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

Comunicación

042

PROCESO HACIA LA CERTIFICACIÓN DE LA OFICINA VIRTUAL DE LA CONSEJERÍA DE ECONOMÍA Y HACIENDA COMO SGSI

Manuel Narbona Sarria
Gabinete de Sistema
Servicio de Producción
Dirección General de Sistemas de Información Económico-Financiera
Consejería de Economía y Hacienda
Junta de Andalucía

Manuel Narbona Sarria

Palabras clave

Sistema, gestión, seguridad, información

Resumen de su Comunicación

Con el advenimiento de la administración electrónica se hace necesario garantizar la confidencialidad, integridad y disponibilidad de la información y de los servicios que prestamos al ciudadano.

En este contexto se enmarca el proyecto de Evaluación de la Seguridad que la CEH ha puesto en marcha desde comienzos de 2005 y que pretende la creación de un SGSI durante 2006 que garantice a la CEH, como prestador de servicios de administración electrónica a través de su Oficina Virtual, y a los ciudadanos, como consumidores de dichos servicios, que los procesos que dan soporte a los servicios de administración electrónica están controlados mediante un sistema de gestión de Seguridad de la Información (SGSI).

Dicho SGSI debe servir, además, para sentar las bases de un Sistema de Gestión de las Tecnologías de la Información Integral que ayude a la gestión y al control efectivo de las Tecnologías de la Información en la CEH.

Manuel Narbona Sarria

PROCESO HACIA LA CERTIFICACIÓN DE LA OFICINA VIRTUAL DE LA CONSEJERÍA DE ECONOMÍA Y HACIENDA COMO SGSI

1. Introducción[1]

Diario EL PAÍS, miércoles 18 de Enero de 2006:

Una gigantesca estafa por Internet deja a la Hacienda británica al borde del colapso. Los criminales usurparon la identidad de miles de trabajadores para, alterando sus datos laborales, solicitar pequeños pagos a través del portal digital del erario público.

La Consejería de Economía y Hacienda (CEH) de la Junta de Andalucía (JA) da soporte a las aplicaciones contables de ingresos y gastos de la Junta de Andalucía: Sur y Júpiter. Además, dichas aplicaciones tienen una importante presencia en la Oficina Virtual (OV) de la CEH, sobre todo SUR, siendo posible la tramitación completa, incluyendo el pago electrónico, de determinados tributos autonómicos.

La CEH siendo consciente de la importancia creciente que tiene la Administración Electrónica, y lo importante que resulta para el ciudadano que sus trámites electrónicos cuenten con las mismas garantías, si no más, que los de la administración tradicional, contrató en 2003 un test de intrusión de la Oficina Virtual. Dicho test, aunque arrojó resultados satisfactorios para la CEH, no fue suficiente para garantizar que la Oficina Virtual estuviera a salvo de intrusiones, entre otras razones porque un test de intrusión mide tanto la fortaleza de la organización que sufre el ataque como la debilidad del atacante, o a la inversa, siendo imposible establecer la frontera entre ambos. Para aumentar las garantías de que el ataque ha sido intenso, quizá sería conveniente cambiar la contratación de este test por la concesión de un premio a quién consiga vulnerar nuestros sistemas, aunque este método tiene el riesgo de llamar la atención sobre nuestros sistemas.

Además, lo que muestra el test de intrusión es sólo una imagen estática, una foto, de la situación en un instante dado, lo cual es insuficiente debido al rápido avance de las Tecnologías de la Información (TI).

En 2004 la CEH se volvió a plantear medir su nivel de seguridad TI, pero esta vez quiso asegurarse además de disponer de los elementos técnicos y, sobre todo, de gestión que le permitieran realizar una evaluación continua de la seguridad de la información.

Hay que recordar que con independencia de la necesidad de protección de la información y de los SI detectada por la CEH, las leyes nos obligan a ello (LOPD, RMS, LSSI, Código Penal, LGTel, Firma Electrónica, DNI electrónico, LPI, ...). En concreto, el artículo 9 de la LOPD dice:

Seguridad de los Datos El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, ...

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

[1] Véase el Anexo para las definiciones de los términos relativos a la seguridad de la información

2. El proyecto de Evaluación de la Seguridad (ES)

Visión de la CEH

El planteamiento que hizo la CEH para el proyecto de Evaluación de la Seguridad se basó en lo antes comentado: No basta con obtener una foto fija del estado de la seguridad TI, es necesario también aprender a gestionar el riesgo.

Con esta premisa, se definieron los siguientes aspectos: (1) el alcance incluía todos los SI de la CEH; (2) la metodología de evaluación de la seguridad comprende (2.1) OSSTMM para el test externo (a ciegas), (2.2) herramientas y listas de control para la inspección interna de la infraestructura tecnológica de la CEH, (2.3) MAGERIT para el análisis y gestión del riesgo y (2.4) la ISO 17799 para la evaluación de la seguridad; (3) todo el trabajo se repetiría 3 veces en 1 año, de tal modo que pudiéramos tener una visión de la evolución de la seguridad TI en la CEH.

Por parte de la CEH el personal implicado ha sido el siguiente: Un director de proyecto y 6 técnicos de sistemas del Servicio de Producción (SP) de la Dirección General de Sistemas de Información Económico-Financiera (DGSIEF) presentes en la mayor parte del trabajo, más 2 técnicos por cada uno de los 2 grandes sistemas –Sur y Júpiter– para la definición de los procesos de ambos sistemas y para responder al apartado correspondiente sobre la seguridad en el desarrollo del cuestionario ISO 17799, y el responsable del servicio de Coordinación y Planificación para responder a ciertas preguntas del cuestionario sobre la ISO 17799 que eran de su competencia

Visión de la empresa consultora

El análisis de las ofertas presentadas al concurso puso de manifiesto que las empresas que concurrieron al mismo o bien eran expertas en test de intrusión y análisis de vulnerabilidades, o lo eran en los aspectos organizativos y de gestión de la seguridad, pero no en ambos. Finalmente, elegimos la oferta que no siendo deficiente en el test de vulnerabilidad obtuviera una alta calificación en los aspectos organizativos y de gestión.

La razón de esta decisión ya se ha apuntado antes: Necesitamos disponer de metodologías y herramientas para la autogestión de la seguridad TI.

La empresa consultora que finalmente ganó el concurso ofreció como valor añadido a lo definido por la CEH lo siguiente: (4) Análisis de procesos y flujos de información; (5) definición de un SGSI; (6) evaluación previa por AENOR del SGSI construido.

El grupo de trabajo presentado por la consultora comprendía: (a) un jefe de proyecto, (b) un experto en Análisis y Gestión de Riesgo, (c) un experto en evaluación ISO 17799, (d) un experto en análisis de procesos, (e) un experto en SGSI, (f) un técnico para el test externo y (g) un técnico para la inspección interna. La consultora adquirió el compromiso de que no transferir ninguna información sobre la infraestructura tecnológica de la CEH al técnico que efectuaría el test externo.

3. La Seguridad de la Información

Auditoría remota (OSSTMM)

La metodología OSSTMM (Open Source Security Testing Methodology Manual) indica cómo debe realizarse una auditoría de la seguridad de la información. Cubre los siguientes dominios: (1) Seguridad de la Infor-

mación, (2) Seguridad de los Procesos, (3) Seguridad en las Tecnologías de Internet, (4) Seguridad en las Comunicaciones, (5) Seguridad Inalámbrica y (6) Seguridad Física.

Puesto que se trataba de un test de intrusión externo y a ciegas, los únicos dominios aplicables en nuestro caso eran el (1) y el (3).

Los ataques que se realizaron fueron de 3 tipos: (1) pasivo -recogida de información de dominio público-, (2) activo -acciones para intentar violar la seguridad- e (3) intrusivo -explotación de vulnerabilidades para alcanzar mayor nivel de acceso a la red interna.

Se pretendía con ello evaluar: la (1) visibilidad -lo que puede ser visto, registrado o monitorizado, con o sin la ayuda de dispositivos electrónicos-, el (2) acceso -puntos de acceso públicos o semipúblicos susceptibles de ser vulnerables o contener fallos que permitan acceder al sistema-, la (3) confianza -la clase, cantidad y calidad de la autentificación, el control de acceso, la confidencialidad e integridad entre dos o más factores dentro del contexto de seguridad- y la (4) alarma -la velocidad y calidad de notificación de información que indican la intención de violar los puntos anteriores.

Auditoría interna

Se pretendía analizar los siguientes aspectos: (1) prevención de intrusos en tiempo real (IPS), (2) seguridad en accesos remotos, (3) análisis de firewalls y routers, (4) servicios de red, (5) análisis de vulnerabilidades en los sistemas, (6) actualizaciones y parches, (7) seguridad de aplicaciones (pendiente la seguridad en el desarrollo), (8) código HTML de servidores web (pendiente), (9) protección antivirus, (10) sistemas de cifrado, (11) detección de troyanos, sniffers, gusanos y códigos maliciosos, (12) listas de control sobre los sistemas.

El resultado de este trabajo, ejecutado íntegramente por la consultora con el soporte de técnicos del SP, es un informe de vulnerabilidades.

Análisis y Gestión de Riesgos (AGR)

Permite determinar qué tiene la Organización y estimar lo que podría pasar.

El esquema conceptual del AGR tiene en cuenta los siguientes elementos: (1) activos -los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la organización-, (2) amenazas -incidencias que les pueden pasar a los activos causando un perjuicio a la organización- y (3) salvaguardas (o contramedidas) -elementos de defensa desplegados para que aquellas amenazas no causen [tanto] daño: Técnicas, físicas, organizativas y de personal.

Con estos elementos se puede estimar: (1) el impacto -lo que podría pasar- y (2) riesgo -lo que probablemente pase.

Así, el riesgo es una función del valor de los activos, de la degradación provocada por la materialización de las amenazas y de la frecuencia estimada de la materialización de las amenazas. Por otra parte las salvaguardas reducen el riesgo actuando bien de forma correctiva sobre el impacto, reduciéndolo, bien actuando de forma preventiva sobre la frecuencia estimada de materialización, reduciéndola.

Análisis de Riesgos (AR)

Para la realización del análisis los pasos a seguir son: (1) identificación de los activos, (2) identificación de las dependencias entre activos, (3) valoración de los activos, (4) identificación de las amenazas significati-

vas y valoración de frecuencia de ocurrencia y degradación, (5) identificación de las salvaguardas y valoración de la eficacia, (6) estimación del impacto y el riesgo y (7) interpretación del significado del impacto y el riesgo.

Para el AR se usó la herramienta PILAR. Lo primero que hicimos fue intentar entender la clasificación propuesta para los tipos de activos -servicios, aplicaciones informáticas, equipos informáticos, soportes de información, equipamiento auxiliar (SAI, ...), redes de comunicaciones, instalaciones (CPD, ...) y personas-, y cómo adaptarla a nuestras necesidades dentro de lo que la herramienta permite. También fue necesario clarificar lo más posible la dependencia entre activos. Entendíamos que no se podía permitir cualquier dependencia directa, por ejemplo, no nos parece correcto que los servicios dependan directamente del hardware. Los servicios tienen una dependencia directa con las aplicaciones y los datos. Las aplicaciones a su vez dependen del software base, el cual sí depende directamente del entorno físico, el hardware.

Salvando las limitaciones que la propia herramienta nos imponía, definimos las siguientes capas de activos: (1) servicios (los que percibe el usuario), (2) servicios horizontales, (3) servicios de comunicaciones, (4) software de aplicación, (5) software base, (6) hardware de servidores, (7) hardware de almacenamiento, (8) hardware de comunicaciones, (9) equipamiento auxiliar, (10) instalaciones y (11) personas, e intentamos que las dependencias se establecieran ordenadamente, como se ha explicado antes.

En total se han definido en torno a 250 activos que incluyen toda la infraestructura de la CEH. Algunos activos están definidos de modo genérico como un grupo que engloba muchos activos que tienen un comportamiento común, y cuyas dependencias se pueden establecer de modo conjunto. Se han definido las dependencias y se han asignado valores a los activos. Basándose en las relaciones de dependencia, la herramienta PILAR es capaz que imputar valor a los activos en las capas inferiores a partir del valor asignado en las superiores. Quiere esto decir que, aunque puedan ser necesarios ajustes más finos, basta con asignar valor a los activos de servicios y datos para tener el valor del resto de los activos.

Gestión de riesgos (GR)

Para la GR hay que seguir los siguientes pasos: (1) se elige una estrategia para mitigar impacto y riesgo, (2) se determinan las salvaguardas oportunas para el objetivo anterior, (3) se determina la calidad necesaria para dichas salvaguardas, (4) se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables, y (5) se lleva a cabo el plan de seguridad.

- De momento, sólo se está haciendo una GR puntual que no está soportada por ningún Plan de Seguridad.

Evaluación de la seguridad: ISO 17799

La norma ISO 17799 considera los siguientes dominios respecto a la seguridad: (1) política de seguridad, (2) aspectos organizativos para la seguridad, (3) clasificación y control de activos, (4) seguridad ligada al personal, (5) seguridad física y del entorno, (6) gestión de comunicaciones y operaciones, (7) control de accesos, (8) desarrollo y mantenimiento de sistemas, (9) gestión de continuidad del negocio y (10) cumplimiento.

El procedimiento que se ha seguido ha sido la realización al personal de la DGSIEF implicado en la seguridad de la información de un extenso cuestionario, más de 1.500 preguntas, en torno a los dominios antes citados.

4. El SGSI

Norma UNE 71502: SGSI

La norma española UNE 71502:2004 "Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)" certifica la norma ISO17799 "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información" para un determinado ámbito definido en el alcance del proyecto (en nuestro caso, la Oficina Virtual de la CEH).

La Organización debe establecer y mantener un SGSI documentado. Éste debe identificar los activos a proteger, el enfoque de la gestión del riesgo adoptado por la organización, los objetivos y controles, así como el grado de protección requerido.

La Dirección de la Organización (en adelante la Dirección) aprobará formalmente la implantación y operación del SGSI.

SGSI: Planificación y diseño

Los pasos a seguir en la planificación y diseño del SGSI son los siguientes: (1) definir la política de seguridad, (2) definir el alcance del SGSI, (3) realizar un análisis de riesgos, (4) identificar los riesgos a gestionar identificados basándose en la política de la Organización sobre seguridad de la información y el grado de seguridad requerido, (5) la Dirección deberá aprobar los riesgos residuales resultantes, (6) seleccionar de la Norma UNE-ISO/IEC 17799 los controles adecuados, (7) seleccionar, si es necesario, controles específicos adicionales, fuera de la Norma UNE-ISO/IEC 17799 y (8) elaborar el documento de selección de controles aplicables para conseguir el nivel de riesgo residual aprobado.

Factores críticos de éxito

Para asegurar el éxito de la implantación de un SGSI es necesario: (1) el apoyo explícito y visible y el compromiso de la dirección, (2) que la política, objetivos y actividades reflejen los objetivos de negocio de la organización, (3) que el enfoque para implantar la seguridad sea consistente con la cultura de la organización, (4) una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo, (5) la convicción de la necesidad de la seguridad a todos los directivos y empleados, (6) la distribución de guías sobre la política de seguridad de la información de la organización y de normas a todos los empleados y contratistas, (7) la formación y capacitación adecuadas, (8) un sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información y sugerir mejoras.

5. Resultados

Auditoría remota (OSSTMM)

Tras las pruebas llevadas a cabo, no se ha podido detectar ningún fallo en la configuración de los sistemas, en la versión del software ni en la programación de las aplicaciones que, a día de hoy, puedan permitir que un atacante, desde Internet, pueda dañar los sistemas de la Consejería.

¿Fortaleza nuestra o debilidad del atacante?.

Auditoría interna

Se detectó alguna vulnerabilidad en cierto sistema que está controlado. La vulnerabilidad, conocida y con-

trolada por el SP, se debe a la imposibilidad de actualizar el sistema de operativo ya que la aplicación que se está ejecutando sobre dicho sistema no soporta la actualización mencionada.

Se detectó también alguna vulnerabilidad en el servidor de aplicaciones Citrix que ya han sido corregidas, y otras en alguna aplicación que ya ha sido comunicada a sus responsables.

Algunas listas de control en sistemas específicos (Adabas-Natural y z/OS) no han convencido al SP, pero la consultora no ha sido capaz de proporcionarnos especialistas en esas áreas.

AGR según metodología MAGERIT y evaluación ISO/IEC 17799

El estado actual de eficacia de las salvaguardas aplicadas es preocupante, sobre todo en los aspectos organizativos de la seguridad –cosa que ya sabíamos pero no habíamos cuantificado-, aunque no tanto en el técnico.

Análisis de procesos

En este apartado no se ha avanzado mucho. Sólo en el proyecto SUR han definido sus procesos principales en la Oficina Virtual, aunque faltan por definir ciertas características de los mismos como son las métricas asociadas a los procesos que aseguren que los mismos se están ejecutando como está previsto o los responsables de los mismos.

El SP está revisando sus procesos críticos.

SGSI

Este apartado no ha sido abordado. Las causas principales son: (1) el equipo de trabajo de la consultora se ha ido disgregando como consecuencia de la absorción de parte de la empresa por otra empresa, (2) no ha existido un compromiso serio y coordinado de todos los implicados en la definición del SGSI cuyo ámbito se ha definido como el correspondiente a los servicios prestados en la Oficina Virtual de la CEH.

6. El futuro

Varias han sido las consecuencias positivas de este proyecto: (1) se ha tomado conciencia, aunque no completamente, de la necesidad de establecer un SGSI, (2) se dispone por primera vez de un análisis de riesgo completo de la infraestructura TI de la CEH en lo que respecta al soporte a los servicios (falta el análisis de riesgo de las aplicaciones, sobre todo SUR y Júpiter), (3) se conoce el estado actual de la eficacia de las salvaguardas aplicadas en materia de seguridad de la información, (4) somos conscientes de la necesidad de definir adecuadamente los procesos que dan soporte a los servicios, de establecer indicadores para controlar su ejecución y de designar a los responsables de los mismos.

Lo que nos queda por hacer es mucho pero no es imposible: (1) definir el marco general del SGSI (requisitos, planificación y diseño del SGSI, documentación y control de la misma, roles y responsabilidades, ...), (2) implantar el SGSI (definir los controles y medir la eficacia de los mismos), (3) explotar el SGSI (proveer recursos técnicos y humanos), (4) revisar el SGSI (auditorías internas) y (5) establecer el proceso de mejora.

La documentación que todo esto generará hace referencia a los dominios definidos en la ISO 17799.
La meta propuesta es ambiciosa: Certificar la Oficina Virtual de la CEH como un SGSI, pero el ciudadano merece, puesto que es nuestro cliente, que le garanticemos los servicios de administración electrónica que les estamos prestando a través de la OV.

No debemos olvidar, sin embargo, que para conseguir el éxito en este tipo de proyectos es necesario un alto grado de compromiso de todos los grupos de interés implicados, y por supuesto, el **apoyo explícito y visible** por parte de la dirección.

7. Anexo: Definiciones

- Seguridad de la Información: Consiste en preservar la:
  - Confidencialidad: Sólo quienes estén autorizados pueden acceder a la información
  - Integridad: La información y sus métodos de proceso son exactos y completos
  - Disponibilidad: Los usuarios autorizados TI tienen acceso a la información y a sus activos
  - asociados cuando lo requieran. (ISO 17799:2002)
- Información: Datos que poseen significado (ISO9000:2000):
  - En soportes magnéticos
  - En soportes no magnéticos
- Sistema: Una colección de componentes organizados para llevar a cabo una función o un grupo de funciones (ISO 9000)
- Sistema de Información (SI): Colección organizada de HW, SW, aplicaciones, políticas, procedimientos y personas, que almacenan, procesan y proporcionan acceso a la información
  - Manuales
  - Semi-automáticos
  - Automáticos
- Gestión: Actividades coordinadas para dirigir y controlar una organización (ISO 9000)
- Sistema de Gestión: Sistema para establecer la política y los objetivos y para lograr dichos objetivos (ISO 9000)