Gerencia de riesgos informáticos

Esther Cerdeño
Subdirectora Informática Técnica
MAPFRE REASEGUROS (España)

"El mercado demanda una respuesta por parte de las entidades aseguradoras sobre la posibilidad de asegurar los costes de la pérdida de información, y éstas se plantean las correspondientes preguntas sobre la posibilidad de cubrir estos riesgos."

1. Introducción

La dependencia que las empresas tienen de sus sistemas informáticos, además de la complejidad de estos sistemas produce una creciente preocupación por su seguridad y funcionamiento continuo, con los que quedar a salvo de errores e intromisiones. También, la protección de datos de terceras personas, clientes y empleados, contenidos en las bases de datos, está en el punto de mira de los controles para salvaguardar su privacidad y mantenerlos libres de intromisiones o pérdidas de información a favor de terceros. Todo lo anterior implica establecer una serie de medidas que garanticen que los sistemas informáticos se encuentran perfectamente protegidos frente a interrupción de los servicios.

La preocupación de las empresas por la seguridad y el buen funcionamiento de los equipos se ha traducido en un incremento de gastos del 60% en las aplicaciones informáticas dedicadas a la protección de los datos y medidas de seguridad, mientras que otras aplicaciones de trabajo, como son las actualizaciones de *software*, han mantenido constante su crecimiento en los últimos años. Las agresiones debidas a sabotajes ó virus, o bien los accidentes naturales como terremotos, incendios y huracanes pueden producir daños importantes en los equipos y en las bases de datos, hasta el punto de ocasionar pérdidas de información y costes directos importantes, a lo que habría que añadir los efectos negativos que pueden provocar en la imagen y confianza en las capacidades de la empresa en cuestión, comprometiendo así su futuro.

Esta gran preocupación por la seguridad se traduce en gastos considerables, destinados a establecer planes de contingencia y seguridad, cuyo mantenimiento y puesta a punto permanente requiere de personal especializado en las distintas áreas que componen la red informática de la empresa. Algunas han subcontratado estos servicios a otras empresas, pero esto no elimina el problema, puesto que hay que establecer las mismas defensas en las empresas que prestan dicho servicio.

Ante esta situación, el mercado demanda una respuesta por parte de las entidades aseguradoras sobre la posibilidad de asegurar los costes de la pérdida de información, y éstas se plantean las correspondientes preguntas sobre la posibilidad de cubrir estos riesgos y acerca de los estudios que hay que realizar para analizarlos tanto los riesgos como los costes y, en definitiva, si es posible llevar a cabo la cobertura de dichos riesgos.

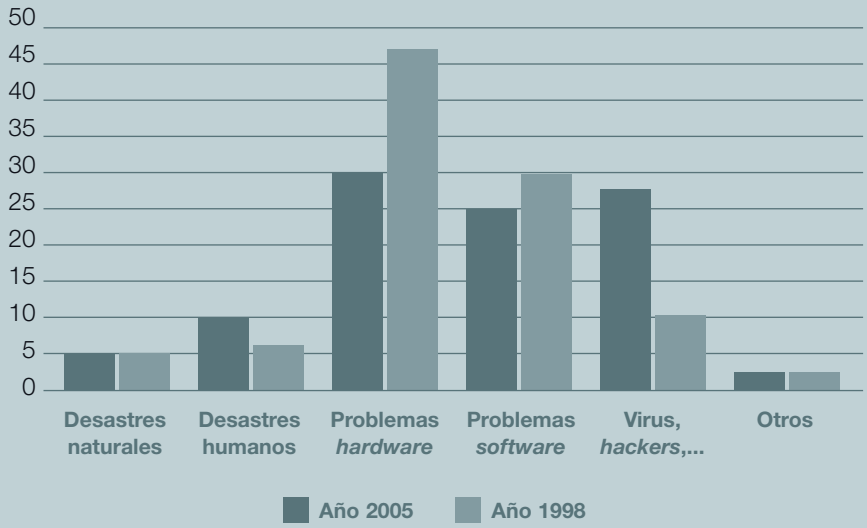
El presente artículo trata de identificar cuáles son los riesgos, de forma general, a los que deben enfrentarse y cuáles son también las medidas preventivas que se pueden adoptar para asegurar la información. Por otra parte se hace una revisión breve de un posible plan de continuidad del negocio y recuperación de información ante desastres, además de mostrar qué ofrecen las compañías de seguros para paliar los costes económicos derivados de la pérdida de información y de los equipos.

2. Análisis de Riesgos-Planes de Contingencia

Factores de riesgo

En distintos estudios realizados sobre las causas que pueden producir la pérdida de datos, contenidos en los sistemas de

Gráfico 1: Causa de pérdida de datos (%)



información, se aprecia que hasta hace tan solo seis años las principales pérdidas provenían de errores de *hardware* o de mal funcionamiento de los equipos, mientras que en la actualidad han aumentado las pérdidas debidas a virus, sabotajes y otros agentes externos.

Entre las causas (véase tabla 1-pág. 14) que pueden producir pérdidas de información en las empresas, se puede establecer la siguiente clasificación:

- Errores del *hardware* de los Sistemas de Información.
- Errores humanos.
- Errores del *software*.
- Amenazas provenientes de fuentes externas como virus, *hackers* externos o internos, como pueden ser los propios empleados de la organización.
- Desastres naturales y desastres provocados por el hombre, entre ellos los de naturaleza política.

Situación de las empresas

En un momento en el que constantemente aparecen nuevas amenazas en los Sistemas de Información de las empresas e instituciones, el poder asegurar la continuidad del negocio es fundamental, para lo cual las empresas deben desarrollar unos planes de contingencia ante desastres que les permitan continuar con su actividad cotidiana , pese a cualquier incidente que pudiera suceder.

Básicamente, el diseño de un "Plan de Continuidad de Negocio" implica analizar los potenciales riesgos y valorar las posibles pérdidas. No obstante, de acuerdo con algunos estudios, hasta el ejercicio 2007 sólo el 35 % de las grandes empresas dispondrá de una sólida infraestructura de continuidad de negocio, a pesar de las recomendaciones realizadas por los responsables de las Tecnologías de la Información en este sentido.

Como ejemplos recientes de los riesgos mencionados, cabe recordar que algunas empresas ubicadas en las Torres Gemelas de New York desaparecieron tras los atentados del 11 de septiembre porque no disponían de copias de seguridad fuera de dichos edificios. El apagón de Nueva York y Canadá también supuso un gran impacto económico. En febrero del 2005 el incendio de la Torre Winsor, en pleno centro financiero de Madrid, provocó un parón de la actividad que afectó a miles de trabajadores y se requirió, en algunos casos, hasta 96 horas para recuperar la actividad normal de algunas de las empresas afectadas.

Con estos datos en la mano, es obvio que el gasto en seguridad y continuidad del negocio crecerá de forma rápida en los próximos años hasta situar su valor en aproximadamente USD 116.000 millones (EUR 91.172,52 millones) en 2007, según datos del IDC (*International Data Group*), que analiza los mercados mundiales y predice las tendencias sobre el futuro de Internet y de las Tecnologías de la Información. También, un trabajo de Gartner Dataquest nos indica que *"uno de cada tres negocios norteamericanos podrían perder datos críticos para continuar con su capacidad operativa si ocurriera un desastre, a menos que se inviertiera de modo inmediato en un plan de contingencia ante desastres",* y añade que *"más que priorizar las inversiones lo importante debe ser asegurarse de que los negocios puedan recuperar rápidamente la productividad después de un incidente..."*.

Según se apunta en los párrafos anteriores, la solución es disponer de un plan de contingencia o continuidad de negocio que afecte a toda la organización y Sistemas de Información, bien se encuentren en papel o en soportes electrónicos. Se trata de analizar cómo se puede elaborar dicho plan, quiénes deben intervenir en su elaboración y seguimiento, y, por último, cuál sería su coste.

Norma ISO 17799

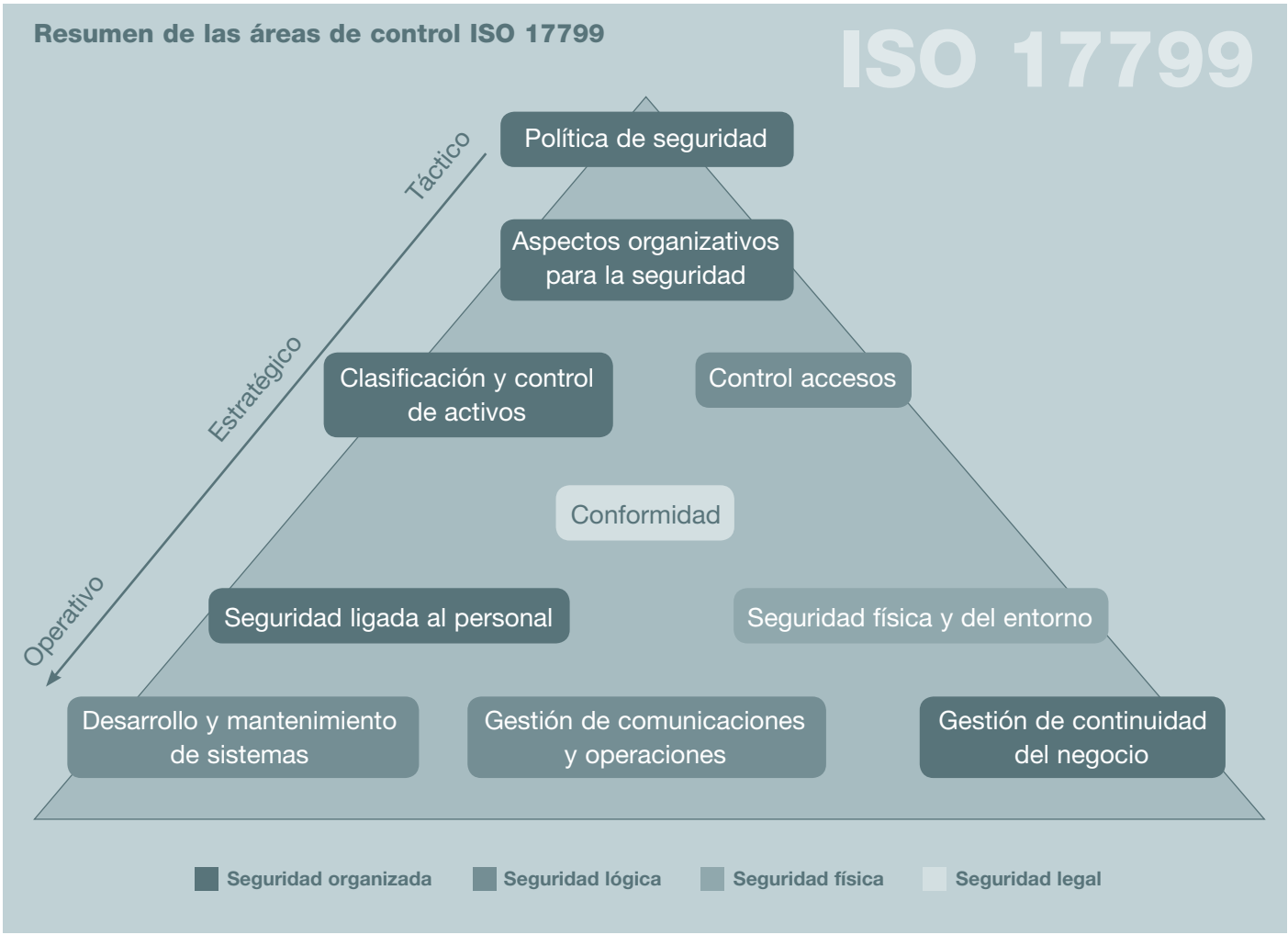
La “Norma ISO 17799” es una compilación de recomendaciones flexibles que ayuda a los responsables de la seguridad de la información de las empresas a establecer un plan eficiente, con independencia de su tamaño o sector.

La norma técnica fue redactada con una clara intención de que fuera flexible, sin inducir el uso de una solución de seguridad específica. Las recomendaciones de la Norma Técnica ISO 17799 son neutrales en cuanto a la tecnología, y ayudan a evaluar y entender las medidas de seguridad existentes.

Define un modelo progresivo, basando la seguridad en distintos escalones, de entre los que se deberá elegir el más realista o acorde de acuerdo con la actividad de la empresa.

Niveles de seguridad de la Norma Técnica ISO 17799

Nivel básico	Riesgo bajo de fraude. Ausencia de datos personales. Baja dependencia de la tecnología.
Nivel medio	Riesgo alto de fraude. Datos personales y regulación legal. Alta dependencia de la tecnología.
Nivel alto	Riesgo elevado de fraude. Datos personales y regulación legal. Dependencia total de la tecnología.
Nivel gubernamental	Información que debe ser protegida y cuya divulgación puede poner en riesgo la seguridad y defensa del Estado.



Dentro del Área asociada al mantenimiento de la continuidad de la empresa, estas normas aconsejan estar preparado para contrarrestar las interrupciones en las actividades y proteger los activos en caso de producirse un desastre natural o daño causado por el hombre.

En la tabla 2 (ver pág.16) se muestra una posible metodología para la implantación de un "Plan de Contingencia" el cual, al menos, debería contemplar los siguientes puntos:

- Clasificación de recursos tecnológicos. Análisis e inventario de:
  - Los equipos electrónicos de los que depende la empresa.
  - Las aplicaciones (contabilidad, administración, RR. HH., etc.).
  - Los servicios (conexiones entre sedes, acceso a Internet, etc.).
- Clasificación de los recursos logísticos.
  - Mobiliario.
  - Material de oficina.
- Clasificación de los recursos operativos.
  - Definición e identificación de las actividades que se llevan a cabo en la empresa, priorizando los procesos críticos.
  - Seguridad.
  - Enumeración de los responsables de las distintas áreas (bases de datos, servidores de aplicaciones, etc.).
  - Suministros de agua, luz, etc.
- Análisis de riesgos. Enumeración de riesgos (errores humanos, sabotajes, etc.) y su pertinente clasificación.
- Búsqueda de posibles puntos de fallo en la infraestructura actual.

- Estimación del tiempo máximo de inactividad (tiempo de ruptura) y también del periodo máximo en el que un proceso crítico puede verse interrumpido sin afectar a la viabilidad de la organización.
- Definición de los intervalos de recuperación en un grado mínimo aceptable inicial y, después de forma progresividad, comprobar los tiempos de recuperación total de la actividad de la empresa.
- Alternativas a los fallos (duplicidad, replicación, terceras copias de seguridad, etc.).
- Definición de los procedimientos que deben ser desarrollados en caso de incidencia.
- Establecimiento de un calendario de revisiones periódicas y actualizaciones.
- Establecimiento de un calendario de pruebas.

Tabla 1: Causas y Medidas Preventivas.

Fallos de hardware: Funcionamiento incorrecto

Causas	◣ Errores en algún dispositivo crítico: o Discos. o Controladoras. o Procesadores. o Memoria. ◣ Fallos eléctricos.
Medidas preventivas	◣ Duplicidad de equipos servidores. ◣ Duplicidad de componentes como son ventiladores y fuentes de alimentación, entre otros. ◣ Redundancia de controladores. ◣ Redundancia de discos. ◣ Salas de ordenadores protegidas contra incendios, inundaciones, temperaturas elevadas, etc. ◣ Sistemas de Alimentación Ininterrumpida (UPS). ◣ Realización de copias de seguridad. Ubicación de los dispositivos de copia en lugares separados de los centros de cálculo.

Errores humanos

Causas	◣ Borrado accidental de ficheros, datos, etc. ◣ Inicialización por confusión de discos con datos válidos. ◣ Ejecución de secuencias incorrectas en aplicaciones.
Medidas preventivas	◣ Desarrollo de aplicaciones en sistemas de no-producción. ◣ Pruebas de todas las aplicaciones en sistemas denominados de pre-producción, con un conjunto de datos similares a los de producción. ◣ Sistemas de *backups* diarios.

Continuación, Tabla 1: Causas y Medidas Preventivas.

Corrupción de *software*

Causas	◣ Actualización de nuevas versiones de los sistemas operativos. ◣ Actualización de nuevas versiones de alguna aplicación en concreto. ◣ Instalación de parches no compatibles con todo el sistema actual. ◣ Instalación de nuevos controladores de elementos. ◣ Fallos producidos por configuraciones complejas. ◣ Fallos producidos por aplicaciones no registradas.
Medidas preventivas	◣ Instalación de *drivers,* parches, etc. en sistemas de no-producción. ◣ Realización diaria de copias de seguridad. ◣ Sistemas de copias de seguridad *on line.* ◣ Sistemas de tercera copia. ◣ Elementos de análisis y diagnóstico antes de instalar nuevas aplicaciones.

Virus, *hackers,* códigos maliciosos

Causas	◣ Reenvío masivo de *e-mails* que colapsan el tráfico y los buzones de las empresas. ◣ Uso de huecos de seguridad que impiden que los sistemas se conecten. Ataques de denegación de servicios. ◣ Re-inicios inesperados del sistema. ◣ Acceso a direcciones *webs* clasificadas como peligrosas. ◣ Utilización de programas tipo *e-Donky*, etc.
Medidas preventivas	◣ Establecimiento de normas preventivas para la apertura de e-mails de origen desconocido para los usuarios. ◣ Utilización de antivirus. Actualización de antivirus al menos 1 vez al día. ◣ Utilización de herramientas de análisis de paquetes situados en la red. ◣ Herramientas de análisis de contenidos y bloqueo de acceso a sitios clasificados en las listas negras de la *Web Internacional*.

Desastres naturales o causados por el hombre

Causas	◣ Fuegos. ◣ Tormentas. ◣ Terremotos. ◣ Inundaciones. ◣ Sabotajes. ◣ Terrorismo.
Medidas preventivas	◣ Definición de políticas de seguridad. ◣ Locales protegidos (doble suelo, doble techo, etc.). ◣ Sistemas de extinción de incendios. ◣ Sistemas de aire acondicionado. ◣ Duplicidad de sistemas en ubicaciones separadas.

Tabla 2: Metodología de un Plan de Contingencia

Análisis del impacto en el negocio	◣ Constitución del grupo de desarrollo del Plan. ◣ Identificación de las funciones críticas. ◣ Análisis del impacto de un siniestro en cada función crítica. ◣ Definición de los niveles mínimos de servicio. ◣ Evaluación de la relación coste/beneficio de cada alternativa.
Planificación	◣ Enumeración de las aplicaciones. ◣ Nombramiento de responsables. ◣ Elaboración de planes. ◣ Documentación del plan. ◣ Validación del plan.
Estrategia de recuperación	◣ Sistemas de backups *on line–off line.* ◣ Sistemas duplicados de respaldo, terceras copias, etc.
Simulacros	◣ Estimación del alcance del simulacro. ◣ Determinación de las aplicaciones o servicios. ◣ Posibilidad de pruebas en tiempo real. ◣ Ejecución de pruebas. ◣ Documentación de dichas pruebas.
Mantenimiento de los planes	◣ Actualizar el plan de contingencia de acuerdo con los resultados obtenidos en las pruebas. ◣ Revisiones periódicas. ◣ Actualizaciones que incluyan nuevos servicios, aplicaciones, sistemas, etc. ◣ Auditorías.

Tabla 3: Resumen de las Fases para la Elaboración del Plan de Continuidad de Negocio

Definir y documentar la estrategia de continuidad	◣ Tiempo de activación del Plan. ◣ Infraestructuras tecnológicas. ◣ Ubicaciones críticas. ◣ Procedimientos alternativos manuales, etc.
Desarrollo del Manual del Plan de Continuidad	◣ Información de soporte. ◣ Grupos de trabajo. ◣ Procedimientos de respuesta. ◣ Fases de recuperación. ◣ Fases de restauración. ◣ Procedimientos.
Aprobación del Plan por parte de la alta dirección	◣ Responsables de la ejecución.
Plan de pruebas	◣ Identificación de posibles deficiencias. ◣ Actualización del Plan.
Plan de mantenimiento	◣ Concienciación. ◣ Formación continua. ◣ Revisión.

Empresas de Seguros

Ante la situación descrita en los apartados anteriores, se debe analizar qué pueden ofrecer las empresas aseguradoras y en qué deben basar sus estudios para la aceptación de los anteriores riesgos. Las empresas que más están contratando este tipo de seguros son las tecnológicas y las".com", por ser más conscientes de las vulnerabilidades en este sentido.

En cuanto a las coberturas, existe un desconocimiento por parte de los asegurados. Algunas encuestas sobre si existe un seguro y cuáles son entonces las coberturas por los daños o pérdidas sufridas en los sistemas informáticos nos indican que cerca del 40% de los asegurados desconoce estos datos. En la mayor parte de los casos, las pólizas no cubren los incidentes que provienen de terremotos, tormentas, asimismo, se ha observado que alrededor del 34% no disponía de ningún tipo de seguro. Para poder obtener una cobertura adecuada y la compañía de seguros poder ofrecerla, se debería realizar una cuantificación e identificación de los riesgos que se quieren asegurar, lo que requiere tiempo, conocimiento y recursos humanos para su definición y posterior cuantificación.

Las pólizas de seguros que cubren los equipos informáticos pueden ubicarse dentro del ramo de Ingeniería, clasificados como "Seguro de ordenadores" o "Seguro de equipos electrónicos". A mero título informativo, el "Seguro de ordenadores" puede garantizar los daños sufridos en los equipos de procesamientos de datos, de acuerdo con los datos descritos en los contratos. Quedan excluidos, en cambio, los daños derivados del desgaste, montaje, influencia de temperatura, etc.

Las coberturas pueden extenderse también a los gastos de reintegración de las informaciones, provocados por daños sufridos en soportes como discos, cintas, etc.

"En un momento en el que constantemente aparecen nuevas amenazas en los Sistemas de Información de las empresas e instituciones, el poder asegurar la continuidad del negocio es fundamental, para lo cual las empresas deben desarrollar unos planes de contingencia ante desastres."

En la modalidad básica de las pólizas, contamos con la cobertura de "Daños materiales sufridos en los equipos", incluyendo los soportes magnéticos de datos, incluso durante su transporte (golpes, incendios, caídas, etc.).

Concretamente, la cobertura de "Riesgos extraordinarios del Consorcio de Compensación de Seguros Español" recoge una serie de garantías que incluyen los daños causados por:

- Terremotos, inundaciones extraordinarias, erupciones volcánicas, tempestades ciclónicas o caídas de cuerpos siderales y aerolitos.
- Terrorismo, rebelión, revolución, motín y tumulto popular.

Otras garantías complementarias, que se pudieran dar, corresponden a indemnizaciones por los gastos que deba sufragar el asegurado por el alquiler o utilización de otros equipos, como consecuencia de la imposibilidad de acceso a la sala del ordenador, debido a un accidente en las inmediaciones del local o sala del equipo asegurado. Se considera asimismo como siniestro cubierto la falta de suministro público de energía eléctrica que por causa accidental llegue a provocar una interrupción en las operaciones del equipo asegurado, incurriéndose en gastos de alquiler y utilización de otros equipos.

Conforme a lo anterior, cualquier empresa de seguros, antes de aceptar un contrato debería poder realizar un análisis de la situación de los equipos informáticos de la empresa que suscribe el seguro. Una medida importante sería analizar si se dispone de un Plan de Contingencia o, sin llegar a tal extremo, solicitar qué medidas se están aplicando de duplicidad de equipos, políticas de seguridad, antivirus, detectores de intrusos, tal y como se detalla en los apartados anteriores. Lógicamente, la cobertura de los riesgos y su precio dependerán del grado de conocimientos y medidas que tenga la empresa sobre estos temas, y del plan de acción para evitar las contingencias y reducir los costos y el tiempo de paralización.

Por otra parte, y conforme a lo que recogen las cláusulas suscritas en los contratos de seguros, gran parte de los gastos deben ser abonados por las empresas aseguradoras aunque, como se indicaba en las encuestas, la mayor parte de las empresas actualmente desconocen el alcance de las coberturas ofrecidas. ■