Zeitschrift: Vermessung, Photogrammetrie, Kulturtechnik : VPK = Mensuration, photogrammétrie, génie rural

Herausgeber: Schweizerischer Verein für Vermessung und Kulturtechnik (SVVK) = Société suisse des mensurations et améliorations foncières (SSMAF)

Band: 89 (1991)

Heft: 3

Artikel: La sicurezza dei dati : una esigenza fondamentale dei sistemi informativi territoriali

Autor: Carosio, A.

DOI: https://doi.org/10.5169/seals-234571

La sicurezza dei dati

Una esigenza fondamentale dei sistemi informativi territoriali

A. Carosio

L'impiego dei moderni strumenti dell'informatica nella gestione dei dati spaziali è diventata una necessità per il geometra di oggi. Grazie alla riforma della misurazione ufficiale le nuove tecniche si diffonderanno rapidamente. La sicurezza dei dati è una premessa indispensabile per gestire le nostre informazioni efficacemente e a lungo termine. Quali sono i probleme da risolvere? A quali misure ricorrere? Sono domande di grande attualità.

Die modernen Werkzeuge der Informatik sind für den heutigen Geometer eine Notwendigkeit geworden. Dank der Reform der amtlichen Vermessung werden sich die neuen Techniken rasch verbreiten. Die Datensicherheit ist eine der Voraussetzungen, um unsere Informationen wirksam und während längerer Zeit verwalten zu können. Welche Probleme sind zu lösen? Welche Massnahmen können wir treffen? Es handelt sich um sehr aktuelle Fragen.

Introduzione

I sistemi d'informazione, con cui siamo abituati a lavorare da tempo, contengono un'immensa quantità di dati il cui valore cresce continuamente e supera di molte volte il costo dei sistemi informatici utilizzati. Nei sistemi d'informazione territoriali il fenomeno è chiaramente visibile e ben noto.

Per i gerenti di tali sistemi si pone da sempre il problema della sicurezza dei dati. Lo sviluppo dell'informatica e la gestione di grandi quantità di informazioni con i calcolatori hanno incrementato l'efficienza delle operazioni ma reso contemporeamente più critici i rischi di perdita di dati.

Le esigenze di sicurezza in geodesia e topografia sono molto elevate perché il costo di acquisizione delle nostre informazioni è grandissimo. Una perdita dei dati può causare costi di ricostruzione ingenti. Inoltre considerazioni puramente finanziarie sono in gran parte illusorie. In caso di perdita dei dati molte informazioni non potrebbero più essere ricostruite nemmeno se ci fossero messi a dispozione mezzi finanziari considerevoli (per es. copertura assicurativa).

La sicurezza dei dati è quindi una necessità fondamentale per la nostra attività: non possiamo permetterci perdite di dati, dobbiamo garantirne la sicurezza.

La sicurezza dei dati nel quadro dell'integrità dell'informazione

Prima di concentrare l'attenzione sul tema specifico della sicurezza dei dati è opportuno un riferimento in un quadro più generale: le misure volte a conservare la qualità dei dati e a garantirne l'uso legittimo. A questo livello si parla *d'integrità dell'informazione o integrità dei dati.*

L'integrità dei dati comprende:

- la correttezza dei dati
- la consistenza dei dati (assenza di contraddizione)
- la sicurezza dei dati
- la protezione dei dati (protezione contro l'uso abusivo).

La presente pubblicazione si limiterà a considerare solamente la problematica della sicurezza dei dati geodetici o topografici gestiti con sistemi elettronici, anche se gli altri aspetti sono altrettanto importanti e molto attuali.

La sicurezza dei dati

E'un concetto conosciuto. Nel linguaggio corrente sicurezza significa disporre di una sufficiente protezione contro i rischi.

Chiunque si occupi di informatica o amministri un centro di calcolo piccolo o grande deve considerare il rischio di perdita delle informazioni memorizzate e decidere le opportune contromisure. La sicurezza dei dati è lo scopo da raggiungere.

Ma non è sempre facile vedere cosa significhi esattamente e concretamente sicurezza dei dati. E' dunque opportuno investire qualche riga per rispondere a questa domanda fondamentale. Dobbiamo mettere in relazione gli scopi della sicurezza dei dati con i rischi di perdita per chairire e delimitare il problema.

Tutto sarebbe molto semplice se le informazioni trattate fossero costanti nel tempo. In un contesto topografico le informazioni mutano frequentemente e non è così evidente sapere cosa significhi una perdita d'informazione in un contesto dinamico.

L'introduzione della Norma tecnica svizzera «sicurezza dei dati nella misurazione ufficiale» e il piano di sicurezza dell'Ufficio federale di topografia ci forniscono alcune indicazioni (SNV 1987 [1], Carosio 1988 [2]):

> I dati e memorizzati (in un calcolatore) possono essere cancellati o modificati in seguito ad una manipolazione erronea, a danni materiali del mezzo di memorizzazione, a errori dei programmi o, e questo è il pericolo maggiore, a causa di eventi inattesi.
> Le cause principali di perdita di dati sono gli errori umani durante l'elaborazione. Ciò provoca di regola una perdita limitata d'informazione. I danni fisici ai supporti magnetici o equivalenti sono meno frequenti ma causano perdite di dati molto più considerevoli.
> Per ridurre i rischi bisogna ricorrere a contromisure che assicurino anche in caso di avarie o altri eventi dannosi:
>
> a) Che i dati invariati si conservino indefinitamente e possano essere utilizzati in ogni momento.
> b) Che i dati modificati correttamente siano conservati così come sono stati ottenuti o che almeno sia possibile ricostruirli.
> c) Che i dati modificati erroneamente possano essere riportati allo stato iniziale, anche nel caso in cui gli errori siano scoperti con ritardo.

Questa breve descrizione dà un'idea degli scopi da raggiungere e lascia intravvedere le difficoltà principali.

Forma delle contromisure, prescrizioni di sicurezza

Per raggiungere lo scopo della sicurezza dei dati sono necessarie contromisure che devono essere disposte a due livelli:

a) Prescrizioni generali (legislazione, norme tecniche).
b) Prescrizioni esecutive (disposizioni dei responsabili dei sistemi informativi, dei centri di calcolo ecc.).

Le prescrizioni generali non possono contenere liste complete di misure di sicurezza esplicite perché le misure opportune dipendono dall'infrastruttura disponibile. In particolare dipendono:

- dall'hardware che determina e limita i mezzi a disposizione per la memorizzazione dei dati
- dal sistema operativo e dalle banche di dati utilizzate che offrono una scelta limitata di procedure di sicurezza
- dai programmi applicativi che contengono o richiedono misure di sicurezza specifiche.

I responsabili del sistema possono influenzare solo molto limitatamente queste componenti, si tratta dunque di costrizioni esterne e la concezione delle prescrizioni di sicurezza esecutive deve essere adattata agli strumenti disponibili.
Le prescrizioni generali possono dunque richiedere il rispetto solo di norme operative di carattere universale mentre le misure specifiche possono essere prescritte indirettamente, richiedendo un'analisi approfondita dei rischi e misure di protezione adeguate. I responsabili decideranno secondo le necessità e sceglieranno tra le diverse alternative.
L'analisi dei rischi è in ogni caso un'esigenza fondamentale. La conoscenza delle categorie di rischio è una premessa.

Categorie di rischio, efficacia delle misure di sicurezza

Per classificare le categorie di rischio cui sono soggetti i dati di un sistema informativo ci si può riferire all'estensione dei rischi e al livello di conoscenza dei pericoli. La scelta di questa prospettiva è particolarmente utile perché la pianificazione di misure di sicurezza deve tener conto dei rischi di cui siamo coscienti come dei rischi sfuggiti alle nostre previsioni. Così come le nostre contromisure copriranno una parte dei rischi lasciandone scoperta un'altra parte.
Possiamo distinguere le seguenti categorie di rischio:

- rischio complessivo (o totale)
- rischio conosciuto
- rischio residuo
- rischio accettato.

Altrettando importante per le considerazioni sulla sicurezza è il campo d'azione delle contromisure. E' opportuno distinguere tra

- efficacia pianificata (o prevista)
- efficacia ottenuta.

La seguente rappresentazione grafica mostra il significato delle diverse categorie.

Prescrizioni operative generali

Le prescrizioni operative sufficientemente generali da poter essere proposte indipendentemente dal sistema utilizzato (hardware, sistema operativo e applicazioni) non sono molte. Si limitano a prescrivere forme organizzative che possono apparire persino banali. Esaminando però la situazione attuale specialmente negli studi d'ingegneria o centri di calcolo di piccole dimensioni ci si può convincere subito della loro necessità.
Mi limiterò a tre prescrizioni operative generali:

> 1 I responsabili di un sistema informativo devono redigere fin dall'inizio un piano operativo di sicurezza. Il piano deve essere scritto ed essere sottoposto a revisione periodica. L'esecuzione delle misure previste deve essere controllata.

Garantire la sicurezza dei dati è un compito importante e tocca le responsabilità dirigenziali. Per raggiungere lo scopo occorrono disposizioni operative precise. I compiti devono essere chiaramente attribuiti, le operazioni da eseguire chiaramente descritte, l'esecuzione deve essere controllabile. La forma scritta è una premessa ragionevole per compiti non limitati nel tempo. Sulla base di un piano di sicurezza scritto ci si può attendere un'esecuzione precisa delle misure decise in modo che l'efficacia ottentuta copra il meglio possibile la loro efficacia pianificata.
La seconda perscrizione generale ci suggerisce di far tesoro dell'esperienza:

> 2 Gli eventi che hanno causato perdite di dati devono essere analizzati e registrati.

Il modello dei rischi su cui ci si basa è incompleto e si limita a descrivere il rischio conosciuto. Ogni avvenimento imprevisto permette una conoscenza migliore dei pericoli e un adattamento del piano di sicurezza. Lo scopo della seconda contromisura è la riduzione del rischio residuo.
Il protocollo degli eventi che hanno provocato perdite di dati costituisce una raccolta di esperienze che, trasmesso agli interessati, permette di adeguare il piano di sicurezza ai rischi reali osservati.
L'ultima prescrizione operativa generale ha carattere tecnico.
Le misure di sicurezza sono diversificate sia per quanto riguarda la natura delle operazioni decise sia per l'estensione dell'efficacia prevista.
Le misure di sicurezza si possono suddividere nei seguenti gruppi:

a) Misure globali gestite dal sistema operativo (comprese le banche di dati) che sono eseguite automaticamente senza lacune per spazi estesi delle memorie (copie di dischi magnetici interi, protocolli delle mutazioni in una banca di dati ecc.).
b) Misure puntuali collegate alle applicazioni eseguite dai programmi applicativi o dagli utenti stessi. Ad esempio: le copie di files prima di un'operazione

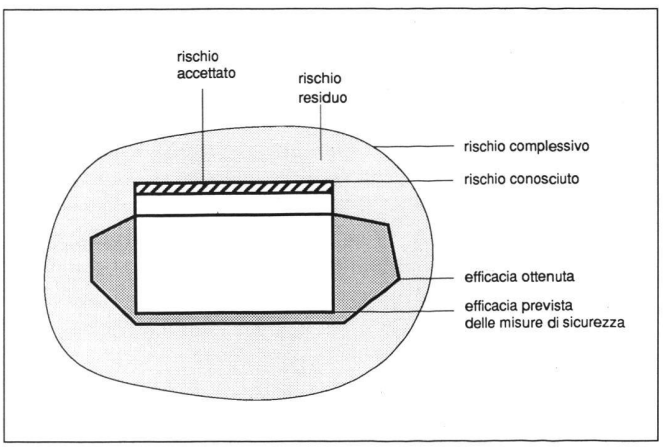

Fig. 1: Categorie di richio e efficacia delle contromisure.

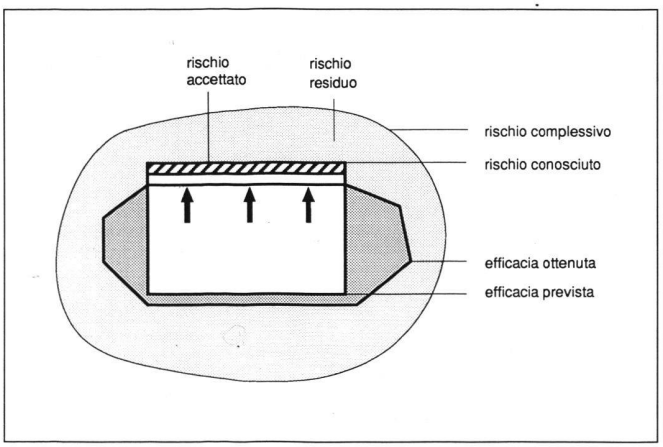

Fig. 2: L'efficacia prevista deve corrispondere il meglio possibile all'efficacia ottenuta.

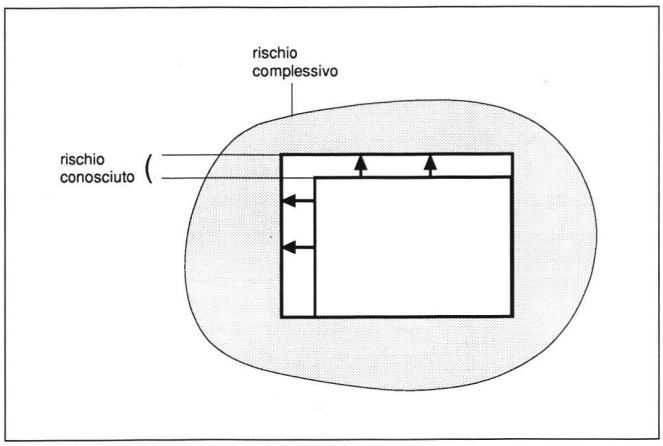

Fig. 3: Il rischio conosciuto si modifica nel tempo.

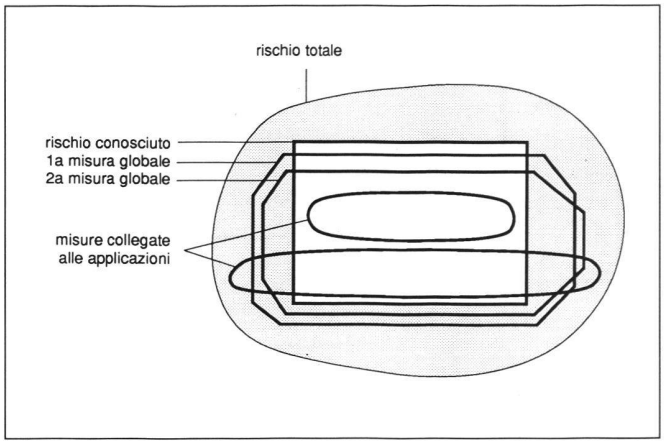

Fig. 4: Misure collegate alle applicazioni.

particolare, i protocolli delle operazioni eseguite ecc.

c) Le misure collegate alle applicazioni possono essere operazioni manuali quali l'archiviazione di formulari, la registrazione di operazioni ecc.

d) Misure organizzative che regolano le procedure di sicurezza e attribuiscono le competenze.

In base alla classificazione sopraindicata si giunge alla terza prescrizione generale:

> 3 Il piano di sicurezza può contenere misure dei diversi gruppi ma deve basarsi su misure globali e tener conto che le misure collegate alle applicazioni come le operazioni manuali possono essere incomplete o inefficaci.

Prescrizioni operative specifiche

Le altre procedure di sicurezza da eseguire dipendono dalle condizioni locali, dal sistema e da altre condizioni specifiche. Le misure operative sono da decidere nel dettaglio caso per caso. Ci si limiterà dunque a rispettare una regola di comportamento generale:

> I pericoli che incombono sui dati memorizzati nel sistema informativo sono da identificare mediante un'analisi dettagliata dei rischi.
> Il piano di sicurezza deve contenere tutte le contromisure necessarie per evitare che ad un evento sfavorevole conseguano perdite di dati inaccettabili.

L'analisi dei rischi

Lo scopo dell'analisi dei rischi è di rispondere a domande relative agli eventi temuti, agli oggetti minacciati, al tempo e al luogo in cui gli eventi possono realizzarsi.

Cosa può accadere?
In che modo può avvenire?
Cosa può venir danneggiato?
Quando e dove esiste il pericolo?

Esistono diversi metodi per l'analisi dei rischi nei quali le relazioni tra gli elementi minacciati, le cause di pericolo ecc. sono da analizzare e descrivere mediante matrici di rischio (Bauknecht 1990 [3], Simos-Rapin 1990 [4]:

pericolo / oggetto	Errore di elaborazione	Difetti tecnici	Azioni criminali
Memoria a disco			
Catalogo dei dati			
Programmi			

Fig. 5: Esempio di matrice di rischio.

Limitando l'esposizione ai pericoli che in senso stretto minacciano la sicurezza dei dati si possono riconoscere le seguenti cause di rischio.

a) Perdita di dati in seguito a danni al mezzo di memorizzazione

Esempi:
- Incendio, inondazione, danni naturali
- Distruzione volontaria (provocata da terzi o dal personale autorizzato)
- Danneggiamento del supporto di memorizzazione (graffi, rotture, invecchiamento del materiale, logorio prodotto da difetti dell'unità di lettura ecc.)
- Informazioni divenute illegibili col tempo.

b) Perdita o falsificazione di dati in seguito a elaborazioni errate o inopportune

Esempi:
- Esecuzione di istruzioni non indicate (cancellare, copia di un file su un altro da conservare, confusione di nome ecc.)
- Operazioni eseguite da programmi contenenti errori
- Azioni malevoli del proprio personale (sabotaggio, corruzione ecc.)
- Azioni malevoli di terzi (molto di moda: virus, bombe logiche, cavalli di Troia, vermi)
- Danni causati da terzi che accedono al sistema senza essere autorizzati
- Difetti o errori del sistema operativo o dell'hardware.

c) Perdita di dati se le procedure d'accesso divengono inutilizzabili

Esempi:

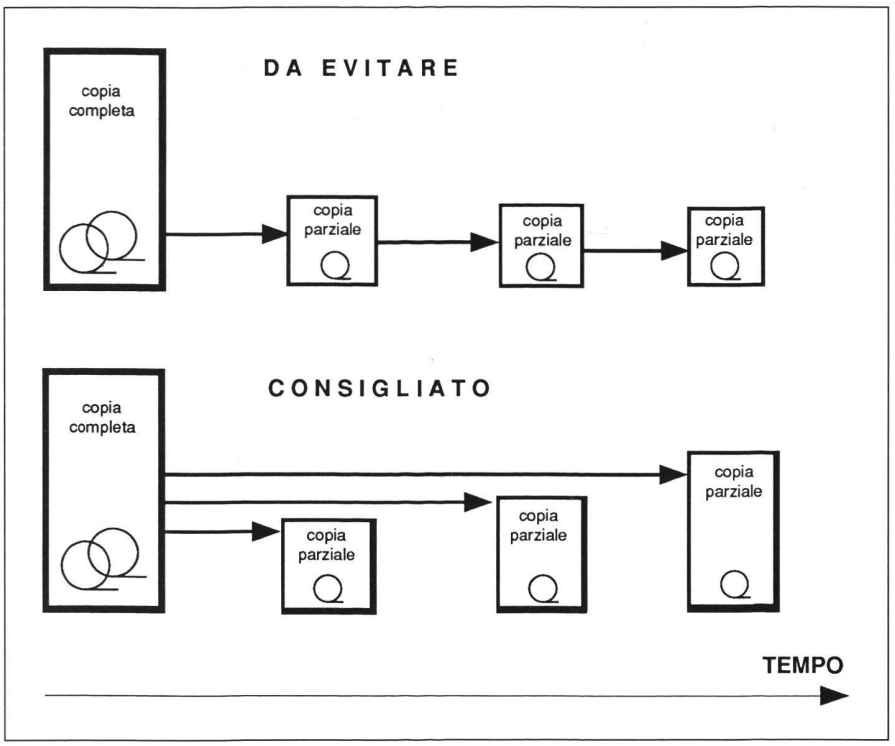

Fig. 6: Contromisure globali.

- Calcolatori o componenti antiquati non più riparabili
- La banca di dati (sistema di gestione della banca di dati) non funziona più.

d) Perdita di dati causati da organizzazione inefficiente

- Le conoscenze necessarie al funzionamento del sistema sono perdute
- I soli collaboratori responsabili competenti sono assenti o impediti a svolgere l'attività.

Contromisure tecniche

Per neutralizzare i rischi alle misure di carattere generale sono da aggiungere misure tecniche specifiche adatte alle caratteristiche del sistema.
La scelta può esser fatta conoscendo la configurazione del sistema e in base all'analisi dei rischi. Tra le contromisure possibili troviamo:

a) Contromisure tecniche globali, Esempi

- Copie dei dati memorizzati complete da eseguire periodicamente (NB: importante è che oltre al contenuto dei files siano copiate anche le strutture e l'organizzazione; nomi dei files, directories parametri di protezione ecc.).
- Copie incrementali da eseguire periodicamente tra una copia completa e la seguente. Per ridurre il lavoro si può ricorrere alla tecnica delle copie incrementali (solo i files modificati vengono copiati).
- Le copie di sicurezza sono da eseguire su supporti diversi da quelli usati per i dati originali.
- Registrazione di tutte le transazioni (protocollo delle transazioni su un supporto diverso da quello usato per i dati originali).
- Copie periodiche dei dati archiaviati.
- Assicurare il trasferimento dei dati sulla generazione successiva di calcolatori.

b) Contromisure tecniche collegate alle applicazioni, Esempi

- Copie di files particolari prima di un'operazione.
- Raccolta degli appunti usati per eseguire le operazioni.
- Realizzare i programmi applicativi in modo da poter ripetere l'elaborazione in caso di interruzione.

c) Contromisure organizzative, Esempi

- Organizzazione decentralizzata dell'acquisizione e gestione dei dati.
- Le copie complete sono da conservare in più esemplari in luoghi diversi.
- Le copie sono da conservare per lunghi periodi (anni), da identificare e registrare con precisione.
- Regolamentazione dell'accesso ai locali.
- Regolamentazione dell'accesso al sistema e ai dati (password, ecc.).
- Scelta prudente del personale.
- Nomina di sostituti.
- Le misure di sicurezza e la procedura decise sono confidenziali.
- I manuali d'istruzione sono da conservare in luogo sicuro.

Redazione del piano di sicurezza

Per la redazione del piano di sicurezza si può suggerire il seguente procedimento iterativo:

a) Redazione dell'analisi dei rischi.
b) Redazione di una prima versione del piano di sicurezza in base all'esperienza, al buon senso e alle disponibilità, rispettando le prescrizioni generali.
c) Controllo se le misure coprono adeguatamente i rischi previsti.
d) Completare il piano di sicurezza e ripetere le fasi c) e d) fino ad ottenere un risultato soddisfacente.

Conclusione

La sicurezza dei dati è una necessità che non possiamo ignorare. E' chiaro a tutti che l'elimazione completa dei rischi è uno scopo irraggiungibile e sarebbe finanziariamente insopportabile. Le analisi presentate e l'esperienza quotidiana mostrano però che con uno sforzo limitato è possibile raggiungere un livello di sicurezza più che soddisfacente. Per raggiungere lo scopo occorre preoccuparsi della sicurezza dei dati fin dall'inizio con una scelta ragionevole delle componenti e nel seguito con prescrizioni operative opportune, da riesaminare periodicamente e da rispettare con precisione e senza compromessi.

Bibliografia:

[1] Società svizzera di normalizzazione, Kirchenweg 4, CH-8032 Zurigo: Sécurité des données dans la mensuration officielle, Norma Svizzera 612010, Zurigo 1987.

[2] A. Carosio: Datenintegrität, Bundesamt für Landestopographie, Bulletin des RZ Nr. 14, CH-3034 Wabern.

[3] K. Bauknecht: Der Computer als offenes System: Grenzen der Computersicherheit, Sicherheit in der Informatik, Institut für Informatik der Universität Zürich, 5.6.1990.

[4] Béatrice Simos-Rapin: La sécurité des données, Vue par un responsable de centre informatique, Mensuration, Photogrammétrie, Génie rural Nr. 8, 1990.

Prof. Dr. Alessandro Carosio
Politecnico federale di Zurigo
ETH-Hönggerberg
CH-8093 Zurigo