
II DPS – analisi dei rischi

Ing. Gianfranco Pontevolpe

Centro Nazionale per l'Informatica nella Pubblica Amministrazione



Art. 31 – Obblighi di sicurezza

- I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di **idonee** e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.



Una misura è idonea se

- È in grado di ridurre i rischi in relazione alle conoscenze acquisite (teoricamente efficace)
- È equilibrata rispetto alle altre protezioni
- È proporzionata rispetto agli obiettivi ed al contesto
- All'atto pratico non si rivela inadeguata



Una misura è idonea se

- È in grado di ridurre i rischi in relazione alle conoscenze acquisite (teoricamente efficace)
 - È equilibrata rispetto alle altre protezioni
 - È proporzionata rispetto agli obiettivi ed al contesto
 - All'atto pratico non si rivela inadeguata
- Pianificazione (DPS)
- Analisi dei rischi
- Verifica periodica



L'individuazione delle misure idonee

- Documento programmatico
 - analisi dei rischi
 - scelta delle misure ottimali
 - verifica rispetto misure minime
- Adozione delle contromisure
- Verifica periodica



Misure idonee e misure minime

misure idonee \neq misure minime

- Le misure "idonee" sono individuate tenendo conto del contesto ed hanno l'obiettivo di conseguire un livello di sicurezza adeguato
- Le misure "minime" sono predefinite ed hanno il fine di tutelare l'interessato
- Se l'analisi del rischio individua misure idonee inferiori a quelle minime, occorre comunque adottare quest'ultime



Gli elementi dell'analisi del rischio

- **bene** (o asset) ciò che bisogna salvaguardare (persone, oggetti, software, informazioni, ecc.)
- **vulnerabilità** caratteristiche dei sistemi e dei processi che, in particolari condizioni, possono comportare la perdita di riservatezza, integrità o disponibilità delle informazioni
- **minacce** possibili eventi non desiderati che portano alla perdita di riservatezza, integrità o disponibilità delle informazioni

Seminario di studio - 24/3/06 Il Documento programmatico per la sicurezza - analisi dei rischi G. Pontevolpe



Il rischio

Il **rischio** è la probabilità che una minaccia nei confronti di un bene si attui sfruttando una vulnerabilità del sistema



Seminario di studio - 24/3/06

Il Documento programmatico per la sicurezza - analisi dei rischi G. Pontevolpe



I metodi di analisi del rischio

- **Quantitativi**
 - valore dei beni in termini economici
 - analisi in base ad algoritmi matematici
 - scelte secondo criteri oggettivi
- **Qualitativi**
 - valore dei beni in termini relativi (alto, medio, basso)
 - analisi in base a tabelle
 - scelte secondo criteri qualitativi



Esempio di analisi quantitativa

Bene: **autovettura**, valore € 20.000

Vulnerabilità: **trasportabilità**

Minaccia: **furto**



	Senza antifurto	Con bloccapedali	Con antifurto satellitare
Statistica furti annui per 100.000 vetture	1000	200	2
Probabilità furto (rischio)	0,01	0,002	0,00002
Esposizione economica al rischio	€ 200	€ 40	€ 0,4
Costo annuo della protezione	-	€ 12	€ 300



Limiti dei metodi basati su analisi quantitativa

- Difficoltà nel monetizzare il valore dei beni
- Necessità di statistiche
- Difficilmente applicabile ad eventi con probabilità molto bassa

Nel caso della pubblica amministrazione

- Il rapporto costi/benefici non deve essere valutato nell'ambito del singolo ente ma nel contesto generale dell'economia del paese



Esempio di analisi qualitativa

Bene: documenti amministrativi (memorizzati su server NT)

Vulnerabilità: **accesso al sistema NT**

Minaccia: **acquisizione non autorizzata dei diritti di amministratore**

Classe di criticità del bene → **media**

Probabilità di subire danni imputabili ad attacco → **bassa**



Livello di rischio → **medio**

Funzioni di sicurezza per livello di rischio medio

- Consentire accesso come amministratori solo localmente
- Aggiornamento trimestrale dei Service pack
- Traccia degli utenti che hanno modificato il registro



La gestione dei rischi

Per ogni rischio occorre:

- valutare se sia opportuno ridurre il rischio ed in caso affermativo valutare in che misura
- scegliere le modalità con cui ridurre il rischio
- predisporre le misure con cui fronteggiare situazioni in cui il rischio si concretizza in un attacco
- predisporre le procedure per il recupero dei beni in situazioni in cui il rischio si concretizza in un evento negativo



L'analisi del rischio di un sistema complesso

- Il numero dei beni è dell'ordine di decine di migliaia (elaboratori, programmi e dati)
- Il numero dei rischi è in teoria dello stesso ordine di grandezza, con opportune semplificazioni, il numero può diventare dell'ordine di centinaia
- Le possibili soluzioni per ridurre i rischi sono decine (protezioni hardware, soluzioni organizzative, contromisure software che a loro volta possono avvalersi delle funzioni native dei sistemi ecc.)
- Il numero dei possibili eventi dannosi (o attacchi) è di difficile determinazione, quelli attualmente più diffusi sono migliaia



La constatazione dei rischi (gap analysis)

Processi di risk analysis

- Adatti a sistemi nuovi ed esistenti
- I rischi sono valutati esaminando beni, vulnerabilità e minacce
- Sono svolti con il supporto di tool specifici
- Popolano una base informativa utile per la fase di gestione

Processi di gap analysis

- Idonei per sistemi esistenti
- I rischi sono valutati sulla base di
 - analogie
 - buona prassi
 - esperienza
- Utilizzano principalmente check-list
- Producono rapporti sul livello di sicurezza e sulle criticità



La terminologia

	ISO 2382-8	Fornitori
▪ Pianificazione	Valutazione dei rischi (<i>risk assessment</i>)	Risk analysis Risk assessment Vulnerability assessment Security assessment
▪ Verifica	Verifica della sicurezza (<i>security auditing</i>)	Security audit
▪ Miglior. continuo		Gap analysis Security benchmarking Security snapshot



La guida ISO 73 – vocabolario per la gestione del rischio

- Gestione dei rischi (*risk management*)
 - Valutazione dei rischi (*risk assessment*)
 - Analisi dei rischi (*risk analysis*)
 - Stima di impatto (*risk evaluation*)
 - Trattamento dei rischi (*risk treatment*)
 - Accoglimento dei rischi (*risk acceptance*)
 - Comunicazione relativa ai rischi (*risk communication*)

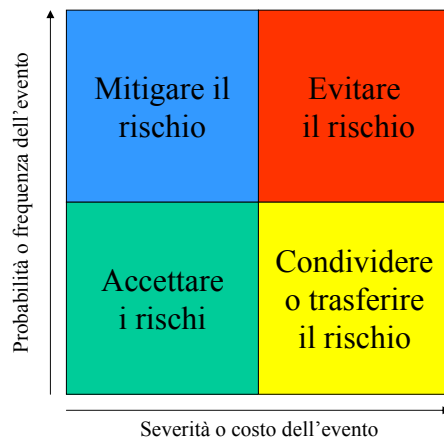


Il trattamento dei rischi

- Per ogni rischio individuato bisogna decidere se:
 - rifiutarlo (*risk avoidance*) evitando il coinvolgimento nella situazione a rischio (ad esempio rinunciando ad un progetto)
 - mitigarlo (*risk optimization*) con opportune contromisure
 - trasferirlo (*risk transfer*) completamente od in parte a terzi (ad esempio con contratti assicurativi),
 - accettarlo (*risk retention*)



La logica di trattamento dei rischi



La pianificazione della sicurezza

- L'attività di analisi del rischio produce generalmente risultati
 - condivisi
 - indicativi (il livello di dettaglio è funzione del metodo seguito)
 - dipendenti dal contesto
- Necessita di revisioni cicliche



- E' opportuno che abbia un costo ed una durata commisurati a costo e durata dell'intero processo



L'offerta di mercato

- Consulenza
 - Società di consulenza
 - Fornitori/integratori di sistemi
 - Produttori
- Metodologie
- Strumenti di supporto alle metodologie



Conoscenza e metodologie

- La conoscenza è la cognizione delle tematiche e dei metodi con cui trattarle
 - È una caratteristica individuale
 - Si fonda sullo studio e sull'esperienza
- La metodologia è la formalizzazione dei metodi in una determinata disciplina
 - E' una proprietà aziendale
 - E' di supporto alle competenze individuali



Il fattore umano

- **Importanza del fattore umano:**
 - esperienza di chi conduce l'attività, determinante per il buon esito dello stesso,
 - atteggiamento collaborativo di chi deve cooperare all'interno della amministrazione (utenti e personale IT).
- Occorre conoscere a fondo il settore, i processi di business e il portafoglio delle applicazioni tipiche delle organizzazioni che vi operano.



... il fattore umano

- Di particolare importanza è l'esperienza specifica riferita al preciso settore economico al quale appartiene l'organizzazione in esame. E' infatti completamente diverso effettuare una valutazione o verifica del sistema informativo in una azienda industriale, in una banca o in un istituto previdenziale



Le metodologie

- Mitigano la soggettività dell'intervento umano
- Facilitano il trasferimento delle competenze
- Consentono di vendere *know how* indipendente dalle competenze individuali
- Facilitano la standardizzazione dei processi



Metodologie e strumenti

- Tutte le metodologie sono oggi supportate da strumenti informatici
- Lo strumento può:
 - Rendere automatiche alcune fasi del processo (ad es. acquisizione dati)
 - Velocizzare le fasi che richiedono la gestione di notevoli quantità di informazioni
 - Aiutare a prendere decisioni (sistema esperto o DB della conoscenza)



Le metodologie di analisi del rischio

- Pianificazione
 - Analisi
 - progettazione
 - realizzazione
- Verifica (assessment)
- Miglior. continuo

Valutazione dei rischi
(risk assessment
risk analysis
risk evaluation
risk treatment)

Verifica della sicurezza
(security auditing)

Gestione del rischio



Le fasi dell'analisi del rischio

- Rilevazione dello scenario (delimitazione del campo d'indagine, censimento dei beni)
- Modellizzazione (accorpamento, normalizzazione, condivisione del modello)
- Classificazione dei beni (categorizzazione, individuazione del valore economico o qualitativo, raggruppamento in classi)



... le fasi dell'analisi del rischio

- Valutazione di vulnerabilità e minacce (identificazione del livello di esposizione a minacce o attacchi)
- Calcolo del rischio (valutazione del livello di rischio intrinseco)
- Trattamento del rischio (scelta del trattamento ed individuazione delle contromisure)
- Reportistica



Modellizzazione

- Consente di rappresentare in forma schematica le informazioni raccolte nella fase di rilevazione dello scenario
- Il modello relaziona gli elementi dell'indagine: dati, beni fisici, software, utenti, logistica, ecc.
- Il modello deve essere condiviso dai responsabili delle entità rappresentate



Classificazione dei beni

- L'efficacia del metodo dipende dalla cura con cui viene svolta questa fase
- La classificazione aiuta i gestori della sicurezza a ponderare le scelte che dovranno essere prese durante il trattamento del rischio
- La semplicità della classificazione è fondamentale per l'utilizzabilità dei risultati
- La classificazione può avvenire per: criticità del dato, valore economico, impatti, ecc.



Valutazione di vulnerabilità e minacce

- Riporta le vulnerabilità delle entità censite o di loro aggregazioni
- Stima, per ogni entità o aggregazione di entità, la probabilità di subire un attacco o che si manifestino specifiche minacce
- La stima delle vulnerabilità può essere fatta in base a conoscenze pregresse, quella delle minacce con il ricorso a questionari

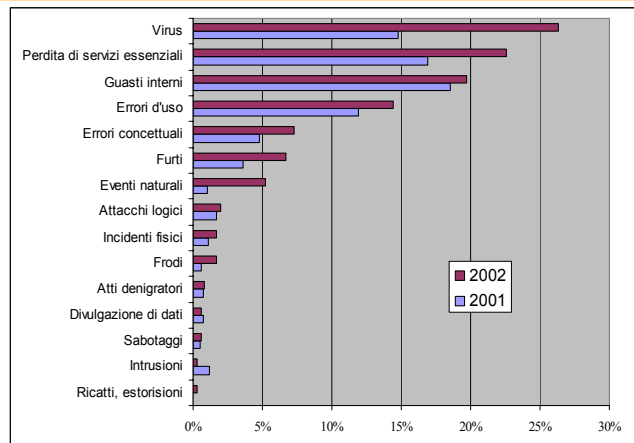


Calcolo del rischio

- Consiste nel valutare il rischio che insiste sui beni in base agli elementi che sono stati individuati nelle precedenti attività
- Può essere fatto con l'ausilio di formule (metodi quantitativi) o di tabelle (metodi qualitativi)



Gli osservatori sulla criminalità informatica



Fonte Clusif – étude et statistiques sur la sinistralité informatique en France 2002



Guida operativa per la redazione del DPS

- Stabilisce i contenuti essenziali del DPS
- Viene individuato un insieme di eventi (minacce) che occorre in ogni caso considerare
- Per ciascun evento il rischio deve essere espresso in termini di "impatto sulla sicurezza", perlomeno con una valutazione qualitativa (probabilità alta\media\bassa)



Minacce: comportamenti degli operatori

- sottrazione di credenziali di autenticazione
- carenza di consapevolezza, disattenzione o incuria
- comportamenti sleali o fraudolenti
- errore materiale



Minacce: eventi relativi agli strumenti

- azione di virus informatici o di programmi suscettibili di recare danno
- spamming o tecniche di sabotaggio
- malfunzionamento, indisponibilità o degrado degli strumenti
- accessi esterni non autorizzati
- intercettazione di informazioni in rete



Minacce: eventi relativi al contesto fisico-ambientale

- ingressi non autorizzati a locali/aree ad accesso ristretto
- sottrazione di strumenti contenenti dati
- eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria
- guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
- errori umani nella gestione della sicurezza fisica



Per maggiori informazioni

www.cnipa.gov.it