tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

104

DEFINICIÓN Y EJECUCIÓN DEL PLAN DIRECTOR DE SEGURIDAD DE LOS SS.II. DEL MAPA

Manuel Ruiz del Corral
Técnico Superior de Proyecto Informático
Subdirección General de Informática y Comunicaciones
Ministerio de Agricultura, Pesca y Alimentación

Palabras clave

Plan Director de Seguridad, Análisis de Riesgos, Test de Intrusión, Comunicaciones, Procedimientos, Vulnerabilidad, salvaguarda, comunicaciones, cortafuegos, firewall, respaldo, backup.

Resumen de su Comunicación

Definición, planificación y ejecución, desde una perspectiva de gestión directiva ,del Plan Director de Seguridad de los SSII del Ministerio de Agricultura y Alimentación.

DEFINICIÓN Y EJECUCIÓN DEL PLAN DIRECTOR DE SEGURIDAD DE LOS SS.II. DEL MAPA

1. Introducción y Antecedentes

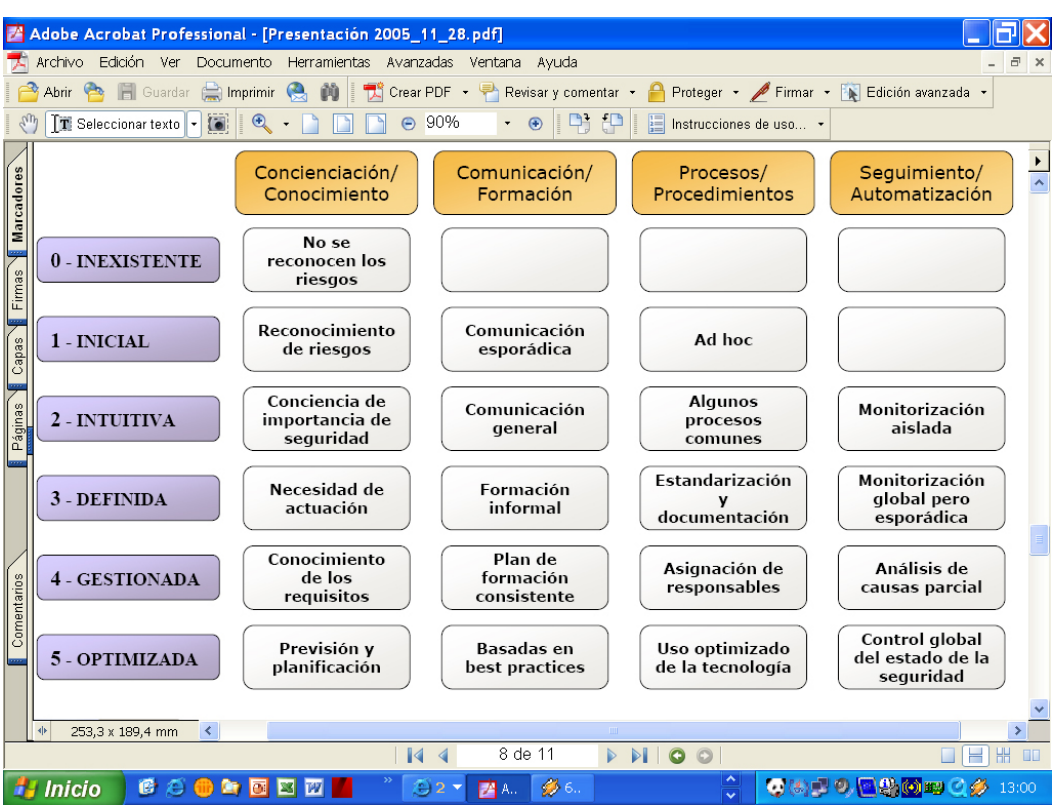
El enorme crecimiento de los activos de información experimentado por las organizaciones actuales, unido a las cambiantes condiciones y las nuevas plataformas tecnológicas disponibles, implica necesariamente una nueva dimensión de gestión de los sistemas de información y comunicaciones.

Asimismo, la posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las Administraciones Públicas para mejorar su servicio al ciudadano, y asimismo, ha traído consigo la aparición de nuevas amenazas para los sistemas de información. Esta situación provoca la exposición graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensible y la imagen institucional.

En las organizaciones modernas, los problemas y riesgos de seguridad no sólo toman sentido en el marco de una serie de actuaciones técnicas, sino en una dimensión de gestión y procedimientos de alto nivel, sin olvidar las imposiciones legales (por ejemplo, la Ley de Protección de Datos).

En definitiva, la seguridad se consolida como un nuevo activo estratégico de la organización, que necesitará ser planificado, implantado y gestionado para mejorar el nivel de servicio ofrecido, y que incidirá directamente en el grado de madurez, eficacia y eficiencia de la organización.

En este sentido, se adjunta como referencia un modelo de gestión de la seguridad desarrollado por el IT Governance Institute. Este modelo establece 6 niveles de madurez de la seguridad en la organización (vertical), para cada nivel asigna un grado de madurez en 4 aspectos (horizontal):



En el caso particular del Ministerio de Agricultura, Pesca y Alimentación (en adelante MAPA), el crecimiento de los activos de la información ha sido muy considerable en los últimos años, lo que ha generado paralelamente vulnerabilidades en materia de seguridad, tanto a nivel técnico como de gestión, que pueden incidir directa o indirectamente en la disponibilidad de los servicios e imagen pública.

En este sentido, la concienciación en materia de seguridad ya queda claramente plasmada en el Plan Director de Sistemas de Información 2003-2006, y en la consecuente creación de un servicio de seguridad en el año 2005, para planificar, coordinar y gestionar las actuaciones en materia de seguridad.

2.1. Definición de Objetivos y Ámbito de Aplicación

El Plan Director de Seguridad del MAPA se concibe inicialmente para planificar y formalizar las actuaciones en seguridad, creando un marco de trabajo en la materia. En concreto, se plantean los siguientes objetivos:

- Analizar la seguridad de la organización.
- Asentar y formalizar la conciencia de seguridad existente.
- Crear un Marco de Trabajo en materia de seguridad.
- Definir los proyectos a realizar, a corto, medio y largo plazo en materia de seguridad.
- Establecer y formalizar procedimientos de gestión de la seguridad.

Todos ellos se conciben desde un triple ámbito de aplicación:

- Técnico:
    - Sistemas
    - Comunicaciones
    - Aplicaciones
- Legal y Normativo:
    - Imposiciones legales
    - Creación de Normativa Corporativa basada en ISO 17799
- Organizativo – Procedimientos:
    - Pautas para la Gestión de la Seguridad
    - Adecuación y Formalización de Procesos que inciden de forma directa en la seguridad de la organización.

2.2 Sumario de Trabajos Realizados

Los objetivos anteriores se han definido, a lo largo del proyecto, en los siguientes entregables (se indica el ámbito asociado a cada entregable).

- Política y Normativa de Seguridad (Organizativo, Normativo)
    - Documento basado en la ISO 17799, como referencia de la Seguridad del MAPA.
- Política y Normativa de Seguridad para los Usuarios de los SSII (Normativo)
    - Documento basado en la normativa de referencia, para distribuir al usuario final.

- Test de Intrusión (Técnico)
    - Realización de pruebas de intrusión, a través de Internet, de los equipos visibles desde el exterior.
- Análisis de Riesgos (Técnico, Organizativo)
    - A partir de entrevistas y de análisis técnicos, se ha realizado una evaluación de la seguridad de los sistemas y procedimientos internos de la organización.
- Plan Director de Seguridad (Técnico, Organizativo, Normativo)
    - A partir del análisis de riesgos, se definen más de 100 líneas de acción en materia de seguridad.

Se adjunta un gráfico que muestra las interrelaciones de los entregables del proyecto:

2.3 Análisis de Riesgos

2.1.1 Entradas

Las entradas para el análisis de riesgos, han sido las siguientes:

Entrevistas:

Se realizaron numerosas entrevistas a personal de la Subdirección, comenzando desde los niveles directivos hasta los niveles más técnicos. Asimismo, se anotaron ineficiencias, propuestas de mejora, y problemas relacionados con la seguridad.

Análisis Técnicos.

Se realizaron, contando con personal experto, un análisis de instalaciones, servidores, comunicaciones y aplicaciones, priorizado por su criticidad.

Test de Intrusión.

Un equipo independiente realizó, desde el exterior, un exhaustivo análisis de las vulnerabilidades de los equipos visibles desde el exterior. Los resultados han dado lugar a un documento con un mapa de todos los equipos, anotando las vulnerabilidades categorizadas en:

- Configuración
- Tecnología
- Diseño
- Desarrollo

Asimismo, cada vulnerabilidad lleva asociada una descripción técnica y un nivel de riesgo:

- Alto
- Medio
- Bajo

2.1.2 Salida

La salida del trabajo la constituye el Documento de Análisis de Riesgos, que consta de un análisis de 26 procesos estándar de seguridad, para cada uno de ellos se indica:
Una evaluación de la Situación actual
Acciones de mejora sobre el proceso

En concreto, los procesos son:

1. Política, planificación y concienciación de la seguridad
2. Máquinas de la red pública (DMZ)
3. Redes Corporativas e Intranet
4. Firewalls y balanceo
5. Comunicaciones
6. Gestión de incidencias en sistemas
7. Gestión de datos
8. Mecanismos de backup y restauración
9. Correo Electrónico
10. Antivirus, spyware y malware en general.
11. Parcheado de sistemas
12. Gestión de usuarios
13. Atención a usuarios (CAU)
14. Centros de proceso de datos (CPD)
15. Redes inalámbricas
16. Suministros
17. Desarrollo de Aplicaciones
18. Control de navegación
19. Monitorización y Auditorias
20. Recursos humanos
21. Cumplimiento Normativo

22. Inventario
23. Seguridad en puesto usuario
24. Servicios de voz (Telefonía)
25. Accesos externos a las Infraestructura
26. Relaciones con terceros

Para todos ellos se efectúan recomendaciones, que posteriormente se formalizarán como tareas en el Plan de Seguridad.

2.4 Plan Director de Seguridad

A partir del Análisis de Riesgos y de la Política de Seguridad, se han establecido las siguientes líneas de acción:

1.Procesos generales (19 procesos)
- Política de Seguridad
- Inventario de activos
- Actuaciones de seguridad en las máquinas de DMZ.
- Actuaciones de seguridad en la red corporativa e intranet.
- Cortafuegos y balanceadores
- Dispositivos de comunicaciones
- Almacenamiento de datos
- Mecanismos de backup y restauración
- Mecanismos de seguridad en el correo electrónico
- Antivirus, spyware y malware
- Gestión de incidencias de usuario
- Medidas de seguridad para los CPDs
- Medidas de seguridad en redes inalámbricas
- Suministro eléctrico
- Servicio de navegación a través de Internet para usuarios
- Seguridad en el tratamiento de recursos humanos
- Medidas de seguridad en los sistemas de transimisión de voz
- Seguridad en las conexiones desde terceros
- Seguridad y calidad en los servicios y desarrollos de terceros

2.Monitorización y auditoría
3.Plan de Contingencias
4.Gestión de Usuarios
5.Parcheado y Actualización de Sistemas
6.Gestión de incidencias e intervenciones
7.Seguridad frente a intrusiones
8.Desarrollo Seguro
9.Flujos de información en la arquitectura de tres capas

Todas estás líneas de acción incluyen recomendaciones para formalizar, mejorar, implantar, y/o gestionar los procesos de seguridad. En concreto, el Plan de Seguridad contempla 140 tareas priorizadas, las cuales incluyen:

- Una estimación de RRHH/esfuerzo, útil especialmente para comparar cuantitativamente esfuerzos

entre tareas.
- Relaciones con otras tareas.
- Entradas y salidas.
- Periodicidad de revisión.

Como ejemplo, se adjunta un gráfico con las tareas para un proceso determinado: gestión de la seguridad en cortafuegos:

Para estas tareas, se adjunta un cuadro con su esfuerzo y salidas asociadas:

TAREA		Salidas	Esfuerzo
1	Elaboración de políticas de flujo de información entre capas a través de los cortafuegos	Política de flujo de información a través de cortafuegos	4
		Flujo de aceptación de reglas	
2	Elaboración de un procedimiento de petición de creación de reglas en los cortafuegos	Formulario de petición de alta de reglas en cortafuegos	2
3	Elaboración de un procedimiento de gestión, registro y aceptación de excepciones	Procedimiento de gestión de excepciones	2
		Flujo de aceptación de excepciones	
4	Elaboración de un guía técnica de alta/baja de reglas en cortafuegos para cada plataforma usada en el MAPA	*Guía técnica de creación y eliminación de reglas en cortafuegos*	1
5	Revisión de los flujos de datos a través de los cortafuegos	Listado de reglas del cortafuegos que satisfacen los requisitos de seguridad	4
		Listado de reglas del cortafuegos que no satisfacen los requisitos de seguridad y deben ser eliminadas	

2. Gestión y Desarrollo del Plan Director de Seguridad de los SSII del MAPA. Primeros Pasos

La gestión del correcto desarrollo del Plan Director de Seguridad se hará desde la Unidad de Seguridad en dependencia directa de la Subdirección General de Informática y Comunicaciones, y el apoyo técnico del resto de las unidades de la Subdirección.
En concreto, se desarrollará un sistema de seguimiento de proyectos del Plan de Seguridad, marcando hitos, prioridades, recursos y plazos.

Las líneas prioritarias, a corto plazo, serán todos los proyectos orientados a la integración de las actividades de seguridad ya existentes en el Ministerio, y que incidan de forma definitiva en la disponibilidad y salvaguarda de la imagen y servicio ofrecidos por el Ministerio.

En este sentido, en una primera fase se abordarán los siguientes proyectos:

- Plan de Contingencias
    - Se elaborará un Plan de Contingencias, a partir de los activos del Ministerio, y utilizando los medios físicos ya disponibles, como los CPDs y líneas de comunicaciones de respaldo.
- Consolidación de la Monitorización de Servicios
    - Se desarrollará un sistema que unifique y complete la amplia monitorización de servicios ya existente en el Ministerio.
- Consolidación y Formalización del Ciclo Desarrollo – Producción:
    - Se desarrollará un proyecto para formalizar el desarrollo y los pasos a producción, unificando las iniciativas ya existentes y formalizando su carácter normativo.
- Asimismo, y como herramienta de control y seguimiento de los proyectos anteriores, se consolidará un Inventario Corporativo de Activos orientado a la gestión de la seguridad:
    - Se consolidará una base de datos, alimentada a partir de herramientas de inventariado automático y datos manuales, que ofrezca la siguiente información:
        - Servidores
        - Aplicaciones
        - Bases de Datos
        - Datos de Ubicaciones físicas y lógicas
        - Responsables
        - Administradores
        - Copias de Seguridad

Se adjunta un gráfico con las interrelaciones de los proyectos de esta primera fase.

3. Resumen Final

Como se ha descrito, el Plan de Seguridad del MAPA representa un conjunto recomendaciones definidas en 140 tareas agrupadas en 9 líneas de acción para dotar a la organización de un nivel de seguridad adecuado a los requisitos operativos determinados en el análisis de riesgos previo. La ejecución completa de las líneas de acción se estima requerirá un periodo de 2 o 3 años.

La aplicación de estas tareas permitirá asegurar la disponibilidad de los servicios y la imagen pública del Ministerio, así como ofrecer garantías en la confidencialidad de datos sensibles y la integridad de los flujos de Información.