Buone pratiche a tutela della Disponibilità

Gregorio D'Agostino

23 Aprile 2021

Disponibilità

Una buona pratica

- Abbiamo già visto una buona pratica:
  "Quando si installa un software è opportuno verificarne l'origine e l'integrità."

Una buona pratica

- Abbiamo già visto una buona pratica:
  "Quando si installa un software è opportuno verificarne l'origine e l'integrità."
- L'integrità si verifica tramite una hash function.

Una buona pratica

- Abbiamo già visto una buona pratica:
  "Quando si installa un software è opportuno verificarne l'origine e l'integrità."
- L'integrità si verifica tramite una hash function.
- L'origine si verifica tramite un certificato digitale, cioè con la firma digitale del digest.

Una buona pratica

- Abbiamo già visto una buona pratica:
  "Quando si installa un software è opportuno verificarne l'origine e l'integrità."
- L'integrità si verifica tramite una hash function.
- L'origine si verifica tramite un certificato digitale, cioè con la firma digitale del digest.
- Utilizzando gli aggiornamenti dei sistemi operativi, il meccanismo di verifica è automatico per il software dello stesso produttore, ma la verifica va fatta manualmente per il software delle "terze parti".

Esempi in aula

- La divisione in colonna senza resto: or esclusivo componente per componente. Attenzione è diversa dalla divisione intera.

Esempi in aula

- La divisione in colonna senza resto: or esclusivo componente per componente. Attenzione è diversa dalla divisione intera.
- Esempio con il polinomio $g(x) = x^5 + x^3 + x^2 + 1$.

Esempi in aula

- La divisione in colonna senza resto: or esclusivo componente per componente. Attenzione è diversa dalla divisione intera.
- Esempio con il polinomio $g(x) = x^5 + x^3 + x^2 + 1$.
- Sequenza equivalente $(1, 0, 1, 1, 0, 1)$.

Esempi in aula

- La divisione in colonna senza resto: or esclusivo componente per componente. Attenzione è diversa dalla divisione intera.
- Esempio con il polinomio $g(x) = x^5 + x^3 + x^2 + 1$.
- Sequenza equivalente $(1, 0, 1, 1, 0, 1)$.
- Esercizio per casa: aggiungere il digest (con la hash function del polinomio g) ad una sequenza casuale di 10 bit.

Esempi in aula

- La divisione in colonna senza resto: or esclusivo componente per componente. Attenzione è diversa dalla divisione intera.
- Esempio con il polinomio $g(x) = x^5 + x^3 + x^2 + 1$.
- Sequenza equivalente $(1, 0, 1, 1, 0, 1)$.
- Esercizio per casa: aggiungere il digest (con la hash function del polinomio g) ad una sequenza casuale di 10 bit.
- Verificare la sequenza.

Esempi in aula

- La divisione in colonna senza resto: or esclusivo componente per componente. Attenzione è diversa dalla divisione intera.
- Esempio con il polinomio $g(x) = x^5 + x^3 + x^2 + 1$.
- Sequenza equivalente $(1, 0, 1, 1, 0, 1)$.
- Esercizio per casa: aggiungere il digest (con la hash function del polinomio g) ad una sequenza casuale di 10 bit.
- Verificare la sequenza.
- Verificare che il resto (diversamente dalla divisione intera) è sempre minore di 2^n.

Esempi in aula

- La divisione in colonna senza resto: or esclusivo componente per componente. Attenzione è diversa dalla divisione intera.
- Esempio con il polinomio $g(x) = x^5 + x^3 + x^2 + 1$.
- Sequenza equivalente $(1, 0, 1, 1, 0, 1)$.
- Esercizio per casa: aggiungere il digest (con la hash function del polinomio g) ad una sequenza casuale di 10 bit.
- Verificare la sequenza.
- Verificare che il resto (diversamente dalla divisione intera) è sempre minore di 2^n.
- Correggiamo esercizio della volta scorsa.

La disponibilità

- La disponibilità dei dati è il primo requisito. In alcuni casi di particolare segretezza può essere meglio la perdita totale di dati che la loro pubblicazione accidentale.

La disponibilità

- La disponibilità dei dati è il primo requisito. In alcuni casi di particolare segretezza può essere meglio la perdita totale di dati che la loro pubblicazione accidentale.
- I fattori che possono intaccare la disponibiltà sono naturali: (alluvioni, incendi, terremoti, blackout) ed antropici: (scioperi, attacchi fisici, attacchi informatici, errori umani, errori di programmazione etc).

La disponibilità

- La disponibilità dei dati è il primo requisito. In alcuni casi di particolare segretezza può essere meglio la perdita totale di dati che la loro pubblicazione accidentale.
- I fattori che possono intaccare la disponibiltà sono naturali: (alluvioni, incendi, terremoti, blackout) ed antropici: (scioperi, attacchi fisici, attacchi informatici, errori umani, errori di programmazione etc).
- Gli strumenti per la protezione sono gli impianti antincendio, le idrovore e gli allarmi umidità, accelerometri, UPS, gruppi di continuità, squadre di sorveglianza etc.

La disponibilità

- La disponibilità dei dati è il primo requisito. In alcuni casi di particolare segretezza può essere meglio la perdita totale di dati che la loro pubblicazione accidentale.
- I fattori che possono intaccare la disponibiltà sono naturali: (alluvioni, incendi, terremoti, blackout) ed antropici: (scioperi, attacchi fisici, attacchi informatici, errori umani, errori di programmazione etc).
- Gli strumenti per la protezione sono gli impianti antincendio, le idrovore e gli allarmi umidità, accelerometri, UPS, gruppi di continuità, squadre di sorveglianza etc.
- Gli strumenti di difesa sono i meccanismi di sicurezza, i mezzi anti intrusione, i meccanismi di controllo automatizzato, sorveglianza (system manager), meccanismi di autenticazione, antivirus, rivelatori di anomalie etc

La disponibilità

- La disponibilità dei dati è il primo requisito. In alcuni casi di particolare segretezza può essere meglio la perdita totale di dati che la loro pubblicazione accidentale.
- I fattori che possono intaccare la disponibiltà sono naturali: (alluvioni, incendi, terremoti, blackout) ed antropici: (scioperi, attacchi fisici, attacchi informatici, errori umani, errori di programmazione etc).
- Gli strumenti per la protezione sono gli impianti antincendio, le idrovore e gli allarmi umidità, accelerometri, UPS, gruppi di continuità, squadre di sorveglianza etc.
- Gli strumenti di difesa sono i meccanismi di sicurezza, i mezzi anti intrusione, i meccanismi di controllo automatizzato, sorveglianza (system manager), meccanismi di autenticazione, antivirus, rivelatori di anomalie etc
- Quando gli strumenti allocati non riescono a prevenire o impedire l'evento indesiderato si attuano le politiche di resilienza.

La disponibilità

- La disponibilità dei dati è il primo requisito. In alcuni casi di particolare segretezza può essere meglio la perdita totale di dati che la loro pubblicazione accidentale.
- I fattori che possono intaccare la disponibiltà sono naturali: (alluvioni, incendi, terremoti, blackout) ed antropici: (scioperi, attacchi fisici, attacchi informatici, errori umani, errori di programmazione etc).
- Gli strumenti per la protezione sono gli impianti antincendio, le idrovore e gli allarmi umidità, accelerometri, UPS, gruppi di continuità, squadre di sorveglianza etc.
- Gli strumenti di difesa sono i meccanismi di sicurezza, i mezzi anti intrusione, i meccanismi di controllo automatizzato, sorveglianza (system manager), meccanismi di autenticazione, antivirus, rivelatori di anomalie etc
- Quando gli strumenti allocati non riescono a prevenire o impedire l'evento indesiderato si attuano le politiche di resilienza.
- L'insieme dei dispositivi definisce la "politica per la sicurezza".

Resilienza

- La caratteristica strutturale e organizzativa del sistema che consente di mitigare gli effetti delle situazioni indesiderate; raggiungere il massimo livello di funzionalità del sistema

Resilienza

- La caratteristica strutturale e organizzativa del sistema che consente di mitigare gli effetti delle situazioni indesiderate; raggiungere il massimo livello di funzionalità del sistema
- Recovery: raggiungere il massimo livello di fruibilità del sistema o di un livello accettabile utilizzando le risorse residue.

Resilienza

- La caratteristica strutturale e organizzativa del sistema che consente di mitigare gli effetti delle situazioni indesiderate; raggiungere il massimo livello di funzionalità del sistema
- Recovery: raggiungere il massimo livello di fruibilità del sistema o di un livello accettabile utilizzando le risorse residue.
- Restoration: ripristino delle condizione di totale funzionalità del sistema.

Resilienza

- La caratteristica strutturale e organizzativa del sistema che consente di mitigare gli effetti delle situazioni indesiderate; raggiungere il massimo livello di funzionalità del sistema
- Recovery: raggiungere il massimo livello di fruibilità del sistema o di un livello accettabile utilizzando le risorse residue.
- Restoration: ripristino delle condizione di totale funzionalità del sistema.
- I piani di contingenza consentono di affrontare efficacemente classi di eventi indesiderati, ma prevedibili.

Resilienza

- La caratteristica strutturale e organizzativa del sistema che consente di mitigare gli effetti delle situazioni indesiderate; raggiungere il massimo livello di funzionalità del sistema
- Recovery: raggiungere il massimo livello di fruibilità del sistema o di un livello accettabile utilizzando le risorse residue.
- Restoration: ripristino delle condizione di totale funzionalità del sistema.
- I piani di contingenza consentono di affrontare efficacemente classi di eventi indesiderati, ma prevedibili.
- Risorse di contingenza sono l'insieme delle risorse ridondanti (aggiuntive) allocate alla resilienza del sistema. La ridondanza è la principale risorsa contro la perdita dei dati.

Resilienza

- La caratteristica strutturale e organizzativa del sistema che consente di mitigare gli effetti delle situazioni indesiderate; raggiungere il massimo livello di funzionalità del sistema
- Recovery: raggiungere il massimo livello di fruibilità del sistema o di un livello accettabile utilizzando le risorse residue.
- Restoration: ripristino delle condizione di totale funzionalità del sistema.
- I piani di contingenza consentono di affrontare efficacemente classi di eventi indesiderati, ma prevedibili.
- Risorse di contingenza sono l'insieme delle risorse ridondanti (aggiuntive) allocate alla resilienza del sistema. La ridondanza è la principale risorsa contro la perdita dei dati.
- Nel 2017 è stato definito uno standard per la Resilienza Organizzativa ISO 22316:2017
  ISO significa International Organization for Standardization, lo standard è consultabile gratuitamente, ma non scaricabile. https://www.iso.org/obp/ui#iso:std:iso:22316:ed-1:v1:en .

Copiatura di riserva "Backup"

- Abbiamo visto che tra le buone pratiche per la gestione ordinaria e la manutenzione dei sistemi vi è l'esecuzione delle copie conformi di riserva. Inoltre esiste una specifica prescrizione di legge Decreto Legislativo 30 giugno 2003, n. 196 Art 34 comma f: "f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilita' dei dati e dei sistemi.

Copiatura di riserva "Backup"

- Abbiamo visto che tra le buone pratiche per la gestione ordinaria e la manutenzione dei sistemi vi è l'esecuzione delle copie conformi di riserva. Inoltre esiste una specifica prescrizione di legge Decreto Legislativo 30 giugno 2003, n. 196 Art 34 comma f: "f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilita' dei dati e dei sistemi.
- Il termine in inglese utilizzato è "Backup" che significa secondo il Webster

Copiatura di riserva "Backup"

- Abbiamo visto che tra le buone pratiche per la gestione ordinaria e la manutenzione dei sistemi vi è l'esecuzione delle copie conformi di riserva. Inoltre esiste una specifica prescrizione di legge Decreto Legislativo 30 giugno 2003, n. 196 Art 34 comma f: "f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilita' dei dati e dei sistemi.
- Il termine in inglese utilizzato è "Backup" che significa secondo il Webster
  - a: one that serves as a substitute or support "a backup plan".

Copiatura di riserva "Backup"

- Abbiamo visto che tra le buone pratiche per la gestione ordinaria e la manutenzione dei sistemi vi è l'esecuzione delle copie conformi di riserva. Inoltre esiste una specifica prescrizione di legge Decreto Legislativo 30 giugno 2003, n. 196 Art 34 comma f: "f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilita' dei dati e dei sistemi.
- Il termine in inglese utilizzato è "Backup" che significa secondo il Webster
  - a: one that serves as a substitute or support "a backup plan".
  - b: musical accompaniment

Copiatura di riserva "Backup"

- Abbiamo visto che tra le buone pratiche per la gestione ordinaria e la manutenzione dei sistemi vi è l'esecuzione delle copie conformi di riserva. Inoltre esiste una specifica prescrizione di legge Decreto Legislativo 30 giugno 2003, n. 196 Art 34 comma f: "f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilita' dei dati e dei sistemi.
- Il termine in inglese utilizzato è "Backup" che significa secondo il Webster
  - a: one that serves as a substitute or support "a backup plan".
  - b: musical accompaniment
  - c: additional personnel who provide assistance.

Copiatura di riserva "Backup"

- Abbiamo visto che tra le buone pratiche per la gestione ordinaria e la manutenzione dei sistemi vi è l'esecuzione delle copie conformi di riserva. Inoltre esiste una specifica prescrizione di legge Decreto Legislativo 30 giugno 2003, n. 196 Art 34 comma f: "f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilita' dei dati e dei sistemi.
- Il termine in inglese utilizzato è "Backup" che significa secondo il Webster
  - a: one that serves as a substitute or support "a backup plan".
  - b: musical accompaniment
  - c: additional personnel who provide assistance.
  - d: a copy of computer data (as a file or the contents of a hard drive); also : the act or an instance of making a backup

Backup ed archiviazione

- Sono due procedure diverse che si eseguono spesso e si somigliano.

Backup ed archiviazione

- Sono due procedure diverse che si eseguono spesso e si somigliano.
- Entrambe consistono nella copiatura fedele su altri supporti di dati.

Backup ed archiviazione

- Sono due procedure diverse che si eseguono spesso e si somigliano.
- Entrambe consistono nella copiatura fedele su altri supporti di dati.
- L'archiviazione è la collocazione ordinata dei dati. Storicamente nasce come esecuzione di una copia conforme depositata in una specifica data. Ma la chiave o le chiavi di archiviazione possono essere molteplici. Un archivio temporale è una sequenza di contenuti informativi ordinata secondo la data.

Backup ed archiviazione

- Sono due procedure diverse che si eseguono spesso e si somigliano.
- Entrambe consistono nella copiatura fedele su altri supporti di dati.
- L'archiviazione è la collocazione ordinata dei dati. Storicamente nasce come esecuzione di una copia conforme depositata in una specifica data. Ma la chiave o le chiavi di archiviazione possono essere molteplici. Un archivio temporale è una sequenza di contenuti informativi ordinata secondo la data.
- Dopo l'archiviazione i dati possono essere cancellati se non sono utilizzati. Dopo il backup, i dati continuano ad essere utilizzati ed eventualmente modificata ed elaborati normalmente.

Archiviazione

- Le Basi di dati (data base) o banche dati (DB) sono delle strutture ordinate di dati che consentono l'archiviazione.

Archiviazione

- Le Basi di dati (data base) o banche dati (DB) sono delle strutture ordinate di dati che consentono l'archiviazione.
- In base all'organizzazione i DB possono essere "relazionali", "gerarchici" (ad albero) etc.

Archiviazione

- Le Basi di dati (data base) o banche dati (DB) sono delle strutture ordinate di dati che consentono l'archiviazione.
- In base all'organizzazione i DB possono essere "relazionali", "gerarchici" (ad albero) etc.
- Esistono programmi specifici "database management system" (DBMS) che consento l'accesso alle basi di dati.

Archiviazione

- Le Basi di dati (data base) o banche dati (DB) sono delle strutture ordinate di dati che consentono l'archiviazione.
- In base all'organizzazione i DB possono essere "relazionali", "gerarchici" (ad albero) etc.
- Esistono programmi specifici "database management system" (DBMS) che consento l'accesso alle basi di dati.
- Le operazioni fondamentali sono: Aggiungere/eliminare entità; Modificare i dati esistenti (attributi); Aggiornare dati; Eseguire richieste (queries) Organizzare e visualizzare dati dinamicamente.

Archiviazione

- Le Basi di dati (data base) o banche dati (DB) sono delle strutture ordinate di dati che consentono l'archiviazione.
- In base all'organizzazione i DB possono essere "relazionali", "gerarchici" (ad albero) etc.
- Esistono programmi specifici "database management system" (DBMS) che consento l'accesso alle basi di dati.
- Le operazioni fondamentali sono: Aggiungere/eliminare entità; Modificare i dati esistenti (attributi); Aggiornare dati; Eseguire richieste (queries) Organizzare e visualizzare dati dinamicamente.
- Le procedure consentite possono essere differenziate in base agli utenti o classi con diverse autorizzazione.

Archiviazione

- Le Basi di dati (data base) o banche dati (DB) sono delle strutture ordinate di dati che consentono l'archiviazione.
- In base all'organizzazione i DB possono essere "relazionali", "gerarchici" (ad albero) etc.
- Esistono programmi specifici "database management system" (DBMS) che consento l'accesso alle basi di dati.
- Le operazioni fondamentali sono: Aggiungere/eliminare entità; Modificare i dati esistenti (attributi); Aggiornare dati; Eseguire richieste (queries) Organizzare e visualizzare dati dinamicamente.
- Le procedure consentite possono essere differenziate in base agli utenti o classi con diverse autorizzazione.
- Il più famoso DBMS è SQL (Structured Query Language) che secondo l'ANSI (American National Standards Institute) costituisce lo "standard de facto", insieme alla versione "aperta" MySQL.

Altri Sistemi di archiviazione

- Nei sistemi apple si usa PostgeSQL, perfettamente analogo a SQL.

Altri Sistemi di archiviazione

- Nei sistemi apple si usa PostgeSQL, perfettamente analogo a SQL.
- Tutti i sistemi di gestione delle banche dati sono disponibili in versione per tutti i sistemi operativi: Linux, Windows e Mac. Oracle, Amazzon, Microsoft, Inspirer, Zoho etc.

Altri Sistemi di archiviazione

- Nei sistemi apple si usa PostgeSQL, perfettamente analogo a SQL.
- Tutti i sistemi di gestione delle banche dati sono disponibili in versione per tutti i sistemi operativi: Linux, Windows e Mac. Oracle, Amazzon, Microsoft, Inspirer, Zoho etc.
- Tutti i sistemi di gestione delle banche dati possiedo un loro linguaggio che consente la definizione delle le strutture dati DDL (Data Definition Language); la loro elaborazione DML (Data Manipulation Language) e la gestione delle autorizzazioni alla fruibilità DCL (Data Control Language)

Altri Sistemi di archiviazione

- Nei sistemi apple si usa PostgeSQL, perfettamente analogo a SQL.
- Tutti i sistemi di gestione delle banche dati sono disponibili in versione per tutti i sistemi operativi: Linux, Windows e Mac. Oracle, Amazzon, Microsoft, Inspirer, Zoho etc.
- Tutti i sistemi di gestione delle banche dati possiedo un loro linguaggio che consente la definizione delle le strutture dati DDL (Data Definition Language); la loro elaborazione DML (Data Manipulation Language) e la gestione delle autorizzazioni alla fruibilità DCL (Data Control Language)
- Esistono infine dei nuovi sistemi detti NoSQL che consentono l'acquisizione di dati a struttura variabili (banche dati non relazionali) in cui gli attributi di una entry sono variabili. Esempio open source MongoDB o il commerciale Oracle.

Scelta del Sistema di archiviazione

- Ognuno dei sistemi di gestione dati pone in atto delle misure di sicurezza. Nell'adottare un sistema occorre considerare diversi fattori tra cui: interoperabilità, sicurezza, portabilità, policy (open source, free o commercial), assistenza, risorse richieste, costo etc.

Scelta del Sistema di archiviazione

- Ognuno dei sistemi di gestione dati pone in atto delle misure di sicurezza. Nell'adottare un sistema occorre considerare diversi fattori tra cui: interoperabilità, sicurezza, portabilità, policy (open source, free o commercial), assistenza, risorse richieste, costo etc.
- Attenzione che esiste il Vendor Lock-in, condizione per cui un software pur essendo open source di fatto per ogni miglioria o variazione richiede l'intervento di un venditore specifico, diventando di fatto commercial.

Scelta del Sistema di archiviazione

- Ognuno dei sistemi di gestione dati pone in atto delle misure di sicurezza. Nell'adottare un sistema occorre considerare diversi fattori tra cui: interoperabilità, sicurezza, portabilità, policy (open source, free o commercial), assistenza, risorse richieste, costo etc.
- Attenzione che esiste il Vendor Lock-in, condizione per cui un software pur essendo open source di fatto per ogni miglioria o variazione richiede l'intervento di un venditore specifico, diventando di fatto commercial.
- Tutti i principali venditori di sistemi informatici in generale e banche date in particolare vendono prodotti (anche open source) compatibili con il DGPR. In pratica definita una policy dell'azienda, consentono la gestione dei dati secondo la legge (anonimizzazione, detenzione e cancellazione) e la costituzione automatica del registro dei trattamenti.

Copie di riserva (Backup)

- La prima differenza fondamentale è la duplicazione dei dati.

Copie di riserva (Backup)

- La prima differenza fondamentale è la duplicazione dei dati.
- Diversamente dalla verifica di integrità, il backup deve consentire il ripristino totale dei dati in caso di loro perdita.

Copie di riserva (Backup)

- La prima differenza fondamentale è la duplicazione dei dati.
- Diversamente dalla verifica di integrità, il backup deve consentire il ripristino totale dei dati in caso di loro perdita.
- I backup si differenziano in base alla loro collocazione (locale o remota); alla frequenza con cui si applica la procedura; al numero di copie; alla segretezza ed alla automazione.

Copie di riserva (Backup)

- La prima differenza fondamentale è la duplicazione dei dati.
- Diversamente dalla verifica di integrità, il backup deve consentire il ripristino totale dei dati in caso di loro perdita.
- I backup si differenziano in base alla loro collocazione (locale o remota); alla frequenza con cui si applica la procedura; al numero di copie; alla segretezza ed alla automazione.
- Il GDPR impone l'uso di Backup ma lascia al responsabile dei dati valutarne la strategia più adatta. In caso di perdita (data leak), il giudice valuterà se le misure adottate fossero sufficienti. In ottemperanza all'oblio la cancellazione deve avvenire anche in tutti i backup. Stesso principio per la rettifica dei dati.

Backup locale

- Consiste nel copiare su un supporto collocato fisicamente nello stesso disco (diverse partizioni), nella stessa piattaforma, su dispositivi esterni, nella stessa sede fisica o nello stesso edificio o centro. In realtà si tratta di copie a livelli di prossimità crescente.

Backup locale

- Consiste nel copiare su un supporto collocato fisicamente nello stesso disco (diverse partizioni), nella stessa piattaforma, su dispositivi esterni, nella stessa sede fisica o nello stesso edificio o centro. In realtà si tratta di copie a livelli di prossimità crescente.
- Difetti:

Backup locale

- Consiste nel copiare su un supporto collocato fisicamente nello stesso disco (diverse partizioni), nella stessa piattaforma, su dispositivi esterni, nella stessa sede fisica o nello stesso edificio o centro. In realtà si tratta di copie a livelli di prossimità crescente.
- Difetti:
  - Vulnerabilità agli si eventi fisici avversi (furti, incendi, allagamenti, black out, inibizioni all'accesso etc) la perdita dei dati originale implica (o può implicare) anche la perdita della copia.

Backup locale

- Consiste nel copiare su un supporto collocato fisicamente nello stesso disco (diverse partizioni), nella stessa piattaforma, su dispositivi esterni, nella stessa sede fisica o nello stesso edificio o centro. In realtà si tratta di copie a livelli di prossimità crescente.
- Difetti:
  - Vulnerabilità agli si eventi fisici avversi (furti, incendi, allagamenti, black out, inibizioni all'accesso etc) la perdita dei dati originale implica (o può implicare) anche la perdita della copia.
  - L'accesso ai dati può avvenire solo nella stessa sede in cui sono conservati.

Backup locale

- Consiste nel copiare su un supporto collocato fisicamente nello stesso disco (diverse partizioni), nella stessa piattaforma, su dispositivi esterni, nella stessa sede fisica o nello stesso edificio o centro. In realtà si tratta di copie a livelli di prossimità crescente.
- Difetti:
  - Vulnerabilità agli si eventi fisici avversi (furti, incendi, allagamenti, black out, inibizioni all'accesso etc) la perdita dei dati originale implica (o può implicare) anche la perdita della copia.
  - L'accesso ai dati può avvenire solo nella stessa sede in cui sono conservati.
- Pregi:

Backup locale

- Consiste nel copiare su un supporto collocato fisicamente nello stesso disco (diverse partizioni), nella stessa piattaforma, su dispositivi esterni, nella stessa sede fisica o nello stesso edificio o centro. In realtà si tratta di copie a livelli di prossimità crescente.
- Difetti:
  - Vulnerabilità agli si eventi fisici avversi (furti, incendi, allagamenti, black out, inibizioni all'accesso etc) la perdita dei dati originale implica (o può implicare) anche la perdita della copia.
  - L'accesso ai dati può avvenire solo nella stessa sede in cui sono conservati.
- Pregi:
  - Si ha il controllo diretto della affidabilità dei dispositivi di immagazzinamento e della loro custodia.

Backup locale

- Consiste nel copiare su un supporto collocato fisicamente nello stesso disco (diverse partizioni), nella stessa piattaforma, su dispositivi esterni, nella stessa sede fisica o nello stesso edificio o centro. In realtà si tratta di copie a livelli di prossimità crescente.
- Difetti:
  - Vulnerabilità agli si eventi fisici avversi (furti, incendi, allagamenti, black out, inibizioni all'accesso etc) la perdita dei dati originale implica (o può implicare) anche la perdita della copia.
  - L'accesso ai dati può avvenire solo nella stessa sede in cui sono conservati.
- Pregi:
  - Si ha il controllo diretto della affidabilità dei dispositivi di immagazzinamento e della loro custodia.
  - Il recupero dei dati non dipende dalla disponibilità della rete. Il tempo di recupero è più breve. La sicurezza è quella locale.

Backup remoto

- Consiste nel copiare su un supporto collocato su piattaforme diverse raggiungibili tramite la rete. Anche in questo caso vi sono livelli di prossimità decrescente. La rete può essere locale, nello stesso autonomous system, o completamente fuori dalla giurisdizione.

Backup remoto

- Consiste nel copiare su un supporto collocato su piattaforme diverse raggiungibili tramite la rete. Anche in questo caso vi sono livelli di prossimità decrescente. La rete può essere locale, nello stesso autonomous system, o completamente fuori dalla giurisdizione.
- Difetti:

Backup remoto

- Consiste nel copiare su un supporto collocato su piattaforme diverse raggiungibili tramite la rete. Anche in questo caso vi sono livelli di prossimità decrescente. La rete può essere locale, nello stesso autonomous system, o completamente fuori dalla giurisdizione.
- Difetti:
  - Dipendenza dal funzionamento della rete e dei suoi eventuali gestori (Service providers, tier di altro livello etc). Questo può compromettere anche l'integrità e la sicurezza.

Backup remoto

- Consiste nel copiare su un supporto collocato su piattaforme diverse raggiungibili tramite la rete. Anche in questo caso vi sono livelli di prossimità decrescente. La rete può essere locale, nello stesso autonomous system, o completamente fuori dalla giurisdizione.
- Difetti:
  - Dipendenza dal funzionamento della rete e dei suoi eventuali gestori (Service providers, tier di altro livello etc). Questo può compromettere anche l'integrità e la sicurezza.
  - La copiatura ed Il ripristino dei dati necessitano le procedure di accesso alla rete e tempi di attuazione (latenza e bandwidth).

Backup remoto

- Consiste nel copiare su un supporto collocato su piattaforme diverse raggiungibili tramite la rete. Anche in questo caso vi sono livelli di prossimità decrescente. La rete può essere locale, nello stesso autonomous system, o completamente fuori dalla giurisdizione.
- Difetti:
  - Dipendenza dal funzionamento della rete e dei suoi eventuali gestori (Service providers, tier di altro livello etc). Questo può compromettere anche l'integrità e la sicurezza.
  - La copiatura ed Il ripristino dei dati necessitano le procedure di accesso alla rete e tempi di attuazione (latenza e bandwidth).
- Pregi:

Backup remoto

- Consiste nel copiare su un supporto collocato su piattaforme diverse raggiungibili tramite la rete. Anche in questo caso vi sono livelli di prossimità decrescente. La rete può essere locale, nello stesso autonomous system, o completamente fuori dalla giurisdizione.
- Difetti:
  - Dipendenza dal funzionamento della rete e dei suoi eventuali gestori (Service providers, tier di altro livello etc). Questo può compromettere anche l'integrità e la sicurezza.
  - La copiatura ed Il ripristino dei dati necessitano le procedure di accesso alla rete e tempi di attuazione (latenza e bandwidth).
- Pregi:
  - Si diviene resilienti rispetto agli eventi naturali e attacchi deliberati locali (alluvioni. incendi, distruzioni, NON al furto).

Backup remoto

- Consiste nel copiare su un supporto collocato su piattaforme diverse raggiungibili tramite la rete. Anche in questo caso vi sono livelli di prossimità decrescente. La rete può essere locale, nello stesso autonomous system, o completamente fuori dalla giurisdizione.
- Difetti:
  - Dipendenza dal funzionamento della rete e dei suoi eventuali gestori (Service providers, tier di altro livello etc). Questo può compromettere anche l'integrità e la sicurezza.
  - La copiatura ed Il ripristino dei dati necessitano le procedure di accesso alla rete e tempi di attuazione (latenza e bandwidth).
- Pregi:
  - Si diviene resilienti rispetto agli eventi naturali e attacchi deliberati locali (alluvioni. incendi, distruzioni, NON al furto).
  - Si può usare il backup dei dati per renderli disponibili in qualunque punto.

Buona pratica I

- Effettuare sia backup locali che backup remoti se è possibile ed sostenibile economicamente.

Buona pratica I

- Effettuare sia backup locali che backup remoti se è possibile ed sostenibile economicamente.
- Collocare le copie su dispositivi mobili (come dischi usb esterni) in località diverse. Esempio casa ed ufficio.

Buona pratica I

- Effettuare sia backup locali che backup remoti se è possibile ed sostenibile economicamente.
- Collocare le copie su dispositivi mobili (come dischi usb esterni) in località diverse. Esempio casa ed ufficio.
- Mantenere gli stessi livelli di sicurezza per tutte le copie di backup.

Buona pratica I

- Effettuare sia backup locali che backup remoti se è possibile ed sostenibile economicamente.
- Collocare le copie su dispositivi mobili (come dischi usb esterni) in località diverse. Esempio casa ed ufficio.
- Mantenere gli stessi livelli di sicurezza per tutte le copie di backup.
- Nella pianificazione della sicurezza informatica si realizza un compromesso con il miglior rapporto costi/benefici.

Frequenza di Backup

- Si eseguono dei backup straordinari mirati quando si realizzano condizioni ottimali di funzionamento di un sistema.

Frequenza di Backup

- Si eseguono dei backup straordinari mirati quando si realizzano condizioni ottimali di funzionamento di un sistema.
- Gli altri backup rientrano nella manutenzione ordinaria e sono a periodicità variabile: giornaliera, settimanale, istantanea etc. Questi backup sono spesso su supporti permanenti.

Frequenza di Backup

- Si eseguono dei backup straordinari mirati quando si realizzano condizioni ottimali di funzionamento di un sistema.
- Gli altri backup rientrano nella manutenzione ordinaria e sono a periodicità variabile: giornaliera, settimanale, istantanea etc. Questi backup sono spesso su supporti permanenti.
- I backup più frequenti in genere si fanno in forma incrementale e si tende ad averli localmente. I backup incrementali si possono realizzare osservando l'identità (bit a bit) tra i filie sorgente ed in memoria oppure tramite delle hash function ed i parametri informativo del sistema operativo: data di scrittura, creazione, lunghezza etc.

Frequenza di Backup

- Si eseguono dei backup straordinari mirati quando si realizzano condizioni ottimali di funzionamento di un sistema.
- Gli altri backup rientrano nella manutenzione ordinaria e sono a periodicità variabile: giornaliera, settimanale, istantanea etc. Questi backup sono spesso su supporti permanenti.
- I backup più frequenti in genere si fanno in forma incrementale e si tende ad averli localmente. I backup incrementali si possono realizzare osservando l'identità (bit a bit) tra i filie sorgente ed in memoria oppure tramite delle hash function ed i parametri informativo del sistema operativo: data di scrittura, creazione, lunghezza etc.
- I backup integrali si realizzano con una periodicità mensile o di lunga durata.

Frequenza di Backup

- Si eseguono dei backup straordinari mirati quando si realizzano condizioni ottimali di funzionamento di un sistema.
- Gli altri backup rientrano nella manutenzione ordinaria e sono a periodicità variabile: giornaliera, settimanale, istantanea etc. Questi backup sono spesso su supporti permanenti.
- I backup più frequenti in genere si fanno in forma incrementale e si tende ad averli localmente. I backup incrementali si possono realizzare osservando l'identità (bit a bit) tra i filie sorgente ed in memoria oppure tramite delle hash function ed i parametri informativo del sistema operativo: data di scrittura, creazione, lunghezza etc.
- I backup integrali si realizzano con una periodicità mensile o di lunga durata.
- Nella pianificazione della sicurezza informatica si realizza un compromesso con il miglior rapporto costi/benefici. Più è elevato in numero di copie (frequenza), più aumentano i costi e le vulnerabilità del sistema rispetto alla confidenzialità, ma più aumenta la resilienza della disponibilità.

Automazione Backup

- Nella maggioranza dei casi il backup (ordinario) avviene in modalità automatica: esiste un processo in perenne esecuzione sul sistema operativo che, con le cadenze previste esegue le copie sui supporti predefiniti.

Automazione Backup

- Nella maggioranza dei casi il backup (ordinario) avviene in modalità automatica: esiste un processo in perenne esecuzione sul sistema operativo che, con le cadenze previste esegue le copie sui supporti predefiniti.
- Il backup è un tipico processo di ridondanza quindi implica allocazione di risorse e tempo di elaborazione sottratte alla disponibilità dell'utente.

Automazione Backup

- Nella maggioranza dei casi il backup (ordinario) avviene in modalità automatica: esiste un processo in perenne esecuzione sul sistema operativo che, con le cadenze previste esegue le copie sui supporti predefiniti.
- Il backup è un tipico processo di ridondanza quindi implica allocazione di risorse e tempo di elaborazione sottratte alla disponibilità dell'utente.
- Anche in questo caso occorre definire delle funzioni di "merito" e di "costo" per ottimizzare la scelta.

Backup e Sicurezza

- I dispositivi di sicurezza adottati per il backup devo essere almeno uguali a quelli impiegati per la normale gestione dei dati.

Backup e Sicurezza

- I dispositivi di sicurezza adottati per il backup devo essere almeno uguali a quelli impiegati per la normale gestione dei dati.
- Nel caso di backup remoto è possibile criptare i dati prima della loro copiatura. Lo standard della criptazione deve essere coerente.

Backup e Sicurezza

- I dispositivi di sicurezza adottati per il backup devo essere almeno uguali a quelli impiegati per la normale gestione dei dati.
- Nel caso di backup remoto è possibile criptare i dati prima della loro copiatura. Lo standard della criptazione deve essere coerente.
- Si può apporre una firma digitale ai file di backup per garantirne la provenienza o l'integrità.

Buone pratiche II

- Differenziare i dati in base alla loro rilevanza, non copiare tutto con le stessa strategia.

Buone pratiche II

- Differenziare i dati in base alla loro rilevanza, non copiare tutto con le stessa strategia.
- Eseguire periodicamente backup dei dati più importanti su supporti non riscrivibilie collocarli in altra sede.

Buone pratiche II

- Differenziare i dati in base alla loro rilevanza, non copiare tutto con le stessa strategia.
- Eseguire periodicamente backup dei dati più importanti su supporti non riscrivibilie collocarli in altra sede.
- Crittare i file quando necessario.

Buone pratiche II

- Differenziare i dati in base alla loro rilevanza, non copiare tutto con le stessa strategia.
- Eseguire periodicamente backup dei dati più importanti su supporti non riscrivibilie collocarli in altra sede.
- Crittare i file quando necessario.
- Anonimizzazione: eliminazione o alterazione dei dati sensibili in modo che non siano collegabili ai pazienti (medici, personale sanitario).

Buone pratiche II

- Differenziare i dati in base alla loro rilevanza, non copiare tutto con le stessa strategia.
- Eseguire periodicamente backup dei dati più importanti su supporti non riscrivibilie collocarli in altra sede.
- Crittare i file quando necessario.
- Anonimizzazione: eliminazione o alterazione dei dati sensibili in modo che non siano collegabili ai pazienti (medici, personale sanitario).
- Automatizzare le procedure di backup ordinario e utilizzare protocolli di rete sicuri.

Buone pratiche II

- Differenziare i dati in base alla loro rilevanza, non copiare tutto con le stessa strategia.
- Eseguire periodicamente backup dei dati più importanti su supporti non riscrivibilie collocarli in altra sede.
- Crittare i file quando necessario.
- Anonimizzazione: eliminazione o alterazione dei dati sensibili in modo che non siano collegabili ai pazienti (medici, personale sanitario).
- Automatizzare le procedure di backup ordinario e utilizzare protocolli di rete sicuri.
- Eseguire il backup anche dei Registri di trattamento dei dati sensibili.

RAID Redundant Array of Independent Disks

- Consiste nel disporre di diversi dischi per la memoria di massa sui quali si scrive simultaneamente con procedure hardware (o software al livello di scheda madre motherboard)

RAID Redundant Array of Independent Disks

- Consiste nel disporre di diversi dischi per la memoria di massa sui quali si scrive simultaneamente con procedure hardware (o software al livello di scheda madre motherboard)
- La velocità di scrittura di solito è lievemente minore della velocità di scrittura su singolo disco perché si eseguono verifiche di integrità sui dati.

RAID Redundant Array of Independent Disks

- Consiste nel disporre di diversi dischi per la memoria di massa sui quali si scrive simultaneamente con procedure hardware (o software al livello di scheda madre motherboard)
- La velocità di scrittura di solito è lievemente minore della velocità di scrittura su singolo disco perché si eseguono verifiche di integrità sui dati.
- Le principali configurazioni sono: RAID 0 (non è ridondanza); RAID 1 (due dischi identici); RAID 5 (DATI Su tre dischi), RAID 6 (DATI Su 4 o più dischi di cui basta che ne sopravvivano 2).

RAID Redundant Array of Independent Disks

- Consiste nel disporre di diversi dischi per la memoria di massa sui quali si scrive simultaneamente con procedure hardware (o software al livello di scheda madre motherboard)
- La velocità di scrittura di solito è lievemente minore della velocità di scrittura su singolo disco perché si eseguono verifiche di integrità sui dati.
- Le principali configurazioni sono: RAID 0 (non è ridondanza); RAID 1 (due dischi identici); RAID 5 (DATI Su tre dischi), RAID 6 (DATI Su 4 o più dischi di cui basta che ne sopravvivano 2).
- Gli altri RAID: RAID 0 non sono vere ridondanze totali, ma suddivisioni dei dati su diversi supporti. Si utilizzano raramente.

Software RAID

- Consiste nel disporre di diversi dischi per la memoria di massa sui quali si scrive sequenzialmente ed è il sistema operativo ad occuparsene.

Software RAID

- Consiste nel disporre di diversi dischi per la memoria di massa sui quali si scrive sequenzialmente ed è il sistema operativo ad occuparsene.
- La velocità di scrittura d solito è notevolmente minore della velocità di scrittura su singolo disco e si ha anche consumo di cpu.

Software RAID

- Consiste nel disporre di diversi dischi per la memoria di massa sui quali si scrive sequenzialmente ed è il sistema operativo ad occuparsene.
- La velocità di scrittura d solito è notevolmente minore della velocità di scrittura su singolo disco e si ha anche consumo di cpu.
- Le principali configurazioni sono le stesse: RAID 0 (non è ridondanza); RAID 1 (due dischi identici); RAID 5 (DATI Su tre dischi)

File System Distribuiti

- Negli anni si sono sviluppati sistemi sofisticati per gestire automaticamente file-systems (porzioni di memoria strutturate) collocate su diverse piattaforme detti file system distribuiti DFS (distributed file systems).

File System Distribuiti

- Negli anni si sono sviluppati sistemi sofisticati per gestire automaticamente file-systems (porzioni di memoria strutturate) collocate su diverse piattaforme detti file system distribuiti DFS (distributed file systems).
- Uno dei pià antichi fu nfs (Network File System) che in origine (1985) era un'area di memoria di un unico computer condivisa usando la rete. Oggi la gestione del metodo è più elaborata ed è possibile gestire aree di memoria distribuite tra molti sistemi in modalità RAID.

File System Distribuiti

- Negli anni si sono sviluppati sistemi sofisticati per gestire automaticamente file-systems (porzioni di memoria strutturate) collocate su diverse piattaforme detti file system distribuiti DFS (distributed file systems).
- Uno dei pià antichi fu nfs (Network File System) che in origine (1985) era un'area di memoria di un unico computer condivisa usando la rete. Oggi la gestione del metodo è più elaborata ed è possibile gestire aree di memoria distribuite tra molti sistemi in modalità RAID.
- In seguito nacquero altri sistemi come afs (Andrew File System) a memoria distribuita. Poi evoluto in Coda (clustered file system). Oggi vi sono vari sistemi google file system, IPFS, CEPH che consentono diversi equilibri tra la replica dei dati e la loro distribuzione.

File System Distribuiti

- Negli anni si sono sviluppati sistemi sofisticati per gestire automaticamente file-systems (porzioni di memoria strutturate) collocate su diverse piattaforme detti file system distribuiti DFS (distributed file systems).
- Uno dei pià antichi fu nfs (Network File System) che in origine (1985) era un'area di memoria di un unico computer condivisa usando la rete. Oggi la gestione del metodo è più elaborata ed è possibile gestire aree di memoria distribuite tra molti sistemi in modalità RAID.
- In seguito nacquero altri sistemi come afs (Andrew File System) a memoria distribuita. Poi evoluto in Coda (clustered file system). Oggi vi sono vari sistemi google file system, IPFS, CEPH che consentono diversi equilibri tra la replica dei dati e la loro distribuzione.
- La velocità di accesso dipende dal numero di repliche e dalla rete che si interpone tra le piattaforme su cui è distribuita l'informazione.

Buone pratiche

- Il backup è lo strumento principale per la tutela della disponibilità dei dati. Calcolando le hash function dei backup e cifrandole con la nostra chiave privata, possiamo avere una verifica della loro integrità.

Buone pratiche

- Il backup è lo strumento principale per la tutela della disponibilità dei dati. Calcolando le hash function dei backup e cifrandole con la nostra chiave privata, possiamo avere una verifica della loro integrità.
- Per evitare la perdita anche in tempo reale è utile impiegare configurazioni di memoria di massa ridondante RAID, hardware e software.

Buone pratiche

- Il backup è lo strumento principale per la tutela della disponibilità dei dati. Calcolando le hash function dei backup e cifrandole con la nostra chiave privata, possiamo avere una verifica della loro integrità.
- Per evitare la perdita anche in tempo reale è utile impiegare configurazioni di memoria di massa ridondante RAID, hardware e software.
- Nel caso di dati sensibili o confidenziali è consigliabile utilizzare banche dati dotate di meccanismi di sicurezza a tutela delle autorizzazioni.

Buone pratiche

- Il backup è lo strumento principale per la tutela della disponibilità dei dati. Calcolando le hash function dei backup e cifrandole con la nostra chiave privata, possiamo avere una verifica della loro integrità.
- Per evitare la perdita anche in tempo reale è utile impiegare configurazioni di memoria di massa ridondante RAID, hardware e software.
- Nel caso di dati sensibili o confidenziali è consigliabile utilizzare banche dati dotate di meccanismi di sicurezza a tutela delle autorizzazioni.
- Nel caso di gestione di dati sensibili dal 25 maggio 2018 è obbligatorio dotarsi di meccanismi per il registro dei trattamenti. Anche questi sono disponibili nei sistemi di gestione delle banche dati.

Buone pratiche

- Il backup è lo strumento principale per la tutela della disponibilità dei dati. Calcolando le hash function dei backup e cifrandole con la nostra chiave privata, possiamo avere una verifica della loro integrità.
- Per evitare la perdita anche in tempo reale è utile impiegare configurazioni di memoria di massa ridondante RAID, hardware e software.
- Nel caso di dati sensibili o confidenziali è consigliabile utilizzare banche dati dotate di meccanismi di sicurezza a tutela delle autorizzazioni.
- Nel caso di gestione di dati sensibili dal 25 maggio 2018 è obbligatorio dotarsi di meccanismi per il registro dei trattamenti. Anche questi sono disponibili nei sistemi di gestione delle banche dati.
- Verificare il software prima dell'installazione. Nel caso dei sistemi operativi la verifica è automatica, ma il problema si sposta nella certificazione della sorgente.

Messaggio

- Abbiamo iniziato la tematica della disponibilità dei dati e visto alcuni strumenti: RAID, Database, Backup.

Messaggio

- Abbiamo iniziato la tematica della disponibilità dei dati e visto alcuni strumenti: RAID, Database, Backup.
- Il Backup è lo strumento principe che necessita una diversificazione per frequenza e localizzazione.

Messaggio

- Abbiamo iniziato la tematica della disponibilità dei dati e visto alcuni strumenti: RAID, Database, Backup.
- Il Backup è lo strumento principe che necessita una diversificazione per frequenza e localizzazione.
- La disponibilità e la Riservatezza non sono ottimizzabili simultaneamente, occorre un compromesso.

Messaggio

- Abbiamo iniziato la tematica della disponibilità dei dati e visto alcuni strumenti: RAID, Database, Backup.
- Il Backup è lo strumento principe che necessita una diversificazione per frequenza e localizzazione.
- La disponibilità e la Riservatezza non sono ottimizzabili simultaneamente, occorre un compromesso.
- La verifica dell'integrità non confligge con la disponibilità e la riservatezza, ma richiede solo maggiori allocazioni di risorse e quindi costi.