Autorità per l'energia elettrica e il gas

LINEE GUIDA PER AFFRONTARE E RISOLVERE IL PROBLEMA DEL CAMBIAMENTO DI DATA DELL'ANNO 2000

Indirizzi e strumenti per i soggetti esercenti i servizi di pubblica utilità nei settori dell'energia elettrica e del gas

8 giugno 1999

INDICE

PREMESSA

L'azione dell'Autorità per l'energia elettrica e il gas (di seguito: l'Autorità) intesa a informare e sollecitare gli esercenti i servizi dell'energia elettrica e del gas affinché essi provvedano all'adeguamento dei sistemi informatici al fine di superare gli eventuali problemi connessi con il cambiamento di data dell'anno 2000, si affianca alle iniziative intraprese o avviate da altri organismi e amministrazioni pubbliche. Tra questi, si segnalano:

- Forum permanente per la Società dell'informazione, istituito presso la Presidenza del Consiglio dei ministri.

- Comitato dei ministri per la Società dell'informazione, istituito con decreto del Presidente del Consiglio dei ministri in data 15 maggio 1997, che assicura il coordinamento delle azioni delle diverse amministrazioni interessate.

- Comitato di studio ed indirizzo per l'adeguamento dei sistemi informatici e computerizzati all'anno 2000 (di seguito: Comitato anno 2000), istituito presso la Presidenza del Consiglio dei ministri il 6 agosto 1998 e aggiornato nella sua composizione con decreto del Presidente del Consiglio dei ministri, 14 dicembre 1998, al quale il decreto medesimo ha assegnato, tra l'altro, il compito di "definizione ed attuazione di una strategia di comunicazione volta a sensibilizzare gli operatori pubblici e privati sul potenziale impatto derivante dal cambio di data dell'anno 2000" (articolo 2, lettera h) e di "assicurazione dell'adeguamento all'anno 2000 da parte dei fornitori dei servizi di pubblica utilità, quali l'energia elettrica, le telecomunicazioni, i trasporti ed altri" (articolo 2, lettera j).

- Autorità per l'informatica nella pubblica amministrazione (di seguito: AIPA), cui il decreto legislativo 12 febbraio 1993, n. 39, che la istituisce, ha assegnato, tra l'altro, il compito di "dettare criteri tecnici riguardanti la sicurezza dei sistemi" (articolo 7 lettera a) e di "proporre al Presidente del Consiglio dei ministri l'adozione di raccomandazioni e di atti di indirizzo alle regioni, agli enti locali e ai rispettivi enti strumentali o vigilati ed ai concessionari di pubblici servizi" (articolo 7, lettera h).

- Ministero dell'industria, del commercio e dell'artigianato (di seguito: Ministero dell'industria), che partecipa ai lavori del Comitato anno 2000 attraverso un suo esperto.

Nell'ambito delle attività del Forum per la società dell'informazione, il Ministero dell'industria e la Presidenza del Consiglio dei ministri hanno avviato una consultazione con le parti interessate, con l'obiettivo di presentare un primo quadro della situazione, delle problematiche e delle azioni avviate in ambito pubblico e privato.

In risposta ad una specifica richiesta della Commissione europea ai paesi membri dell'Unione europea, il Ministero dell'industria ha fornito un quadro di sintesi, a fine 1998, del livello di preparazione al cambiamento di data dell'anno 2000 di vari settori, tra i quali elettricità e gas. Dal questionario sottoposto ad Enel S.p.a. ed Eni S.p.a. è

emerso come queste due società e le loro controllate abbiano in avanzato stato di attuazione i programmi di adeguamento dei rispettivi sistemi informatici e siano impegnate nella esecuzione dei test e nella predisposizione di piani di emergenza.

Meno nota è la situazione per quanto riguarda gli esercenti i servizi di fornitura dell'energia elettrica e del gas di piccole e medie dimensioni (rispettivamente circa 200 e 800), il cui grado di conoscenza dei problemi legati al cambiamento di data dell'anno 2000 e le cui competenze tecniche per affrontarli variano da caso a caso.

Le indicazioni contenute nel presente documento sono pertanto in linea di massima rivolte a soggetti esercenti i servizi di pubblica utilità nei settori dell'energia elettrica e del gas di piccole e medie dimensioni. Il documento si propone di fornire indirizzi e strumenti anche al fine di evitare errori rilevati in esperienze effettuate in circostanze similari.

Il documento dà pertanto indicazioni generali, che dovranno essere adattate a seconda della dimensione, del livello di organizzazione e della strumentazione informatica ed elettronica di cui dispongono i singoli esercenti. Le indicazioni proposte tengono conto della varietà dei componenti, degli apparati, del modo in cui sono interconnessi e delle situazioni specifiche di utilizzo.

L'assicurazione della continuità del servizio e la esecuzione degli interventi indicati rimangono sotto la piena responsabilità degli esercenti.

1 IL *MILLENNIUM BUG* E LE AZIONI PER AFFRONTARLO

1.1. Cos'è il *millennium bug*

Il problema informatico del cambio della data in corrispondenza dell'anno 2000, a cui nella letteratura anglosassone sono stati attribuiti diversi nomi tra cui quelli di: "*millennium bug*" (letteralmente: inconveniente inatteso del millennio), di "*Year 2000*" (anno 2000) o di "*Y2k*" (Y = year, 2k = 2 × 1000 = 2000), consiste in un **malfunzionamento diffuso** da ascrivere al fatto che, a causa della prassi informatica di codificare le date con le sole ultime due cifre dell'anno (prassi seguita sin dagli anni '60 al fine di risparmiare i costi di elaborazione e di memorizzazione) i programmi software dei sistemi informatici delle aziende, e taluni sistemi computerizzati basati su microprocessori o su sistemi di elettronica digitale (sistemi *embedded*), in assenza di una adeguata procedura di correzione, non riconoscono la codifica "00" come l'anno 2000, ma come relativa ad altra data o come data non comprensibile (e quindi non elaborabile), producendo errori o l'eventuale blocco del sistema interessato.

Poiché anche nel settore dell'energia elettrica e del gas si è fatto largo uso di sistemi informatici e di sistemi computerizzati per ottimizzare l'uso delle risorse ed incrementare la produttività e la sicurezza, appare necessario verificare i sistemi informatici ed eventualmente adeguarli affinché essi risultino indenni dai problemi del *millennium bug.*

1.2 Le azioni per affrontare il *millennium bug*

Non esiste uno standard formalizzato per l'adeguamento al cambiamento di data dell'anno 2000, anche se è divenuto di riferimento comune quanto previsto dal British Standard DISC PD 2000-1 (vedi Allegato 1), che può quindi essere considerato una linea guida di comune accettazione.

Gli esercenti operanti nella fornitura di servizi nei settori dell'energia elettrica e del gas, così come tutte le altre imprese indipendentemente dalla tipologia di attività, devono effettuare una programmazione delle attività per fronteggiare il *millennium bug* al fine di:

- acquisire la **consapevolezza** dei problemi di raggiungimento della conformità all'anno 2000 e delle connesse implicazioni aziendali, partendo da una **maggiore coscienza del relativo rischio**, iniziando dal più alto livello di "management" per finire ad ogni addetto che operi a livello degli impianti, degli uffici interni e delle squadre che assistono il pubblico, e predisponendo una **adeguata campagna informativa**;
- adottare, di conseguenza, una **idonea organizzazione aziendale** che contempli un "progetto anno 2000" di alta priorità alla quale assegnare il potere necessario per operare e un budget adeguato e nominare **un responsabile unico** del problema del cambio di data dell'anno 2000, che goda di autorevolezza consolidata dall'esperienza e dal proprio corretto comportamento all'interno dell'organizzazione,

che risponda al massimo livello di management e che sia dotato dei necessari poteri per agire con la tempestività che il caso richiede;

- effettuare un accurato **inventario** di tutti gli oggetti da convertire all'anno 2000 (apparecchiature hardware e di telecomunicazioni, sistemi software acquisiti dal mercato o prodotti all'interno, sistemi *embedded*), stimare i costi di conversione, contattare i fornitori, valutare l'impatto del *millennium bug* sull'azienda;
- scegliere le **applicazioni** e i **sistemi critici**, da cui dipende la sopravvivenza e lo sviluppo dell'azienda, da convertire con priorità e concentrare su di essi le migliori risorse umane e strumentali;
- scegliere di effettuare la conversione all'interno o di affidarla all'esterno;
- scegliere di effettuare una mera conversione o di riprogettare;
- scegliere le strategie tecnico-organizzative di conversione all'anno 2000;
- scegliere le strategie tecniche di migrazione dei dati e di interfacciamento tra le applicazioni;
- scegliere l'ambiente informatico di migrazione e le tecniche di gestione di detto ambiente;
- **effettuare le conversioni;**
- **effettuare le verifiche e i collaudi** tesi ad accertare il grado di conformità;
- **stabilire i piani di emergenza** per assicurare comunque l'operatività;
- **informare** il personale, i clienti, i fornitori, i partner, le parti sociali e le associazioni di consumatori;
- **predisporre misure amministrative e legali** per evitare possibili contenziosi.

1.3 Mobilitazione e piano di comunicazione

La conoscenza dei problemi e delle difficoltà da affrontare per risolverli debbono essere chiaramente veicolate a tutti i livelli dell'organizzazione ai fini della sua mobilitazione. Un piano d'azione può includere:

a) **incontri con il vertice aziendale**, atti ad esporre la tematica in corso ed a rendere tutti consapevoli circa la serietà delle conseguenze che l'avvento dell'anno 2000 comporta, se non affrontato adeguatamente;

b) **definizione del livello di adeguatezza**, atta a stabilire, in forma concreta e condivisa, il livello di adeguamento alle nuove necessità che l'azienda ritiene di raggiungere, nei tempi proposti, dopo una analisi dei rischi, dei costi e dei benefici;

c) **comunicazione** di notizie aziendali per informare l'azienda che lo sforzo di conversione è in atto e che tutti devono essere responsabilizzati in merito.

La comunicazione può essere realizzata in due tempi.

a) Una prima comunicazione che sia finalizzata a dare avvio al progetto anno 2000. L'informazione deve partire dai vertici aziendali e discendere ai livelli intermedi informando e chiedendo la necessaria cooperazione.

b) Una seconda comunicazione che coinvolga direttamente i responsabili del progetto anno 2000. La comunicazione dovrà considerare una serie di informative destinate espressamente a chi istituzionalmente deve riceverle. L'obiettivo è di chiarire il ruolo di ciascuno (persona singola, reparto o gruppo di lavoro) e di richiederne l'assistenza, la collaborazione e la capacità di reazione nonché l'operatività immediata affinché il problema sia controllato e non evolva in maniera rischiosa.

2 I SETTORI DELL'ENERGIA ELETTRICA E DEL GAS DI FRONTE AL *MILLENNIUM BUG*

2.1. Considerazioni di carattere generale

I settori dell'energia elettrica e del gas e le aziende che vi operano devono affrontare le anomalie ascrivibili al *millennium bug*: malfunzionamenti dell'hardware, del *firmware*, del software di base, del software di ambiente e del software applicativo di calcolatori (*mainframe*, *minicomputer*, *server*, personal computer), di sistemi e reti di comunicazione, nonché di apparati e sistemi di sicurezza dotati di microprocessori o di sistemi di elettronica digitale. Inoltre, i dati erronei che vengono scambiati tra più soggetti per motivi di business, ove non si proceda alla creazione di adeguate protezioni (*firewall*), possono provocare errori anche là dove si é effettuato un lavoro di eliminazione dei guasti ascrivibili al *millennium bug*. Nelle aziende ciò significa che i programmi residenti su calcolatori che trattano gli aspetti amministrativo-gestionali (contabilità, amministrazione, fatturazione, ecc), ove non siano accuratamente esaminati e depurati dagli effetti del *millennium bug*, possono fornire risultati erronei in modo silente o esplicito, ovvero possono interrompere il proprio funzionamento.

Nelle aziende dei settori dell'energia elettrica e del gas il problema più critico indotto dal *millennium bug* è quello del funzionamento della rete e degli impianti, il quale viene messo a rischio dalla presenza di microprocessori e di sistemi di elettronica digitale (*chip*) che sono stati inseriti a fini di miglioramento dell'efficacia, dell'efficienza e della sicurezza del sistema complessivo.

I *chip*, di norma prodotti dalla relativa industria di base con tecniche di produzione di massa, sono usati nelle comunicazioni e in molti dispositivi di comando e controllo dei sistemi di energia. Nella eventualità che i *chip* contengano orologi interni (*clock*) che trattano la data, possono verificarsi malfunzionamenti associati al *millennium bug* solo in alcuni esemplari di una determinata produzione; ciò complica di molto l'identificazione dei prodotti finali difettosi, nonché i relativi test e collaudi. Ai dispositivi che contengono *chip* si dà la denominazione di sistemi *embedded* (vedi Allegato 2); poiché di norma la progettazione di questi sistemi è coperta da segreto industriale, si comprende anche perché i costruttori di dispositivi abbiano cercato, utilizzando varie tecniche industriali, di renderli inaccessibili (*embedded*).

2.2. Il sistema informatico amministrativo-gestionale

Gli esercenti i servizi di fornitura dell'energia elettrica e del gas devono, al pari delle altre imprese, affrontare il problema del *millennium bug* per quanto riguarda il proprio sistema informatico di tipo amministrativo-gestionale. Pertanto, dovranno essere adeguatamente inventariati tutti i componenti fisici (ad esempio: calcolatori, apparati, nodi di rete, terminali, eventuali sistemi a microprocessore) e logici (sistemi operativi, software d'ambiente, linguaggi di programmazione, programmi applicativi, dati), verificati, rimpiazzati o convertiti, sottoposti a test unitari e di integrazione, verificati e collaudati. Inoltre, andranno verificate le interrelazioni informatizzate con i fornitori, con i clienti, con le banche con cui si intrattengono rapporti finanziari, con la pubblica

amministrazione, con gli eventuali “partner” e le aziende facenti parte dello stesso gruppo.

2.3. Il settore dell’energia elettrica e il *millennium bug*

Il *millennium bug* può influenzare i componenti di un sistema elettrico che sono essenziali alla produzione, trasmissione e distribuzione dell'elettricità. L'identificazione dei punti di un sistema elettrico dove il *millennium bug* può verificarsi costituisce un problema complesso; tuttavia, se ci si concentra sui sottosistemi che sono critici nei confronti dello scopo ultimo di un sistema elettrico (fornire energia ai clienti in condizioni di qualità e di sicurezza), il problema diviene più gestibile.

Esistono cinque aree in cui il *millennium bug* può presentare i maggiori rischi, per quanto concerne la fornitura dell'energia elettrica in condizioni di assoluta affidabilità:

- produzione dell’energia elettrica;
- controllo della produzione e della trasmissione dell’energia elettrica;
- telecomunicazioni e teleconduzione;
- sistemi di trasmissione e controllo delle stazioni e sistemi di protezione;
- sistemi di distribuzione e vendita.

2.3.1 Produzione dell'energia elettrica

I generatori devono poter funzionare correttamente e non andare fuori linea nei periodi di tempo in cui il *millennium bug* può essere più pericoloso. Di norma i generatori sono programmati in maniera tale da poter essere messi in funzione ed erogare elettricità secondo piani stabiliti in funzione delle caratteristiche della domanda. La minaccia posta in essere dal *millennium bug* è tanto più grave quanto più l'impianto di produzione di energia elettrica è dotato di sistemi computerizzati o di sistemi basati su elettronica digitale e quanto più è rilevante l’impianto nel sistema di produzione. Molti sistemi di controllo e di protezione (che utilizzano sistemi computerizzati e sistemi basati su elettronica digitale) possono dar luogo a condizioni di interruzione automatica quando si trovano di fronte ad una anomalia indotta dal *millennium bug*.

2.3.2 Controllo della produzione e della trasmissione dell'energia elettrica

Il controllo di un sistema di produzione e trasmissione dell’energia elettrica è costituito dall’insieme di operazioni volte a conseguire la massima regolarità e continuità del servizio compatibili con le esigenze di economia globale di funzionamento. Tramite gli appositi centri di controllo viene effettuato il monitoraggio del sistema elettrico e, in riferimento a tale continua rilevazione, viene generata e dispacciata in tempo reale l'energia per soddisfare la domanda. Di norma, all'interno di questi centri di controllo, sistemi computerizzati utilizzano programmi basati su algoritmi complessi per gestire le operazioni di dispacciamento dei generatori e di trasmissione. In ogni istante, una predeterminata percentuale di generatori è posta sotto controllo automatico al fine di

seguire le variazioni della domanda elettrica e per regolare la frequenza di interconnessione. Molte applicazioni software dei calcolatori che operano nei centri di controllo contengono componenti software precostituiti dipendenti dalla data (dove quindi il *millennium bug* può verificarsi), utilizzati per gestire le operazioni di monitoraggio, dispacciamento e controllo dei sistemi di energia. Oltre il primo livello nazionale di controllo del sistema elettrico, operano centri secondari di controllo che gestiscono i sistemi di produzione e trasmissione di ordine inferiore. Di norma, tali sistemi sono fatti funzionare utilizzando un sottosistema di gestione dell'energia, a cui si dà il nome di *Supervisory Control and Data Acquisition* (SCADA).

2.3.3 Telecomunicazioni e teleconduzione

I sistemi di trasmissione e distribuzione di energia elettrica sono molto dipendenti da sistemi di telecomunicazione e teleconduzione in cavo coassiale, via telefono, tramite linee di trasmissione dati, per mezzo di radio VHF, o altro. Le telecomunicazioni costituiscono un punto nevralgico essenziale del funzionamento del sistema elettrico, la cui responsabilità tuttavia, nel caso dei medi e piccoli operatori, è in carico ad un gestore di telecomunicazioni esterno. Le aziende che operano nel settore dell'energia elettrica dovranno pertanto indagare accuratamente con la collaborazione di detti fornitori la funzionalità del proprio sistema di comunicazioni e verificarne l'incolumità in riferimento ai rischi posti dal *millennium bug*.

2.3.4 Sistemi di trasmissione e controllo delle stazioni e sistemi di protezione

Lungo tutto il percorso dei sistemi di trasmissione dell'energia elettrica sono posizionate le stazioni dotate di interruttori, sezionatori e trasformatori. Le stazioni, di norma, sono dotate di terminali remoti connessi con i centri di controllo per gestire i flussi informatici inviati dai terminali periferici (misure, segnali e allarmi) al centro operativo e viceversa. Le stazioni inoltre contengono dispositivi di protezione e controllo associati agli elementi costitutivi dell'impianto che servono per azionare gli interruttori, al fine di isolare prontamente l'apparato ove si manifesti un guasto elettrico (linea di trasmissione, trasformatore o altro elemento del sistema). La gran parte dei dispositivi e dei relé esistenti nelle stazioni sono di tipo analogico o digitale e quindi deve essere sottoposta a controllo.

2.3.5 Sistemi di distribuzione e vendita

I sistemi di distribuzione forniscono elettricità dalla rete di trasmissione ai consumatori. Essi, per quanto attiene i rischi del *millennium bug*, sono assimilabili ai sistemi di trasmissione.

2.4. Il settore del gas e il *millennium bug*

Per quanto riguarda il gas naturale, gli effetti del *millennium bug* possono essere particolarmente critici per le fasi di estrazione, importazione, stoccaggio, dispacciamento e trasporto.

In termini generali, i principali punti di rischio che vanno controllati ed eventualmente corretti o rimpiazzati sono:

- i sistemi di controllo delle apparecchiature di regolazione, misura e odorizzazione del gas attraverso le cabine di prima ricezione;
- i sistemi SCADA di supervisione, controllo e acquisizione dati;
- i calcolatori destinati a funzioni di controllo di processo;
- i dispositivi di correzione e gli apparati di misura, ivi inclusi i dispositivi mobili e a trasporto manuale che misurano il consumo del gas;
- i moduli prodotti da calcolatori e i formulari elettronici riguardanti ordini di lavoro, assegnazioni di date ad attività da compiere, pianificazioni dell'acquisizione o della distribuzione del gas;
- le operazioni da eseguire, le calibrature di strumenti o le registrazioni di conformità alle norme di sicurezza;
- i sistemi di supporto alle cabine di ricezione e di alimentazione di tutte le reti, ivi inclusi i sistemi di sicurezza, i sistemi di gestione dell'energia, i sistemi di continuità, i sistemi di preriscaldamento del gas, i sistemi di ventilazione, i sistemi di condizionamento dell'aria, ecc.

Concentrando l'attenzione sugli impianti di distribuzione, le parti maggiormente soggette ai rischi insiti nell'accadimento del *millennium bug* sono le seguenti:

- cabine di prima ricezione;
- valvole regolatrici di portata;
- correttori volumetrici;
- sistemi di regolazione della portata erogata da cabine di prima ricezione interconnesse**.**

2.4.1 Cabine di prima ricezione

Il gas proveniente dalla rete primaria dei gasdotti attraverso le cabine di prima ricezione viene filtrato, decompresso, misurato e odorizzato prima di essere immesso nella rete di distribuzione. Le cabine sono dotate di dispositivi di sicurezza e di controllo. Parte dei dispositivi esistenti nelle cabine di maggiori dimensioni sono di tipo analogico o digitale e quindi deve essere sottoposta a controllo. Inoltre, le cabine di maggiori dimensioni sono di norma attrezzate con calcolatori e terminali remoti connessi con i centri operativi di controllo per gestire i flussi informatici inviati dai terminali periferici (misure, segnali e allarmi) al centro operativo e viceversa. Nei casi in cui siano installati odorizzatori dosimetrici essi possono essere azionati e controllati mediante dispositivi elettronici.

2.4.2 Valvole regolatrici di portata

Le valvole regolatrici di portata, possono essere azionate per via elettronica con sistemi a microprocessore.

2.4.3 Correttori volumetrici

Nei casi di installazione, sia in cabina sia su utenti finali alimentati in media pressione, essi provvedono mediante algoritmi di calcolo elaborati da microprocessori alla correzione della misura per la fatturazione o del gas acquistato o del gas fornito all'utente.

2.4.4 Sistemi di regolazione della portata erogata da cabine di prima ricezione interconnesse

Nei casi di reti complesse di distribuzione del gas, possono essere installati sistemi di telegestione e regolazione delle portate di gas immesso in rete da diversi punti di alimentazione tra loro interconnessi. Possibili anomalie di funzionamento originate dal *millennium bug* possono creare problemi di bilanciamento dell'assetto della rete.

3 IL PERCORSO DI CONVERSIONE ALL'ANNO 2000

Da un punto di vista generale, il percorso di conversione all'anno 2000 previsto dal progetto anno 2000, teso ad eliminare il problema del *millennium-bug*, si articola in più fasi successive:

- inventario;
- valutazione commerciale, tecnica e dei rischi;
- scelte tecniche fondamentali e scelta delle applicazioni prioritarie;
- stima dei costi aziendali;
- creazione dell'ambiente di conversione;
- esecuzione delle conversioni;
- test, verifiche e collaudi.

Il questionario riportato in Allegato 3 è finalizzato esclusivamente a consentire all'esercente una autodiagnosi di massima del suo stato di preparazione rispetto all'intero percorso di conversione all'anno 2000.
Di seguito sono esposte in dettaglio le attività di alcune fasi.

3.1. Inventario

La fase dell'inventario consiste nell'individuazione dell'architettura e degli ambienti tecnici esistenti, con particolare attenzione ai sistemi *embedded*, alle piattaforme hardware, al software, agli archivi, alle banche dati, ai fogli elettronici ed ai grafici in uso nell'azienda e nell'individuazione degli oggetti influenzati dalla conversione (apparecchiature, programmi, dati, modulistica, ecc).

Le piattaforme hardware consistono in elaboratori centrali (*mainframe*), elaboratori di servizio (*server*), stazioni di lavoro (*workstation*), terminali e Personal Computer (PC *desktop* e portatili) ed altro hardware di supporto (apparati di rete, *modem, router, PAD, multiplexer*, centralini, terminali telefonici, dispositivi di sicurezza, ecc).

Il software consiste nel software di base (sistemi operativi), nel software di supporto (SORT, programmi di utilità), software d'ambiente (gestori di banche dati, software d'automazione d'ufficio, software di telecomunicazione, ecc.), nei programmi specifici del business acquistati dall'esterno o sviluppati internamente, nel microcodice (*firmware*) quale il Basic Input/Output System (BIOS). L'informazione raccolta sarà introdotta in una biblioteca elettronica (*repository*) dedicata all'operazione di conversione per la compatibilità all'anno 2000. Si avrà cura di riempire tutti i campi (*field*) definiti nella fase di analisi propedeutica all'inventario. Per migliorare la conoscenza del sistema, i dati raccolti nel *repository* dovrebbero essere verificati con le informazioni ottenute dall'uso di strumenti (*tool*) automatici e controllate da elementi del personale in possesso di una conoscenza approfondita del sistema.

3.1.1. Hardware e sistemi operativi

I sistemi operativi sono facili da inventariare: questa fase dovrebbe essere completata rapidamente.

A) Calcolatori *mainframe* a connotazione centralizzata

Nell'ambiente *mainframe* non è difficile rendere compatibile il sistema operativo con l'anno 2000, se il modello hardware non è obsoleto e consente la sostituzione del sistema operativo. Si procede nel modo seguente:

- si comunica alla società costruttrice il modello e l'anno di acquisizione dell'hardware e la versione del sistema operativo;
- la società costruttrice fornisce l'eventuale aggiornamento (*update*) e rilascia una certificazione di conformità del sistema operativo all'anno 2000.

B) Calcolatori dipartimentali a connotazione distribuita

Nei calcolatori di fascia media è facile rilevare la versione del sistema operativo e predisporre le misure tendenti a rendere conforme il sistema all'anno 2000, eseguendo gli stessi passi riportati precedentemente per i mainframe.

C) Sistemi UNIX

I sistemi UNIX (*server*, stazioni di lavoro collegate in rete o indipendenti) sono per lo più immuni dal problema dell'anno 2000; avranno un problema simile, con retrocessione della data, soltanto il 19 gennaio 2038 alle ore 3, 14 minuti e 7 secondi. In pratica però solo le versioni più recenti sono completamente compatibili.

D) Stazioni di lavoro Apple e Macintosh

Le stazioni di lavoro Apple e Macintosh, non dovrebbero avere problemi derivanti dal 2000; infatti:
1) i vecchi Macintosh azzereranno la data il 6 febbraio 2040 alle 6:28:15;
2) i nuovi Macintosh azzereranno la data nell'anno 2940;
3) i vecchi Apple II, IIc, IIc+, IIe non hanno un *clock* di sistema;
4) gli Apple IIgs con System 6 o seguenti non hanno problemi legati alla data del 2000;
5) gli Apple IIgs impiegati con applicazioni a 8 bit, necessitano la versione proDOS 8V2.0 o le seguenti.

E) Stazioni di lavoro PC Windows compatibili

Nelle stazioni di lavoro costituite da PC la soluzione del problema risulta più ardua poiché le famiglie dei sistemi operativi comunemente riscontrabili possono essere cinque:
1) MS-DOS;
2) Microsoft Windows 3.x;

3) Microsoft Windows 95/98;
4) Microsoft Windows NT;
5) IBM OS/2 Warp.

Le incompatibilità dei PC con il cambiamento di secolo possono dipendere dall'hardware e dal sistema operativo; a tal fine è consigliabile procedere ai test descritti nei siti Internet dei fornitori.

Nel caso questi test dovessero fallire, considerando i vari rilasci (*release)* dei sistemi operativi ed il numero dei differenti dispositivi e sistemi guida di dispositivi (*device drivers*) ad essi associati, l'unica valida alternativa, e probabilmente la più economica, è la seguente:

1) sostituire tutti i PC con processore di modello inferiore al 486 o prodotti prima del 1996 con nuovi modelli (tutti i nuovi modelli basati su processore Pentium sono compatibili con l'anno 2000 ed hanno il BIOS che può essere modificato per correggere eventuali errori, mentre modelli basati su processori più datati probabilmente non consentono la modifica del BIOS);

2) seguire le disposizioni e i consigli del sito Internet di Microsoft sull'argomento dell'anno 2000.

F) Sistemi in rete locale (LAN)

Le reti locali sono considerate generalmente immuni da problemi perché intrinsecamente conformi all'anno 2000. Purtuttavia anche questi software hanno taluni difetti e ne va effettuata una accurata verifica.

3.1.2 Software applicativo

A) Pacchetti di software applicativo acquisiti dal mercato

Per inventariare pacchetti software in ambiente *mainframe*, occorre l'ausilio di strumenti automatici ad hoc. Se il produttore del software non é più reperibile, i dati rilevati dai *tool* nei programmi eseguibili (*load module*) consentono di determinare se la versione del compilatore utilizzato è compatibile con l'anno 2000. L'incompatibilità rilevata in questo modo mostra che il prodotto non è conforme; se ne deve pertanto richiedere l'aggiornamento o la sostituzione.

In genere, nelle aziende, il software prodotto od acquistato a livello dipartimentale o dagli utenti finali sfugge al controllo del sistema informatico ed è quindi più difficile da inventariare. La grande varietà di questo software e l'eventuale dispersione geografica degli utenti finali, costituisce la maggiore area di rischio per la compatibilità con l'anno 2000, in quanto molti di questi prodotti utilizzano date per l'ordinamento cronologico e per i calcoli.

Un censimento del software installato presso gli utenti è l'unico metodo di costituire un inventario.

B) Software sviluppato all'interno dell'azienda

I programmi basati su *mainframe* sono relativamente i meno complessi da inventariare, perché censiti da *tool* di tipo *librarian*.

I programmi possono esistere in più formati:

a) sorgente;
b) modulo eseguibile;
c) sorgente interpretato;
d) linguaggio di controllo;
e) parametri in input per altri programmi.

Nel caso di una cancellazione irreversibile del codice sorgente, esistono degli strumenti di "*reverse engineering*" che consentono di risalire al codice sorgente partendo dal modulo eseguibile. Il risultato di questa operazione non è sempre soddisfacente e deve quindi essere considerato come l'ultima risorsa possibile.

3.1.3 Il repository anno 2000

Il *repository* anno 2000 è lo strumento base per il controllo della conversione del sistema informatico.

La chiave di ricerca della base dati è costituita dai moduli eseguibili; questi ultimi possono essere *load module*, programmi per *workstation* e programmi sorgente interpretati.

Oltre ai moduli eseguibili, sono da inventariare:

a) ambienti e strumenti per la gestione delle configurazioni, del *change management* e delle librerie;
b) ambienti, dati e strumenti esistenti per l'esecuzione dei test;
c) contratti in essere di manutenzione del software, indici di manutenibilità e complessità dei programmi;
d) risorse umane interne ed esterne dedicate alla gestione e manutenzione del software;
e) strutture organizzative interne e società esterne.

3.2 Creazione dell'ambiente di conversione

Il progetto di conversione si dovrà articolare lungo 4 direttrici:

a) il progetto tecnico di conversione vera e propria;
b) il progetto del Piano di emergenza;
c) il progetto relativo alle implicazioni commerciali;
d) il progetto relativo alle implicazioni amministrativo-legali.

L'esecuzione del progetto a) richiede un ambiente di conversione. La predisposizione dell'ambiente è complessa e richiede una pianificazione molto accurata. Effettuato l'inventario delle applicazioni da convertire, fatte le scelte delle strategie di conversione, stabilite le priorità, fatta una stima dei tempi necessari e dei costi prevedibili, è necessario approvvigionare le risorse necessarie ed organizzare l'ambiente per la conversione.

Le attività principali sono le seguenti:

1) approvvigionamento dell'hardware;
2) approvvigionamento degli strumenti necessari;
3) selezione delle risorse umane, addestramento;
4) creazione del sistema di controllo della configurazione;
5) pianificazione di dettaglio delle attività di conversione.

3.2.1 Approvvigionamento dell'hardware

La conversione è un lavoro aggiuntivo rispetto all'attività corrente. Sono quindi necessarie risorse hardware ulteriori per la modifica dei programmi, per i test e per la conversione degli archivi.

3.2.2 Scelta ed approvvigionamento degli strumenti necessari

Sono disponibili sul mercato molti strumenti che forniscono supporto nelle varie fasi del processo di conversione, accelerandone lo sviluppo e riducendone i costi; anche la loro utilizzazione, però, non è priva di problemi. Infatti:

- per addestrare una persona e renderla efficace nell'uso di un pacchetto software occorrono circa tre mesi;
- il programmatore medio non apprende l'uso di più di due pacchetti nello stesso tempo;
- le conversioni considerate possono richiedere l'uso di 30 o 40 pacchetti diversi;
- l'addestramento richiederebbe quindi un paio d'anni.

Pertanto, conviene concentrarsi sugli strumenti di incremento della produttività già noti e installati o su quelli di cui si prevede in futuro un impiego più esteso (ad es. quelli riguardanti il linguaggio più diffuso: il COBOL).

Sono generalmente disponibili sul mercato strumenti per il supporto e l'automazione delle seguenti funzioni:

1) *repository* dei dati e inventario del software;
2) analisi del codice dei programmi e *editing* del codice;
3) *reverse engineering*;
4) gestione della configurazione;
5) manipolazione del codice eseguibile;
6) generazione di dati di test e test di programma;
7) simulazione di date e simulazione di interfacce;

8) conversione di dati;
9) gestione della documentazione;
10) stima dei costi.

3.2.3 Selezione ed acquisizione delle risorse umane, addestramento

Le azioni che si possono intraprendere per limitare il problema della scarsità di personale specializzato nella conversione all'anno 2000 sono indicate qui di seguito:

a) assicurare la permanenza in azienda delle persone disponibili con le professionalità richieste;

b) ricercare fra i pensionati del settore quelli disponibili a riprendere l'attività nel periodo delle conversioni;

c) creare meccanismi contrattuali a tempo che rendano stabili questi rapporti per la durata necessaria;

d) fornire a questo personale un addestramento specifico per aumentarne l'efficienza e l'efficacia;

e) formare utilizzatori interni all'azienda, per assistere il personale informatico addetto alle conversioni;

f) assumere un numero opportuno di neo-diplomati e neo-laureati e sottoporli ad un addestramento intensivo.

3.2.4 Messa in opera di un sistema di controllo della configurazione

La funzione del controllo della configurazione è quella di assicurare che le applicazioni siano costituite dalle versioni corrette e compatibili dei propri componenti informatici (programmi, moduli, *subroutine*, tabelle, archivi storici, ecc.). Molte applicazioni sono composte da centinaia/migliaia di componenti i quali devono essere coerenti tra loro; una parte di questi elementi é condivisa da più applicazioni e quindi una loro modifica si riflette su più sistemi e rami di business.

Ciascun componente può avere diverse versioni per motivi di manutenzione correttiva, evolutiva o migliorativa imposta da esigenze aziendali interne o da fattori esterni. Le differenti versioni, poi, non operano simultaneamente nei vari ambienti (esercizio, sviluppo, manutenzione, ecc) di cui di norma si compone un sistema informatico medio-grande.

L'avvento dell'anno 2000 impone la gestione di più ambienti che, sommati a quelli consueti, individuano, nel periodo transitorio, una configurazione complessa che necessita di un robusto sistema di controllo; altrimenti la possibilità di perdere il controllo del progetto è elevata. Un sistema di controllo della configurazione robusto deve avere:

1) la capacità di monitoraggio/registrazione eventi e di gestire ambienti plurimi;
2) la capacità di gestire simultaneamente molte modifiche e molti progetti;

3) la capacità di gestire conversioni effettuate fuori azienda e di controllo dell'integrità della transizione;
4) la semplicità di utilizzo e la possibilità di accesso da parte di auditor esterni.

3.3 Esecuzione delle conversioni e test

Le modalità di esecuzione delle conversioni non si discostano da quelle che sono le buone pratiche usate normalmente per la manutenzione. E' necessaria tuttavia una attenzione approfondita per:

- la **creazione/gestione dell'ambiente di conversione** e il coordinamento degli utilizzatori;
- i **test**.

La **creazione di un ambiente di conversione** si snoda attraverso i seguenti passaggi:

a) valutazione della configurazione esistente;
b) acquisizione e impianto dei miglioramenti in termini di organizzazione, risorse umane, risorse strumentali e risorse documentali;
c) installazione degli strumenti di gestione della configurazione e degli ambienti virtuali o fisici necessari;
d) impostazione e creazione dei report di configurazione, personalizzati secondo le esigenze dell'azienda;
e) caricamento delle librerie con il software e i dati aziendali non conformi;
f) accertamento dell'integrità del processo di migrazione.

Le tipologie di **test da eseguire** sono le seguenti:

A) Test unitari sui singoli programmi che, a loro volta, si suddividono in:

1) Test di regressione
Assicura che le modifiche per l'anno 2000 non alterino le funzionalità delle applicazioni correnti e verifica che modifiche funzionali apportate dopo la conversione non inducano errori di conformità all'anno 2000.

2) Test dopo la data limite
E' mirato esclusivamente alla verifica del comportamento delle applicazioni/procedure dopo il 1° gennaio 2000.

3) Test sulle date limite
Effettua la verifica in corrispondenza di date particolari (99° giorno dell'anno = 9999 = *end-of-file*; 9 settembre 1999 = 9999; 31 dicembre 1999 = 311299; 1° gennaio 1999 = 010100; 29 febbraio 2000 = 290200.

4) Test di back-up /recovery
Controlla la funzionalità di tutte le procedure e applicazioni per il ripristino della situazione precedente (programmi e dati) nella evenienza di un qualsiasi fermo o malfunzionamento del sistema convertito.

5) Test di prestazione
In conseguenza della conversione possono essere stati introdotti cambiamenti ai programmi con possibili effetti di degradazione della prestazione globale di uno o più sistemi. Tali effetti vanno annullati con apposite azioni riparatorie.

6) Test di parallelo
Prevede l'elaborazione contemporanea dell'applicazione convertita e di quella precedente, è particolarmente oneroso e di difficile attuazione per cui va limitato alle sole applicazioni critiche.

B) Test integrati che integrano tra loro, con livelli crescenti di complessità, programmi, archivi, domini di applicazione del sistema informatico, sistemi informatici di aziende interconnesse.

3.4 Le verifiche e i collaudi

Gli obiettivi principali delle attività di verifica e collaudo sono:

a) la certificazione della qualità e della flessibilità del sistema al mutare delle condizioni interne ed esterne dovute alla nuova situazione;

b) la valutazione, in caso di non perfetto allineamento, delle soluzioni più efficaci e del rischio commerciale e/o legale nei confronti degli adempimenti societari o verso terzi.

Particolare attenzione, dovrà essere rivolta agli aspetti organizzativi del processo di verifica e collaudo in termini di:

1) rigida pianificazione delle fasi e accurata preparazione di casi prova in relazione ai vari processi aziendali;

2) definizione del numero, della qualità e degli specifici ruoli delle risorse umane necessarie;

3) identificazione dei responsabili delle fasi di collaudo e verifica.

La fase delle verifiche e dei collaudi si compone sostanzialmente delle seguenti attività:

1) definizione organizzativa delle attività della fase;

2) stesura di un piano dettagliato e sua convalida;

3) esecuzione del piano e predisposizione del documento conclusivo.

Il rigoroso rispetto del piano approvato e il suo continuo monitoraggio da parte del responsabile e del settore qualità/audit costituiscono l'elemento essenziale per il raggiungimento degli obiettivi di tale attività.

4 IL PIANO DI EMERGENZA

Per ridurre il livello di rischio, in relazione al limitato tempo ancora disponibile per rendere conforme il sistema informatico alle esigenze dell'anno 2000 è necessario predisporre due piani operativi paralleli d'intervento sul patrimonio informatico:

a) un piano principale che preveda la completa revisione di tutte le applicazioni e procedure interne influenzate dall'anno 2000;

b) un piano di emergenza che, integrato con quello principale, identifichi le sole applicazioni e procedure critiche per il business ed i percorsi di sovrapposizione con quello principale in modo da passare dall'uno all'altro in relazione al superamento di certi limiti temporali e senza evidenti discontinuità operative.

Il responsabile del piano di emergenza dovrà:

- predisporre gli interventi minimi necessari, in base ad una analisi di rischio dei processi aziendali delle applicazioni informatiche di supporto, per consentire la continuità operativa;
- identificare, sulla base dell'analisi condotta in precedenza, i percorsi alternativi rispetto al piano principale e l'impatto sulla riduzione dei tempi d'intervento e sull'organizzazione operativa;
- monitorare costantemente il piano principale in modo che, al verificarsi del superamento dei limiti di tempo massimi previsti per l'esecuzione dello stesso, possa essere avviato immediatamente quello di emergenza acquisendo tutte le attività già sviluppate e comuni ai due piani;
- valutare i tempi necessari per completare il piano principale una volta concluso quello di emergenza.

Lo sviluppo del piano di emergenza, per il quale viene qui definito un approccio strutturato anche se generalizzato, si articola sostanzialmente in quattro fasi principali distinte in attività:

1) pianificazione iniziale;
2) analisi d'impatto sul business;
3) definizione del piano di emergenza;
4) stesura del piano di collaudo.

Ciascuna delle suddette fasi deve prevedere una metodologia di gestione e controllo del progetto con relativi punti critici e percorsi alternativi.

Il questionario riportato in Allegato 4 consente agli esercenti i servizi di pubblica utilità nei settori dell'energia elettrica e del gas una verifica di massima dello stato di preparazione del piano di emergenza, con indicazioni specifiche per quanto riguarda la fornitura di energia elettrica e di gas.

Bibliografia selezionata e siti Internet d'interesse

VOLUMI

- Burne K.C., *Year 2000 Solutions for Dummies*, IDG Book Worldwide Inc., International Data Group Company, 916 E. Hillsdale Blvd. Suite 400, Foster City, California, USA, 1997

- Chapman R.B., *Practical Methods for Your Year 2000 Problem: The Lowest Cost Solution*, Manning, Greewich, Connecticut 06830, USA, 1997

- De Jager P. and Bergeon R., *Managing '00: Surviving the Year 2000 Computing Crisis*, John Wiley and Sons Inc., New York, USA, 1997

- Feiler J. and Butler B., *Finding and Fixing Your Year 2000 Problem: a Guide for Small Business and Organizations*, Academic Press, Chestnut, Massachussets, USA, 1998

- Hayes I.S. and Ulrich W.M., *The Year 2000 Software Systems Crisis: The Continuing Challenge*, Yourdon Press Computing Series, Prentice Hall Building, Upper Saddle River, New Jersey 07458, USA, 1998

- Hyatt M.S., *The Millennium Bug: How to Survive the Coming Chaos* – Regnery Publishing Inc. An Eagle Publishing Company, One Massachussets Av. NW, Washington DC 2001, 1998

- Institution of Electrical Engineers-IEE Technical Guidelines, *Embedded Systems and the Year 2000 Problem, Guidance Notes*, PO Box 96, Stevenage, Herts, SGI 2SD, UK, 1998

- Keogh J.E et al., *Solving the Year 2000 Problem*, Academic Press, 2428 Oval Road, London, NWI 7DX, 1997

- Lefkon D., *Year 2000: Best Practices for Y2K Millennium Computing*, Prentice Hall Inc., Upper Saddle River, New Jersey 07458, USA 1998

- Leggio A., *Euro, anno 2000 e sistemi informativi - L'impatto del cambio di data e della moneta unica: problemi, rischi, soluzioni e opportunità*, Il Sole 24 Ore Libri, Milano, 1998[1]

- Leggio A., *Euro e anno 2000 - Guida pratica per la conversione all'euro e per superare i problemi del cambio data nel 2000*, Il Sole 24 Ore Libri, Milano, 1998

[1] Nei capitoli 1 e 3 delle presenti linee guida sono utilizzati alcuni brani tratti dai volumi di A. Leggio indicati in bibliografia, per gentile concessione dell'editore.

- Sims D., Minahan Robinson J., Mc Connell C., Silo E., Shapiro Y.and Wilkbanks, C., *How To 2000*, IDG Groups Worldwide Inc., An International Data Group Company, 919E Hillsdale Blvd., Suite 400, Foster City, California 94404, USA , 1998

- Ulrich W. and Hayes I.S., *The Year 2000* Software *Crisis, Challenge of the Century*, Yourdon Press Computing Series, Prentice Hall Building, Upper Saddle River, New Jersey 07458, USA, 1997

- UNI, *Prepararsi all'anno 2000 - Come rendere i prodotti e l'azienda a prova di millennio*, traduzione dei documenti BSI DISC PD 2000-1 *A definition of year 2000 conformity requirements* e BSI DISC PD 2000-2 *Managing year 2000 conformity: a code of practice for small and medium enterprises* - British Standard Institution , Via Battistotti Sassi 11, 20133 Milano, 1997

- Utne Reader, *Y2K Citizen's Action Guide*, L.E.N.S. Publishing Co., Minneapolis, Minnesota 55403, USA, 1999

- Yourdon E. and Yourdon J., *Time Bomb 2000: What the Year 2000 Computer Crisis Means to You!*, Prentice Hall Inc., Upper Saddle River, New Jersey 07458, USA, 1998

- Zetlin M., *The Computer Time Bomb: How to Keep the Century Date Change from Killing Your Organization*, American Management Association, Publication Division, 1601 Broadway, New York, 10019, 1998

SITI INTERNET

http://www.aipa.it
http://www.anno2000.it
http://www.bancaditalia.it
http://www.comitatoanno2000.it
http://www.consob.it
http://www.ilsole24ore.it
http://www.isvap.it
http://www.minindustria.it
http://www.mininterno.it
http://www.osservatorio2000.com
http://www.repubblica.it
http://www.ispo.cec.be/y2keuro/src/yearbody.htm
http://www.itpolicy.gsa.gov/mks/yr2000/y201toc1.htm
http://www.year2000.com
http://www.euy2k.com/index.htm

http://www.iee.org.uk/2000risk
http://www.dir.state.tx.us/y2k
http://www.drj.com
http://www.yardeni.com
http://www.gao.gov
http://www.info2000.gc.ca
http://www.year2000.co.nz
http://www.sba.gov/y2k
http://www.global2k.com
http://www.aicpa.org
http://www.itu.int/y2k
http://www.oecd.org
http://www.ccta.gov.uk/mill/mbhome.htm
http://www.usia.gov/topical/global/y2k/
http://www.year2000.com
http://www.everything2000.com
http://www.isaca.org/yr2000.htm
http://www.y2k.com
http://www.dr.org/ppover.htm

ALLEGATO 1

Lo standard di conformità all'anno 2000[2]

Non esiste standard formale di conformità all'anno 2000. Tuttavia, lo standard DISC PD 2000-1, predisposto dal British Standars Institution Committee è universalmente accettato e ad esso si fa comunemente riferimento. Esso è sintetizzato qui di seguito.

Definizione

La conformità all'anno 2000 consiste nel fatto che né la prestazione né la funzionalità è influenzata da date precedenti, contestuali e susseguenti all'anno 2000.

Regola 1

Nessun valore della data corrente deve causare interruzioni delle operazioni.

Regola 2

La funzionalità basata sulla data deve comportarsi in maniera coerente per le date precedenti, contestuali e susseguenti all'anno 2000.

Regola 3

In tutte le interfacce e in tutti i dati memorizzati, il secolo presente in ogni data deve essere specificato in maniera esplicita ovvero tramite algoritmi o regole inferenziali non ambigue.

Regola 4

L'anno 2000 deve essere trattato come un anno bisestile.

Dallo standard PD DISC 2000-1 si traggono le ulteriori regole seguenti.

Integrità generale

Il passaggio tra le demarcazioni significative del tempo (ad esempio: giorni, mesi, anni, secoli) deve essere effettuato correttamente. Inoltre, la data corrente sta a significare la data del giorno, così come nota all'apparecchiatura o al prodotto.

[2] Il BS DISC PD 2000-1 è stato tradotto in italiano dall'UNI nel documento "Prepararsi all'anno 2000 – Come rendere i prodotti e l'azienda a prova di millennio" (si veda la bibliografia selezionata).

Integrità della data

Tutte le apparecchiature e tutti i prodotti devono calcolare, manipolare e rappresentare la data correttamente secondo gli scopi per cui sono stati costruiti. Inoltre, la funzionalità è intesa sia per quanto attiene ai processi, sia per quanto attiene i risultati di tali processi. Nessuna apparecchiatura o prodotto deve usare valori di date per scopi speciali (ad esempio, "00" per significare "non applicabile"/"inizio del file" o "99" per significare "end of file"). Infine, se lo si desidera, può aggiungere un punto di origine delle date e i relativi metodi di calcolo (Calendario Gregoriano).

Secolo esplicito/implicito

Secolo esplicito: se si usano 4 digit o si usa un indicatore del secolo, bisogna inserire un riferimento (ad esempio, l'ISO Standard 8601:1988 se si usa l'anno composto da 4 digit). Sarà tuttavia necessario consentire talune eccezioni nel caso di specifici domini applicativi (EDI, ATM, ecc).
Secolo implicito: se si usano regole inferenziali (ad esempio, un anno con 2 digit con un valore più grande di 10 sta a significare 19xx, e un anno con 2 digit con un valore minore o uguale di 10 sta a significare 20xx), allora la regola di inferenza deve valere in tutti i contesti in cui la data è usata anche se differenti regole inferenziali possono applicarsi a differenti archivi.

ALLEGATO 2

Definizione e descrizione dei sistemi *embedded*

Sistemi *embedded*

Questi sistemi hardware a tecnologia computerizzata che eseguono monitoraggio, controllo e gestione di processi, di componenti, di macchine, di sistemi o dell'ambiente (fabbriche o uffici), sono integrati nella piattaforma tecnologica a cui sono associati e sono essenzialmente una scatola nera (*black box*) modificabile con difficoltà o immodificabile. Infatti, alcuni sistemi hanno software che non può essere modificato, denominato "*embedded firmware*"; in altri, invece, tale software può essere modificato da specialisti.

Cosa si intende per sistema *embedded.*

In generale, un sistema *embedded* è un dispositivo elettronico a logica cablata, usato per controllare, monitorare e assistere l'operatività di una apparecchiatura, di una macchina o di un impianto.
I dispositivi più semplici consistono in un microprocessore singolo ("*chip*") che può essere assemblato con altri *chip* in un sistema ibrido o in un circuito integrato destinato ad una applicazione generalizzata o specifica.
Il dispositivo, in base ad una logica programmata, elabora un input proveniente in genere da un sensore o da un rivelatore e fornisce un output che gestisce un interruttore o un attivatore che, a sua volta, aziona o controlla una macchina. Talora, il dispositivo accetta anche logiche programmate successive: in tal caso si parla di "*firmware*".
Rispetto ai sistemi che contengono programmi software commerciali, un sistema *embedded* è più "all'interno" dell'apparato che lo ospita e ne costituisce in genere una parte inseparabile e segreta, di norma inaccessibile per motivi di protezione industriale.
Inoltre, sovente i sistemi *embedded* lavorano ad intervalli di tempo e non sulle date, hanno un ciclo di vita molto lungo (molto superiore a quello dei sistemi informatici commerciali) e sono in molti casi in situazione di operatività continua non interrompibile.
I sistemi *embedded* si suddividono in:

- microprocessori singoli
- schede assemblate di microprocessori privi di funzioni dipendenti dal tempo
- schede assemblate di microprocessori con funzioni dipendenti dal tempo

sistemi computerizzati usati nei sistemi di controllo di processo o nei sistemi di sicurezza.

I problemi relativi ai sistemi *embedded.*

Un attimo dopo le ore 23, 59 minuti e 59 secondi del 31 dicembre 1999, la data dovrebbe essere 1 gennaio 2000, e il tempo dovrebbe essere scandito come 00 ore, 00 minuti, 00 secondi. Ciò può non accadere, si possono produrre errori nei calcoli della

data, talora è impossibile sapere se nel momento del passaggio il sistema funzionerà per colpa propria o dell'ambiente tecnico in cui è inserito, se opererà correttamente o se si bloccherà.
Inoltre, é da considerare che nessuno sa con precisione quanti tipi di sistemi *embedded* sono stati prodotti a livello mondiale e quali hanno componenti che dipendono dal tempo; inoltre, i problemi si presentano in modo differenziato, continuamente ne vengono scoperti di nuovi, è difficile disporre di documentazione significativa atta a sapere se i sistemi sono a rischio; è infine difficile prendere le migliori decisioni: i problemi importanti sono pochi ma, per scoprirli, bisogna effettuare indagini complesse.
Infine, i dati scambiati con un'altra azienda possono inquinare i dati dell'azienda ricevente, le aziende sono responsabili dei dati errati inviati ai clienti o alle amministrazioni pubbliche, i contratti con i fornitori possono avere un oggetto incerto, è difficile ottenere contratti di assicurazione sul "rischio 2000" e le soluzioni adottate possono creare ulteriori problemi. Nonostante queste difficoltà, le aziende devono agire tempestivamente per attenuare al minimo ogni tipo di inconveniente (che può variare da transitorie diminuzioni dell'efficacia e della profittabilità alla possibilità di gravi offese alle persone o alla scomparsa delle aziende stesse).

ALLEGATO 3

Questionario per la verifica di massima dello stato di adeguamento all'anno 2000[3]

Stato di adeguamento al 2000

A quale livello di adeguamento al 2000 si trova l'azienda? (barrare una sola casella)

Livello 0: l'azienda non ha ancora iniziato alcuna attività per l'adeguamento all'anno 2000 ☐

Livello I: l'azienda è partita, ha assunto consapevolezza sul problema, ha identificato le azioni da intraprendere, e ha iniziato l'inventario delle dipendenze dei business dai sistemi informatici e computerizzati influenzati dall'anno 2000 ☐

Livello II: l'azienda ha effettuato una analisi completa e dettagliata delle dipendenze dei business ☐

Livello III: l'azienda ha predisposto progetti esecutivi, ha allocato le risorse umane e finanziarie, ha stabilito le priorità tra le dipendenze dei business, ha effettuato una valutazione del rischio e ha raggiunto la conformità al 2000 nel 20% dei sistemi critici ☐

Livello IV: l'azienda sta lavorando sul restante 80% dei sistemi critici ☐

Livello V: l'azienda ha raggiunto la conformità completa anche sui sistemi non critici ☐

Verifica puntuale sullo stato di adeguamento al 2000

1) Di quanti *function points* si compone il patrimonio software?

____ *(indicare il numero dei function points)*

2) Se non si hanno dati per rispondere alla domanda 1), di quante istruzioni si compone il patrimonio software e quale è la ripartizione del software tra i vari linguaggi di programmazione?

___ *(indicare il numero totale di istruzioni* software *operative)*

[3] Adattato dal volume di A. Leggio *Euro, anno 2000 e sistemi informativi– L'impatto del cambio di data e della moneta unica: problemi, rischi, soluzioni e opportunità*, Il Sole 24 Ore Libri, Milano 1998. Il questionario proposto è finalizzato esclusivamente a consentire all'esercente una autodiagnosi del suo stato di preparazione all'anno 2000.

___% *(indicare la percentuale di istruzioni scritte in linguaggi di 1ª generazione tipo Assembler, MacroAssembler, caratterizzati da 320-213 istruzioni/Function Point)*

___% *(indicare la percentuale di istruzioni scritte in linguaggi di 2ª generazione tipo C, Basic, Fortran, Algol, Cobol, Pascal, PL/1, etc caratterizzati da 128-80 istruzioni per Function Point)*

___% *(indicare la percentuale di istruzioni scritte in linguaggi di 3ª generazione tipo Lisp, QuickBasic, C++, VisualBasic, etc caratterizzati da 71-32 istruzioni per Function Point)*

___% *(indicare la percentuale di istruzioni scritte in linguaggi di 4ª generazione tipo SmallTalk, Generatori di applicazioni, SQL, fogli elettronici, caratterizzati da 21-6 istruzioni per Function Point)*

3) Si sa quanti sono i campi contenenti una data che l'azienda gestisce nel sistema informatico?

_ Sì, i campi contenenti una data gestiti dall'insieme dei programmi software del sistema informatico sono: _____ *(indicare il numero)*

_ No, stiamo valutando

4) Sono state individuate le applicazioni critiche che devono essere assolutamente convertite per consentire la sopravvivenza e lo sviluppo dell'azienda?

_ Sì, e le 7 applicazioni più importanti sono:

a) _____

b) _____

c) _____

d) _____

e) _____

f) _____

g) _____

_ No, stiamo valutando

5) Qual é il budget stanziato negli anni per raggiungere la conformità al 2000?

Anno 1998: _____ milioni di Lire

Anno 1999: _____ milioni di Lire

Anno 2000: _____ milioni di Lire

Anno 2001: _____ milioni di Lire

Anno 2002: _____ milioni di Lire

6) E' stata richiesta ai vostri fornitori la conformità al 2000?

_ Si

_ No

_ Stiamo valutando

7) Sono stati interessati i vostri maggiori clienti alle problematiche della conformità al 2000?

_ Si

_ No

_ Stiamo valutando

8) E' stato controllato che gli scambi dati con terzi siano conformi al 2000 in corrispondenza delle date critiche?

_ Si

_ No

_ Stiamo valutando

9) E’ stato nominato un responsabile aziendale del raggiungimento della conformità al 2000?

_ Si

_ No

_ Stiamo valutando

10) E’ stata definita una strategia per la sostituzione dei microprocessori presenti negli apparati e nei sistemi di sicurezza della vostra azienda, eventualmente interessati dal 2000?

_ Si

_ No

_ Stiamo valutando

11) E’ stato predisposto un Piano di emergenza per affrontare eventuali situazioni particolari dopo la data del 31 dicembre 1999?

_ Si

_ No

_ Stiamo valutando

ALLEGATO 4

Questionario per la verifica del Piano di emergenza per servizi di pubblica utilità nei settori dell'energia elettrica e del gas[4]

Questo è un elenco di domande "critiche": si rifletta sulla domanda con la collaborazione degli esperti dei vari settori, su quanto è stato fatto, se quanto è stato fatto è affidabile e definite le azioni da intraprendere.

I Organizzazione dell'azienda ai fini del Piano di emergenza

E' stato predisposto un gruppo di lavoro per il Piano di emergenza?
Chi è responsabile del gruppo?
Sono stati coinvolti i responsabili fondamentali dell'azienda?
I membri del gruppo sono in grado di comprendere l'organizzazione della produzione e i rapporti con i clienti, hanno l'autorità necessaria per prendere decisioni che hanno effetto sull'azienda, hanno risorse adeguate per operare efficacemente, sono in grado di registrare gli eventi in caso di crisi?
Il gruppo è organizzato in modo tale da attenuare o evitare situazioni di disastro, di rispondere efficacemente ad una emergenza, di riattivare il servizio?
I membri del gruppo sono stati addestrati per conoscere adeguatamente le esigenze dell'azienda e dei clienti, le vulnerabilità fondamentali, gli scenari di emergenza possibili, le connessioni con il governo, con la comunità in cui vive l'azienda, con i clienti?
Come sarà l'organizzazione dell'azienda il 31 dicembre 1999 nel momento del passaggio al nuovo millennio?
Ci saranno persone in più in servizio tali da poter affrontare e risolvere ogni problema?
Le persone essenziali sono tutte reperibili?
Questi aspetti sono stati concordati con le parti sociali?

II Processo di pianificazione del Piano di emergenza

E' stato definito un metodo ordinato e preciso da seguire nella esecuzione del Piano di emergenza?
E' possibile documentare quello che avverrà se si mette in atto il Piano di emergenza?
Il Piano di emergenza per il *millennium bug* è stato predisposto ad hoc o è l'adattamento di piani preesistenti su cui l'azienda ha esperienza?
Come è stato documentato il Piano di emergenza nei suoi vari aspetti (pianificazione, procedure, addestramento, test)?
Di norma, in azienda, i piani di emergenza sono aggiornati man mano che cambiano le esigenze o le circostanze?
Il Piano di emergenza è stato predisposto per fronteggiare tutti gli aspetti (problemi interni, problemi di fornitori esterni, problemi di clienti, panico del pubblico)?

III Valutazione del Processo di Business

Quali processi di business sono stati individuati come critici per l'operatività? Quali processi, invece, non sono critici?

---

[4] Allegato estratto da *Evaluation of utility Y2K contingency plans: a checklist for public service commissions* preparato da National Association of Regulatory Utility Commissioners (NARUC) P.O. Box 684, Washington, DC 20044-0684, 2152, come documento per la task force da essa istituita per il problema del cambio data del 2000. Il documento esprime in sintesi l'esperienza maturata dai diversi enti regolatori nazionali degli Stati Uniti ed è riportato a titolo di esempio della complessità di una verifica integrale del piano di emergenza.

I processi critici possono essere:

a. Processi di natura generale:
   - Flussi di cassa
   - Forniture

b. Processi tipici delle aziende elettriche:
   - Generazione dell'energia
   - Trasmissione dell'energia
   - Distribuzione dell'energia
   - Vendita e commercializzazione del prodotto elettrico
   - Infrastrutture di telecomunicazioni e loro sicurezza
   - Impianti e dispacciamento della generazione di energia
   - Sistemi SCADA
   - Telerilevamento
   - Servizio al cliente
   - Sistemi informatici
   - Fatturazione
   - Servizi agli azionisti

c. Processi tipici delle aziende del gas:
   - Sistemi di business basati su sistemi informatici tradizionali
   - Sistemi di business orientati al cliente
   - Sistemi *embedded*
   - Sistemi SCADA.

Quali sono i fattori chiave interni ed esterni (telecomunicazioni, fornitori fondamentali, sistemi informatici, sistemi di comando e controllo automatici, personale) che condizionano l'operatività di ciascuna funzione critica di business?

IV Valutazione del rischio

Quale metodo è stato adottato per prevedere gli scenari di rischio? Quali scenari di rischio sono stati previsti? Quali ipotesi sono state fatte e quali di esse sono implicite?
Quali rischi dovuti al *millennium bug* (sistemi *embedded*, sistemi su *mainframe*, sistemi su PC, altre tecnologie informatiche, attività operative, reti di telecomunicazioni, impianti) sono stati previsti?
I rischi possibili sono:

a. Rischi tipici delle aziende elettriche:
   - Caduta delle telecomunicazioni dovuta a sistemi interni
   - Caduta della generazione di energia
   - Caduta della trasmissione di energia
   - Caduta di sistemi EMS e SCADA
   - Isolamento non previsto delle interconnessioni
   - Caduta nel lungo termine della generazione di energia
   - Incremento delle interruzioni automatiche della generazione di energia
   - Difficoltà o impossibilità di partenza o ripartenza dei generatori
   - Isolamento dei centri di controllo
   - Malfunzionamenti nel bilanciamento del carico
   - Malfunzionamenti dei dispositivi di comando e controllo della tensione
   - Sabotaggi

b. Rischi tipici delle aziende del gas

Impossibilità di ricevere il gas e/o di erogarlo ai clienti
Caduta di pressione nella trasmissione del gas
Impossibilità di controllare la pressione lungo il sistema di distribuzione del gas
Impossibilità di fatturare e/o di ricevere pagamenti dai clienti
Impossibilità di mantenere i centri elettronici in condizioni di operatività continua.

Quali rischi esterni sono stati identificati?
I rischi possibili sono:

a. Rischi di natura generale:
   Difficoltà dei fornitori a fornire beni e servizi
   Ritardi nei flussi di cassa
   Calamità naturali o eventi distruttivi esterni

b. Rischi per le aziende elettriche:
   Malfunzionamenti o cadute delle telecomunicazioni dovute a sistemi esterni
   Limiti nella fornitura dei combustibili
   Livelli di carico anomali
   Instabilità della rete
   Caduta dei sistemi informatici di gestione dell'utenza

c. Rischi per le aziende del gas
   Caduta di carico presso l'utenza
   Caduta dell'approvvigionamento di gas da parte di aziende fornitrici
   Caduta dei sistemi informatici di gestione dell'utenza.

V Valutazione degli scenari probabili

Come sono stati sviluppati gli scenari prevedibili?
Quali priorità sono state assegnate ad essi?
Quali criteri sono stati adottati per ritenere probabili taluni scenari e improbabili taluni altri?
E' stata valutata la connessione tra l'impatto potenziale di uno scenario e la probabilità del suo accadimento?
Sono stati valutati gli "Scenari più probabili" e gli "Scenari pessimistici, ma credibili"?
Sono stati definiti i piani necessari per attenuare i rischi in tutte le aree critiche? Come sono documentati questi piani?
I piani prevedono l'attenuazione efficace del rischio, il ripristino del servizio e la gestione dell'emergenza?

VI Rapporti con i fornitori

E' stato predisposto un piano per verificare l'affidabilità delle catene di fornitura?
Sono stati individuati i fornitori principali?
In particolare é stata verificata approfonditamente l'affidabilità dei "fornitori unici" (cioè quelli che forniscono beni e servizi all'azienda, senza che ci siano alternative di fornitura per l'azienda) e i "fornitori *captive*" (cioè quelli che hanno nell'azienda l'unico cliente)?
I piani di fornitura predisposti dai fornitori sono improntati alla collaborazione o sono impostati secondo logiche puramente contrattuali che possono sfociare in disservizi e in contenziosi?
Dopo che i fornitori sono stati richiesti di fornire beni e servizi affidabili, per taluni il colloquio si è interrotto o è proseguito in maniera cooperativa ed efficace?
L'azienda aiuta i fornitori a risolvere i loro problemi in vista dell'obiettivo comune di erogare il servizio in condizioni di qualità e sicurezza, ovvero si arrocca su posizioni tipo quella espressa dalla massima "il cliente ha sempre ragione"?

Sono stati predisposti piani che identificano l'azienda come azienda erogatrice di servizi di pubblica utilità e, come tale, meritevole di trattamento prioritario e speciale da parte dei suoi fornitori, in particolar modo da parte degli altri fornitori di servizi di pubblica utilità (aziende erogatrici o smaltitrici di acqua, aziende erogatrici di servizi di telecomunicazione, istituti di credito) da cui l'azienda è dipendente?

VII Comunicazione e coordinamento

Quali piani sono stati predisposti per comunicare i piani di emergenza dell'azienda ai fornitori, ai mass-media, ai fondamentali soggetti della comunità in cui l'azienda opera, alle aziende erogatrici di servizi di pubblica utilità che sono interconnesse o vicine?
Come saranno informati i clienti?
Come saranno informate le associazioni dei consumatori?
Sono stati predisposti piani per i clienti critici (ad esempio le aziende sanitarie, ovvero i grandi clienti da cui l'azienda dipende finanziariamente)?
Come è stato informato il personale sul Piano di emergenza e sui processi da porre in atto?
C'è necessità di addestrare anche coloro che non avranno parte attiva nel Piano di emergenza?
Come saranno informate le parti sociali?
Come sono coinvolte nel Piano di emergenza le pubbliche amministrazioni da cui l'azienda dipende? Esistono piani in proposito?

VIII Test

Sono state effettuate prove per verificare che il Piano di emergenza è realistico, funziona ed è efficace?
Se le prove non sono state effettuate c'è la possibilità di predisporle ed effettuarle?
Se sono state effettuate, i risultati provenienti da esse sono stati utilizzati per aggiornare e migliorare il Piano di emergenza?

IX Documentazione del Piano di emergenza

Esiste documentazione di tutto quanto è stato esplorato o richiesto nel presente questionario?
Se esiste, é accessibile, come e da chi?
Chi è responsabile della predisposizione, dell'aggiornamento e della diffusione della documentazione?