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

Comunicación

358

DIRECTRICES DEL PLAN DIRECTOR DE SEGURIDAD: ISO 17799

Guillermo B. Mora Marín
Jefe de Servicio de Sistemas Informáticos
Ministerio de Trabajo y Asuntos Sociales

Guillermo B. Mora Marín

Palabras clave

Plan Director, Seguridad, ISO 17799..

Resumen de su Comunicación

Acercamiento a las directrices que han de regir la elaboración de un Plan Director de Seguridad utilizando como base de referencia principal el estándar de buenas prácticas de seguridad UNE ISO/IEC 1779, considerándose cada una de los diez áreas que contempla.

Guillermo B. Mora Marín

DIRECTRICES DEL PLAN DIRECTOR DE SEGURIDAD: ISO 17799

1. Introducción

En la actualidad cualquier organización debe reconocer que el buen funcionamiento de los sistemas de información es crítico en el desarrollo de sus actividades y, al mismo tiempo, que dichos sistemas se encuentran en situación de riesgo tanto por la propia vulnerabilidad de los sistemas como por una insuficiente implantación de políticas y normas de seguridad. Estas vulnerabilidades pueden producir perdidas de activos de la organización o perdida de la continuidad del negocio cuyo alcance hay que conocer para poder decidir el nivel de riesgo que se está dispuesto a asumir.

En esta situación se aborda la elaboración de un Plan Director de Seguridad para la organización con el objetivo de conocer el nivel de seguridad que presentan los sistemas informáticos, definir y diseñar el modelo de seguridad que se desea conseguir y planificar las acciones necesarias para ajustarse a ese modelo. Para responder a estas necesidades se plantea como hilo conductor la norma ISO/UNE/IEC 17799 de buenas practicas en la gestión de la seguridad.

2. La norma ISO/UNE 17799

Tiene su origen en la Británica BS7799 y más concretamente en su revisión del año 1999, adoptándose como ISO/IEC 17799 en el 2000 sin apenas modificaciones. En el 2004 se publica una nueva revisión BS7799-2 que se utiliza para establecer la norma UNE 71502, más enfocada a la auditoria de seguridad. La ISO/IEC 17799 es un reconocido estándar internacional usado como base común para desarrollar normas de seguridad dentro de las organizaciones.

La norma define la seguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información, siendo necesario para ello no solo medidas técnicas sino también políticas y organizativas. Para alcanzarla define diez áreas de control:

1. Políticas de seguridad
2. Organización de la seguridad
3. Clasificación y control de activos
4. Seguridad del 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 la continuidad
10. Conformidad

que cubren todo el ámbito de gestión de la seguridad planteando sobre ellas 36 objetivos de control y un total de 127 controles que nos pueden servir para validar el grado de adecuación a la norma. En cualquier caso es importante darse cuenta que será una labor prioritaria adaptar la ISO17799, y más concretamente el peso que se da a cada una de las áreas de la norma, a las características concretas del ámbito de aplicación del Plan Director que se quiere elaborar. Más detallado, se definen las siguientes áreas de control:

1. Políticas de seguridad

El objetivo principal es la elaboración de un documento de políticas de seguridad publicado por el máximo nivel directivo de la organización con una declaración apoyando sus objetivos y principios. En este documen-

to se describirán brevemente las políticas, principios y normas que en materia de seguridad se consideren esenciales y se establecerá la jerarquía de responsabilidades en la gestión de la seguridad indicando claramente quien se hace responsable de los activos. Incluirá referencias a la legislación aplicable y a los documentos de detalle donde se encuentran desarrolladas las normas. Se debe asegurar que se comunica esta política a todos los usuarios del sistema y que es fácilmente comprensible por todos ellos ya que es el medio de dar a conocer la implicación de la Dirección en las políticas de seguridad además de su contenido.

2. Organización de la seguridad

Se trata de desarrollar el documento gerencial de políticas de seguridad desde tres puntos de vista distintos, cuando los sistemas son gestionados por la propia organización, cuando existen accesos de terceras partes (asistencia técnica, por ejemplo) y cuando todos los sistemas de información están externalizados. En el primer caso debe haber un comité de dirección encargado de impulsar, hacer el seguimiento y revisar las políticas de seguridad, independientemente de que exista un responsable de seguridad encargado de la misma. Para la implementación de los controles puede ser conveniente la existencia de otro foro con representantes de áreas ajenas a las tecnologías de la información y que acuerde funciones, metodologías, revisiones o como realizar la difusión en materias relacionadas con la seguridad de la información. Deben definirse los responsables, en general los dueños, de cada recurso de la organización y de su protección, siendo conveniente delimitar claramente el área de responsabilidad de cada persona para que no existan huecos ni solapamientos; habitualmente habrá un responsable de seguridad que delegará la responsabilidad de seguridad en otras personas, pero en último término será él el responsable tanto del recurso como de validar la correcta implementación de las medidas de seguridad. Es de resaltar la importancia de tener correctamente establecido el protocolo de actuación ante la instalación de nuevos sistemas de información, ya que esta no se debe llevar a cabo sin el pertinente estudio del impacto que producirá en la seguridad y, en su caso, de las medidas suplementarias al plan de seguridad establecido.

En el caso de la contratación de terceros que desarrollarán su labor en nuestro sistema o de externalización total es esencial tener un modelo de contrato, validado por el departamento jurídico si hiciera falta, que contenga todos los requerimientos de seguridad para asegurar el cumplimiento de las políticas y normas de la organización, con especial hincapié en la Ley Orgánica de Protección de Datos. Además será lo suficientemente claro para que no puedan surgir malentendidos entre la organización y el proveedor.

3. Clasificación y control de activos

Para mantener una adecuada protección de los activos hay que identificar claramente cuales son y asignarles un grado de protección según su sensibilidad y criticidad, indicando en cada caso como ha de ser tratado y protegido.

Lo primero será contar con un exhaustivo inventario de activos que incluirá los recursos de información de todo tipo, recursos software y hardware, servicios informáticos y de comunicaciones y aquellos otros recursos que nos afecten como climatización, suministro eléctrico, etc. Una vez realizado se le asignará a cada recurso un grado de protección que marcara las medidas de seguridad que le serán aplicables y el tiempo durante el cual estarán vigentes siendo responsable de esta asignación el dueño o responsable del activo. Por último es conveniente manejar esta información de una manera organizada incluyendo algún tipo de clasificación sistemática que ayude a su mantenimiento y control.

4. Seguridad del personal

En cuanto al personal la seguridad se basará en tres pilares básicos, la seguridad inherente al puesto desempeñado, la formación en materia de seguridad y la respuesta ante incidentes.

La seguridad del puesto deberá enfocarse a evitar que personal malintencionado utilice los medios de la organización para provocar fallos de seguridad y se evitan con una adecuada política de selección de personal, tanto propio como contratado temporalmente, e incluyendo condiciones y términos en los contratos que indiquen claramente las responsabilidades y las obligaciones. El trabajo de todo el personal debe ser periódicamente revisado y nuevamente aprobado por un superior jerárquico.

La formación en materia de seguridad implica que ningún usuario desconozca la política general de seguridad ni las normas especificas que le afectan en el desarrollo de sus funciones. Para ello se promoverán cursos de formación y actualizaciones periódicas de los conocimientos, así como todas aquellas medidas de difusión que se consideren oportunas.

Es esencial para minimizar el numero de incidentes de seguridad y su alcance establecer un sistema de comunicación de incidencias hardware, software o de cualquier tipo, que todos los usuarios puedan utilizar y que sirva para reaccionar con rapidez ante cualquier amenaza o para evitarla antes de que se produzca. También habrá que disponer de un procedimiento establecido de respuesta a incidentes que establezca las acciones a realizar ante un aviso de incidente. Este sistema servirá también para actualizar las políticas de seguridad de la organización teniendo en cuenta los incidentes más habituales o graves. Por último se habrá de establecer y difundir las sanciones disciplinarias cuando sean los propios empleados los que provoquen los incidentes.

5. Seguridad física y del entorno

Un primer objetivo será impedir el acceso a las áreas seguras de personal no autorizado. Estas zonas habrán de estar claramente delimitadas pero no de forma claramente visible sino de una manera formal, con un perímetro permanentemente controlado. Se pueden definir varios tipos de zonas seguras dependiendo del tipo de sistema informático que contengan y de su grado de criticidad y, por lo tanto, las medidas de seguridad en cada tipo serán acordes a dicho grado. Las medidas para evitar accesos no autorizados y daños en los sistemas suelen ser barreras físicas y de control de cualquier tipo, pero también la ausencia de información sobre lo que contiene un área segura y la falta de signos externos que puedan hacer adivinar su contenido.

Deberá tenerse en cuenta cuando se diseñe el sistema de información que la ubicación e infraestructuras del mismo sean las adecuadas para reducir el riesgo de amenazas naturales como incendios, vibraciones, inundaciones, etc. También se pondrán medios para atajar aquellas no directamente relacionadas con el sistema de información pero que pueden afectar a su funcionamiento como pueden ser el suministro de energía incorporando un sistema de alimentación ininterrumpida de capacidad suficiente, proteger contra cortes o intrusiones el cableado de suministro de datos y energía, facilitar un adecuado mantenimiento de los equipos y establecer unas normas de seguridad para el equipamiento que contenga datos sensibles y que salga fuera de la organización y nunca permitir su salida sin autorización. Se debe asegurar que los soportes susceptibles de contener información sensible son físicamente destruidos o sobrescritos antes de desecharlos.

Es conveniente establecer políticas de escritorios sin papeles para evitar el robo o destrucción de datos y de pantallas limpias, no dejando en la misma ningún dato sensible al dejar el puesto sin atención.

6. Gestión de comunicaciones y operaciones

Los procedimientos operativos, cualquiera que sea su tipo, deben estar perfectamente documentados por su política de seguridad, detallándose para cada tarea sus requerimientos de programación, interdependencias con otros sistemas, tareas de mantenimiento previstas y procedimientos de recuperación ante incidentes. Asimismo se ha de dar especial importancia a los cambios en los sistemas o instalaciones ya

que son fuente frecuente de fallos del sistema y de seguridad.

Se debe establecer una serie de procedimientos de manejo de los incidentes para responder lo más rápida y eficazmente posible, estableciéndose como mínimo procedimientos para todos los tipos de incidentes probables, tratando de identificar las causas, indicando el modo de auditado del sistema afectado e incluyendo protocolos detallados de las acciones de recuperación.

Para reducir el riesgo de mal uso del sistema se deben separar las tareas de gestión de las de ejecución impidiendo que haga una misma persona todo el proceso. También se separaran las áreas de desarrollo de la de producción para evitar errores por incorrecciones en los sistemas o fallos forzados.

Cuando el sistema de información se encuentra en una instalación externa los controles deben ser los mismos pero deben encontrarse claramente especificados en el contrato.

Una adecuada monitorización del uso de los recursos del sistema nos permitirá detectar posibles cuellos de botella que derivarían en fallos del sistema y de seguridad, dando tiempo a planificar las ampliaciones o actualizaciones del sistema con la suficiente antelación. Estas ampliaciones se realizarán cuando estén perfectamente asegurado el correcto funcionamiento en el sistema existente y su adecuación a las normas de seguridad.

En cuanto a elementos software es esencial controlar la introducción de software malicioso que pudiera degradar los sistemas o introducir vulnerabilidades, para lo cual se implementarán los controles necesarios para evitar su instalación y se promoverán medidas para concienciar a los usuarios del riesgo que suponen y para formarles en un uso seguro del sistema.

Existirá un programa de copias de respaldo para todos los datos no recuperables de la organización, que se guardarán en una ubicación independiente con los mismos niveles de seguridad que en su emplazamiento original y por un periodo de tiempo que dependerá de la naturaleza y sensibilidad de los datos. Se realizarán ensayos de recuperación para comprobar la viabilidad del protocolo y validez del programa.

Se mantendrá un registro de actividades del personal de operación así como de los errores del sistema detectados, revisándolos para verificar la resolución de los fallos y que las medidas que se tomaron para ello estaban dentro de las normas.

La administración de las redes de datos deben incluir los controles necesarios para garantizar la seguridad de los datos y la protección de los servicios contra el acceso no autorizado. Se tomarán medidas adicionales, principalmente cifrado, cuando los datos sean especialmente sensibles.

Cualquier medio susceptible de almacenar datos ha de ser tenido en cuenta dentro de las políticas de seguridad y especialmente los soportes removibles como discos o papel, estableciéndose procedimientos operativos para protegerlos contra robo, daño o acceso no autorizado y procedimientos para su destrucción o borrado total cuando no vayan a ser utilizados de nuevo. La documentación del sistema debe ser también protegida ya que suele contener información valiosa y que puede ser utilizada para vulnerar el sistema.

Un apartado especial tienen los intercambios que se realizan entre distintas organizaciones que debido a la variedad de formatos implicados (correo electrónico, comercio electrónico, mensajero, fax, teléfono, etc.) exigen un control cuidadoso. Se establecerán acuerdos (preferiblemente escritos) con las otras organizaciones que respeten por una parte la política de seguridad de la organización y por otra la legislación aplicable, solo se utilizarán medios de transmisión que sean seguros y se establecerán normas para que el propio envío (datos, paquetes, etc.) incluya todas las medidas de seguridad consideradas adecuadas a su naturaleza. Respecto al correo electrónico se elaborará una política clara para todos los usuarios respecto al uso de anexos y almacenamiento de los mismos, el uso responsable de tal manera que no se comprome-

ta a la organización y técnicas de cifrado para proteger la confidencialidad y la integridad. En definitiva se promoverá entre el personal de la organización una actitud activa por la seguridad formando sobre actos cotidianos que la comprometen y que son fáciles de evitar como intentar no ser escuchado al hablar por teléfono, no usar contestadores o el envío de fax con información sensible a números equivocados.

7. Control de accesos

Se deben definir y documentar las reglas y derechos de acceso a los recursos del sistema de información para cada usuario o grupo de usuarios en una declaración de política de accesos. Está política debe ser coherente con la clasificación de los activos y recorrer exhaustivamente el inventario de recursos. Por otra parte las reglas que se definan deberán ser preferiblemente restrictivas (no permitir el acceso nunca excepto cuando se necesite mejor que permitirlo siempre excepto cuando exista riesgo) y modificables solo por el administrador.

Se implementará un procedimiento formal que cubra todo el ciclo de vida del registro de un usuario, desde su alta donde se verificará que los accesos otorgados sean los adecuados a las necesidades y que exista un permiso de uso de los recursos accedidos, la cancelación inmediata de permisos ante cambios en las tareas del usuario, verificaciones periódicas de consistencia de los permisos y usuarios del sistema o utilización de identificadores únicos.

Es importante limitar todo lo posible la asignación de privilegios que permitan evitar los controles de acceso estándar ya que son la principal vulnerabilidad de un sistema, por lo que deberán estar perfectamente identificados, asignarse sobre la base de la necesidad de uso y evento por evento y a un identificador de usuario distinto al de uso habitual. Los derechos de acceso serán revisados a intervalos regulares y tras cada cambio en un usuario y los privilegios con una mayor frecuencia.

La asignación de contraseñas se controlará a través de un procedimiento formal que impida su almacenamiento o envió sin la debida protección y que incluya reglas para impedir su captura o adivinación. En entornos especialmente sensibles se proveerán sistemas de identificación más fuertes como huellas, candados hardware u otros. Por otra parte se informará a los usuarios de buenas prácticas en el uso de contraseñas como no compartirlas ni tenerlas escritas o cambiarlas regularmente y usar contraseñas de calidad. Es conveniente bloquear por contraseña las sesiones de terminal o PC cuando el usuario se ausente del puesto.

Es esencial para la organización la protección de los servicios de red para impedir que sean interrumpidos o accedidos ilegalmente. Las normas para su protección, que han de ser coherentes con la política de control de accesos, se plasmarán en un documento de política de uso de los servicios de red. Todo usuario externo o nodo automático que intente acceder al sistema ha de ser autentificado preferiblemente con técnicas fuertes como el cifrado o candados hardware. Es recomendable la definición de caminos forzados entre terminales de usuario y los servicios del sistema así como la división de la red en subredes lógicas y aisladas. Todos los accesos a la red deben ser validados contra las reglas de control de accesos e incluir un control de origen y destino de la conexión, independientemente de las validaciones de seguridad que cada servicio del sistema incluya.

Es importante vigilar el acceso al sistema operativo ya que su control supone el dominio de una parte importante del sistema, por lo que se usarán todas las medidas de seguridad que incluya destacando la identificación y verificación segura de los usuarios, aplicaciones y terminales y el registro de los intentos de conexión al sistema. Se dispondrá de una sólido sistema de administración de contraseñas y se establecerán reglas sobre limitación del horario de uso y desconexión automática por inactividad.

El acceso a las aplicaciones estará limitado a los usuarios autorizados basándose en las normas de control

de accesos y estará claramente documentado para cada aplicación su nivel de sensibilidad, aplicando las medidas de seguridad indicadas a dicho nivel.

Es esencial para preservar la seguridad del sistema la monitorización y seguimiento de todas las incidencias que se produzcan lo que permitirá la detección temprana de incidentes y la validación de la bondad de los controles de seguridad adoptados. Se guardará un registro de los eventos de seguridad como accesos con o sin éxito a aplicaciones o a datos, usuarios que han accedido y por cuanto tiempo, alarmas del sistema y otros que se consideren necesarios para la recolección de evidencias de incidentes. Regularmente este registro debe ser revisado en busca de evidencias que indiquen algún compromiso de la seguridad.

Cuando en el sistema exista la posibilidad de teletrabajo o de computación móvil será necesario estudiar la sensibilidad de los sistemas desplazados e implementar las medidas de seguridad acordes con la misma y, al mismo tiempo, se dictarán normas especificas para este tipo de sistemas como por ejemplo sobre la seguridad física de los equipos contra robo o rotura o sobre el uso en público de los mismos.

8. Desarrollo y mantenimiento de sistemas

Se trata de asegurar que todos los requerimientos de seguridad que se han definido son incluidos en el sistema de información ya que es en el momento del desarrollo de los sistemas cuando más económico es implementarlos.

Las aplicaciones se deben diseñar para que incluyan los controles de acceso necesarios así como para que dejen registro de actividad. Se validarán los datos de entrada y de salida y se verificara la integridad y autenticidad de los mismos según se considere necesario.

Se utilizarán técnicas de cifrado para preservar la confidencialidad, autenticidad e integridad de la información que, tras una evaluación de los riesgos, sea considerada como especialmente sensible. Esta política en materia de cifrado tendrá en cuenta la legislación aplicable así como los estándares técnicos y las necesidades de la organización. También incorporará los casos y condiciones de uso de la firma digital o de servicio de no repudio. Es esencial la gestión de las claves de cifrado por lo que se establecerán normas y procedimientos para su administración, tanto en el caso de técnicas de clave secreta como de clave pública.

En el entorno de producción se controlará el acceso al software de sistema así como a los datos de prueba que se haya podido utilizar y a las bibliotecas de código fuente ya que contienen información interna sensible sobre el funcionamiento del sistema. En el entorno de mantenimiento se verificará que todos los cambios que se realicen en las aplicaciones están autorizados y existirá un procedimiento para llevarlos a cabo, al igual que las revisiones técnicas del sistema operativo o los cambios en los paquetes comerciales de software; todos los cambios han de quedar perfectamente documentados y tener una verificación previa de conformidad con las normas de seguridad.

9. Gestión de la continuidad

Toda organización ha de contar con un plan de actuación ante contingencias que permita identificar y reducir los riesgos de que se produzcan interrupciones en el servicio, atenuar en lo posible las consecuencias de los incidentes y asegurar que se reanuda la actividad lo antes posible.

La implementación de un proceso controlado para el mantenimiento de la actividad debe incluir una identificación clara de los eventos que pueden provocar su interrupción, evaluando el riesgo de ocurrencia y calculando el impacto que tendría sobre la organización, y esto para cada proceso de la organización. En base a esto se documentaran los procedimientos de actuación ante incidencias y se formará al personal

que deba llevarlos a cabo, realizando las pruebas necesarias y actualizando los procedimientos cuando se produzcan cambios en el sistema o cuando las pruebas de reevaluación indiquen fallos. Estos planes contendrán como mínimo las causas de activación, el personal implicado y los procedimientos de actuación y de recuperación con sus diagramas de tiempos correspondientes, y debe tener un propietario o responsable del mismo. Asimismo se realizará el mantenimiento periódico del plan de continuidad para garantizar que es eficaz y que se encuentra vigente.

10. Conformidad

Se exigirá al sistema de información el total respeto a la legislación vigente, y en especial a la Ley Orgánica de Protección de Datos, la Ley de Servicios de la Sociedad de la Información y la Ley de Firma Electrónica, incluyendo también los derechos de propiedad intelectual. Dentro de los controles de la conformidad se incluirán la conservación de aquellos ficheros o registros que determine el marco legal, el uso adecuado por parte del personal de los recursos de la organización y el uso que se hace de las técnicas de cifrado. Es conveniente mantener un registro de evidencias que, desde un punto de vista legal, pudiera ser utilizado en un tribunal, por lo que deberán cumplir todos los requisitos para su admisión como son la validez general a través del cumplimiento de estándares, la calidad con copias fieles y la totalidad de la prueba, conservando todo el registro de la acción.

La política de seguridad de la información debe estar en permanente revisión para, por una parte, vigilar que se esté produciendo un adecuado cumplimiento de la misma por todas las áreas de la organización y por otra mediante el uso de una batería de verificaciones técnicas para comprobar que el sistema es seguro ante las incidencias que se puedan prever. Se proveerán herramientas de auditoria que deben estar separadas del resto de sistemas de información y cuyo uso estará limitado y controlado por un acuerdo donde se indique el alcance de las verificaciones y los procedimientos a llevar a cabo.

3. Conclusiones

En el Plan Director de Seguridad se ha de plasmar la visión estratégica de la seguridad que tiene la organización. La norma ISO 17799 es un estándar internacional comúnmente aceptado que ha de servir de guía exhaustiva de todas las necesidades de seguridad que una organización puede tener, permitiendo verificar el estado actual de la seguridad del sistema e identificar claramente unos objetivos a alcanzar a corto, medio y largo plazo, que posteriormente serán verificados con la misma norma.