El sistema informático dentro de la organización

El responsable de informática

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

PID_00190212

UOC
Universitat Oberta de Catalunya

Índice

Introducción

En este módulo hablamos del responsable de informática y de su relación con la organización y el departamento de informática. En concreto, del tipo de decisiones que tiene que tomar y de cómo se coordina con la figura del administrador del sistema informático.

El sistema informático es la herramienta, y los administradores, las figuras que la mantienen en funcionamiento. Pero el responsable de informática es la figura que toma las decisiones de la función del sistema informático dentro de la organización. Decide qué puede hacer con los recursos de que dispone el departamento, y tiene una visión de futuro sobre qué habrá que hacer. Es decir, cuál tiene que ser la funcionalidad del departamento de informática dentro del conjunto de la organización en el momento presente y en el futuro. Tiene que gestionar aspectos como el plan estratégico y el plan de seguridad informático, que hoy día se pueden implementar con metodologías estándar.

En el módulo también damos algunos criterios que pueden ayudar a tomar decisiones, por ejemplo, en el momento de decidir sobre la implantación de software, o cómo se tiene que actuar ante problemas de seguridad.

Objetivos

En los materiales didácticos de este módulo presentamos los contenidos y las herramientas para alcanzar los objetivos siguientes:

1. Conocer las responsabilidades del responsable de informática.

2. Conocer las decisiones que tiene que tomar el responsable del departamento en el diseño de una aplicación.

3. Saber actuar como es debido ante un problema de seguridad.

4. Conocer el concepto de plan en una organización y conocer algunos de los que puede haber.

5. Conocer los principales planes de seguridad y métodos estándar de gestión del riesgo.

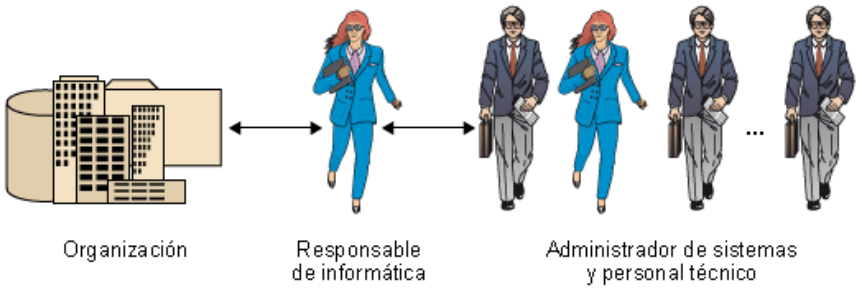
6. Saber prever las posibles amenazas y riesgos que pueden poner en peligro el sistema informático y prepararse para minimizar las consecuencias.

1. El responsable de informática

Para poder ser eficiente el responsable de informática tiene que ejercer una función muy importante como transmisor de información entre el departamento de informática y la organización. Es el puente de comunicación en las dos direcciones (técnicamente hablando).

Esto quiere decir que el responsable de informática tiene información relativa a la situación de la organización que el personal técnico no tiene que conocer necesariamente. Además, el responsable vela por una serie de planes que llevan a cabo los administradores (o incluso otros departamentos o los que estén contratados externamente) relativos a la informática de la organización.

Tal como se ve en el gráfico, la figura del responsable de informática es quien gestiona los recursos del departamento (tanto humanos como materiales). Por lo tanto, tiene que tener un conocimiento de la organización y del departamento perfecto para conseguir que los dos elementos se muevan de forma sincronizada. Ha de conseguir que el departamento de informática se ajuste al máximo a los objetivos de la organización con los recursos que esta última le da. En la práctica, es siempre un canal de comunicación en los dos sentidos para detectar necesidades, conseguir recursos, ajustar objetivos, etc.



El responsable de informática hace de puente

El responsable de informática gestiona los recursos del departamento de informática y hace de unión entre el departamento y la organización.

Como hemos dicho, el responsable de informática tiene una visión más global de todo. Por lo tanto, necesita la figura del administrador, que es quien cuida de los servidores. Esta persona le ofrece la situación y la visión técnica del departamento de informática en cada momento. Por lo tanto, le puede asesorar para tomar muchas decisiones sobre software y hardware. En la práctica, la mayoría de decisiones técnicas se toman con la ayuda del administrador de sistemas.

Así, el responsable de informática tendrá la visión más técnica, así como sus necesidades y la visión del plan estratégico de la empresa, y por lo tanto, la vertiente más dedicada a la gestión de la informática. Muchas veces verá cómo no puede acceder a las peticiones de uno de estos grupos por los requisitos que tenga del otro grupo.

2. Los planes

Todas las organizaciones, con el fin de estar coordinadas y preparadas para cualquier situación, siguen una serie de planes que los jefes de cada departamento tienen que preparar, revisar y tener a punto.

2.1. Plan estratégico de la organización

El plan estratégico es una planificación, normalmente quinquenal, en que se establece la orientación de la organización para alcanzar los objetivos que se propone. Este plan estratégico de la organización se tiene que concretar, posteriormente, en un plan estratégico para cada departamento vinculado al plan estratégico global.

> Una planificación estratégica es un conjunto de propuestas realistas para fijar los objetivos de la organización en un futuro.

Como el responsable de informática tiene que establecer el plan estratégico del departamento de informática, veamos cómo es, a grandes rasgos, el plan estratégico de una organización. El de un departamento parte del plan estratégico de la organización.

2.1.1. La planificación estratégica

Frente a una sociedad cambiante, la organización se tiene que adaptar a ella para cumplir sus objetivos. La planificación estratégica es una herramienta útil y necesaria para ajustar el funcionamiento de la organización en el seno de la sociedad.

La planificación estratégica tiene que ser una herramienta para integrar todos los departamentos en unos mismos objetivos y en un marco de trabajo común.

> La planificación estratégica, para minimizar riesgos y maximizar resultados, tiene que plantear estrategias y objetivos simples, claros, alcanzables y mesurables.

2.1.2. Metodología

Se tiene que recopilar información interna y externa. La externa proviene del análisis del entorno para identificar las **oportunidades** y **amenazas**. La información interna permite identificar las **fortalezas** y **debilidades** de la misma organización.

Ved también

Ved, en el subapartado 2.1.4, cómo se hace un análisis DAFO.

Entre los aspectos fundamentales que tienen que constar en el análisis podemos incluir, por ejemplo, la evaluación de los servicios que se hacen o los sistemas de administración.

2.1.3. Componentes del plan estratégico

A continuación mencionamos los componentes de un plan estratégico:

- **Declaración de la misión**. La declaración de la misión simplemente intenta determinar el objetivo final al cual se pretende llegar.

- **Visión**. Es el camino que hay que seguir para conseguir la misión. La visión será la guía para las acciones que se llevarán a cabo.

- **Problema estratégico general**. Determinar factores internos o externos que pueden afectar a la consecución de la misión.

- **Solución estratégica general**. Dar estrategias que permitan alcanzar la misión y superen, por lo tanto, los problemas estratégicos.

- **Objetivos y estrategias**. Determinar los objetivos e implementar las estrategias es clave para la planificación. Los objetivos, al menos con respecto a los departamentos, tienen que ser de tipo cualitativo. Es decir, tienen que ser cuantificables para poder medir su cumplimiento y poder formularlos en acciones estratégicas.

- **Presupuesto y control**. Los objetivos y las acciones se tienen que prever en los presupuestos.

2.1.4. El análisis DAFO

En los últimos años, el análisis DAFO[1] se ha convertido en una herramienta de diagnóstico dentro de la dirección estratégica de la organización. Junto con el diagnóstico financiero y el funcional, forman las tres partes básicas para el análisis interno de una organización.

(1)DAFO es la sigla de "debilidades, amenazas, fortalezas y oportunidades". En inglés, SWOT: *strengths, weaks, oportunities and threats*.

El objetivo es concretar en una tabla la evaluación de los puntos fuertes y débiles de la organización con las amenazas y las oportunidades externas. Todo esto partiendo de la base de que la estrategia pretende conseguir un ajuste adecuado entre la capacidad interna de la organización y su posición competitiva externa.

Lo más importante es encontrar lo que nos permite identificar y medir los **puntos fuertes**, los **puntos débiles**, las **oportunidades** y las **amenazas** de nuestra organización, que reuniremos en esta tabla. Las fortalezas y debilidades internas son muy importantes, ya que nos ayudan a entender la posición de nuestra organización en un entorno concreto. Cada organización tiene que ver cuáles son las variables adecuadas que determinan la posición dentro del mercado, segmento o sociedad en que está inmersa.

Una vez definidas estas variables, tenemos que hacer un proceso de *benchmarking* o análisis comparativo con las mejores organizaciones competidoras (es posible que, a lo largo de este proceso, identifiquemos alguna oportunidad nueva).

Finalmente, hacemos el gráfico que recoge las posibles estrategias. En esta matriz DAFO, en las columnas estableceremos el **análisis del entorno** (1.ª columna: amenazas, 2.ª columna: oportunidades) y en las filas, el **diagnóstico de la organización** (1.ª fila: puntos fuertes, 2.ª fila: puntos débiles). Cada uno de los cuatro cuadrantes refleja las posibles estrategias que tiene que adoptar la organización.

DAFO	Amenazas	Oportunidades
Puntos fuertes	Estrategias defensivas	Estrategias ofensivas
Puntos débiles	Estrategias de supervivencia	Estrategias de reorientación

El estudio de la matriz se hace mirando aisladamente cada cuadrante. Por ejemplo, si vemos el primer cuadrante (1-1 puntos fuertes-amenazas), tendremos que identificar cada uno de los puntos fuertes que hay en la organización, junto con cada una de las amenazas del exterior que tiene. Así pues, tenemos que analizar cada intersección para ver las consecuencias y las acciones que se pueden derivar.

2.2. Plan de seguridad y análisis de riesgos

El plan de seguridad y análisis de riesgos tiene que velar por la seguridad de todo el equipamiento informático de la organización. La responsabilidad del responsable de informática es hacerlo y asegurar que se llevará a cabo correctamente.

La ISO define el riesgo tecnológico como la probabilidad de que ocurra una amenaza usando vulnerabilidades existentes de un activo o activos generando pérdidas o daños. En base a esta definición, existen diversos elementos en juego (amenazas, vulnerabilidades, activos...), y por lo tanto hay muchas maneras de enfocar el riesgo. Nosotros lo haremos basándonos en el plan de prevención de riesgos laborales. Se fundamenta en la idea de que la seguridad es parte de un mecanismo global de tres componentes:

Observación

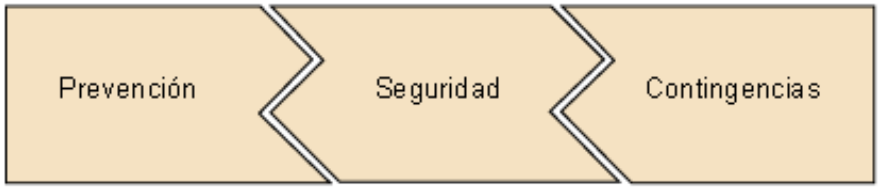
El mecanismo del plan de prevención se aplica a muchos otros sectores con otros nombres, como planes de prevención y evacuación, planes de emergencias, etc.

1) Prevención. El objeto de interés en este componente radica en lo que se desea proteger. Es necesario averiguar qué nos interesa proteger y qué soluciones existen para proteger nuestro sistema.

2) Seguridad. En esta fase tenemos que "implementar" la seguridad. Éste es el plan de seguridad, es decir, cómo protegeremos.

3) Contingencia. Tenemos que tener presente que los sistemas pueden fallar, bien sea por ataques debidos a intrusos o por causas externas que no controlamos, como los desastres naturales. Por lo tanto, es necesario prever los protocolos de actuación ante una situación de estas características, es decir, qué hacer cuando falla la seguridad.

Esquema genérico de un plan de prevención



2.2.1. Prevención

El plan de prevención, aplicado sólo al entorno informático, es un plan que implica analizar los posibles riesgos a los que puede estar expuesto el equipamiento informático y la información que hay (en cualquier medio de almacenamiento). Se trata de analizar qué puede pasar y qué queremos proteger.

En el **análisis de riesgos** es necesario asegurarse de que se tienen en cuenta todas las posibles causas de riesgos que pueden provocar problemas en el sistema. Se hace un análisis de los riesgos, que se basa en calcular la posibilidad de que tengan lugar hechos problemáticos, se obtiene una valoración económica del impacto de estos éxitos negativos y se contrasta el coste de la protección con el hecho de volver a crearla o comprar. Esta operación se repetirá con el resto de los "activos" (equipos informáticos, por ejemplo).

- Imaginarse qué puede pasar (qué puede ir mal).

- Estimar el coste que comportaría para la organización.

- Estimar la probabilidad de que se dé cada uno de los problemas posibles. Eso permite priorizar los problemas y su coste potencial, y desarrollar el plan de acción adecuada.

El análisis de riesgos pasa primeramente por responder preguntas como las siguientes:

- ¿Qué puede ir mal?
- ¿Con qué frecuencia puede pasar?
- ¿Cuáles serían las consecuencias?

Fundamentalmente, evaluar los riesgos representa tener claras cuestiones como las siguientes:

- ¿Qué se intenta proteger?
- ¿Qué valor le da la organización?
- ¿De qué se quiere proteger?
- ¿Cuál es la probabilidad de un ataque?

El procedimiento para hacer un plan de riesgos es el siguiente:

1) Evaluar los riesgos en una reunión del responsable de informática con el resto de jefes de departamento para tratar qué riesgos en seguridad informática tiene que afrontar la organización. Una vez se ha hecho la relación, se tiene que ver cómo se puede actuar para prevenir las causas y cómo es debido actuar para minimizar los efectos.

Riesgos de seguridad

Algunos de los riesgos que una organización puede tener que hacer frente son:

- Al fuego, que puede destruir equipamiento e información.
- Al robo de equipamiento y archivos.
- A actos vandálicos que estropeen equipamiento y archivos.
- A fallos en el equipamiento que estropean archivos.
- A errores que estropean archivos.
- A virus, que estropean equipamiento y archivos.
- A accesos no autorizados, que comprometen la información.

2) Se tiene que evaluar la probabilidad de que tenga lugar cada una de estas causas.

Y así para todas las causas que hayan aparecido en la reunión.

Qué probabilidad hay de que el fuego destruya el equipamiento e información.

- ¿La organización tiene alguna protección contra incendios?
- ¿Son necesarios sistemas de aspersión automática?
- ¿Hacen falta extintores? ¿Hay?
- ¿Son necesarios detectores de humos? ¿Hay?
- ¿El personal tiene alguna formación para actuar ante un incendio?

¿Qué probabilidad hay de que los fallos del equipamiento estropeen la información?

- ¿El personal informático lleva a cabo el mantenimiento de los equipos dentro de los tiempos previstos?
- ¿Cuáles son las condiciones actuales del hardware?

3) Se tiene que determinar la probabilidad para cada riesgo: muy alto, alto, medio, bajo, muy bajo.

4) Se hace el resumen de los riesgos ordenados por el factor de riesgo de cada uno.

Tipo de riesgo	Factores de riesgo
Robo	Alto
Fallos en equipamiento	Medio
Acción de virus	Medio
Robo de datos	Bajo
Fuego	Bajo
Fraude	Muy bajo

Análisis de los puntos débiles de la seguridad de la red informática

Una de las tareas del departamento de informática es estudiar el hardware, el software, su localización, instalación, etc., todo con el objetivo de buscar resquicios en la seguridad. Cualquier ordenador conectado a la red de la organización puede ser una fuente potencial para acceder al sistema. Esto se puede aplicar tanto a portátiles como ordenadores con placa de red (*wi-fi* o cableada).

5) Se hará una relación de las tareas actuales que se llevan a cabo con respecto a la seguridad del sistema general.

¿Se hace una copia diaria de los ficheros críticos de la organización?
¿Se hace el cierre físico de las puertas para evitar el robo?
¿Se mantiene la puerta principal siempre cerrada para evitar el vandalismo?
Respecto al problema de los virus, ¿está controlado todo el software que entra y se analiza con un software antivirus? ¿Los programas de dominio público y de uso compartido (*shareware*) sólo se utilizan si provienen de lugares fiables?

La prevención o plan de prevención se lleva a cabo a través de un análisis de riesgos.

2.2.2. Seguridad

Este plan tiene que velar por la seguridad de todo el sistema informático y, naturalmente, de manera muy especial, por la información de la organización. La responsabilidad del responsable de informática consiste en elaborar este plan y asegurar que se llevará a cabo correctamente.

A través del plan de prevención hemos analizado qué queremos proteger y hemos propuesto soluciones para hacerlo. En el plan de seguridad proponemos la manera de llevar a término las soluciones, es decir, protocolos, mecanismos, herramientas, tecnología, asignación de responsabilidades, etc., para que la seguridad sea una realidad.

Una vez más es muy importante que todos los procedimientos y protocolos de actuación no estén incumpliendo la legislación vigente en ninguna vertiente, ya que si es así pueden convertirse en un agujero de seguridad.

2.2.3. Contingencias

El plan de contingencias es, de hecho, una consecuencia del análisis de riesgos. Si sabemos qué queremos proteger (y naturalmente cómo a través del plan de seguridad), ahora tenemos que decidir qué hacemos ante un fallo del sistema o un resquicio de seguridad.

Un plan de contingencias no tendría sentido si pensáramos que nuestro plan de seguridad es perfecto. Desgraciadamente, los sistemas de seguridad no lo son nunca. Con el paso del tiempo aparecen agujeros no descubiertos antes, o errores de hardware en los equipos que pueden dejar el sistema informático vulnerable. O peor aún, una actualización del sistema (servidores, encaminadores, estaciones de trabajo), que suponemos que mejora la seguridad, en realidad puede abrir nuevas grietas en nuestro sistema sin que nos demos cuenta. También podríamos hablar de contraseñas inseguras o débiles, rotación de personal dentro de la organización, etc., aspectos que tenemos que comprobar periódicamente para asegurar que nuestro sistema se mantiene seguro.

Así que tenemos que suponer que podemos sufrir un incidente de seguridad en cualquier momento y tenemos que prepararnos para el caso "peor". Por lo tanto, es necesario prever las acciones y actuaciones a llevar a cabo en estas situaciones.

Con la condición de que, a pesar de todas las medidas que se puedan tomar, puede tener lugar un desastre, el plan de contingencias incluye un **plan de recuperación de desastres**, que tiene como objetivo restaurar el servicio informático lo antes posible y minimizar el coste y las pérdidas en la medida de lo posible.

Para que el diseño del plan de contingencias tenga sentido se tiene que presuponer el peor caso de todos, el **desastre total**. De esta manera, el plan será el máximo de completo y podrá incluir toda la casuística.

Copias de seguridad

Ya que las copias de seguridad contienen información sensible, casi siempre tienen que "cumplir" las políticas de copia que se hayan fijado en la organización (dentro del plan de seguridad), y tienen que cumplir también la legislación vigente; en este caso, una de ellas es la Ley Orgánica de Protección de Datos Personales (LOPDP).

Ved también

Recordad que hemos estudiado la Ley Orgánica de Protección de Datos Personales en el módulo "Administración de la seguridad".

El plan de contingencias tendrá que tener presente:

- Si hay una pérdida, la asumimos (en coste y tiempo) y volvemos a empezar desde cero.

- No podemos asumir la pérdida (por algún motivo, sea coste, tiempo, etc.) y por lo tanto necesitamos copia de seguridad. Esta información estará dentro del sistema de copias y, posiblemente, dentro del plan de recuperación de desastres.

- También contemplaremos los incidentes, como por ejemplo, fallos de hardware o software que pueden dejar inutilizado total o parcialmente el sistema informático, y confeccionaremos los protocolos a seguir ante este tipo de situaciones.

2.3. Sistemas de gestión de seguridad de la información

Debido a la complejidad de llevar a término un plan de seguridad es necesaria una metodología. Por este motivo aparecieron los sistemas de gestión de la seguridad de la información (SGSI).

Terminología

El sistema de gestión de la seguridad de la información también es conocido como proyecto de gestión de la seguridad, proyecto integral de seguridad, proyecto de seguridad, sistema de seguridad...

En general, cualquier sistema de gestión de la seguridad tendrá que comprender la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información dentro de una organización. Básicamente, un sistema de gestión se caracteriza por:

- Cubrir los aspectos organizativos, lógicos, físicos y legales.
- Ser independiente de plataformas tecnológicas y mecanismos concretos.
- Ser aplicable a todo tipo de organizaciones, independientemente del tamaño y actividad.
- Tener, como todo sistema de gestión, un fuerte contenido documental.

Observación

Bajo la sigla de SGSI, se intenta recoger tanto los modelos como los métodos de gestión de la seguridad de la información.

En los SGSI[2] se define:

[(2)]SGSI es la sigla de *sistema de gestión de la seguridad de la información*.

- **Activo**: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

- **Amenaza**: acontecimiento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.

- **Riesgo**: posibilidad de que una amenaza se materialice.

- **Impacto**: consecuencia sobre un activo de la materialización de una amenaza.

- **Control**: práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

En estas metodologías, la seguridad consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización. En consecuencia, la seguridad se tiene que entender como un proceso.

Los riesgos no se eliminan, se gestionan.

Existen diferentes metodologías para implementar un SGSI, básicamente el MAGERIT y la metodología que incorpora el estándar ISO 27001:2005.

Modelo PDCA

La base para el desarrollo, implementación y funcionamiento de un SGSI se puede resumir en cuatro "tareas" repetitivas: planificar, hacer, verificar y actuar. Es el llamado modelo PDCA *(Plan - Do - Check - Act)*. Es la base de los SGSI.

2.3.1. MAGERIT

El MAGERIT[3] es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas adecuadas que se tendrían que tomar para controlar estos riesgos. Es una metodología pública desarrollada por el Ministerio de Administraciones Públicas.

[(3)]MAGERIT es el acrónimo de Metodología de Análisis y GEstión de RIesgos de las AdminisTraciones públicas.

Dirección recomendada

Por Internet podéis encontrar y descargar [accesible en línea] la documentación sobre la metodología MAGERIT.

MAGERIT consta de cuatro fases:

1) Planificación del análisis y gestión de riesgos. Se hacen estimaciones iniciales de los riesgos que pueden afectar al sistema de información y el tiempo y recursos necesarios para su tratamiento.

2) Análisis de riesgos. Se hace una estimación del impacto que tendrán los riesgos en la organización. Esta área es muy importante porque un uso desproporcionado puede afectar negativamente al rendimiento. Hay que establecer un umbral de riesgo deseable (tolerable) que se tiene que superar para ser objeto de tratamiento.

3) Gestión del riesgo. Se seleccionan posibles soluciones para cada riesgo. Son fundamentales los ejercicios de simulación.

4) Selección de salvaguardias. Se escogen los mecanismos que implementarán las soluciones elegidas en la fase anterior.

2.3.2. ISO/IEC 27001:2005

Dirección recomendada

Podéis consultar la norma ISO/IEC 27001 por Internet.

El 15 de octubre de 2005 nace el estándar ISO 27001:2005, sustituyendo el BS 7799. Se usa para la implantación de un SGSI.

La norma ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) es certificable y especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información según el modelo PDCA[4]. Es consistente con las mejores prácticas descritas en ISO/IEC 17799 y tiene su origen en la norma británica British Standard BS 7799-2, publicada por primera vez en 1998. Esta norma se elaboró para poder certificar los sistemas de gestión de la seguridad de la información implantados en las organizaciones a través de un proceso formal de auditoría.

(4)El modelo PDCA también es conocido como Círculo de Deming.

La ISO/IEC considera la organización como una totalidad, y tiene en cuenta todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que se pueden producir. La mencionada norma está estructurada en **once dominios de control** que cubren completamente la gestión de la seguridad de la información, donde cada uno de ellos se refiere a un aspecto de la seguridad de la organización:

1) Política de seguridad.
2) Aspectos organizativos para 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 incidentes de seguridad de la información.
10) Gestión de continuidad del negocio.
11) Conformidad legal.

La norma pretende aportar las bases para tener en consideración todos los aspectos que pueden suponer un incidente en las actividades de la organización.

3. Detección de necesidades de software en la organización

¿Por qué se necesita software nuevo? Responder a esta pregunta es casi una cuestión filosófica. En esencia, una organización es una entidad "viva" (en un sentido amplio). Eso quiere decir que sus necesidades varían a lo largo del tiempo y, por lo tanto, las necesidades informáticas también. Más concretamente, un software puede tener errores, o bien, al aparecer nuevas versiones, se queda anticuado, o a alguna persona se le ocurren cosas nuevas que mejorarían el rendimiento o la producción, o cambia el equipo directivo o la cadena de producción, o el método de administrar o las leyes, y se tienen que modificar los programas contables, o la organización es absorbida por otra más importante que trabaja de una manera muy diferente, o se cambia completamente el departamento de marketing y ventas, etc. Y todo eso son necesidades que pueden motivar cambios profundos en el software que hay, o bien hacer que se tenga que comprar software nuevo.

Ver esta necesidad, la importancia que puede tener para la organización y el impacto que puede representar para el sistema informático requiere un cierto tiempo. Básicamente, pasa por las etapas siguientes:

1) Detección de necesidades.
2) Concreción del problema.
3) Análisis de la solución del problema.

Cuando la informática está implantada en una organización, en mayor o menor grado, siempre hay necesidades nuevas.

3.1. Detección de necesidades

A menudo, una necesidad es muy evidente, y otras veces es muy difícil de detectar. Puede provenir de muchas fuentes, algunas de las cuales pueden ser las siguientes:

- Desde el centro de atención al usuario (CAU). Por lo tanto, a partir de los usuarios que hagan peticiones.
- Desde el centro de atención al usuario (CAU), mediante quejas reiteradas.
- Desde cualquier sitio de la organización que quiere algo, sin saber si es posible o no técnicamente.
- Desde el propio departamento de informática, para mejorar el servicio.
- Desde el propio departamento de informática, para mejorar el rendimiento.

- Desde cualquier punto externo a la organización pero que interacciona con ésta y tiene problemas.
- Desde la dirección, para analizar relaciones interorganización e intraorganización.
- La propia organización, para evolucionar.
- El propio sector informático/de telecomunicaciones, que evoluciona tecnológicamente.

Lo más importante, cuando se ha detectado una necesidad, es evaluar si se puede llevar a cabo o no. Esta tarea recae en el responsable de informática que, dependiendo de la necesidad, puede trabajar con el administrador de sistemas y elaborar un informe de costes y tiempo para valorar si se pone en marcha el proyecto o no. El responsable de informática, con el consejo directivo de la organización, si son proyectos de mucho tamaño, o con el administrador de sistemas, si son pequeños, decide la forma que se les tiene que dar.

La aparición de una necesidad que tiene que cubrir el departamento de informática puede venir por muchas vías.

3.2. Etapa de concreción

Ya se ha detectado una necesidad. A pesar de eso, muchas veces es una cuestión difusa. La persona o las personas que la han generado saben más o menos qué quieren (muy pocas veces saben exactamente qué quieren), pero además, al no ser expertos en informática, y al no tener conocimiento de la estructura informática de la organización (no tienen que tenerlos necesariamente), la expresión de su necesidad es difusa. Aunque la expresan con claridad (muchas veces ellos mismos creen que se expresan claramente), la "traducción" de lo que dicen, de lo que quieren, etc. en términos informáticos, y en términos de la estructura informática de la organización, no es nada evidente.

Por lo tanto, en esta etapa es necesaria una tarea, que es responsabilidad generalmente del responsable de informática: la concreción de la necesidad. El responsable de informática tiene que establecer conversaciones, hacer reuniones, etc. con las personas que piden la solución, para que concreten y formalicen su problema y necesidad, y se pueda poner en marcha un estudio o plan de viabilidad por parte del departamento de informática. También es posible que en esta etapa tome parte en algún momento alguna figura técnica, que una vez más acostumbra a ser el administrador de sistemas, aunque depende mucho de la necesidad que se haya generado.

En esta etapa recogeremos, además, documentos, papeles, esquemas, etc., a ser posible. Sin embargo, hay que tener presente que muchas veces todas estas necesidades que aparecen cuestan mucho de definir y de precisar, por lo cual es posible que toda la valoración inicial la hagamos sin saber exactamente qué se quiere.

Es muy difícil concretar una necesidad. La comunicación con todas las personas y departamentos relacionados directa o indirectamente con la necesidad puede ser clave para concretar el problema.

3.3. Etapa de análisis

Después de haber hablado en la etapa anterior para saber qué se quiere, en el departamento de informática se hace un primer estudio de viabilidad del proyecto, para determinar cómo puede encajar en el sistema informático actual o cuál sería la mejor manera de solucionar el problema planteado. Esto es responsabilidad del responsable de informática, sobre todo por los aspectos de recursos económicos y humanos, y el aspecto técnico es una tarea conjunta del responsable de informática y el administrador de sistemas, o la figura técnica que sea necesaria según la necesidad planteada.

Prepararemos un **informe técnico preliminar** en el cual se comentarán los aspectos de hardware, software, recursos humanos, económicos y de tiempo, de una manera aproximada (en caso de que sea viable). Si la dirección decide ponerlo en marcha ya se hará un análisis bien hecho, correcto y a fondo del problema.

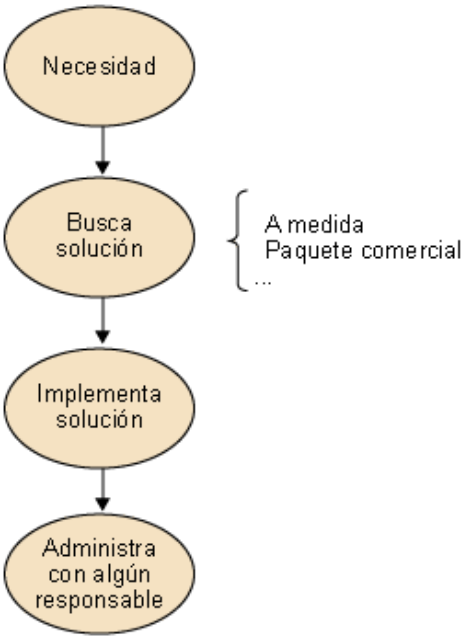
Determinar exactamente una necesidad es muy importante para evaluar el impacto que puede tener en la estructura informática y en la propia organización.

4. Implantación/diseño de aplicaciones

En una organización, como consecuencia de cambios internos (nuevas orientaciones) o cambios externos, o simplemente por mejora del funcionamiento, puede aparecer una necesidad. Esta necesidad puede afectar hasta el punto de que hagan falta modificaciones importantes de software o incluso que se tenga que comprar uno nuevo. Si este es el caso, nos encontramos con las siguientes decisiones:

- ¿Modificamos el software que tenemos (si podemos)?
- ¿Compramos software estándar?
- ¿Nos creamos un software a medida?

En este apartado damos unas pautas o indicaciones que pueden ayudar a resolver este problema.



Implementación de software

Nos tenemos que dar cuenta de que todos los pasos los hacen figuras técnicas, pero con la supervisión de la figura del responsable de informática, que es quien toma las decisiones, en estrecha coordinación con las figuras de los administradores (técnicos).

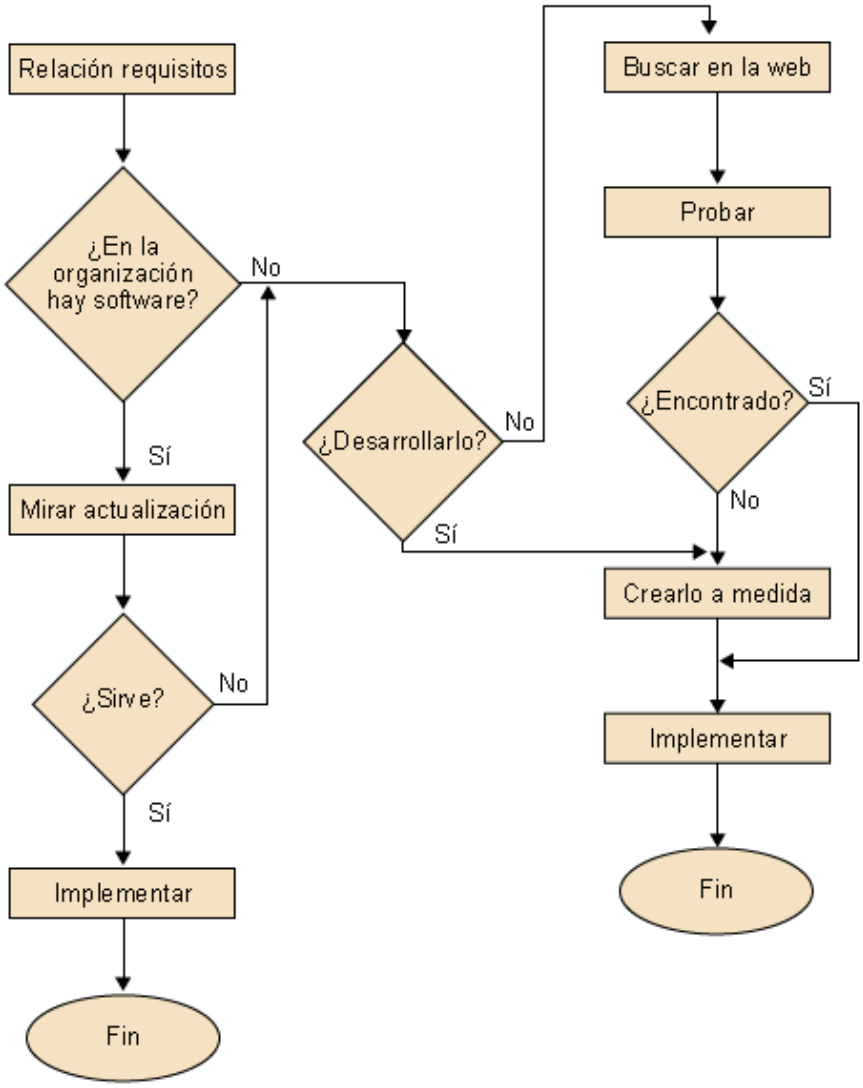
Cuando se detecta una necesidad es el responsable de informática quien toma las decisiones finales sobre si se puede satisfacer o no. Solucionarla tiene un coste y, por lo tanto, ha de verse si se puede llevar a cabo. El responsable de informática conoce el plan estratégico de la organización, los recursos económicos, humanos, etc., de que dispone. Es importante que el responsable de

informática tenga suficientes conocimientos de informática técnica como para entender toda la problemática que pueden tener los técnicos a la hora de realizar su trabajo diario.

Con esta información y el informe técnico preliminar que se ha hecho en la etapa de análisis de la detección de necesidades podremos decidir si se puede resolver o no.

Esta necesidad puede llegar a ser compleja, ya que si se implanta software nuevo, afecta profundamente a toda la estructura informática y también a la organización, dado que modifica la manera de trabajar del personal. Éste es, pues, un método para intentar ser lo más conservadores posible con respecto al software que tenemos para ajustarlo a la necesidad que hay creada.

Método de implantación de software



Cada uno de estos pasos es bastante complejo, y el responsable de informática, conjuntamente con el administrador de sistemas, trabaja para llevar a cabo esta tarea.

Hay muchas soluciones ante el problema de una necesidad. Intentemos buscar las que modifican la estructura informática lo mínimo posible.

4.1. Relación de requisitos

La decisión la tomará el responsable de informática, pero la tarea de elaborar esta relación de requisitos es conjunta del responsable de informática y el administrador del sistema.

Después de que el informe técnico preliminar haya pasado por dirección y se haya decidido poner en marcha el proyecto, el responsable de informática, junto con el administrador, marca los requisitos mínimos que tiene que cumplir el software. Los aspectos básicos que tiene que incluir esta relación tienen que contener:

- Los servidores actuales. Si son heterogéneos, dónde tiene que estar la aplicación. Pueden cambiar en un futuro próximo (planes de actualización, plan estratégico, etc.).

- Los clientes. Son o pueden ser heterogéneos (planes de actualización, plan estratégico, etc.). Cada vez más hay portátiles en determinados departamentos. Se tiene que prever la posibilidad de clientes de diferentes plataformas o tipos.

- Conexiones remotas/red. Cómo y desde dónde se tiene que poder acceder a la aplicación. Cuestiones asociadas a redes locales, intranet, extranet, etc.

- Información pública/privada
  - ¿Hay que hacer parcialmente visible la aplicación?
  - ¿Es necesario extraer (exportar) datos para hacerlos públicos o para introducirlos en otro software de la organización?

- Cuestiones de seguridad asociadas a la red, la información, la aplicación.

- ¿Cómo y qué usuarios pueden acceder a la aplicación? ¿Los usuarios tienen niveles de seguridad o ven toda la aplicación cuando han entrado en ella? ¿Pueden modificar cualquier información? ¿Pueden imprimir cualquier listado?

- También es conveniente plantearse la cuestión de configuración/parametrización, especialmente en listados. El tiempo hace que sea necesario cambiar elementos como, por ejemplo, el "logo" de la organización.

Software ajustado a las necesidades

Aquí hemos hablado de un software multiusuario, en servidor, con usuarios configurables, con propiedades para las redes y facilidades para extraer datos, posiblemente multiplataforma en la parte cliente, etc. Y seguramente para una organización de un cierto tamaño es lo que hace falta. Ahora bien, si nuestra organización es de cinco personas (por ejemplo, un taller mecánico o una tienda), muchas de estas características no son necesarias. Seguramente, con un software monousuario que funcione sobre una sola máquina (si tiene usuarios, mejor), con listados configurables, que pueda funcionar en una red pero sólo con un usuario simultáneo, y que funcione correctamente, es suficiente para resolver el problema. Lo demás estaría totalmente sobredimensionado a las necesidades reales de la organización, y tendría un coste demasiado elevado. Los propios fabricantes de software hacen muchas veces el mismo programa en diferentes "tamaños" y precios, según la organización a que se destina.

Con la relación de requisitos nos tenemos que plantear la cuestión de si dentro de la organización hay un software que haga más o menos lo que se necesita funcionalmente.

Saber qué hace falta técnicamente para resolver el problema y para integrarlo en la estructura de la organización es el primer paso.

4.2. La actualización

Se trata de que veamos si, actualizando algún software que hay en la organización, es suficiente para solucionar la necesidad que se pretende cubrir. La tarea la hará el administrador de sistema, y la decisión sobre la viabilidad de la actualización será del responsable de informática.

Esta tarea puede ser tan sencilla como mirar las características de la última versión del software en papel o vía web, o tan compleja como tener que pedir un CD-ROM de demostración, y necesitar un ordenador de prueba para instalar y hacer una simulación para ver si se ajusta a los requisitos pedidos para resolver el problema.

Buscamos si algún software del que disponemos nos sirve.

4.3. Software estándar

La opción del software estándar representa que, de momento, no queremos desarrollar software propio, y se busca un software que ya esté y se ajuste a las necesidades que se quieren cubrir. Por lo tanto, tenemos que ver, de todo el software que hay en el mercado, cuál se adapta a las necesidades que tiene la organización. Es una tarea que puede hacer el administrador de sistemas, pero que ha de supervisar el responsable de informática, ya que es quien toma

la decisión final. Actualmente, el software es bastante parametrizable y, por lo tanto, la tarea de ver el software que hay y cómo se puede adaptar a la organización todavía es más compleja.

Hay un último factor muy importante que hay que tener en cuenta. Seguramente ningún software se adapta completamente a las necesidades particulares de la organización. Todo software estándar, por muy parametrizable que sea, necesita un poco de esfuerzo de adaptación por parte de la organización, es decir, tiene que haber un ajuste de la organización con respecto al software, y del software con respecto a la organización (esto último es precisamente la parametrización).

Dado que normalmente hay cambios motivados por factores externos o internos en el software, hay que asegurarse de que el proveedor que nos lo proporciona tiene una estabilidad lo bastante buena para garantizarnos el mantenimiento del producto en nuevas versiones y la resolución de problemas.

Una vez se ha tomado la decisión, si optamos por un software estándar, lo tenemos que probar a fondo y hacer todo el proceso de implantación en servidores, y después implantarlo en los usuarios, formarlos, etc. para que no sea problemático.

La decisión final es del responsable de informática, pero la tarea de ver el software que hay en el mercado y valorar su utilidad dentro de la organización es, en gran parte, una tarea del administrador de sistemas.

Buscamos software que ya está hecho, teniendo en cuenta que tendremos que poner software nuevo dentro de la organización, con todas las consecuencias que se asocian a ello.

4.4. Software a medida

La segunda posibilidad implica poner en marcha un proyecto de software, un departamento de desarrollo de software, un análisis, etc. Por lo tanto, es bastante más complejo para obtener al final un paquete ajustado a las necesidades de la organización. Una vez se ha hecho, generalmente no se acaba, ya que, como la organización es una entidad "viva", necesita modificaciones prácticamente constantes. La organización está dentro de una sociedad que también cambia y, por lo tanto, el paquete de software creado también puede necesitar mantenimiento. Eso hace que el departamento de desarrollo, si es de nueva creación para este proyecto, difícilmente desaparezca, ya que es posible que, aparte de mantenimiento, el paquete vaya creciendo más y más con el paso del tiempo.

En este caso, el responsable de informática toma muchas decisiones estratégicas, ya que tiene que proporcionar el marco de trabajo de la aplicación. El administrador de sistemas también tiene que colaborar en crear el marco de trabajo de la aplicación y estar presente en todo el proceso de creación de la aplicación. Seguramente, será responsabilidad del responsable de informática la decisión de quién desarrolla el proyecto, porque depende de si la organización tiene departamento de desarrollo o no. Si no tiene, la tarea de desarrollar el software se crea o se contrata externamente. En este último caso, se tiene que negociar en un contrato la propiedad de las fuentes de la aplicación.

La decisión de hacer a medida una aplicación es la última solución, la más costosa económicamente y en tiempo, pero se obtiene un software que se ajusta completamente a nuestras necesidades.

4.5. La responsabilidad del responsable de informática

Como ya hemos mencionado, el responsable de informática tiene la función de determinar el marco sobre el que tiene que funcionar este software. Tanto si la decisión es un software estándar como si es un software a medida, aquí, tal como ocurría en el diseño del entorno de los usuarios, vuelven a aparecer las cuestiones siguientes:

- Dónde tiene que estar la aplicación.
- Dónde tienen que estar los datos.
- Qué usuarios accederán a ella.
- Con qué permisos.
- Sobre qué tecnología se desarrolla (cliente/servidor, etc.).
- Desde qué puntos de la organización se utilizará el software (dentro de la red, intranet, extranet, etc.).
- Grado de sensibilidad de los datos.
- Nivel de integración de los datos con el resto de aplicaciones.
- ¿Se tienen que hacer públicos parte de estos datos en la web de la organización?
- ¿Hay que exportar datos?

Por lo tanto, nos tenemos que volver a plantear una tabla de soluciones.

		Datos	
		Local	**Remoto**
Aplicación	**Local**		
	Remoto		

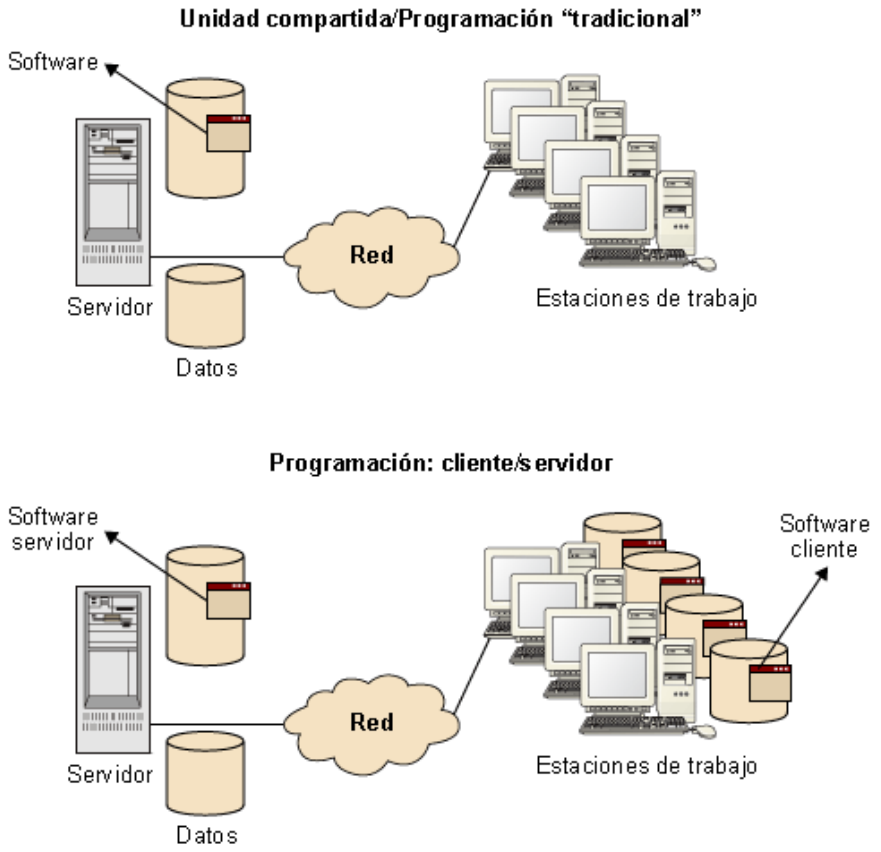
En el caso de los **datos en remoto** probablemente decidiremos que los datos estén en una base de datos en un servidor. Eso facilita las copias de seguridad, su mantenimiento e implantación, especialmente si en la organización ya hay un servidor de bases de datos. También facilita la integración y las búsquedas futuras dentro de esta nueva base de datos. Si se tiene que publicar alguna cosa (hacer extracciones) o controlar permisos, también es más sencillo.

En el caso del **software en remoto** estamos ante dos alternativas posibles:

1) Implantar un programa "tradicional" hecho para que pueda funcionar en el cliente o en el servidor, o un programa con tecnología cliente/servidor que necesita una pequeña parte instalada en el cliente.

2) Aprovechar la tecnología cliente/servidor para crear una aplicación en la que el programa cliente ya esté instalado en las estaciones de trabajo, por ejemplo, un navegador. Es el caso de las arquitecturas en las que el *front-end* (ordenador frontal) es un navegador que hace de cliente y el servidor web ataca las bases de datos. En medio, está la aplicación servidora real.

Tipos de software remoto



Las ventajas del software en remoto son:

- Funciona con clientes heterogéneos. No hay que hacer una versión cliente para cada plataforma.

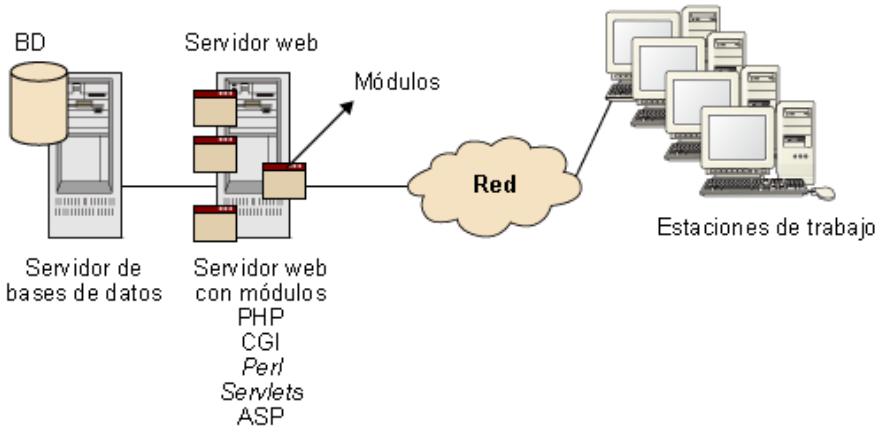
- Funciona con portátiles. Es una buena solución para la informática móvil.

- Funciona fuera de la organización. Si puede haber problemas de seguridad, se tiene que poner sobre un servidor seguro (HTTPS).

- Normalmente, se programa por módulos y no monolíticamente.

Éste es el esquema de la estructura que se acostumbra a utilizar en estos casos, ya que es la más segura.

Esquema de estructura de software remoto



Como la aplicación está en módulos, su mantenimiento y crecimiento son más sencillos, y dado que los datos están en un servidor diferente del de la aplicación es más seguro, porque si llegan a atacar el servidor web con éxito no encontrarán los datos, sino que se tiene que conseguir llegar a otro servidor, por lo que hay otra barrera de seguridad para traspasar. La seguridad es más elevada.

Ved también

Ved los módulos "Administración de la web" y "Administración de la seguridad".

El responsable de informática también se tiene que preocupar de que se lleve a cabo el diseño de la documentación y del plan de formación de los usuarios finales, y proveer de recursos para sacar adelante el proyecto.

El responsable de informática tiene que decidir lo siguiente:

- El marco en que desarrollará la aplicación.
- El diseño de la documentación.
- El plan de formación.

5. Aspectos legales de la administración de redes

Los aspectos legales son muchos, y una vez más tenemos que insistir en la cuestión de los asesores legales para consultas, ya que hoy en día la legislación es muy cambiante.

5.1. Problemas de seguridad

Uno de los aspectos que tiene que conocer especialmente un responsable de informática es qué hay que hacer ante un problema de seguridad. Recordemos que algunos de los problemas de seguridad que se pueden dar son los siguientes:

- Destrucción/robo de información por parte de personal de la organización.
- Destrucción/robo de información externamente a la organización, por ejemplo por Internet.
- Abuso de uso del sistema para finalidades no corporativas.

Cada caso prácticamente es particular, y generalizar aquí puede ser contraproducente. Sí que es importante distinguir las cuestiones técnicas de las decisiones que hay que tomar ante una situación. Las figuras técnicas detectan problemas y avisan de que están. La figura del responsable toma las decisiones y las figuras técnicas las llevan a cabo. Veámoslo con unos ejemplos.

Abuso del sistema por parte del personal con finalidades no corporativas

Si se sospecha que una persona utiliza el sistema indebidamente, esto lo detectan normalmente los administradores de sistema (figuras técnicas). Lo comunican al responsable de informática y, en este caso, la función del responsable es establecer los procedimientos legales dentro de la organización para verificar que realmente esta persona hace un uso indebido del sistema. Una vez puestos en marcha los procedimientos legales, las figuras técnicas pueden llevar a cabo los mecanismos informáticos y técnicos necesarios para reunir las pruebas y verificar que hay un problema legal. Después se procederá con todo el sistema legal necesario, que es responsabilidad del responsable de departamento, con apoyo del administrador de sistemas, si es necesario.

Ataques a servidores web

Esta situación concreta es de las más complejas. Según la situación, la decisión que tiene que tomar el responsable de informática puede variar, porque hay muchos tipos de ataques. Supongamos un ataque con intención de obtener información de la organización. Lo que podría pasar es lo siguiente.

El administrador de sistemas informa al responsable de informática del tipo de problema de seguridad, que decide hacer lo siguiente (siempre es una orientación):

- Que el administrador de sistemas lleve a cabo el protocolo técnico del equipo. Parada, copia, restauración, etc.

Ved también

Ved, en el módulo “Administración de la seguridad”, cuáles son los pasos.

- Hablar con la dirección de la administración sobre el problema de seguridad que ha habido.

- Al mismo tiempo, el responsable de informática informa al cuerpo de policía adecuado para denunciar el hecho, concretar una fecha y consultar los datos o pruebas del sistema que puedan necesitar.

- Los administradores de sistema elaboran un informe exhaustivo sobre lo que ha pasado y aportan toda la información que consideren necesaria en formato CD-ROM. Este informe tiene que contener qué ha pasado, cómo se ha dado la intrusión, cuánto ha durado, cómo se ha solucionado, cuál era el problema de seguridad que la ha provocado y a qué personas/entidades se ha solicitado ayuda para solucionar el problema (desde el punto de vista técnico).

- Un informe de los administradores y el responsable de informática que contiene los daños ocasionados en el sistema, y una valoración de los daños económicos y materiales que ha significado para la organización esta intrusión. Dependiendo de la situación real, esto lo puede hacer un perito externo a la organización.

- En la fecha fijada con el cuerpo de policía, se hace la reunión en que se presenta el informe técnico, el informe de daños (y el coste estimado), el CD-ROM con toda la información, pruebas, etc., y el cuerpo de seguridad se encarga de buscar a la persona que ha ocasionado el daño y actúa de forma policial, después judicialmente y, finalmente, si es necesario, penalmente.

Ahora bien, supongamos el caso siguiente: el administrador de sistemas informa al responsable de informática de que en el servidor web se ha encontrado instalado un servidor de pornografía infantil. Como aquí hay claramente un delito penal, el responsable de informática decide hacer lo siguiente (siempre es una orientación):

- No modificar nada y reunir el máximo de pruebas posibles (ficheros de log, ficheros de datos, imágenes, páginas web, etc.). La finalidad es que el intruso todavía no sepa que nosotros ya tenemos conocimiento de que ha entrado en el sistema. Como acabamos de decir, esta acción la manda poner en marcha el responsable de informática, y la llevan a cabo los administradores de sistema. Estos pasos están descritos en el apartado Administración de la seguridad.

Ved también

Ved, en el módulo “Administración de la seguridad”, cuáles son los pasos.

- Al mismo tiempo, el responsable de informática informa al cuerpo de policía adecuado para denunciar el hecho, concretar una fecha y consultar los datos o pruebas del sistema que puedan necesitar (por ejemplo, pueden decidir clonar el disco o discos duros del servidor y restaurar el sistema; así se evita que el delito se continúe produciendo).

- Con toda la información extraída del sistema, con la denuncia y la consulta hecha al cuerpo de policía sobre la información que hay que extraer, los administradores de sistema pueden proceder a lo siguiente:
  - Restaurar el sistema.
  - Recuperar la información de copias de seguridad.
  - Asegurar el sistema, si es necesario. Eso significa añadir pedazos de sistema operativo o de aplicación destinados a tapar el agujero de seguridad que pueda haber ocasionado la entrada ilegal del intruso.

Estas operaciones destruyen prácticamente todas las pruebas, pistas/rastros que haya podido dejar el intruso en el sistema. Por eso es muy importante haber extraído antes toda la información de pruebas, y haberlo hecho en coordinación con el cuerpo de seguridad del Estado, para estar seguros de no perder ninguna prueba importante. De esta manera, el servidor afectado vuelve a estar operativo lo antes posible.

- Los administradores de sistema elaboran un informe exhaustivo sobre lo que ha pasado y aportan toda la información que consideran necesaria en formato CD-ROM. Este informe tiene que contener qué ha pasado, cómo ha sido la intrusión, cuánto ha durado, cómo se ha solucionado, cuál era el problema de seguridad que la ha provocado, a qué personas/entidades se ha solicitado ayuda para solucionar el problema (desde el punto de vista técnico).

- Un informe hecho por los administradores y el responsable de informática que contiene los daños ocasionados en el sistema, y una valoración de los daños económicos

y materiales que ha significado para la organización esta intrusión. Dependiendo de la situación real, eso lo puede hacer un perito externo a la organización.

- En la fecha fijada con el cuerpo de policía, se hace la reunión en que se presenta el informe técnico, el informe de daños (y el coste estimado), el CD-ROM con toda la información, pruebas, etc., y el cuerpo de seguridad se encarga de buscar a la persona que ha ocasionado el daño y actúa de forma policial y después judicialmente y, finalmente, si es necesario, penalmente.

Las dos maneras de actuar son muy parecidas, pero dependiendo de cada caso hay variaciones. No hay, pues, reglas fijas sobre la manera de actuar ante situaciones irregulares.

5.2. Aspectos legales del software a medida

Muchas veces el software a medida se contrata a compañías ajenas a la propia organización. Estas compañías fabrican el software y lo implantan, pero hay que aclarar en el contrato, con los asesores legales correspondientes, los términos de propiedad del código fuente y hasta dónde llega este código fuente (librerías, entre otros).

Se han dado muchos casos de compañías que han cambiado la orientación, han discontinuado el producto y, por lo tanto, han dejado de dar apoyo al software que han fabricado, de manera que la organización que ha pedido el software a medida en realidad no tiene nada, porque nadie, ni la propia organización contratando programadores, será capaz de hacer el mantenimiento de la aplicación. La compañía tiene un elemento conocido como "saber hacer[5]", que es el conocimiento que ha desarrollado y aplica a los programas, que no tiene por qué dar necesariamente a la organización, pero es bueno llegar a algún tipo de acuerdo, antes de empezar un proyecto, para que haya alguna vía para mantener la aplicación en caso de que no lo haga la compañía que la ha creado.

(5)En inglés, *know-how*.

El problema legal de la propiedad del código fuente (o de alguna parte de este código) se tiene que negociar antes de empezar el proyecto.

6. Tareas del responsable de informática

Una relación aproximada de las tareas/responsabilidades del responsable de informática es la siguiente:

- Elaboración de la parte del plan estratégico del departamento, subordinado al plan estratégico de la organización, y velar por ella.
- Detección de necesidades.
- Concreción de necesidades con el personal de la organización.
- Decisión de implantar necesidades y la manera de hacerlo.
- Planes de actualización informática.
- Plan de contingencias.
- Determinación de los permisos de los usuarios en el software.
- Supervisión de los proyectos de software.
- Actuación y respuesta ante situaciones que comprometan la seguridad del sistema.
- Decisión ante situaciones legales.
- Gestión de la seguridad.

Resumen

El responsable de informática es la figura que toma las decisiones estratégicas que afectan al departamento. Tiene que tener la visión de futuro de cómo será la informática.

Con los planes se intenta prever qué puede pasar para tomar medidas para minimizar las consecuencias. Desde cómo evolucionará la informática para adaptarse a ellas hasta cómo es debido reaccionar ante un desastre.

La gestión de la seguridad, a través de alguna de las metodologías existentes, se ha convertido en fundamental para garantizar un buen funcionamiento del sistema informático.

Detectar, ver o incluso prever necesidades de la organización es un poco un arte. Concretar la necesidad es una tarea de comunicación, y hacer un análisis y un informe es una tarea técnica.

Cuando se necesita software nuevo intentamos ir por la vía más conservadora, ya que en un primer momento parece la vía menos traumática para la organización. El responsable de informática toma las decisiones, aunque hay mucho trabajo técnico que hacer.

Ser un buen jefe de informática quiere decir tener todas las facetas mencionadas anteriormente, es decir, ser un buen técnico, un buen dialogador, un buen jefe, tener visión de futuro, tener capacidad de previsión y muchas otras cualidades más que están fuera del alcance de estos materiales.

Ejercicios de autoevaluación

1. Han entrado en vuestro servidor web y os han cambiado la página inicial. La primera vez la restauráis, pero a lo largo de una semana pasa tres veces. ¿Qué haríais?

2. ¿Cuáles de estas frases son ciertas y cuáles falsas?
a) Las necesidades siempre provienen del CAU.
b) Es mejor hacer a medida un programa, ya que lo podremos modificar cuando queramos.
c) El responsable de informática sólo gestiona recursos; no tiene que tener necesariamente grandes conocimientos técnicos.
d) Siempre es mejor un software multiplataforma y multiusuario corriente en servidor, porque no se sabe nunca cómo crecerá la organización.

3. ¿Cuál de estas frases sobre la implantación de aplicaciones es falsa?

a) El último paso es la implementación del software escogido.
b) Sólo nos plantearemos crearlo a medida si no encontramos ningún estándar.
c) Si la actualización sirve, la utilizaremos de base para crearnos el software a medida.
d) La relación de requisitos nos sirve en todo el proceso.

4. Relacionad el concepto con la definición.

Definición
Conjunto de propuestas realistas para fijar objetivos de la organización
Definir el marco de una aplicación nueva
Herramienta de diagnóstico dentro de la dirección estratégica
Analizar riesgos a los que puede estar expuesto el equipo informático
Relación de requisitos

Concepto
DAFO
Detección de necesidades
Plan estratégico
Plan de contingencias
Responsabilidades del jefe

5. Una de estas tareas no es responsabilidad del responsable de informática.

a) Dar acceso a las aplicaciones corporativas.
b) Elaborar la parte del plan estratégico del departamento, subordinado al plan estratégico de la organización, y velar por ella.
c) Detección de necesidades.
d) Concreción de necesidades con el personal de la organización.
e) Supervisión de los proyectos de software.
f) Actuar y responder ante situaciones que comprometan la seguridad del sistema.

Solucionario

Ejercicios de autoevaluación

1. Es corriente entre los intrusos intentar entrar en servidores web. Cuando lo han conseguido una vez, se dan por satisfechos y no lo intentan más. Por lo tanto, lo mejor sería restaurar la página inicial, mirar los ficheros de log y hacer una búsqueda en el sistema para comprobar que no han cambiado nada más, y finalmente buscar el agujero de seguridad y taparlo. Esta acción puede comportar diversos días de trabajo.

Como parece que, mientras se hace eso, se vuelve a atacar el servidor por segunda vez, posiblemente intentan provocar al administrador, pero ya no está claro qué buscan, porque no es el procedimiento habitual. Por lo tanto, posiblemente lo mejor en este caso es volver a poner la página inicial, pero paralelamente empezar a buscar los ficheros de log, registrar las acciones, activar elementos que registren acciones y ver qué pasa.

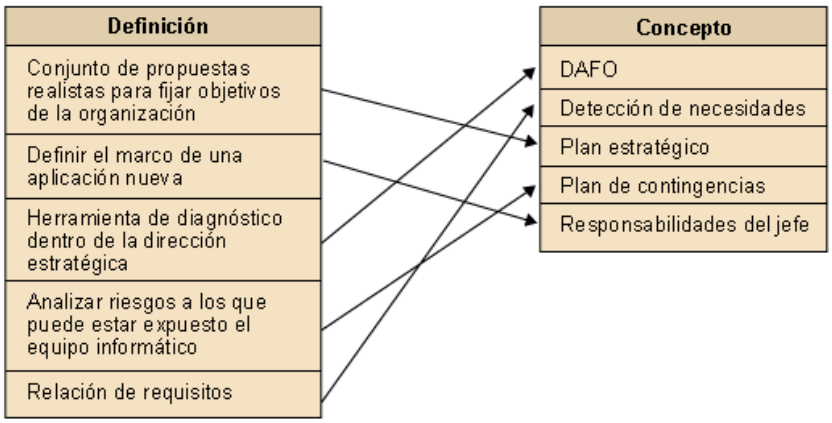
Cuando los intrusos atacan por tercera vez, está claro que buscan algo. Seguramente creen que hay información sensible como, por ejemplo, números de tarjetas de crédito o cuestiones similares y, por lo tanto, es posible que el ataque no esté limitado a la sustitución de la página inicial del servidor, sino que pretendan ir más lejos. En este punto, como ya estaremos prevenidos, registraremos sus acciones hasta donde queramos, ya que ahora se trata de que ellos no sepan que nosotros sí que sabemos que están dentro de la máquina, y pondremos en marcha todo el dispositivo de registro de acciones. Cuando cerremos y aseguremos el servidor, es porque tenemos toda la información de lo que hacen que consideramos necesaria para poder localizarlos. Cuando se vuelva a abrir el servidor, ya estará arreglado y asegurado. Ellos ya sabrán que nosotros tenemos conocimiento de que han entrado, y posiblemente no lo vuelvan a probar. Si lo hacen, será por otro lugar, o por alguna puerta escondida que hayan dejado antes, pero no por el mismo sitio. Pero nosotros ya tendremos información suficiente para actuar con la policía en su contra (y ellos no lo saben).

2. Argumentémoslo un poco:

a) Falso. Muchas sí que vienen del CAU, pero no todas. Por ejemplo, hay necesidades generadas por la dirección.
b) Falso con condiciones. Siempre que hablamos de una aplicación grande. Un programa a medida tiene un coste elevado con respecto a un programa estándar. El tiempo para confeccionarlo también es muy grande. La cuestión de la facilidad de modificación es una cuestión negociada. Podría ser cierto si la organización del departamento tiene un desarrollo propio, de manera que entonces es un proyecto interno de la propia organización.
c) Falso. Por ejemplo, en el caso de un proyecto informático se establece el marco sobre el cual se hará la aplicación. En la definición de necesidades, también hace de interlocutor con las personas implicadas. Tiene que tener grandes conocimientos técnicos.
d) Falso. Siempre depende del tamaño de la organización y de su plan estratégico. El software tiene que estar dimensionado en la organización y sus expectativas futuras. En principio, es información que posee el responsable de informática.

3. c

4.



5. a

Glosario

activo *m* Recurso del sistema de información, o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

amenaza *f* Acontecimiento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.

DAFO *f* Ved **debilidades, amenazas, fortalezas, oportunidades**.

debilidades, amenazas, fortalezas, oportunidades *f* Técnica de diagnóstico para el análisis interno de una organización. Son las siglas que se ponen en una matriz 2×2.
sigla: **DAFO**.

logo *m* Imagen corporativa que identifica una organización. Desde el punto de vista informático, normalmente es un fichero gráfico.

monousuario *adj* Dicho del software en el que sólo puede trabajar un usuario cada vez. Este adjetivo no indica nada sobre la tecnología del software (cómo está hecho, si está en un servidor ni dónde se guardan los datos).

multiplataforma *f* Dicho del software estándar, que puede funcionar sobre arquitecturas diferentes.

multiusuario *adj* Dicho del software en el que pueden trabajar diversos usuarios a la vez. Este adjetivo no indica nada sobre la tecnología del software, aunque parece claro que los datos están centralizados en algún lugar común al cual acceden todos los usuarios cuando trabajan de forma concurrente.

parametrización *f* Acción de ajustar software estándar a las necesidades particulares de la organización mediante una configuración, que puede ser por medio de ficheros, ventanas, un programa, etc.

PDCA *m* Modelo PDCA (*Plan* - *Do* - *Check* - *Act*). Planificar - Hacer - Verificar - Actuar. Es la base de los SGSI.

riesgo tecnológico *m* La ISO define el riesgo tecnológico como la probabilidad de que ocurra una amenaza usando vulnerabilidad existente de un activo o activos generando pérdidas o daños.

riesgo *m* Posibilidad de que una amenaza se materialice.

Bibliografía

Barcelo García, M.; Pastor i Collado, J. (1999). *Gestió d'una organització informàtica*. Barcelona: Universitat Oberta de Catalunya.

Microsoft Corporation (1997). *Windows NT 4.0 Workstation Kit de Recursos*. Madrid: Mc-Graw Hill.

Ministerio de Administraciones Públicas (2006). *Metodología de análisis y gestión de riesgos MAGERIT*. Madrid: BOE. ISBN 84-340-0960-9

Piattini, M.; Calvo-Manzano, J.; Cervera, J.; Fernández, L. (1996). *Análisis y diseño detallado de aplicaciones informáticas de gestión*. Madrid: Ra-Ma.

Pfleeger, C. (1997). *Security in computing*. Estados Unidos: Prentice Hall.

Tena Millán, J. (1989). *Organización de la empresa: Teoría y aplicaciones*. Barcelona: EADA.