368

NORMATIVA DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES. ACCIONES DE FORMACIÓN

Javier Candau
Centro Criptológico Nacional

Volver

Javier Candau

Palabras clave

ITIL, ISO20000, Gestión de Capacidad, Pruebas de prestaciones

Resumen de su Comunicación

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.

Este conjunto normativo tiene por objetivo que los responsables de seguridad (Auditores, Supervisores de Seguridad, Administradores de Seguridad...) y Administradores de redes dispongan de las necesarias referencias que les faciliten el cumplimiento de los requisitos de seguridad exigibles a sus Sistemas.

La acción de formación completa a la publicación de la formativa con objeto de incrementar las seguridad en lo sistemas de información de la Administración.

Así, el conjunto normativo se ha estructurado de la siguiente manera:

- *Serie 100 Procedimientos STIC..*
- *Serie 200 Normas STIC.*
- *Serie 300 Instrucciones Técnicas STIC..*
- *Serie 400 Guías Generales. Son recomendaciones a los responsables de seguridad relativas a temas concretos de la seguridad de las TIC (redes inalámbricas, telefonía móvil, cortafuegos, herramientas de seguridad...).*
- *Serie 500 Guías entornos Windows. Estas guías establecerán las configuraciones mínimas de seguridad de los diferentes elementos basados en la tecnología Windows.*
- *Serie 600 Guías otros entornos. Estas guías establecerán las configuraciones mínimas de seguridad de otras tecnologías (HP-UX, SUN-SOLARIS, LINUX, equipos de comunicaciones,...)*

Javier Candau

NORMATIVA DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES. ACCIONES DE FORMACIÓN

1. Introducción

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 a éste 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).

Una de las funciones más destacables que el Real Decreto 421/2004 de 12 de marzo por el que se regula el Centro Criptológico Nacional, asigna al mismo, 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 (y en especial aquel que tenga a cargo información clasificada) lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Este conjunto normativo tiene por objetivo que los responsables de seguridad (Auditores, Supervisores de Seguridad, Administradores de Seguridad, Administradores de redes...) dispongan de las necesarias referencias que les faciliten el cumplimiento de los requisitos de seguridad exigibles a sus Sistemas.

Así, el conjunto normativo se ha estructurado de la siguiente manera:

• Serie 000 Políticas. Desarrollo del RD 421/2004.

• Serie 100 Procedimientos STIC. Establecerán el marco común de actuación en los procesos de acreditación, certificación TEMPEST, gestión de material de cifra y de cualquier otro campo que se considere.

• Serie 200 Normas STIC. Son reglas generales que deben seguirse, o a las que se deben ajustar las conductas tareas o actividades de las personas y Organizaciones en relación con la protección de la información cuando es manejada por un Sistema.

• Serie 300 Instrucciones Técnicas STIC. Atienden a un objetivo de seguridad específico, y serán eminentemente técnicas. Establecerán los requisitos de seguridad generales a implantar en un Sistema y sus interconexiones.

• Serie 400 Guías Generales. Son recomendaciones a los responsables de seguridad relativas a temas concretos de la seguridad de las TIC (redes inalámbricas, telefonía móvil, cortafuegos, herramientas de

Volver

seguridad...).

• Serie 500 Guías entornos Windows. Estas guías establecerán las configuraciones mínimas de seguridad de los diferentes elementos basados en la tecnología Windows.

• Serie 600 Guías otros entornos. Estas guías establecerán las configuraciones mínimas de seguridad de otras tecnologías (HP-UX, SUN-SOLARIS, LINUX, equipos de comunicaciones,...)

• Serie 900 Informes técnicos. Son documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o evaluación.

Las series 100-200-300 son de obligado cumplimiento para los sistemas que manejan información clasificada nacional o internacional, las series 400-500-600 abordan temas concretos sobre seguridad de las distintas tecnologías que se considera pueden ser de mucho interés para tener una aproximación de seguridad a las mismas que minimice las vulnerabilidades de las redes o sistemas.

2. SERIES 100/200/300

Las series 100-200-300 establecen un marco de referencia común para la aplicación / verificación de la seguridad en las distintas fases de diseño, desarrollo y explotación de los sistemas clasificados.

Las tareas a las que se hace referencia son:

• La realización de análisis de riesgos.

• La redacción de la documentación de seguridad requerida en estos (Concepto de operación, requisitos de seguridad y procedimientos de operación).

• Los requisitos de seguridad mínimos requeridos según el nivel de clasificación del Sistema

• Homogeneización de la verificación de seguridad teniendo como objetivo la obtención de resultados repetibles y la generación de los mismos formatos de informe para los diferentes equipos que realicen auditorias de seguridad en el ámbito de la información clasificada.

Se considera que el objetivo de este conjunto formativo son los sistemas que manejan información clasificada por lo que no se detalle el objeto y ámbito de cada documento en esta comunicación.

A continuación se muestra el índice de normas disponibles:

Serie 100: Procedimientos		
CCN-STIC-101 Procedimiento de Acreditación Nacional	Marzo 2005	SIN CLAS.
CCN-STIC-103 Catálogo de Productos Certificados	Noviembre 2000	SIN CLAS.
Serie 200: Normas		
CCN-STIC-201 Estructura de Seguridad	Marzo 2005	SIN CLAS.
CCN-STIC-202 Estructura y Contenido DRS	Abril 2005	SIN CLAS.
CCN-STIC-203 Estructura y Contenido POS	Abril 2005	SIN CLAS.
CCN-STIC-204 CO-DRES-POS Pequeñas Redes	Marzo 2005	SIN CLAS.
CCN-STIC-205 Actividades de seguridad en el ciclo de vida del Sistema	2006	SIN CLAS.
CCN-STIC-206 Análisis de Riesgos a Sistemas Clasificados.	Noviembre 2005	SIN CLAS.
CCN-STIC-207 Estructura y contenido del CONCEPTO OPERACIóN	Diciembre 2005	SIN CLAS.
Serie 300: Instrucciones Técnicas		
CCN-STIC-301 Requisitos STIC	Marzo 2005	DIF. LIMITADA
CCN-STIC-302 Interconexión de CIS	Marzo 2005	DIF. LIMITADA
CCN-STIC-303 Inspección STIC	Marzo 2005	DIF. LIMITADA

3. SERIES 400

Las series 400 proporcionan información sobre diversos aspectos de seguridad y diferentes tecnologías.

Se hace especial énfasis en:

• **Serie 100: Procedimientos CCN-STIC 405.** Algoritmos y parámetros de firma electrónica. El objeto de esta Guía es crear un marco de referencia que establezca las recomendaciones en cuanto a algoritmos criptográficos y parámetros asociados para obtener garantías de seguridad en la utilización de la firma electrónica, tanto por los DSCFE como por los Prestadores de Servicios de Certificación (PSC)

• **CCN-STIC 406. SEGURIDAD EN REDES INALÁMBRICAS BASADAS EN ESTÁNDAR 802.11.** Crear un marco de referencia que establezca las recomendaciones STIC en la implantación y operación de redes inalámbricas basadas en el estándar 802.11.

• **CCN-STIC 407. SEGURIDAD EN TELEFONIA MÓVIL.** Aportar un conocimiento técnico sobre los sistemas de telefonía móvil basados en el estándar GSM (redes D -900 MHz- y E -1800 MHz-), para establecer recomendaciones de seguridad en su utilización, y orientar hacia fuentes de documentación a seguir en caso de mayor necesidad de detalle.

• **CCN-STIC 408. SEGURIDAD PERIMETRAL. CORTAFUEGOS.** El objeto de esta guía es familiarizarse con las distintas tecnologías y estrategias existentes actualmente en el campo de la seguridad perimetral, muy especialmente en el de las tecnologías de cortafuegos, y a partir de aquí ser capaz de seleccionar cuáles de ellas se adaptan mejor a las necesidades concretas de una Organización para poder posteriormente realizar un diseño e implementación que sea lo más óptima posible en términos de arquitectura y procedimientos y que a la vez asegure la perdurabilidad en el tiempo de la seguridad obtenida inicialmente.

• **CCN-STIC 410. ANÁLISIS DE RIESGOS EN SISTEMAS DE LA ADMINISTRACIÓN.** Esta guía presenta un ejemplo ficticio en el ámbito de la administración electrónica. El ejemplo recopila una variedad de elementos típicos en sistemas de información para, por la vía del ejemplo, ayudar a los responsables a llevar a cabo el análisis de riesgos del sistema a su cargo. El ejemplo se ha intentado hacer rico en componentes, sin saturar al usuario. Como metodología se empleará Magerit y como herramienta PILAR.

• **CCN-STIC 430. HERRAMIENTAS DE SEGURIDAD**. Permitir establecer los requisitos relativos a la selección, aprobación, implementación, uso y mantenimiento de las herramientas de seguridad en los Sistemas

• **CCN-STIC 432. SEGURIDAD PERIMETRAL - IDS.** El objeto de esta guía es familiarizarse con las distintas tecnologías y estrategias existentes actualmente en el campo de la seguridad perimetral, muy especialmente en el de las tecnologías de detección de intrusos, y a partir de aquí ser capaz de seleccionar cuáles de ellas se adaptan mejor a las necesidades concretas de una Organización para poder posteriormente realizar un diseño e implementación que sea lo más óptima posible en términos de arquitectura y procedimientos y que asegure la perdurabilidad a largo plazo de la seguridad inicial obtenida

A continuación se muestra índice de guías disponibles y previstas para 2006:

NOMBRE	DISPONIBLE	CLASIFICACIÓN
Serie 400: Guías Generales		
CCN-STIC-401 Glosario / Abreviaturas	2006	SIN CLAS.
CCN-STIC-402 Organización y Gestión TIC	Enero 2006	SIN CLAS.
CCN-STIC-403 Gestión de Incidentes de Seguridad	Marzo 2005	SIN CLAS.
CCN-STIC-404 Control Soportes Informáticos	2006	SIN CLAS.
CCN-STIC-405 Algoritmos y Parámetros de Firma Electrónica	Marzo 2005	SIN CLAS.
CCN-STIC-406 Seguridad Wireless	Marzo 2005	SIN CLAS.
CCN-STIC-407 Seguridad en Telefonía Móvil	Abril 2005	SIN CLAS.
CCN-STIC-408 Seguridad Perimetral - Cortafuegos	Mayo 2005	SIN CLAS.
CCN-STIC-410 Análisis de Riesgos en Sistemas de la Administración	Octubre2005	SIN CLAS.
CCN-STIC-430 Herramientas de Seguridad	Marzo 2005	SIN CLAS.
CCN-STIC-431 Herramientas de Análisis de Vulnerabilidades	2006	SIN CLAS.
CCN-STIC-432 Seguridad perimetral - IDS	Abril 2005	SIN CLAS.
CCN-STIC-435 Herramientas de Monitorización del Tráfico	2006	SIN CLAS.

4. SERIES 500

Esta serie es conjunto de normas desarrolladas para entornos basados en el sistema operativo Windows de Microsoft siendo de aplicación para la Administración y de obligado cumplimiento para los Sistemas que manejen información clasificada Nacional.

Esta serie CCN-STIC-500 se ha diseñado de manera incremental de tal forma que dependiendo del Sistema se aplicarán consecutivamente varias de estas guías. Por ejemplo, si se trata de securizar un puesto de trabajo Windows XP con Microsoft Office 2003 se deberán seguir las siguientes guías:

• CCN-STIC-501B Windows XP Professional SP2.

• CCN-STIC-513 Aplicaciones Cliente Windows (Office 2003 y Office XP).

Las configuraciones se han diseñado para ser lo más restrictivas posible indicándose dentro del documento aquellas situaciones que pueden causar problemas con algún servicio. En algunos casos, dependiendo de la funcionalidad requerida en el equipo, será necesario modificar la configuración aquí planteada para permitir que se proporcionen los servicios no incluidos.

En concreto este conjunto de documentos incluyen:

• Mecanismos para automatizar la instalación: en el proceso de instalación se incorporan la mayor parte posible de configuraciones.

• Mecanismos para aplicar configuraciones: para implementar de forma automática las configuraciones de seguridad susceptibles de ello.

• Guía paso a paso: que permita establecer las configuraciones de seguridad en los diferentes puesto cliente independiente.

• Lista de comprobación: con objeto de que sea posible verificar el grado de cumplimiento de un equipo cliente con respecto a las configuraciones de seguridad aquí proporcionadas.

Se hace especial énfasis en las guías:

• CCN-STIC 501 A/B. Seguridad en Windows XP SP2. Por tratarse de un sistema operativo desplegado en muchos entornos administrativos tanto como cliente independiente como perteneciente a un Dominio.

• CCN-STIC 502. Seguridad en Aplicaciones Cliente Windows (Web y correo electrónico) Por ser las aplicaciones de correo y navegación Web servicios asociados al puesto de trabajo de cualquier usuario.

• CCN-STIC 503 A/B. Seguridad en Windows 2003 SERVER. Ya que se trata de un sistema operativo que tanto como servidor independiente, servidor miembro y controlador de Dominio está desplegado en muchos entornos administrativos soportando las tareas de identificación / autenticación (con directorio activo) y otras funciones críticas.

• CCN-STIC 504. Seguridad para Internet Information Services 6.0. Al ser los servicios Web muy demandados ya sea en entornos corporativos (Intranet) o para publicar información de unterés general en Internet..

• CCN-STIC 508. Seguridad en Windows 2000 (Cliente Independiente) . Por ser un sistema operativo de uso todavía común en muchos entornos de la Administración.

No se recomienda se utilice Windows 95/98/Millenium o XP Home por no incluir todas las funcionalidades de seguridad de la versión profesional de esta tecnología.

Existen guías de configuración de seguridad del S.O. Windows NT aunque no reincluyen en esta colección por estar fuera del mantenimiento y actualización del fabricante.

A continuación se muestra índice de guías disponibles y previstas para 2006:

Serie 500: Guías para Entornos Windows		
CCN-STIC-501A Seguridad en Windows XP SP2 (Miembro de Dominio)	2005	SIN CLAS.
CCN-STIC-501B Seguridad en Windows XP SP2 (Cliente Independiente)	2005	SIN CLAS.
CCN-STIC-502 A/B Seguridad para aplicaciones Cliente Windows. Navegador y correo electrónico	2006	SIN CLAS.
CCN-STIC-503A Seguridad en Windows 2003 Server (Controlador de Dominio y Servidor Miembro))	2005	SIN CLAS.
CCN-STIC-503B Seguridad en Windows 2003 Server (Servidor Independiente)	2005	SIN CLAS.
CCN-STIC-504 Seguridad en Internet Information Server	2005	SIN CLAS.
CCN-STIC-505 Seguridad para Microsoft SQL Server	2006	SIN CLAS.
CCN-STIC-506 Seguridad para Microsoft Exchange Server 2000	2006	SIN CLAS.
CCN-STIC-507 Seguridad ISA Server	2006	SIN CLAS.
CCN-STIC-508 Seguridad en Clientes W2000 (Cliente Independiente)	2005	SIN CLAS.
CCN-STIC-514 Seguridad para Microsoft Exchange Server 2003	2006	SINCLAS

5. SERIES 600

De la experiencia en auditorias de seguridad del Centro Criptológico Nacional se detecta que las configuraciones aplicables a distintas tecnologías que normalmente proporcionan servicios básicos en los sistemas de la Administración están normalmente por defecto.

Esta serie es un conjunto de guías que tienen por objetivo facilitar la aplicación de seguridad enlas mismas.

Así Se hace especial énfasis en:

CCN-STIC 60X. Seguridad en HPUX. El objeto de este documento es presentar la guía de configuración de seguridad para los sistemas HPUX.

CCN-STIC 61X. Seguridad en entornos LINUX. El objeto de este documento es proporcionar a los administradores de sistemas una guía que les permita configurar de forma segura los servidores/clientes que ejecuten distintos entornos LINUX (Suse; Red-Hat, Debian...).

CCN-STIC 62X. Seguridad en entornos SUN-SOLARIS. El objeto de este documento es presentar la guía de securización para los sistemas Sun Solaris según la funcionalidad con la que se van a utilizar.

CCN-STIC 63X. Seguridad en entornos de BBDD. El objeto de este documento es presentar la guía de securización para las bases de datos. Actualmente solo existen recomendaciones para BBDD ORACLE.

CCN-STIC 64X. Seguridad en equipos de comunicaciones Nivel 2/3 capa OSI. En estos documentos se discuten y analizan los diferentes aspectos de la seguridad en los router / switches, como elementos básicos en la comunicación de redes IP, y en particular los del proveedor Cisco / enterasys (disponibles actualmente), por ser ampliamente usados en redes de la Administración. Si bien los ejemplos de comandos y algunos aspectos en particular se refieren particularmente a estos fabricantes y a algunas versiones software, los conceptos cubiertos en estos documentos son válidos para cualquier tipo de equipo de comunicaciones router/switch de cualquier proveedor.

CCN-STIC 65X/66X.... Seguridad en otras tecnologías. El objeto de estos documento es presentar buenas prácticas de seguridad en otras tecnologías EWB, Correo, aplicaciones....

A continuación se muestra índice de guías disponibles y previstas para 2006:

NOMBRE	DISPONIBLE	CLASIFICACIÓN
Serie 600: Guías para Otros Entornos		
CCN-STIC-601 Seguridad HP-UX v 10.20	Diciembre 2003	SIN CLAS.
CCN-STIC-602 Seguridad HP-UX 11i	Marzo 2004	SIN CLAS.
CCN-STIC-610 Seguridad Red Hat Linux	2006	SIN CLAS.
CCN-STIC-611 Seguridad SUSE linux	Abril 2005	SIN CLAS.
CCN-STIC-612 Seguridad DEBIAN	2006	SIN CLAS.
CCN-STIC-621 Seguridad Sun-Solaris 8.0	Septiembre 2004	SIN CLAS.
CCN-STIC-622 Seguridad Sun-Solaris 9.0 para ORACLE 8.1.7	Agosto 2005	SIN CLAS.
CCN-STIC-623 Seguridad Sun-Solaris 9.0 para ORACLE 9.i	Agosto 2005	SIN CLAS.
CCN-STIC-624 Seguridad Sun-Solaris 10 para ORACLE 9.2	Septiembre 2005	SIN CLAS.
CCN-STIC-625 Seguridad Sun-Solaris 10 para ORACLE 10g	Septiembre 2005	SIN CLAS.
CCN-STIC-631 Seguridad en BD Oracle (solaris)	Diciembre 2005	SIN CLAS.
CCN-STIC-641 Seguridad en Eq. Comunicaciones. Routers de CISCO	Diciembre 2005	SIN CLAS.
CCN-STIC-642 Seguridad en Eq. Comunicaciones. Switches ENTERASYS	Diciembre 2005	SIN CLAS.
CCN-STIC-650 Seguridad en VPN	2006	SIN CLAS.
CCN-STIC-671 Seguridad de Servidor WEB APACHE	Junio 2005	SIN CLAS.

6. SERIES 900

Este conjunto de guías tienen por objetivo facilitar el empleo de algún tipo de producto de seguridad o producto.

A continuación se muestra índice de guías disponibles y previstas para 2006:

Serie 900: Informes Técnicos		
NOMBRE	**DISPONIBLE**	**CLASIFICACIÓN**
CCN-STIC-910 Borrado Seguro Datos	2006	SIN. CLAS
CCN-STIC-920 Seguridad en PDA,S. HP-IPAQ 6340 V2.0	2006	SIN. CLAS
CCN-STIC-951 Recomendaciones empleo Herramienta ETHEREAL	2006	SIN. CLAS
CCN-STIC-952 Recomendaciones empleo Herramienta NESSUS	2006	SIN. CLAS

7. PILAR / NORMATIVA CCN-STIC

La herramienta PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos) tiene como objetivo permitir a un usuario realizar un análisis y gestión de riesgos sobre un Sistema de las Tecnologías de la

Información y Comunicaciones (TIC) en un plazo breve de tiempo y de una forma intuitiva. El objetivo último es evaluar la seguridad del Sistema de las TIC considerándose de mucha utilidad para el personal directivo de los organismos responsables de los sistemas de información. La última actualización de la herramienta se puede descargar desde la siguiente dirección http://www.ar-tools.com/pilar/.

Actualmente dispone de un catálogo de aproximadamente 2000 salvaguardas.

Para 2006 se intentará incrementar este catálogo con la información proporcionada por las guías de seguridad.

8. ACCIONES DE FORMACIÓN / NORMATIVA CCN-STIC

El hecho de que gran parte de las actividades humanas sea cada vez más dependiente de las Tecnologías de la Información y las Comunicaciones (TIC) hace que la seguridad juegue un papel decisivo en cualquier Organización que trabaje con sistemas de información.

Entre las medidas de la protección de la información se pueden encontrar:

• Medidas de carácter físico: tratan de proteger al Sistema y a su entorno de amenazas físicas externas a los mismos.

• Medidas técnicas: pretenden proteger tanto el software como los datos (seguridad lógica).

• Medidas de carácter organizativo: se ocupan de dictar controles de índole administrativo y organizativo.

• Medidas de protección legal: comprenden el conjunto de disposiciones legales adoptadas por los poderes legislativo o ejecutivo para proteger la información y los sistemas que la soportan.

Dentro de este marco, el factor humano es el elemento más vulnerable. La ingeniería social es tan efectiva que raras veces hay que recurrir a un ataque técnico, además constituye el ataque más fácil y menos complejo.

No todos los ataques con éxito basados en ingeniería social son debidos a la ingenuidad de los empleados, la mayoría de los casos se debe a la ignorancia de buenas prácticas de seguridad y a la falta de concienciación por parte de los usuarios del Sistema. Cuanto más sofisticadas son las tecnologías empleadas para proteger la información, los ataques se van a centrar más en explotar las debilidades de la persona.

El usuario del Sistema constituye el mejor aliado para la seguridad ya que puede detectar problemas, totalizan de largo más de la mitad de la información del Sistema y asumen responsabilidades. El problema es que los usuarios necesitan ser formados/mentalizados y hay que saber como hacerlo.

De lo contrario, el usuario se erige como el peor enemigo por el desconocimiento de buenas prácticas de seguridad, por su afán de modificar las cosas y ser un componente inconformista.

Hay tres pilares fundamentales en los que se basa la Seguridad de las Tecnologías de la Información y las Comunicaciones:

- La tecnología.
- Los procedimientos.
- Las personas

Hasta ahora, las Organizaciones se han preocupado por invertir grandes cantidades de dinero y esfuerzos en tecnologías de seguridad y en la definición de procedimientos pero han dejado a un lado a las personas haciendo de éstas el eslabón más débil de la cadena de seguridad.

Los diferentes usuarios de los Sistemas deben asumir su responsabilidad en la protección de la confidencialidad, integridad y disponibilidad de los activos (información) de la Organización y comprender que esto no es sólo competencia de los especialistas en seguridad.

Se hace necesaria, por tanto, la implementación de un programa apropiado de formación debidamente apoyado por políticas corporativas y con un adecuado proceso de seguimiento y actualización.

El programa de mentalización y sensibilización debe perseguir dejar claro no sólo cómo proteger los Sistemas sino también porqué es importante su protección y cómo los usuarios se convierten en la primera barrera de seguridad para ellos. La implementación del programa ayuda a minimizar los costos ocasionados por los incidentes de seguridad dado que actúa directamente sobre uno de los eslabones más débiles en la cadena de seguridad, los usuarios.

Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones es una de las principales funciones asignadas al el Centro Criptológico Nacional (CCN) por el Real Decreto 421/2004 que viene a desarrollar lo ya indicado en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional Inteligencia.

Con tal fin el Centro Criptológico Nacional ha elaborado un Plan de Formación en Seguridad de las Tecnologías de la Información y Comunicaciones (STIC), dirigido al personal especialista de la Administración:

- Cursos Informativos y de Concienciación en Seguridad
- Jornada de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)
- Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)
- Cursos Básicos de Seguridad
- Curso Básico STIC - Entornos Windows
- Curso Básico STIC - Entornos Linux
- Curso Básico STIC - Infraestructura de Red
- Curso Básico STIC - Bases de Datos
- Cursos Específicos de Gestión en Seguridad
- Curso Gestión STIC
- Curso Especialidades Criptológicas
- Cursos de Especialización en seguridad
- Curso Acreditación STIC - Entornos Windows
- Curso Acreditación STIC - Entornos Unix
- Curso Acreditación STIC - Entornos Linux (Servicio de Correo)
- Curso Acreditación STIC - Entornos Linux (Servicio Web)
- Curso STIC - Cortafuegos
- Curso STIC - Detección de Intrusos
- Curso STIC - Redes Inalámbricas
- Curso STIC - Herramientas de Seguridad
- Curso STIC - Verificaciones de Seguridad
- Curso STIC - Inspecciones de Seguridad

La normativa de seguridad es de aplicación a todo este programa de formación y en especial, las guías de seguridad son de aplicación a los cursos de especialización de seguridad expuestos arriba.

9. CONCLUSIONES

A lo largo de las páginas anteriores se ha cubierto someramente la propuesta de guías de seguridad a desarrolladas y a desarrollar por el Centro Criptológico Nacional.
El objetivo que se intenta lograr con las diferentes series es:

• SERIES 100/200/300. Establecen un marco de referencia común para la aplicación / verificación de la seguridad en las distintas fases de diseño, desarrollo y explotación de los sistemas clasificados. Su objetivo son los sistemas que manejan información clasificada.

• SERIES 400. Son recomendaciones a los responsables de seguridad relativas a temas concretos de la seguridad de las TIC (redes inalámbricas, telefonía móvil, cortafuegos, herramientas de seguridad...).

• SERIES 500. Estas guías establecerán las configuraciones mínimas de seguridad de los diferentes elementos basados en la tecnología Windows.

• SERIES 600. Estas guías establecerán las configuraciones mínimas de seguridad de otras tecnologías (HP-UX, SUN-SOLARIS, LINUX, equipos de comunicaciones,...).

La posibilidad que la aplicación de configuraciones de seguridad que minimicen las vulnerabilidades de los sistemas y que estas se puedan realizar de una manera lo más sencilla posible con una compresión de las acciones que se realizan es fundamental para un completo control por parte del personal de administración / seguridad de os sistemas que se tienen a su cargo.

En caso de subcontratación de servicios a consultoras externas, estas guías pueden servir de referencia común para cual es la aproximación de seguridad del organismo que lo contrate y establecer un marco de referencia que permita una identificación más clara de los objetivos de seguridad.

La formación con el apoyo de la normativa es una oportunidad que tienen las diferentes administraciones de proporcionar unos servicios más seguros.