ANEXO A

LÍNEAS DE ACCIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

LÍNEAS DE ACCIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

JAVIER CANDAU ROMERO

Línea de acción 1: Desarrollo del Esquema Nacional de Seguridad

Como se ha descrito anteriormente el ENS acaba de nacer. Los organismos tienen un plazo de 12 meses, en principio hasta enero de 2011 para su completa implementación.

Se considera que para los sistemas categorizados en nivel ALTO las medidas de seguridad a implementar podrían necesitar a un tiempo de implantación mayor por lo que tras la presentación del correspondiente plan de adecuación, el RD permite una prórroga de hasta 48 meses (enero del 2014).

Este tiempo de aplicación es una muestra del nivel de exigencia que conlleva el cumplimiento del esquema. Además, para cumplir eficazmente muchas de las medidas de seguridad es necesario formar personal especialista, realizar los análisis de riesgos pertinentes, supervisar la implantación de las medidas mediante auditorias, adquirir tecnología o contratar servicios especializados. Por ello su aplicación requerirá una inversión extraordinaria continuada en el tiempo que no está contemplada en la publicación del Real Decreto y que queda bajo responsabilidad de los diferentes organismos.

Sería necesario por tanto, dentro de la estrategia nacional de ciberseguridad, impulsar mediante las dotaciones presupuestarias que se estimen convenientes proyectos que faciliten esta implantación.

Además se deben impulsar programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas.

Línea de acción 2: Gestión homogénea de las redes de las AAPP

Para poder gestionar la amenaza de una manera adecuada se debería realizar una gestión única desde el punto de vista de seguridad de las redes de las AAPP. Las interconexiones con INTERNET deben ser las mínimas posibles y deben cumplir los mismos requisitos de seguridad (este aspecto se trata parcialmente en el ENS).

Actualmente la gestión y la seguridad de las redes corporativas es responsabilidad de cada uno de los Ministerios, CCAA, organismos autónomos y Ayuntamientos. Siendo responsabilidad de cada organismo la seguridad tanto de su red corporativa como de las interconexiones.

Para ello y a través del Consejo Superior de Administración Electrónica, la conferencia sectorial de las AAPP y la conferencia nacional de la Administración local se deben alcanzar unos requisitos mínimos de interconexión que aseguren una defensa homogénea.

Línea de acción 3: Sistemas de protección de las redes de las AAPP

Para garantizar el nivel de seguridad adecuado en los sistemas de las administraciones públicas es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Se debe impulsar la entrada en servicio de sistemas de Alerta Temprana para la detección rápida de incidentes y anomalías dentro de las redes de la Administración. Estos sistemas, basado en el análisis y correlación de registros (logs) generados por las herramientas de seguridad instaladas en las citadas redes, permite detectar de manera proactiva cualquier anomalía y ataque analizando el tráfico que circula en y entre los diferentes Ministerios y Organismos.

Por otro lado es del máximo interés la potenciación de los sistemas similares que permitan monitorizar en tiempo real el tráfico entrante y saliente de las salidas de Internet de los diferentes organismos, recolectando información de seguridad relevante y proporcionando información de los ataques recibidos. Se debe considerar además, la inclusión de los sistemas de las empresas que manejan infraestructuras críticas en estos programas.

Entre otros beneficios, los sistemas de alerta temprana permiten:

– Ofrecer una visión en tiempo real del estado de la seguridad de las redes monitorizadas, relacionando la información proporcionada por los diferentes sensores y disponiendo de estadísticas que permitan medir la eficacia de las medidas de seguridad.
– Disponer de información técnica que permita la implantación de medidas de seguridad adicionales que impidan que ataques similares se vuelvan a reproducir.
– Detección de patrones de ataque comunes a diversas organizaciones que permitan aplicar de forma eficaz medidas de contención y eliminación de los mismos.

La implantación de esta línea de acción será muy costosa en recursos humanos y económicos y su aplicación es muy prolongada en el tiempo, por ello se debe considerar como un servicio horizontal al mayor número de organizaciones posible.

Línea de acción 4: Desarrollo del PPIC ante ciberamenazas

Esta línea de acción se encuentra en su fase inicial pues el borrador de normativa solo lo contempla marginalmente. Sería necesario, por tanto, impulsar la colaboración entre el CNPIC y los organismos especializados en la ciberamenaza en los siguientes campos:

– Gestión de incidentes de seguridad para un tratamiento adecuado de los ciberataques sobre infraestructuras críticas.
– Actualización de información sobre vulnerabilidades tanto de sistemas SCADA como de otros sistemas que soporten estas infraestructuras.
– Cumplimiento por parte de los operadores de los estándares de seguridad que se definan como mínimos.
– Realización de análisis de riesgos y auditorias de seguridad que establezcan los niveles de riesgos a los que están sometidos estos sistemas.

La coordinación debe llevarse a cabo a través de las estructuras que se establezcan al efecto. Sería del máximo interés que estos operadores que manejan infraestructuras críticas se acojan a servicios de alerta temprana similares a los descritos en la línea de acción nº 3.

Línea de acción 5: Programa de formación y concienciación

Según establece la disposición adicional primera del ENS, el personal de las AAPP recibirá la formación necesaria para garantizar el co-

nocimiento de las medidas de seguridad a implementar. Es necesario por tanto un esfuerzo continuado en acciones de formación del personal encargado de su aplicación.

Además serán necesarias acciones de concienciación a todos los usuarios para que conozcan y en la medida de lo posible reduzcan las nuevas amenazas a las que nos enfrentamos y que por su naturaleza cambiante se deben plantear a largo plazo.

Por tanto se deben implicar diversos organismos y se deben desarrollar actividades de formación en seguridad horizontales en los diferentes cursos de acceso a las Administraciones Públicas, programas de sensibilización dirigidos a personal que maneje información sensible o clasificada en sistemas, a usuarios de todas las AAPP que estén implicados en servicios de administración electrónica, a empresas que gestionen infraestructuras criticas con sistemas informáticos que los soporten y especialmente a la alta dirección de los diferentes organismos para que proporcione el apoyo necesario a las actividades de seguridad.

También se debe potenciar el desarrollo de cátedras y jornadas en Universidades y otros centros de formación que traten la seguridad en los sistemas de información y comunicaciones.

Con estas acciones, a largo plazo, se debería construir una cultura de seguridad en el manejo de los sistemas de información que actualmente es prácticamente inexistente en ciudadanos, empresas y administraciones.

Línea de acción 6: Coordinación de recursos en la respuesta ante incidentes de seguridad

El intercambio fluido de información es fundamental para mitigar los daños causados por los ataques desde el ciberespacio al permitir una pronta identificación de éste y la ejecución temprana de una respuesta rápida y adecuada.

Con esta línea de acción se pretende aumentar las capacidades de inteligencia y defensa por ello, se deben mejorar los procedimientos de intercambio de información entre los centros de operación y los centros de respuesta ante incidentes. Es del máximo interés la realización de ejercicios que demuestren la efectividad de estos canales de coordinación.

Esta coordinación se podrá mejorar si se crean estructuras de ciberdefensa similares a las de otras naciones en las que se integren las capacidades de respuesta ante incidentes de seguridad existentes actualmente.

Línea de acción 7: Coordinación de esfuerzos de investigación y desarrollo

Observando la rapidez con la que evolucionan los sistemas, la continua aparición de vulnerabilidades que suponen una amenaza para la integridad de éstos, y la creciente dependencia de la sociedad respecto a las tecnologías de la información, se hace necesario el desarrollo de programas, estrategias y tecnologías que proporcionen unos niveles de seguridad superiores a las que ofrecen los actuales sistemas.

En España, además, una de las deficiencias más importantes que se detectan es la escasez de empresas que desarrollen tecnologías de seguridad. Este vacío, empieza a ser crítico cuando se trata del desarrollo de productos de cifra.

Para poder disponer de autonomía en el empleo de las estas tecnologías es necesario potenciar la coordinación en la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación de productos de seguridad, especialmente si incluyen cifra.

Esta iniciativa se considera crítica para evitar redundancias y para identificar huecos o deficiencias en estos esfuerzos así como para intentar evitar el empleo de tecnologías de terceros países en aspectos tan críticos como la protección de la información.

Es necesario por tanto impulsar el desarrollo de sistemas más seguros, involucrando para ello al sector privado por su papel en muchas de las infraestructuras críticas nacionales.

Línea de acción 8: Potenciar la colaboración internacional

Por la naturaleza transnacional de la amenaza y del ciberespacio hace necesario una cooperación internacional para hacerle frente. Se deben impulsar la firma de acuerdos en materia del ciberdelito y crear unas normas de comportamiento en el ciberespacio consensuadas por todas las naciones que pueda facilitar la atribución de los ataques.

Línea de acción 9: Potenciar el empleo de productos de seguridad certificados

Aunque el ENS contempla que las AAPP valoraran positivamente el empleo de productos que tengan sus funciones de seguridad certificadas, este aspecto no es de obligado cumplimiento para poner cualquier sistema en servicio.

Es necesario que las tecnologías y productos hayan sido revisadas desde el punto de vista de seguridad. Estos procesos son costosos y difíciles de abordar especialmente para pequeñas y medianas empresas. Por tanto se deben impulsar programas que faciliten esta actividad que indudablemente elevará la calidad de los mismos y mejorará la calidad de los productos que consigan esta certificación.

Esta acción permitiría que los productos desarrollados nacionalmente puedan competir en el ámbito internacional pues normalmente poseer una certificación según un estándar internacional (Common Criteria (1) por ejemplo) es requisito imprescindible para poder acceder a cualquier concurso internacional.

Línea de acción 10: Mejoras de seguridad en los sistemas clasificados

Estas redes manejan la información clasificada y sensible de la Administración para conducir Operaciones de Mantenimiento de Paz, Operaciones Militares, actividades diplomáticas, actividades contraterroristas, actividades de las FCSE o de inteligencia así como las actividades de seguridad interior. La integridad de estas redes es crítica y cualquier incidente declarado en las mismas puede dañar de forma grave la soberanía nacional.

Se deben reforzar por tanto las medidas de seguridad de estos adaptando las salvaguardas y procedimientos existentes a la evolución de los ciberataques.

Para ello a través de las estructuras que es establezcan se debería diseñar un plan de mejora de las mismas y potenciar las capacidades de los organismos que deben auditar y monitorizar la actividad de estas redes.

(1) Common Criteria. www.commoncriteria.org

ANEXO B

GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

ANEXO B
GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

Acrónimo / voz	*Significado*
Amenaza (Threat) (OTAN)	La posibilidad de compromiso, pérdida o robo de información clasificada OTAN o de servicios y recursos que la soportan. Una amenaza puede ser definida por su origen, motivación o resultado y puede ser deliberada o accidental, violenta o subrepticia, externa o interna.
ANS	Autoridad Nacional de Ciberdefensa
Bot Botnet	Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación [distribuida] de servicio.
Brecha de seguridad (Security breach) (OTAN)	Una acción u omisión, deliberada o accidental, contraria a la Política de Seguridad de la OTAN o normativas de aplicación de la Política que resulte en un compromiso real o potencial de información clasificada OTAN o los servicios y recursos que la soportan.
Caballo de Troya	Ver troyano
CACD	Centro Asesor para la ciberdefensa (CACD)
Carding	Uso ilegítimo de las tarjetas de crédito.
Catálogo Nacional de Infraestructuras Estratégicas	La información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.
CCC	Centro de Coordinación de Ciberdefensa.
CCN	Centro Criptológico Nacional

CCRIS	Centro de coordinación y respuesta a incidentes de Seguridad
CERT	Computer Emergency Response Team
Ciberataque	Forma de ciberguerra / ciberterrorismo donde combinado con un ataque físico o no se intenta impedir el empleo de los sistemas de información del adversario o el acceso la misma
Ciberdefensa	La aplicación de medidas de seguridad para proteger las los diferentes componentes de los sistemas de información y comunicaciones de un ciberataque.
Ciberespacio (Cyber space) (OTAN)	El mundo digital generado por ordenadores y redes de ordenadores, en el cual personas y ordenadores coexisten y el cual incluye todos los aspectos de la actividad «online».
Ciberevento (Cyber event) (OTAN)	Cualquier suceso observable en un sistema de información y comunicaciones.
Ciberincidente (Cyber incident) (OTAN)	Ciberevento adverso en un sistema de información y comunicaciones o la amenaza de que se produzca.
Ciberseguridad	Protección de los componentes de las infraestructuras de los sistemas de información y comunicaciones ante amenazas cibernéticas
Ciberterrorismo	Un ciberataque para causar la inutilización o interrupción de redes de ordenadores o comunicaciones para generar temor o intimidar a la sociedad con un objetivo ideológico
Código dañino o malicioso (malicious code o software)	Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. [http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S]
EGC	*European Government CERT*
Exploit	Pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado).
FIRST	Forum for Incident Response and Security Teams

Gestión de Riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
Gestión del riesgo (Risk Management) (OTAN)	Aproximación sistemática, basada en la valoración de las amenazas y las vulnerabilidades, para la determinación de las contra-medidas necesarias para la protección de la información o los servicios y recursos que la soportan.
Información (Information) (OTAN)	Conocimiento que puede ser comunicado de cualquier forma.
Información clasificada (Classified information) (OTAN)	Información o materia determinada que requiere protección contra revelación no autorizada y a la que, consecuentemente, se le ha asignado un grado de clasificación de seguridad.
Infraestructuras críticas (IC)	Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos esenciales
Infraestructuras críticas europeas (ICE)	Aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya interrupción o destrucción afectarían gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114/CE.
Infraestructuras estratégicas (IE)	Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios públicos esenciales
INTECO	*Instituto Nacional de Tecnologías de la Comunicación.*
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
Interdependencia	Los efectos que una interrupción en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y/o en otros sectores, y las repercusiones de ámbito local, regional, nacional o internacional.
OTAN	*North Atlantic Treaty Organization* Organización del Tratado del Atlántico Norte

Phishing	Los ataques de «phishing» usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar as sus posibilidades de éxito, utilizan el correo basura («spam») para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares de Internet falsificados, páginas web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de convencer al usuario a que introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc. *[http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S]*
RAT	*Remote Administrations Tool.* Herramienta de administración remota. Estas apliaciones pueden ser legítimas o no y pueden ser utilizadas con o sin autorización del usuario. En el mundo del malware estas aplicaciones generalmente son troyanos que abren una puerta trasera (backdoor) en el equipo del usuario para permitir dicha administración.
RAT (2)	*Troyano de Acceso Remoto.* Son programas de software malintencionados que permiten a los delincuentes controlar un equipo mediante la conexión a Internet. Un RAT puede permitir a un delincuente ver y cambiar los archivos y funciones del equipo, supervisar y registrar sus actividades y utilizar su equipo para atacar a otros.
Riesgo (Risk) (OTAN)	La probabilidad de que una vulnerabilidad sea explotada con éxito por una amenaza produciendo un compromiso de confidencialidad, integridad y/o disponibilidad y daños.
Rootkit	Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos. *[http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S]*

SCADA	Supervisory Control And Data Acquisition Control Supervisor y Adquisición de Datos, nombre de los sistemas de control industrial.
Sistema de Información	Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
Spam	*Correo basura* Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es una extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de usuarios están expuestos a este correo basura, más del 80% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet. *[http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S]*
Spyware	Código dañino diseñado habitualmente para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos como puede ser mostrar publicidad o robo de información personal del usuario. [STIC-400:2006]
STIC	Seguridad de las Tecnologías de Información y Comunicaciones.
TERENA	*Trans-European Research and Education Networking Association* Grupo de coordinación de CERT,s europeos
TF-CSIRT (TERENA)	Trans-European Research and Education Network Association
Troyano – Caballo de Troya	Introducción subrepticia en un medio no propicio, con el fin de lograr un determinado objetivo. Diccionario de la Lengua Española. Vigésimo segunda edición. Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc. [STIC-430:2006]

Vulnerabilidad (Vulnerability) (OTAN)	Una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada OTAN o los servicios y recursos que la soportan.
Vulnerabilidad	Una debilidad que puede ser aprovechada por una amenaza.
Zombi	Ver bot / botnet