridad pertinentes. De estos últimos recaba respuestas y soluciones que, una vez coordinadas, son notificadas a la Alta Dirección.

55. Recaba de los Responsables de Seguridad informes regulares del estado de seguridad de la Organización y de los posibles incidentes. Estos informes, se consolidan y resumen para la Alta Dirección.
56. Coordina y da respuesta a las inquietudes transmitidas a través de los Responsables de Seguridad.
57. Debe definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de tareas.

7.3. RESPONSABLE DE SEGURIDAD CORPORATIVA

58. Actúa como Secretario del Comité de Seguridad Corporativa.
59. Convoca al Comité de Seguridad Corporativa, recopilando la información pertinente.
60. Escucha las inquietudes de la Alta Dirección y de los responsables de seguridad y las incorpora al orden del día para su discusión en las reuniones del Comité de Seguridad Corporativa.
61. Es responsable, junto con los diferentes Responsables de Seguridad, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la Organización, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad Corporativo y proponiendo las medidas oportunas de adecuación al nuevo marco.
62. Es el responsable de la toma de decisiones día a día entre las reuniones del Comité de Seguridad Corporativa. Estas decisiones serán respuesta a propuestas de los responsables de seguridad, velando por la unidad de acción y la coordinación de actuaciones, en general y en especial en caso de incidencias que tengan repercusión fuera de la Organización y en caso de desastres.
63. En caso de desastre se incorporará al Comité de Crisis y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la Organización.

7.4. COMITÉ STIC

64. Coordina todas las actividades relacionadas con la seguridad de las TIC.
65. Es responsable de la redacción de la Política de Seguridad de las TIC, que será presentada al Comité de Seguridad Corporativa para su aprobación.
66. Es responsable de la creación y aprobación de las normas que enmarcan el uso de los servicios TIC.
67. Aprobará los procedimientos de actuación en lo relativo al uso de los servicios TIC.
68. Aprobará los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.

69. El Comité STIC se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

    – Grupos de trabajo especializados internos, externos o mixtos.
    – Asesoría externa.
    – Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

7.5. RESPONSABLE STIC

70. Actúa como Secretario del Comité STIC.

71. Es responsable de estar al tanto de cambios de la tecnología y/o del entorno en el que vive la Organización, tales que afecten a la Organización, debiendo informarse de las consecuencias para las actividades STIC, alertando al Comité de STIC y proponiendo las medidas oportunas de adecuación al nuevo marco. Así mismo trasladará al Comité de Seguridad Corporativa las decisiones adoptadas por el Comité STIC.

72. Es responsable de la redacción de los procedimientos de actuación el lo relativo al uso de los servicios TIC. Estos procedimientos se presentarán al Comité STIC para su aprobación. La redacción de los procedimientos puede delegarse en los Responsables STIC de Áreas.

73. Es responsable de la correcta ejecución de las instrucciones emanadas del Comité STIC, ejecución que materializará transmitiendo instrucciones a los administradores y operadores STIC, directamente o a través de los Responsables STIC de Áreas.

74. Es responsable de la presentación regular de informes sobre el estado de seguridad de los servicios TIC. Estos informes se presentarán al Comité STIC. Se elaborará así mismo un informe ejecutivo para ser presentado al Comité de Seguridad Corporativa.

75. Es responsable de la preparación de informes en caso de incidentes excepcionalmente graves y en caso de desastres. Se presentará un informe detallado al Comité STIC y un informe ejecutivo al Comité de Seguridad Corporativa.

76. Es responsable de la elaboración de un Análisis de Riesgos de los sistemas de las TIC, análisis que será presentado al Comité STIC para su aprobación. Este análisis deberá actualizarse regularmente (por ejemplo, cada 6 meses, aunque depende de la criticidad del sistema).

77. Es responsable de que se ejecuten regularmente verificaciones de seguridad según un plan predeterminado y aprobado por el Comité STIC. Los resultados de estas inspecciones se presentarán al Comité STIC para su conocimiento y aprobación. Si como resultado de la inspección aparecen incumplimientos, el Responsable STIC propondrá medidas correctoras que presentará al Comité STIC para su aprobación, responsabilizándose de que sean llevadas a cabo.

78. Es responsable de la elaboración y seguimiento del Plan de Seguridad. En la elaboración de este plan intervendrán los Responsables STIC de Áreas. Este plan será presentado al Comité STIC para su aprobación y al Comité de Seguridad Corporativo para su conocimiento y aprobación.

79. Elaborará para su aprobación por el Comité STIC los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.
80. Es responsable de la identificación de tareas de administración y operación que garanticen la satisfacción de los criterios y requisitos de segregación de tareas impuestos por el Comité de Seguridad Corporativa.
81. Es el interlocutor oficial en comunicaciones con otras Organizaciones, tarea que puede asumir personalmente o delegar según las circunstancias, pero nunca debe haber más de un interlocutor.
82. Es el responsable de coordinar la respuesta ante incidentes que desborden los casos previstos y procedimentados. Es el responsable de coordinar la investigación forense relacionada con incidentes que se consideren relevantes.

7.6. RESPONSABLES STIC DELEGADOS

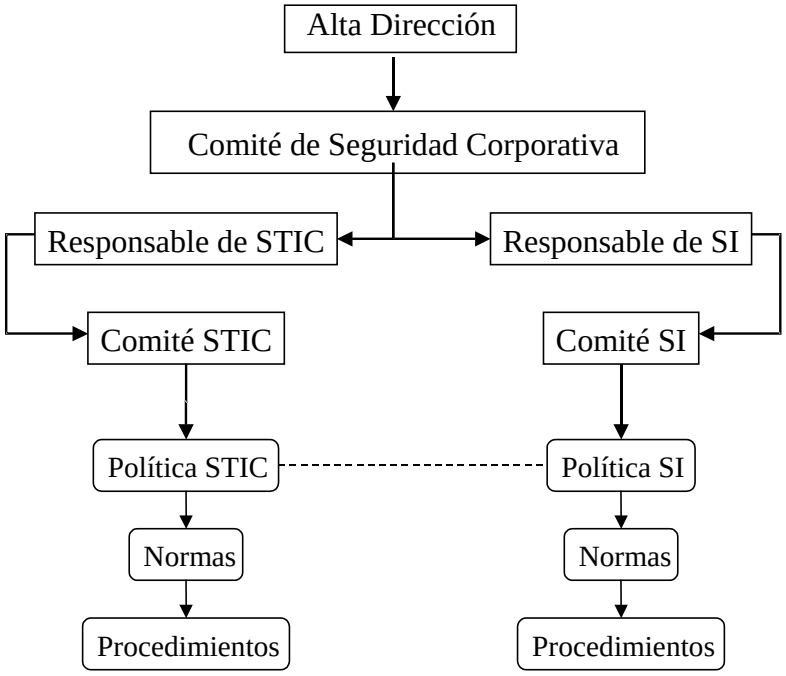
83. En aquellos casos en que existan varios Sistemas que por su complejidad, diversidad, distribución, etc... requieran de una mayor dedicación, se podrán nombrar Responsables STIC Delegados cuyo ámbito de responsabilidad se limitará al área TIC para el que son designados. Estos responsables dependen funcionalmente del Responsable STIC que será, en última instancia, responsable de su adecuado desempeño.
84. Elaborarán procedimientos de actuación en el área que les compete, siguiendo las instrucciones recibidas del Responsable STIC.
85. Elaborarán informes regulares para el Responsable STIC sobre el estado de seguridad del área que les compete.
86. Elaborarán informes detallados para el Responsable STIC de incidencias no rutinarias en el área que les compete.
87. Se responsabilizarán de la adecuada competencia y formación continua de los administradores y operadores asignados a su área de competencia.

8. SEGURIDAD DE LA INFORMACIÓN

88. Aunque la seguridad de la información no es lo mismo que la seguridad de las TIC, la relación entre ambas es fuerte y crítica.
89. La clasificación de la información (como SECRETO, RESERVADO, CONFIDENCIAL o de DIFUSIÓN LIMITADA) no se decide por criterios TIC o STIC. Pero una vez determinada su clasificación, esta implica una serie de requisitos sobre su manipulación mediante servicios TIC. Ver Anexo A.
90. La clasificación de la información de carácter personal (nivel alto, medio o bajo) no se decide por criterios TIC o STIC. Pero una vez determinado su nivel, este implica una serie de requisitos sobre su manipulación en entornos TIC.
91. Otros tipos de clasificación propios de la Organización y derivados de la política propia o de obligaciones regulatorias o sectoriales no se decide por criterios TIC o STIC. Pero una vez determinada su clasificación, esta implica una serie de requisitos dentro del entorno de las TIC.

92. La Política de Seguridad Corporativa recogerá los tipos de clasificación de la información que se maneja. Esta Política de Seguridad Corporativa se desarrollará de forma coordinada en las Políticas de Seguridad de las TIC. Esta coordinación se garantiza en el Comité de Seguridad Corporativa y los Responsables STIC y SI son responsables de su traslado a los correspondientes Comités STIC y SI.

93. El Responsable STIC es responsable del desarrollo de normas y procedimientos que permitan satisfacer los requisitos de los diferentes tipos de información, así como de vigilar su cumplimiento.



94. El Comité STIC se responsabilizará de que la normativa y procedimientos STIC estén alineados con las necesidades establecidas en la política para los diferentes tipos de información.

95. En particular, el Comité STIC aprobará el Documento de Seguridad relativo a información de carácter personal.

9. DOCUMENTACIÓN DE SEGURIDAD

96. La Política de Seguridad Corporativa será elaborada por el Responsable de Seguridad Corporativa y aprobada por el Comité de Seguridad Corporativa y por la Alta Dirección.

97. La Política de Seguridad de las TIC será elaborada por el Responsable STIC y aprobada por el Comité STIC y el Comité de Seguridad Corporativa.

98. Las normas STIC serán elaboradas por el Responsable STIC y aprobadas por el Comité STIC. La elaboración podrá delegarse en los Responsables STIC de Áreas, en particular cuando las normas no sean de carácter general.

99. Los procedimientos STIC serán elaborados por el Responsable STIC y aprobados por el Comité STIC. La elaboración podrá delegarse en los Responsables STIC de Áreas, en particular cuando los procedimientos no sean de carácter general.

100. El Documento de Seguridad, necesario si la Organización trata datos de carácter personal, deberá ser elaborado por el Responsable STIC y aprobado por el Comité STIC, que informará al Comité de Seguridad Corporativa.

10. PROYECTOS

101. La realización de proyectos supone la existencia temporal de dominios de seguridad específicos en los que la seguridad debe ser gestionada de forma acorde a las políticas de seguridad y, además, el resultado de los proyectos debe facilitar una explotación acorde a dichas políticas de seguridad.

102. Para cada proyecto se designará un Responsable de Seguridad del Proyecto. Este responsable reportará a los Responsables de Seguridad STIC y SI, según corresponda.

103. El Responsable de Seguridad del Proyecto se hará cargo de los procedimientos de trabajo durante el desarrollo, en particular del tratamiento de la información empleada: especificaciones, diseños, datos de prueba y manuales de explotación.

104. El Responsable de Seguridad del Proyecto realizará un análisis de riesgos del entorno de desarrollo y del resultado del proyecto, análisis que serán reportados a los Comités STIC y SI para su conocimiento, aprobación y toma de decisiones relativas a las salvaguardas y controles que se empotrarán en el sistema para su adecuada explotación. El Responsable de Seguridad del Proyecto será responsable de la adecuada ejecución de dichas decisiones.

105. El Responsable de Seguridad del Proyecto informará de los incidentes y del progreso en general del proyecto a los Comités STIC y SI.

11. ANEXOS

ANEXO A. CLASIFICACIÓN DE LA INFORMACIÓN

106. La información manejada por un sistema TIC es uno de los bienes críticos a proteger. Como tal, debe estar muy bien definido quién debe hacer qué con qué información. Como no toda la información requiere el mismo tratamiento, y el tratamiento puede ser laborioso y costoso, es muy conveniente establecer niveles de información en función de sus exigencias de seguridad. A esto se le denomina "clasificar la información" (o sea, establecer clases de información) y a la información cuya clase se conoce se la denomina "información clasificada".

107. La información clasificada requiere algunos procedimientos de control:

    a. procedimiento para clasificar la información; que establece quién determina a qué clase pertenece y en base a qué criterios

    b. procedimiento para cambiar la clasificación (incluida su desclasificación); que establece quién puede alterar la etiqueta de una información, en base a qué criterios y dejando qué registro

    c. procedimientos para tratar la información en base a su nivel:

        i. ¿quién puede acceder a la información?, ¿en qué condiciones?, ¿dejando qué registros?

        ii. cifrado de los ficheros y gestión de claves,

        iii. realización de copias y gestión de copias,

        iv. etiquetado de soportes de información,

        v. impresión y gestión de información impresa,

        vi. transmisión (fax, redes, e-mail, ...),

        vii. acceso por terceras partes: autorización, obligaciones contraídas, etc.

        viii. copias de seguridad y gestión de copias,

        ix. destrucción de copias y soportes

108. La clasificación de la información tiene en cuenta las consecuencias que se derivarían de su conocimiento por personas que no deben tener acceso a ella

Nivel	**Características**
confidencial	Su revelación supondría un grave daño: • supondría una ventaja comercial desproporcionada para la competencia • supondría un grave quebranto económico • podría quebrar la capacidad de operar de la Organización • supondría un serio daño a la imagen de la Organización

	• supondría un serio incumplimiento de obligaciones de confidencialidad adquiridas por la Organización con respecto a terceros • supondría un serio incumplimiento de obligaciones legales Ejemplos: secretos industriales, planes de I+D, acuerdos estratégicos,...
difusión limitada	Su revelación causaría daños indeseables: • supondría un ventaja comercial para la competencia • supondría un quebranto económico • dañaría significativamente a la capacidad de operar de la Organización • supondría un cierto daño a la imagen de la Organización • supondría un incumplimiento de las obligaciones de confidencialidad adquiridas por la Organización con respecto de terceros • supondría un incumplimiento de obligaciones legales Ejemplos: datos de carácter personal, salarios, acuerdos con clientes y proveedores, ...
Sin clasificar	En este capítulo se suele dejar la información interna que no es pública, y a la que pueden acceder todos los miembros de la Organización. Su revelación no supondría un gran perjuicio, aunque pudiera ser embarazosa. Ejemplos: listín telefónico, guías de procedimientos internos, borradores de documentos, ...

109. Cuando la información afecta a temas de Estado, suelen aparecer dos categorías superiores:

secreto	• daños graves a la seguridad nacional • incidentes graves internacionales
reservado	• afectaría a la seguridad nacional • afectaría al orden público • causaría incidentes internacionales

110. El sistema de clasificación de la información debe satisfacer una serie de características:

a. ser simple y comprensible
b. determinar claramente los roles de las personas involucradas
c. aplicarse homogéneamente en toda la Organización
d. debe controlarse regularmente su cumplimiento

ANEXO B. PEQUEÑAS ORGANIZACIONES

111. En organizaciones de pequeño tamaño es difícil que pueda diferenciarse el Comité de Seguridad Corporativa del Comité STIC que, típicamente, asumirá igualmente las funciones del Comité de Seguridad de la Información. Es decir, dispondremos de un único Comité de Seguridad.

112. Igualmente, se concentrarán en pocas personas los roles de Responsable de Seguridad. En sitios muy pequeños bastará con el Responsable de Seguridad Corporativa que asumirá todas las responsabilidades.

ANEXO C. ORGANIZACIONES MEDIANAS

113. En organizaciones de tamaño medio se recomienda un punto de diferenciación intermedio entre el recomendado para organizaciones pequeñas y el recomendado para organizaciones grandes.

114. Probablemente se diferencien varios Responsables de Seguridad, siendo típico distinguir entre Seguridad STIC (también denominada Seguridad Lógica) y la Seguridad Física (también denominada Seguridad Pasiva). La aparición de diferentes roles lleva a la necesidad de designar un Responsable de Seguridad Corporativa. Aunque estos papeles deben ser ejercidos por personas diferentes, pueden no requerir dedicación total.

115. Al crecer la organización se segregarán otros Responsables de Seguridad (de la Información, industrial, operacional, etc.)

116. Según crece la Organización de pequeña a grande, se debe ir incorporando el principio de "Segregación" de forma que nunca esté en la misma mano la forma completa de hacer algo. Más concretamente hay que evitar que los administradores STIC disfruten de un poder absoluto sobre el sistema que, hipotéticamente, pudieran llegar a configurar a su antojo.

117. La segregación suele tomar una de estas formas[2]:

- segregación de roles: diferenciar y separar la capacidad de actuar de la capacidad de supervisar, de forma que estas capacidades recaigan en personas diferentes
- segregación de responsabilidades: diferenciar y separar la capacidad de actuar de la custodia de los registros de actividad, de forma que nunca esté en manos de una misma persona la capacidad de gestionar sus propios registros de actividad

118. La segregación sólo es posible si existe un sistema adecuado de identificación y autenticación.

[2] La segregación debe contemplar también que no es la misma persona quien autoriza y ejecuta; pero esta segregación aparece contemplada en la propia organización STIC propuesta como base. En todo caso, este principio debería ser tenido en cuenta en aquellas organizaciones que sigan modelos diferentes.

ANEXO D. GRANDES ORGANIZACIONES

119. En organizaciones suficientemente grandes se recomienda que aparezcan diferenciados todos los roles identificados en el presente documento, separando claramente los diversos Comités de Seguridad Corporativa y STIC, así como los diferentes Responsables STIC.

120. Se recomienda la identificación de áreas donde se puedan designar Responsables STIC Delegados que vertebren cómodamente la ejecución diaria de las tareas del Responsable STIC.

121. La “Segregación” descrita en el anexo C se convierte en imprescindible.

ANEXO E. ABREVIATURAS

SSHH	SERVICIOS HORIZONTALES
SI	SEGURIDAD DE LA INFORMACIÓN
STIC	SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
TIC	TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

ANEXO F. REFERENCIAS

[Ref.- 1] ISO/IEC 13335-1:2004 - Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

[Ref.- 2] ISO/IEC 17799:2005 - Information technology -- Security techniques -- Code of practice for information security management