

LA PROTEZIONE DEI DATI

Scheda tecnica

Viene di seguito riportato un approfondimento tecnico finalizzato a definire :

- le strategie
- i prodotti
- il mercato

relativo all'ambito DATI (siano essi tecnici, amministrativi, grafici, etc.)

<i>Focus</i>	♦ Protezione del dato
<i>Contesti</i>	♦ Razionalizzazione della gestione dati amministrativo – contabili (risparmi ottenibili, scalabilità delle soluzioni) ♦ Misure di protezione dati (guasti, errori umani, furti di server o desktop) ♦ Misure anti-intrusione ed antivirus
<i>Obiettivi</i>	♦ analisi sui sistemi informativi aziendali (stato dell'arte) ♦ consulenza sui sistemi di protezione dati (anche per permettere alle aziende di ottenerne la relativa certificazione da parte di appositi istituti o enti)
<i>Servizi</i>	♦ Analisi Sistemi Informativi aziendali e consulenza per ottimizzazione sistemi di protezione dei dati ♦ Progettazione di sistemi ♦ Verifica Hardware e Software ♦ Servizi di Remote Control ♦ Servizi di Supporto telefonico ♦ Consulenza sulla razionalizzazione sistemi di gestione amministrativo - contabile

Specifiche tecniche

Tecnicamente la protezione dei dati viene effettuata interagendo con il Sistema Informativo in diverse modalità, in funzione dei livelli di problematiche ed esigenze presenti.

I livelli di protezione (quindi di Business Continuity) riguardano i seguenti componenti e sistemi :

- | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> ▪ Dischi protetti (interni ed esterni) ▪ Back-up (server, software, supporti, periodicità di esecuzione, DAT, VXA, Librerie) ▪ Cluster (sistemi ridondanti su unico sito o su più siti) ▪ Sistemi Antivirus (Software, periodicità di aggiornamento) ▪ Router | <ul style="list-style-type: none"> ▪ Dischi Raid (interni od esterni) ▪ Archiviazione delle copie e siti di archiviazione (armadi ignifughi e blindati), sistemi anti-intrusione, etc. ▪ Supporti (Nastri, dischi, etc.) ▪ Firewall (Hardware e Software) ▪ Sistemi di Disaster Recovery e Disaster Tollerance |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

I livelli di protezione adottabili sono direttamente dipendenti al grado di Business Continuity che si vuole adottare ovvero il tempo considerato accettabile tra il verificarsi del disastro e la ripresa totale dell'attività precedente ad esso.

Definito **T** questo periodo di tempo, le scelte possibili sono :

Livello di Business Continuity	Soluzione da adottare
<p>Scarso T => giorni</p>	<p>Protezione scarsa. Il ripristino della completa operatività può richiedere anche giorni.</p> <ul style="list-style-type: none"> • Sistemi singoli • Dischi interni possibilmente RAID per Sist. Oper. e Dati • Backup periodico , con copie del backup conservate in altro sito • Antivirus con aggiornamento periodico • Firewall in ingresso al sistema
<p>Discreto T => ore</p>	<p>Protezione media. Il ripristino della completa operatività dipende dalle risorse disponibili. Nel migliore dei casi può richiedere alcune ore.</p> <ul style="list-style-type: none"> • Sistemi singoli con similari di Standby • Dischi esterni RAID per Sist. Oper. e Dati • Server di backup esterno e possibilmente in altro sito • Copie del backup conservate in altro sito • Antivirus con aggiornamento giornaliero • Firewall in ingresso al sistema
<p>Buono T => secondi</p>	<p>Protezione buona. Il ripristino della completa operatività avviene in alcuni secondi. Richiede risorse aggiuntive.</p> <ul style="list-style-type: none"> • Sistemi ridondanti in Cluster su unico sito • Dischi interni RAID per Sistema Operativo • Dischi esterni RAID per Dati • Server di backup esterno e possibilmente in altro sito • Copie del backup conservate in altro sito • Antivirus con aggiornamento orario • Firewall in ingresso al sistema
<p>Ottimo T = 0</p>	<p>Protezione eccellente. La completa operatività non viene mai interrotta anche nel caso di completa distruzione di uno dei siti.. Richiede notevoli risorse aggiuntive.</p> <ul style="list-style-type: none"> • Sistemi ridondanti in Cluster su siti diversi • Dischi interni RAID per Sistema Operativo • Dischi esterni RAID per Dati • Replica remota dei Dati • Server di backup esterno e possibilmente in altro sito • Copie del backup conservate in altro sito • Antivirus con aggiornamento orario • Firewall in ingresso al sistema