novática
UPGRADE Revista de la Asociación de Técnicos de Informática

*Novática*, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de ATI (Asociación de Técnicos de Informática). *Novática* edita también *Upgrade*, revista digital de CEPIS (*Council of European Professional Informatics Societies*), en lengua inglesa.

**<http://www.ati.es/novatica/>**
**<http://www.upgrade-cepis.org/>**

ATI es miembro fundador de CEPIS (*Council of European Professional Informatics Societies*) y tiene un acuerdo de colaboración con ACM (*Association for Computing Machinery*). Tiene asimismo acuerdos de vinculación o colaboración con AdaSpain, AI2 y ASTIC.



**Coordinación Editorial, Redacción Central y Redacción ATI Madrid**
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
**Composición, Edición y Redacción ATI Valencia**
Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
**Administración y Redacción ATI Cataluña**
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
**Redacción ATI Andalucía**
Isaac Newton, s/n, Ed. Sadiel,
Isla Cartuja 41092 Sevilla, Tlfn./fax 954460779 <secreand@ati.es>
**Redacción ATI Aragón**
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
**Redacción ATI Asturias-Cantabria** <gp-astucant@ati.es>
**Redacción ATI Castilla-La Mancha** <gp-clmancha@ati.es>
**Redacción ATI Galicia**
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlfn.986581413; fax 986580162 <secregal@ati.es>
**Suscripción y Ventas**
<http://www.ati.es/novatica/interes.html>,o en ATI Cataluña o ATI Madrid
**Publicidad**
Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <novatica.publicidad@ati.es>
**Imprenta**
9 Impressió S.A., Juan de Austria 66, 08005 Barcelona.
**Depósito legal:** B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
**Portada:** Antonio Crespo Foix / © ATI 2003
**Diseño:** Fernando Agresta / © ATI 2003

Nº 166, noviembre-diciembre 2003

# sumario



**Monografía del próximo número: "Redes inalámbricas"**

Roberto Moya Quiles[1],
Stefano Zanero[2]
*[1] GISI (Grupo de Interés de Seguridad Informática de ATI); [2] Analista de Seguridad de la Información, IDG Corporation*

<rmoya@dimasoft.es>,
<zanero@elet.polimi.it>

# Presentación
# Planes de Contingencia TIC: más que tecnología

## 1. Introducción

Los Planes de Contingencia de Tecnologías de la Información y las Comunicaciones (TIC) son una de las preocupaciones tradicionales en las organizaciones, especialmente para aquellas de tamaño medio y grande, que, como casi todas hoy en día, basan la realización de sus procesos de negocio en sistemas y tecnologías de la información.

Dichos planes, desacertadamente considerados en épocas anteriores como responsabilidad única del Área de Explotación de los Centros de Proceso de Datos (en general por dejadez y desconocimiento de la Dirección de las empresas), están experimentado una importante evolución en su alcance hasta integrarse en los denominados Planes de Recuperación de Negocio (*Business Recovery Plans*) o Planes de Continuidad de Negocio (*Business Continuity Plans*).

No obstante lo anterior, los objetivos conceptuales básicos de los Planes de Contingencia no se han alterado en el devenir de los años: evaluación de riesgos específicos, tiempo de respuesta a una gran diversidad de incidencias, nivel de tolerancia a pérdida de datos y al tiempo de duración del servicio degradado, fiabilidad de los procesos en relación a la integridad de las transacciones y de la información en situaciones de interrupciones o incidencias, sincronización de las copias de respaldo, coste de la realización del plan y su mantenimiento, entre otros.

Adicionalmente están requiriendo una especial relevancia los contratos de "Acuerdo de Nivel de Servicio", con proveedores de Servicios de Respaldo (*Backup Services*), y de "Continuidad del Servicio", con proveedores externos de servicios de tecnología y comunicación.

Sin embargo, los cambios de las tecnologías disponibles, en extenso e intenso, han ido matizando estos planes, al mismo tiempo que complicando su realización, dada la necesidad de incluir una ingente y siempre creciente cantidad de detalles que hay que tener en cuenta para cada configuración y arquitectura de aplicaciones particular.

Adicionalmente, regulaciones de diverso rango van imponiendo requisitos a los planes. Desde Directivas hasta Reglamentos, así como regulaciones sectoriales, estando entre las más relevantes las del sector financiero, tanto las provenientes de Basilea (*Bank for International Settlements*, <http://www.bis.org/>) como de la Reserva Federal estadounidense (*The Federal Reserve*, FED, <http://www.federalreserve.gov/>).

## 2. Tres escenarios

En un esfuerzo por sintetizar las situaciones tipo que se dan en el presente, cabría dibujar como mínimo tres escenarios:

1. En el primer escenario los centros de procesos realizan sus copias de respaldo por duplicado y mantienen una de las copias en un centro externo *ad hoc*, convenientemente custodiadas, etc. La obligación más relevante del contrato (Acuerdo de Nivel de Servicio) que se mantiene con el proveedor de servicios de Centro Alternativo consisten, básicamente, en restaurar en éste centro las copias que se guardan en el centro externo ad hoc e iniciar los servicios. Este escenario es característico de centros cuyos procesos son mayoritariamente por lotes (*batch*).
2. Un segundo escenario consiste en añadir al escenario anterior la comunicación permanente con el centro alternativo mediante líneas (VLANs, Internet, RDSI, etc.), manteniéndose de esta forma actualizadas las bases de datos más críticas y posibilitando, tal como se suele reflejar en el contrato, una respuesta más rápida para los servicios que implican comunicaciones.
3. Por último el tercer escenario lo puede representar la utilización de la tecnología de discos multiplataforma y la conexión directa por fibra entre los dos centros, que no siempre es posible, pues la limitación de distancia puede conducir a que el centro de respaldo tenga similares riesgos que el respaldado, por ejemplo frente a desastres naturales. Este escenario es el que mejor se adapta para dar respuesta a incidencias graves en grandes centros de explotación con servicios web *front-end*.

En el tema que nos ocupa existe una gran lista de referencias, por cierto incrementada después de los atentados del 11 de septiembre de 2001 (como puede comprobarse utilizando buscadores como Google, Altavista, etc.), así como bibliografía, tanto para el proyecto de elaboración del plan, como para el plan resultante en sí. Las fuentes principales son los fabricantes de ordenadores y las empresas consultoras especializadas.

Cabe mencionar en este punto el documento MAGERIT, el cual contiene un ejemplo de aplicación a la elaboración de un Plan de Recuperación (disponible en <http://www.map.es/csi/pg5m20.htm>).

Para la elaboración del plan y su posterior puesta en servicio, es innegable que las alternativas de solución posible dependen de los servicios disponibles (tanto de proceso como de comunicaciones) en cada lugar geográfico, pues, aún pensando en un mundo global, es evidente que esos servicios no son iguales en todos los puntos del globo ni en disponibilidad, ni en calidad, ni en precio.

La multitud de pequeños detalles a tener en cuenta, unos aparentemente nimios (como por

Editores invitados

**Roberto Moya Quiles** es Doctor en Ciencias Físicas, rama de Ciencias de la Computación, Licenciado en Informática y Auditor CISA (*Certified Information Systems Auditor*). Tiene 34 años de experiencia en diversas funciones directivas del área de Sistemas de Información (Dirección de Tecnologías de la Información, consultoría, formación, seguridad y control, auditoría, y aplicaciones informáticas, etc.) en grandes compañías de fabricación de ordenadores, software y empresas proveedora de energía. Participa como ponente en seminarios y forma parte de foros relacionados con la Seguridad de Tecnologías de la Información en instituciones privadas, así como en universidades públicas. Es miembro del Sub Comité de ISO/IEC SC 27 (Técnicas de Seguridad para la Tecnología de la Información) y coordina el Grupo de Interés en Seguridad Informática (GISI, <http://www.ati.es/gt/seguridad/>) de la Asociación de Técnicos de Informática (ATI).

**Stefano Zanero** es Licenciado en Informática y se graduó *cum laude* en la Escuela de Ingeniería del Politécnico de Milán (Italia) con una tesis sobre el desarrollo de un sistema de detección de intrusiones basado en algoritmos de aprendizaje no supervisado. Actualmente estudia doctorado en el depto. de Electrónica e Informática de la citada universidad. Entre sus intereses en el campo de la investigación, además de los sistemas de detección de intrusiones, se cuentan hoy el rendimiento de los sistemas de seguridad y técnicas de ingeniería del conocimiento. Es miembro del IEEE (*Institute of Electrical and Electronics Engineers*) y de la ACM (*Association for Computing Machinery*). Es analista de seguridad de la información en la empresa IDG Corporation y como tal participa en conferencias nacionales e internacionales. Escribe en la revista semanal "Security Manager's Journal" de Computer World Italia, habiendo recibido recientemente un premio periodístico. Tiene además experiencia como consultor en seguridad de redes y de información.

ejemplo: lugar donde se guardan las llaves de acceso al armario donde están las copias de seguridad, cambio de contraseñas en la máquina de producción real al finalizar las pruebas, más un largo etc.) y otros no tan sencillos (como por ejemplo, designación de las personas autorizadas para dar la orden de activación del Plan o las pruebas del mismo), nos lleva a concluir que es imprescindible la realización de pruebas, a pesar del coste que implican.

En lo que respecta a la frecuencia de las pruebas, es frecuente contestar con la frase "*una al año es poco pero dos son mucho*", pero, en cualquier caso, es recomendable realizarlas cuando hay cambios en la configuración de la arquitectura o de las aplicaciones.

De acuerdo con nuestra larga experiencia en este campo, una de las aportaciones más valoradas de la realización anual de las pruebas es su incorporación natural a la cultura del personal de la organización, pues se consigue que tanto los responsables de las áreas usuarias como los desarrolladores tengan en cuenta en los diseños la situación de contingencia grave y, por qué no decirlo, la realización de esas mismas pruebas.

Como es bien es sabido por los profesionales de este 'oficio', lo que se cambia rara vez funciona 'a la primera', de ahí que sea un criterio frecuente el requerir que no existan, o sean mínimos, los cambios a los procedimientos del día a día de la explotación, sobre todo en el caso de los centros alternativos.

Finalmente hay que tener en cuenta que ninguna prueba puede ser un reflejo al 100% de la situación real pues es inviable realizar una prueba TOTAL, dado el gran impacto que causaría en la organización. Por ello, para no afectar negativamente en el servicio real se eligen aplicaciones y lugares puntuales, horas fuera del horario laboral, se aislan segmentos de red cambiando direcciones en los DNS, etc.

Cabría decir pues, que las pruebas tienen un carácter asintótico, por lo que se convierten en una condición necesaria pero no suficiente.

### 3. El contenido de esta monografía

Teniendo en cuenta todo lo anterior hemos solicitado a varios profesionales en la materia europeos (españoles e italianos) que nos expresen sus puntos de vista, cubriendo una panorámica limitada pero significativa de algunos de los aspectos más significativos de la misma, incluidos los legales.

En su artículo "*Estudio empírico de la evolución de la Seguridad y la Auditoría Informáticas en la empresa española*", ***Francisco José Martínez López***, ***Paula Luna Huertas***, ***Francisco J. Martínez López*** y ***Luis Martínez López*** nos ofrecen los resultados de una investigación sobre empresas de tamaño medio y grande, que, aunque realizada en España, es aplicable en buena medida a otros países.

***Agatino Grillo*** contribuye con su artículo "*Auditoría de Sistemas de Información y Planes de Continuidad del Negocio*", en el que describe, haciendo especial énfasis en el sector financiero, cómo estos planes son no sólo una necesidad empresarial en cuanto la continuidad de los servicios es una necesidad primaria del negocio, sino también, progresivamente, un requisito legal.

La comparación detallada entre las más importantes normativas a nivel mundial para el control de la continuidad del negocio desde la perspectiva TIC es el objeto del artículo "*Controles para la continuidad de negocio en ISO 17799 y COBIT*" de ***José Fernando Carvajal Vión*** y ***Miguel García Menéndez***.

"*Ejecución de una auditoría de un Plan de Contingencias*" es el título de la contribución de ***Marina Touriño Troitiño***, en la que aboga por la necesidad de que los Planes de Contingencia TIC sean también objeto de auditorías dada la importancia de dichos planes para asegurar la continuidad del negocio.

El artículo "*Iniciativas públicas norteamericanas y europeas frente a contingencias en las infraestructuras de información*", también de ***Miguel García Menéndez*** y ***José Fernando Carvajal Vión***, muestra la importancia que las instituciones públicas asignan al funcionamiento sin interrupciones de dichas infraestructuras, claves para la vida económica y social de los países desarrollados, describiendo los planes del Gobierno de los EE.UU. y de la Unión Europea a tal respecto.

"*La continuidad del negocio y los operadores de telefonía móvil*" es el título autoexplicativo del artículo de ***Miguel Andrés Santisteban García***.

***Paloma Llaneza González***, en "*Planes de Contingencia y regulación legal en materia de comercio electrónico y de protección de datos*", basa su artículo en el hecho de que cualquier Plan de Contingencia TIC ha de tener en consideración los requerimientos legales y reglamentarios aplicables, analizando la normativa española, que es muy similar a la de los países de la Unión Europea.

"*Las Tecnologías de la Información y la protección de la privacidad en Europa*", de ***David D'Agostini*** y ***Antonio Piva***, realizan una evaluación de la Directiva Europea 95/46/CE sobre Protección de Datos Personales, deteniéndose especialmente el correo electrónico masivo no solicitado (*spamming*), que constituye cada día más una amenaza para el correcto funcionamiento de Internet.

La monografía se cierra con el artículo de "*Análisis legal de un supuesto de delincuencia informática transnacional*" de ***Nadina Foggetti***, en el que muestra como la discordancia de las legislaciones sobre las intrusiones en los sistemas y las redes abren espacios de impunidad para la delincuencia tecnológica.

Y nosotros concluimos esta presentación agradeciendo a todos los autores su colaboración y esperando que el trabajo de todos, incluidos los editores de ***Novática*** y de ***Upgrade***, sea de interés y utilidad para los lectores de ambas revistas.