Nota del profesor: este guión es únicamente orientativo, y no se obliga a seguir este mismo orden y división en secciones ni a utilizar LaTeX. Sin embargo, se recomienda que el formato usado, sea cual sea, contenga la información recogida en este esquema. Es posible que no todo sea necesario, particularmente en organizaciones de menor tamaño.
Se recomienda hacer referencia y seguir las recomendaciones de las normas UNE-ISO/IEC 27001 [3], UNE-ISO/IEC 27002 [1] (disponible a través de NORWEB en biblioteca.uca.es), UNE 71501 [2], la metodología MAGERIT [4] y el resto del material del Campus Virtual. En particular, la norma UNE 71501-3 da ciertas guías sobre el contenido que debería tener una política de seguridad de TI de una organización.

Universidad de Cádiz
Seguridad y Competencias Profesionales
Curso 2012/2013

Política de Seguridad de Tecnologías de la Información de ABC S.A.

Miembro Primero
Miembro Segundo
Miembro Tercero
Miembro Cuarto

8 de octubre de 2012

Índice general

Índice de figuras

Índice de tablas

Historial de cambios

Fecha	***Cambios***
8 de octubre de 2012	Primera versión del documento.

Compromiso de la dirección

En este capítulo (no numerado) se escribirá una carta formal firmada y sellada por los miembros relevantes de la dirección de la compañía y por el Responsable de Seguridad, en la que se relaciona la seguridad con las metas de la organización, se valida la versión actual de la política y se compromete a proveer los recursos necesarios para su ejecución.

1. Introducción

1.1. Descripción de la organización

Nombre de la organización, a qué se dedica, de qué activos (a alto nivel: locales, edificios, etc.) dispone, cuál es su organigrama, etc.

1.2. Objetivos y alcance de la política

Aquí se indica qué nivel de seguridad se desea obtener, y se relacionan con los objetivos de la organización. Hay que además limitar el alcance de la política, para evitar cubrir demasiado terreno, que puede exigir demasiado tiempo.

1.3. Gestión de cambios de la política

Una política de seguridad no es algo estático, sino que se va revisando continuamente. Habrá que describir la forma en que se recogen las propuestas de cambio, se realizan los cambios pertinentes y se difunde de nuevo al resto del personal la última versión de la política, de forma clara e inequívoca.

1.4. Organización de la seguridad

En esta sección se describe cómo se va a organizar la gestión de la seguridad en la organización, a lo largo de todo su organigrama. Debería tenerse en cuenta a todos los departamentos, y no sólo al de Informática.

Hay que definir responsabilidades y gestión de los informes de las incidencias. También se deberían definir a alto nivel los mecanismos que se usarían para comprobar que se llevan a cabo las medidas indicadas en este documento.

En este apartado se deberían tener en cuenta las medidas explicadas en «Seguridad en el entorno» para limitar el riesgo por ataques internos, tomando en cuenta la matriz de peligrosidad mostrada en las transparencias.

2. Política de seguridad de la información

Este capítulo puede dedicarse a los riesgos que afectan a la información almacenada y obtenida en la organización (consúltese la metodología MAGERIT - versión 2 [4]). Para ello, habrá que describir qué información a nivel abstracto trata la organización y cuál es su nivel de sensibilidad.

Habrá que relacionarla con la Ley Orgánica de Protección de Datos, aunque **los documentos de seguridad para la LOPD tendrán que elaborarse por separado de este trabajo**. Para los documentos de seguridad se pueden seguir los modelos disponibles en el Campus Virtual.

Este capítulo hará referencia a las medidas implantadas en otros capítulos dedicados a la seguridad de las comunicaciones (capítulo 6 on page 11), del software y hardware (capítulo 5 on page 9) y de la seguridad física (capítulo 3 on page 5), entre otros.

2.1. Información recogida

Descripción a alto nivel de la información que utiliza la organización para llevar a cabo sus fines.

2.2. Análisis de riesgos y sensibilidad

Aquí se haría un estudio de lo delicada que es la información tratada, y de a qué riesgos se halla sometida, de acuerdo con las tres bases de la seguridad (confidencialidad, integridad y disponibilidad).

2.3. Conformidad con la legislación vigente

Se equiparará la información antes recogida con los requisitos impuestos por la Ley Orgánica de Protección de Datos y otras leyes aplicables, si las hay, y se hará referencia a sus documentos de seguridad, a elaborar por separado.

3. Política de seguridad física

En este capítulo se indicarán las medidas que se usarán para proteger los activos de la organización, de acuerdo con lo indicado en el tema de «Seguridad en el entorno». Las medidas a implantar se basarán en un análisis previo de los riesgos existentes.

Se recomienda consultar «Seguridad física COMO», MAGERIT (versión 2) [4], el estándar UNE-ISO/IEC 27002 [1] y las normas UNE 71501 [2] disponibles en el Campus Virtual. En la norma UNE 71501-3 se recogen algunos de los tipos de riesgos más comunes: entradas no autorizadas, rayos, robos, incendios, accesos no autorizados a estaciones de trabajo, etc.

3.1. Activos

Activos de la organización a nivel físico: locales a proteger, teniendo en cuenta su división en áreas más y menos sensibles.

3.2. Seguridad del edificio

Edificio en general: fluido eléctrico, líneas de teléfono, protección contra entradas no autorizadas, protección contra incendios, etc.

3.3. Seguridad del centro de datos

Protección del centro de datos en que se alojan los servidores: emplazamiento, uso de falso techo/suelo, aire acondicionado, control de acceso y auditorías, etc. Es posible que la protección a incendios o alguna de las medidas a nivel de edificio cambie aquí.

3.4. Seguridad del lugar de trabajo

Protección de la estación de trabajo de cada empleado, evitando accidentes laborales, entradas no autorizadas, robos, volcado de líquidos, etc.

4. Política de control del personal

En este capítulo se deben tratar aquellos riesgos correspondientes con los ataques provenientes de atacantes externos e internos, y la formación de los usuarios, entre otras cosas, de acuerdo con el tema «Seguridad en el entorno».

Además de los recursos situados en el Campus Virtual, deberían tenerse en cuenta las recomendaciones de la guía UNE-ISO/IEC 27002 [1].

4.1. Proceso de contratación

Se describirán las modificaciones necesarias sobre el proceso de contratación para asegurar la seguridad en TI. No es necesario describir el resto del proceso (p. ej. aspectos administrativos).

4.2. Proceso de despido

Como el anterior apartado, pero para cuando alguien deja la organización.

4.3. Formación y concienciación del personal

Especifica qué acciones se llevarán a cabo para que el personal conozca la importancia de la seguridad y sepa qué hacer en cada caso.

4.4. Medidas disciplinarias

Acciones a realizar cuando el personal voluntaria o involuntariamente rodea o va en contra de alguna de las medidas de este documento.

4.5. Personal temporal y subcontratado

Indica cómo se atajarán los problemas de seguridad que supone el acceso de personal externo a la organización a sus facilidades.

5. Política de seguridad en software y hardware

En este capítulo se tratarán los aspectos relacionados con la seguridad del software desarrollado y/o utilizado internamente, y la prevención, detección y diagnóstico del software malicioso. También se tratarán los aspectos relacionados con el hardware de los activos de la organización.

Para los aspectos de desarrollo de software, se puede tomar como guía en la sección de desarrollo las recomendaciones de las transparencias y los informes CWE más relevantes, posiblemente integrándolos en las revisiones periódicas del código, si se desean implantar.

Habrá que analizar los riesgos que supone el software malicioso, y en base a ellos plantear las debidas medidas de prevención, detección y recuperación.

5.1. Identificación y autenticación

Se recogen las distintas medidas a través de las cuales se limitará el acceso a los distintos equipos al personal que los necesite para su trabajo.

5.2. Registro de accesos

En algunos equipos puede ser útil llevar un control de quién ha accedido, desde dónde, etc.

5.3. Protección ante software malicioso

Medidas para mitigar los riesgos relacionados con el software malicioso.

5.4. Uso aceptable de los equipos

Se recogería cuál es el uso aceptable de los equipos de la organización, dividiéndolos según su aplicación (servidores, estaciones de trabajo y portátiles).

5.5. Gestión de soportes

Medidas a la hora de almacenar y desechar los soportes de almacenamiento.

6. Política de seguridad de las comunicaciones

Esta sección se dedicará a describir cómo se protegerán las conexiones internas y externas, los datos que recorran la red interna de la organización, y cómo se evitarán las fugas de información hacia el exterior.

6.1. Infraestructura y topología de la red

Hay que describir la red existente a alto nivel, con el equipamiento utilizado. Como mínimo debe describirse la topología a alto nivel, con sus enrutadores, conmutadores y estaciones de trabajo. Normalmente se seguirá un cableado estructurado, si la organización es lo suficientemente grande.

6.2. Seguridad de las conexiones al exterior

Se describirán las conexiones al exterior (Internet, PBX) y cómo se protegerán ante accesos no autorizados. Si se estima necesario, pueden tomarse medidas para asegurar la disponibilidad de la conexión (enlaces redundantes, por ejemplo).

Normalmente habrá que establecer un perímetro de seguridad para proteger la red de la organización de las amenazas exteriores.

6.3. Seguridad de la información transmitida

Medidas para evitar que la información transmitida sea bloqueada, interceptada, modificada o falsamente fabricada.

6.4. Seguridad en el teletrabajo

Si en la organización se permite el teletrabajo, habrá que tomar las medidas necesarias para que esto no suponga una amenaza de seguridad.

7. Política de continuidad del negocio

Este capítulo se dedica fundamentalmente a las medidas de recuperación en caso de un ataque o un desastre.

7.1. Introducción

En esta primera sección se puede describir qué partes son especialmente vitales para el funcionamiento continuado de la organización, y que por lo tanto requieren de una mayor inversión de sus recursos.

Habrá que priorizar la recuperación de ciertos activos frente a otros: servidores frente a estaciones de trabajo, datos sensibles frente a información derivada, etc.

7.2. Copias de seguridad

Esta sección se dedica a las copias de seguridad, indicando de qué se harán copias, con qué frecuencia, de qué tipos, usando qué soportes y juegos de copias, etc.

7.3. Recuperación de activos

Planificación para la recuperación de un activo ante un desastre o un ataque. Puede tratarse de una parte de las infraestructuras, hardware, software (con su configuración asociada), o datos.

Para software, por ejemplo, lo usual es mantener documentación actualizada sobre el estado de la configuración de los sistemas, de forma que ante un ataque al software se pueda reinstalar y volver a configurar. Esto requiere señalar quién será responsable de mantener dicha documentación al día, con qué periodicidad será revisada, y quién llevará el control de dichas medidas, entre otros aspectos.

A. Presupuestos de material

Aquí se listará una serie de presupuestos iniciales para los distintos elementos que puedan utilizarse para llevar a cabo la política.

A.1. Software

Presupuestos del software necesario: cortafuegos, antivirus, etc.

A.2. Hardware

Presupuestos del hardware necesario: equipamiento de red, sistemas de alimentación ininterrumpida, etc.

A.3. Infraestructuras

Presupuestos para los materiales de infraestructuras: detectores de humo, detectores de presencia, cámaras de seguridad, armarios ignífugos, cerrojos de múltiples cilindros, extintores, etc.

A.4. Servicios

Presupuestos para cursos de formación y concienciación (a menos que sean internos), contratación de personal de seguridad, alquiler de cámaras conectadas a una centralita remota, etc.

B. Otros anexos

Se dedicarán más anexos para aquellas listas y materiales que por su extensión rompan el flujo normal del texto de una determinada política, o que se consideren que pueden cambiar con más frecuencia.

Posibles anexos incluyen:

- Formularios a utilizar para gestionar las incidencias
- Normativa y legislación aplicable
- Procedimientos del responsable de seguridad y/o el comité de seguridad

Bibliografía

[1] AENOR. UNE-ISO/IEC 27002:2005 - código de buenas prácticas para la gestión de la seguridad de la información.

[2] AENOR. UNE 71501:2003 - guía para la gestión de seguridad de TI, 2003.

[3] AENOR. UNE-ISO/IEC 27001:2005 - tecnología de la información - técnicas de seguridad - sistemas de gestión de seguridad de la información (SGSI) - requisitos, noviembre 2007.

[4] Ministerio de Política Territorial y Administración Pública. MAGERIT (versión 2). URL http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184