

VERITAS Conformità alle normative

**DECRETO LEGISLATIVO N.196/2003**  
**CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

## INDICE

. PREMESSA .....	3
1. IL DECRETO LEGGE .....	4
1.1 TRATTAMENTO DEI DATI .....	4
1.2 TIPOLOGIA DEI DATI.....	4
1.3 INCARICATI DEL TRATTAMENTO.....	4
1.4 CHI E' OBBLIGATO.....	4
1.5 LE SCADENZE .....	4
1.6 COSA RISCHIA CHI NON SI ADEGUA.....	4
2. CHE COSA SI DEVE FARE.....	5
2.1 IDENTIFICARE LE CARATTERISTICHE DEL TRATTAMENTO.....	5
2.2 DEFINIRE E ADOTTARE ADEGUATE MISURE DI SICUREZZA .....	5
2.3 REDIGERE IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS) .....	6
3. LE SOLUZIONI DI VERITAS .....	7
3.1 VERITAS BACKUP EXEC™.....	7
VERITAS INTELLIGENT DISASTER RECOVERY™ OPTION (IDR).....	7
3.2 VERITAS NETBACKUP™ (NBU) .....	8
VERITAS NETBACKUP VAULT™ OPTION.....	8
VERITAS NETBACKUP ENCRYPTION™ OPTION.....	8
VERITAS NETBACKUP STORAGE MIGRATOR FOR UNIX.....	8
3.3 VERITAS BARE METAL RESTORE™ (BMR).....	8
3.4 KVS ENTERPRISE VAULT .....	8
3.5 VERITAS DESKTOP AND LAPTOP OPTION™ (DLO).....	9
3.6 VERITAS STORAGE EXEC .....	9
3.7 VERITAS OPFORCE™ .....	9
3.8 VERITAS SECURITY SERVICES™ .....	9
3.9 VERITAS HIGH AVAILABILITY SOLUTION.....	9
VERITAS CLUSTER SERVER (VCS).....	9
VERITAS STORAGE FOUNDATION.....	10
4. CONCLUSIONI .....	11

## PREMESSA

L'evoluzione tecnologica ha determinato il proliferare di informazioni in formato digitale di ogni tipo, che vengono scambiate con tempi e modi nuovi e non originariamente prevedibili all'interno delle normative. Questo processo, inoltre, continua a evolvere con grande rapidità e su scale temporali notevolmente inferiori rispetto a quelle legislative. Per queste ragioni il rapporto tra l'Information Technology e le norme amministrative è da sempre complesso e alla ricerca di un punto di incontro tra esigenze tecnologiche e obblighi che diventano sempre più stringenti.

Nel frattempo il numero di normative e di azioni che esse impongono crescono di giorno in giorno, tanto che si stima che solo negli Stati Uniti e nella regione EMEA siano in vigore, a tutt'oggi, oltre 15.000 normative federali, statali e locali. All'interno di queste è possibile individuare tre mandati principali: la conservazione e reperibilità dei documenti, il controllo dei procedimenti e la produzione di rapporti in tempo reale.

In ambienti IT complessi, caratterizzati da un flusso estremamente elevato di informazioni, è impossibile pensare di poter ottemperare a tutti gli obblighi normativi semplicemente con la buona volontà e l'iniziativa personale. Di fronte a una continua crescita di regole e leggi, virtualmente ogni tipo di business deve riconoscere l'importanza di poter rintracciare e accedere, in maniera meticolosa e in ogni momento, a tutti i propri dati, dalle più recenti e-mail, fino ai dati storici posti nelle "vault".

Per fare ciò si configura la necessità di stabilire una nuova struttura di controllo interno che, oltre ad assicurare la possibilità di archiviare le informazioni vitali aziendali, sia anche in grado di recuperarle in modo efficiente per fini di audit.

Per soddisfare questi nuovi requisiti, VERITAS propone una serie di prodotti software che concorrono a comporre una soluzione integrata e scalabile articolata attorno ai temi del backup, del disaster recovery e della gestione differenziata dei dati durante il loro ciclo di vita.

## 1. IL DECRETO LEGGE

*Chiunque ha diritto alla protezione dei dati personali che lo riguardano.*

*Il decreto legge 196/2003, denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.*

Una delle regole principali di privacy è rappresentata dalla sicurezza dei dati e dei sistemi.

Si tutela la privacy delle persone adeguando i propri archivi e i propri elaboratori a misure di sicurezza che impediscano la perdita accidentale del dato e l'accesso abusivo agli stessi.

Il testo unico della privacy riprende le disposizioni sulla sicurezza presenti nella legge 675/1996 (articolo 15) e ne fornisce una disciplina più analitica.

Le normative stabilite dal codice hanno lo scopo di garantire che il trattamento dei dati personali avvenga conformemente alla disciplina generale vigente nell'Unione Europea, nel rispetto dell'individuo e delle persone giuridiche.

I dati personali oggetto del trattamento devono sempre essere custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee 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.

### 1.1 TRATTAMENTO DEI DATI

Con trattamento si intende l'insieme delle operazioni in qualsiasi modo finalizzate alla raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, blocco, modifica, utilizzo, interconnessione, comunicazione, diffusione, cancellazione, distruzione, selezione, estrazione e raffronto dei dati personali.

### 1.2 TIPOLOGIA DEI DATI

Il Testo Unico si applica alle informazioni personali trattate a qualsiasi titolo e con qualsiasi mezzo da chiunque sul territorio nazionale, siano esse archiviate in Italia o all'estero. La natura stessa dei dati origina a sua volta una ulteriore classificazione e conseguenti specifici obblighi di legge:

- **dati sensibili:** consistono in informazioni etniche, religiose, filosofiche, politiche, sindacali, mediche e sessuali. Sono espressamente elencati all'art.37 del Codice e comportano particolari obblighi per il titolare del trattamento, il quale è tenuto a segnalare l'esistenza del database all'autorità di garanzia secondo una precisa procedura informatizzata.
- **dati personali:** consistono in informazioni che consentono di individuare un soggetto. Comprendono il nominativo, l'indirizzo, codici fiscali e partita IVA, numeri telefonici, riferimenti a documenti di identità, indirizzi di posta elettronica ecc.
- **dati giudiziari:** rappresentati da informazioni correlate ai provvedimenti di carattere giurisdizionale attribuibili ad un soggetto.

### 1.3 INCARICATI DEL TRATTAMENTO

Al titolare del trattamento competono le decisioni inerenti modalità e scopi del trattamento stesso. Il responsabile è la persona fisica o giuridica preposta dal titolare al trattamento dei dati personali. Incaricato è l'individuo che materialmente compie operazioni di trattamento dei dati sulla base di quanto stabilito da titolare e responsabile.

### 1.4 CHI E' OBBLIGATO

Sono obbligati al rispetto delle misure di sicurezza nel trattamento di dati tutti coloro che trattano dati altrui. L'esonero dall'ambito di applicazione della disciplina della privacy non esonera dal rispetto delle regole di sicurezza. La sicurezza la devono rispettare tutti senza eccezioni.

Il Legislatore è chiarissimo: chiunque detenga informazioni o dati personali in qualsiasi forma è formalmente tenuto all'adempimento degli obblighi di legge

### 1.5 LE SCADENZE

Benchè la maggior parte degli adempimenti previsti non siano nuovi per le aziende, la scadenza del 30 Giugno 2005 ha riportato di attualità i necessari provvedimenti di adeguamento probabilmente ignorati da non poche realtà aziendali, in assenza dei quali la Legge prevede sanzioni amministrative da tremila a sessantamila Euro, eventualmente triplicabili in ragione delle dimensioni. Il responsabile trattamento dati deve compilare il Documento Programmatico sulla Sicurezza (DPS) entro il termine ultimo del 30 Giugno 2005 e successivamente aggiornarlo entro il 31 Marzo di ogni anno.

### 1.6 COSA RISCHIA CHI NON SI ADEGUA

Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 del Decreto Legislativo 169/2003 è punito con l'arresto sino a due anni o con l'ammenda da 10.000 a 50.000 Euro (Articolo 169).

## 2. CHE COSA SI DEVE FARE

In estrema sintesi è possibile identificare tre passi fondamentali per adeguarsi:

1. Identificare le caratteristiche del trattamento
2. Definire e adottare adeguate misure di sicurezza
3. Redigere il Documento programmatico sulla sicurezza (DPS)

### 2.1 IDENTIFICARE LE CARATTERISTICHE DEL TRATTAMENTO

Prima di procedere all'attuazione pratica degli adempimenti previsti dalla Legge, sarà quanto mai opportuno studiare le modalità organizzative delle attività di trattamento, gli strumenti adottati, la tipologia delle informazioni gestite e le figure aziendali preposte al trattamento.

L'azienda dovrà quindi:

- a) provvedere a delegare uno o più responsabili del trattamento
- b) identificare in forma scritta ciascun incaricato
- c) istruire i responsabili in forma scritta e in modo dettagliato circa la politica aziendale adottata sull'argomento
- d) verificare puntualmente la corretta applicazione delle direttive.
- e) definire nel dettaglio l'ambito di archiviazione e gestione dei dati, indicando a ciascun incaricato i limiti che gli competono e le procedure da seguire

VERITAS Professional Services ha consulenti con certificazione Internazionale CISA (Certified Information System Auditor) e Auditor BS7799 riconosciuta IRCA (International Register of Certified Auditor) con competenza specifica nell'ambito dell'Auditing sulla Sicurezza dei Sistemi Informativi. VERITAS può quindi aiutare ogni azienda nell'adempimento previsto dalla Legge.

### 2.2 DEFINIRE E ADOTTARE ADEGUATE MISURE DI SICUREZZA

La normativa stabilisce l'adozione di misure di sicurezza volte a impedire la distruzione o la perdita dei dati, gli accessi non autorizzati, i trattamenti non consentiti o non conformi alla Legge. Lo standard minimo definito nel disciplinare tecnico allegato al codice è semplicemente indicativo del livello al di sotto del quale l'azienda non è legittimata al trattamento dei dati personali: non esclude quindi la predisposizione di misure più stringenti.

Una checklist orientativa potrebbe essere la seguente:

- I dati sensibili devono essere protetti contro l'accesso abusivo mediante l'utilizzo di idonei strumenti elettronici.  
Le soluzioni di VERITAS che rispondono a questa richiesta sono:  
VERITAS Storage Exec (pag. 9) e VERITAS Security Services™ (pag. 9)
- Eventuali supporti rimovibili utilizzati per contenere i dati sono soggetti a distruzione obbligatoria non appena esauriscano la loro funzione di archivio.  
Le soluzioni di VERITAS che rispondono a questa problematica sono:  
VERITAS NetBackup Vault™ option (pag. 8), VERITAS NetBackup Storage Migrator for Unix (pag. 8) e KVS Enterprise Vault (pag. 8)
- Il ripristino dell'accesso ai dati in caso di crash dei sistemi informatici o danneggiamento dei database deve essere garantito entro il termine massimo di sette giorni.  
Le soluzioni di VERITAS che rispondono a questa problematica sono:  
VERITAS Bare Metal Restore™ (pag. 8), VERITAS Intelligent Disaster Recovery™ (pag. 7) e VERITAS High Availability Solution (pag. 9)
- Le informazioni devono essere trattate all'interno di locali protetti, con accesso limitato al solo personale autorizzato e trasmissione digitale rigorosamente crittografata.  
Le soluzioni di VERITAS che rispondono a questa problematica sono:  
VERITAS NetBackup Encryption™ option (pag. 8), VERITAS NetBackup Storage Migrator for Unix (pag. 8), KVS Enterprise Vault (pag. 8), VERITAS Desktop Laptop Option™ (pag. 9) e VERITAS Security Services™ (pag. 9)
- L'aggiornamento della piattaforma informatica, a titolo preventivo per evitare che le vulnerabilità compromettano la sicurezza è obbligatorio come minimo una volta all'anno.  
L'azienda dovrà valutare seriamente la sostituzione in blocco dei sistemi precedenti a Windows XP, installando quest'ultimo, una delle più recenti distribuzioni di Linux o soluzioni di altri produttori (sistemi Unix).  
Le soluzioni di VERITAS che rispondono a questa problematica sono:  
VERITAS OpForce™ (pag. 9) e VERITAS Desktop Laptop Option™ (pag. 9)

- Il salvataggio periodico dei dati é parte integrante delle misure minime stabilite dalla Legge. L'installazione di software automatici semplificherá l'incombenza. E' richiesta la pianificazione di backup come minimo settimanali di tutti i dati.  
Le soluzioni di VERITAS che rispondono a questa problematica sono:  
VERITAS NetBackup™ (pag. 8) e VERITAS Backup Exec™ (pag. 7)
- Ad integrazione delle misure minime di protezione, è opportuno prendere in considerazione la possibilità di alloggiare server e backup dei dati in locali dedicati, ai quali applicare ulteriori sistemi di sicurezza.  
Le soluzioni di VERITAS che rispondono a questa problematica sono:  
VERITAS High Availability Solution (pag. 9)

### **2.3 REDIGERE IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)**

Con Documento Programmatico sulla Sicurezza si intende un rapporto dettagliato ed esaustivo compilato e aggiornato con cadenza annuale a cura del responsabile trattamento dati, contenente le seguenti informazioni:

- 1) Elenco dei trattamenti di dati personali
- 2) Distribuzione dei compiti e delle responsabilità in ambito aziendale
- 3) Misure adottate a garanzia del ripristino dei dati in situazione di emergenza
- 4) Analisi dei rischi e misure adottate a garanzia dell'integritá dei dati
- 5) Interventi formativi predisposti per l'aggiornamento del personale
- 6) Criteri fissati in caso di esternalizzazione del trattamento
- 7) Criteri fissati per il trattamento dei dati sensibili

Il documento deve essere compilato entro il termine ultimo del 30 Giugno 2005 e successivamente aggiornato entro il 31 Marzo di ogni anno.

VERITAS Professional Services ha consulenti con certificazione Internazionale CISA (Certified Information System Auditor) e Auditor BS7799 riconosciuta IRCA (International Register of Certified Auditor) con competenza specifica nell'ambito dell'Auditing sulla Sicurezza dei Sistemi Informativi. VERITAS può quindi aiutare ogni azienda nell'adempimento previsto dalla Legge.

### 3. LE SOLUZIONI DI VERITAS

L'obiettivo di VERITAS è quello di rendere possibile l'utility computing attraverso il software. Indipendentemente dalle applicazioni, dai sistemi operativi o dall'hardware installato, VERITAS aiuta i dipartimenti IT ad erogare i livelli di servizio più adatti agli obiettivi di business, offrendo servizi affidabili, misurabili e ripartibili. I vantaggi derivanti dall'implementazione di una struttura corretta di utility computing si traducono in incremento della disponibilità e delle prestazioni, riduzione della complessità e dei costi grazie alla standardizzazione e automazione.

Il software VERITAS contribuisce ad accrescere l'efficienza dell'hardware di storage e dei server, garantisce che le applicazioni business-critical siano sempre disponibili e sensibili alle esigenze dell'utente, automatizza i backup dei dati, il provisioning di storage e la gestione dei server, aumentando drasticamente la produttività delle organizzazioni IT.

Per affrontare i possibili rischi associati alla perdita di dati aziendali (con notevoli ripercussioni sul business e sull'immagine dell'impresa), VERITAS aiuta a definire e implementare le soluzioni di Salvataggio & Rispristino dei dati coerentemente con le tue politiche aziendali e in linea con le tue esigenze di business.

Le soluzioni di VERITAS si possono così suddividere:

Ambienti Microsoft e NetWare	Ambienti Eterogenei (Microsoft, Unix e Linux)
VERITAS Backup Exec™	VERITAS NetBackup™
VERITAS Intelligent Disaster Recovery™ (IDR)	VERITAS NetBackup Vault™ option
VERITAS StorageExec™	VERITAS NetBackup Encryption™ option
KVS Enterprise Vault	VERITAS Bare Metal Restore™
	VERITAS NetBackup Storage Migrator for Unix
Ambienti Microsoft e Ambienti Eterogenei (Microsoft, Unix e Linux)	
VERITAS Desktop and Laptop Option™ (DLO)	
VERITAS Security Services™	
VERITAS OpForce™	
VERITAS High Availability Solution	
VERITAS Cluster™	
VERITAS Storage Foundation™	

Le soluzioni di VERITAS necessarie per adeguarsi alle normative si possono così riassumere:

#### 3.1 VERITAS BACKUP EXEC™ (COMPONENTE FONDAMENTALE DELLA NUOVA "BACKUP EXEC SUITE")

Esistono tre versioni di Backup Exec: Backup Exec for Windows Servers (BEWS), Backup Exec for Netware e Backup Exec for Small Business Server. VERITAS Backup Exec è la soluzione di backup e ripristino che offre una protezione completa e conveniente per gli ambienti server Microsoft Windows, NetWare, Linux e UNIX (SUN Solaris). Una consolle di amministrazione web-based ed un'interfaccia grafica utente intuitiva con wizard semplificano l'installazione e facilitano la gestione. Gli agenti e le opzioni ad alte prestazioni (Desktop and Laptop Option) offrono la flessibilità necessaria per una protezione rapida dei dati presenti su desktop, laptop e server. VERITAS Backup Exec consente la protezione automatica dei dati critici risiedenti in ambienti Windows, NetWare, Linux e UNIX. La protezione automatizzata avanzata di applicazioni quali Microsoft Exchange Server, Microsoft SQL Server e Lotus Notes semplifica le attività quotidiane degli amministratori di rete.

#### VERITAS INTELLIGENT DISASTER RECOVERY™ OPTION (IDR)

Veritas IDR automatizza e semplifica il processo di ripristino dei server, eliminando il bisogno di reinstallare manualmente il sistema operativo in caso di fault sul disco di sistema.

L'amministratore potrà tornare rapidamente con i sistemi online, tramite un bootable media creato con l'Intelligent Disaster Recovery che completerà l'operazione di restore dall'ultimo backup set disponibile evitando errori nella corretta procedura di ripristino. Tale soluzione si integra con Microsoft Windows Server 2003 ASR (Automatic System Recovery) e permette di accedere alla funzionalità di Automated SQL DR.

Grazie alla semplicità dell'opzione IDR, un ripristino completo di un server può essere realizzato in una frazione del tempo normalmente impiegato nella ricostruzione dello stesso, sfruttando qualsiasi set di backup comprendendo anche i last incremental o differential. Oltre a tale caratteristica innovativa, è possibile introdurre modifiche alla configurazione dei dischi e delle schede di rete, rendendo così indipendenti gli amministratori dalle possibili modifiche hardware. IDR è la soluzione ideale per gli ambienti Windows anche di tipo misto con sistemi remoti.

### 3.2 VERITAS NETBACKUP™ (NBU)

VERITAS NBU Enterprise Server e VERITAS NBU Server offrono una data protection di classe enterprise per ambienti UNIX, Windows, Linux e NetWare di qualsiasi dimensione. Le organizzazioni sono in grado di gestire tutti gli aspetti del backup e del ripristino, attraverso un'interfaccia grafica intuitiva, consentendo delle policy di backup omogenee attraverso l'intera infrastruttura IT. VERITAS NBU offre la più avanzata gestione dei media attualmente disponibile, che include capacità quali labeling di nastri magnetici, creazione di pool media su nastro, condivisione di dispositivi, rapporti su media/dispositivi e supporto di codice a barre. Inoltre VERITAS NBU offre l'opzione di soluzioni di backup e recovery sensibili ad applicazioni e database per Oracle, SAP R/3, Microsoft SQL Server, Microsoft Exchange, Microsoft SharePoint Portal Server, DB2, Lotus Notes/Domino, Sybase e Informix. Global Data Manager è lo strumento unico per gestire una serie di domini di NetBackup.

#### VERITAS NETBACKUP VAULT™ OPTION

Opzione integrata per VERITAS NBU, VERITAS NetBackup Vault™ automatizza la rotazione dei nastri magnetici, ossia il complesso e fastidioso processo di duplicazione di backup e di gestione media off-site. I vecchi processi manuali non sono esenti da errori – i nastri sono spesso mal catalogati, persi o cancellati. Con VERITAS NetBackup Vault™, gli utenti possono stabilire dei profili per controllare cosa, quando e come i backup devono essere duplicati e quando i nastri devono essere trasferiti da e verso il deposito (vault) off-site per garantire perdite minime in caso di evento catastrofico. NetBackup Vault si occupa dei dettagli in maniera automatica, limitando in questo modo la gestione manuale e riducendo il numero di errori possibili – evitando dunque la perdita o la cancellazione erronea dei tape. Le copie di dati poste nei vault provengono tipicamente da operazioni di full backup eseguite una volta alla settimana. Un backup incrementale su disco minimizza la perdita dei dati ed è più veloce da ripristinare. La replicazione esegue la copia dei dati in maniera continua, riducendo la perdita dei dati al minimo in caso di disastro. Uno dei motivi per continuare ad eseguire il backup e l'archiviazione dei dati risiede nel fatto che la replicazione copia tutti i dati – virus inclusi – e dunque una metodologia alternativa per la data retention è necessaria al fine di debellare il fenomeno del soft error.

#### VERITAS NETBACKUP ENCRYPTION™ OPTION

Opzione integrata per VERITAS NBU, VERITAS NetBackup Encryption™ permette una crittografia a livello di file di backup a archivi. Quando parte un backup il server determina attraverso un attributo della relativa politica di backup se i dati devono essere criptati o meno. Ci sono due tipi di encryption: standard e legacy. La encryption standard utilizza una cifratura a 128 o 256 bit Open SSL. La encryption legacy utilizza una cifratura a 40 o 56 bit DES.

#### VERITAS NETBACKUP STORAGE MIGRATOR FOR UNIX

NetBackup Storage Migrator for UNIX è un prodotto software che fornisce i tool per automatizzare lo spostamento dei file UNIX più vecchi verso i media storage del tipo più appropriato per caratteristiche, prestazioni e disponibilità. NetBackup Storage Migrator monitorizza costantemente lo storage disponibile on line su disco e, quando il disco raggiunge un prefissato livello di occupazione, sposta i file più vecchi e meno utilizzati che rispondono ai criteri impostati dall'IT manager, liberando capacità disco per gli utenti.

Questo software, quando trasporta fisicamente i dati verso una destinazione più appropriata, provvede a lasciare, al posto originario di ogni file, un indicatore di collegamento. Quando si desidera accedere al dato, esso viene richiamato automaticamente e in modo trasparente in modo parziale, risultando immediatamente accessibile all'utente, mentre NetBackup Storage Migrator completa il trasferimento.

### 3.3 VERITAS BARE METAL RESTORE™ (BMR)

VERITAS BMR automatizza e semplifica il processo di ripristino dei server, eliminando il bisogno di reinstallare manualmente il sistema operativo o di riconfigurare l'hardware. BMR cattura delle snapshot dei server e dei sistemi operativi e memorizza queste informazioni nei backup creati da NetBackup. Grazie alla semplicità dei comandi, un ripristino completo di server può essere realizzato in una frazione del tempo precedentemente necessario senza il bisogno di una complessa formazione o di una difficile amministrazione. Tramite l'interfaccia in stile web-browser ed i suoi wizard, esegui in parallelo il ripristino di più server per completare operazioni di recupero di massa. Una sola soluzione risponde alle esigenze di una molteplicità di piattaforme, eliminando il bisogno di personalizzare le procedure di ripristino per ciascuna piattaforma.

### 3.4 KVS ENTERPRISE VAULT

“KVS Enterprise Vault consente alle organizzazioni una completa gestione dell'intero ciclo di vita delle informazioni in ambiente Windows. Inoltre, KVS Enterprise Vault conferisce la caratteristica di Information Lifecycle Management al portafoglio prodotti VERITAS, aiutando le organizzazioni a ridurre i rischi di business e IT associati alla ritenzione ed alla gestione di dati non strutturati, quali il contenuto dei messaggi e la gestione dello storage di Windows. Questa soluzione riduce i costi dello storage, semplifica la ritenzione e la gestione dei dati, e permette una rapida ricerca del contenuto storico di Windows. KVS Enterprise Vault è uno strumento per l'archiviazione dei file system, delle e-mail, degli Instant Messaging e dei siti web di Microsoft Office SharePoint in ambiente Windows. L'archiviazione basata su policy consente alle organizzazioni di archiviare i dati fuori dei server Windows, riponendoli nei server Enterprise Vault, al fine di amministrare al meglio la crescita dei dati, fornendo così la soluzione di archiviazione leader agli utenti VERITAS. In data 31 Agosto 2004, VERITAS ha annunciato l'intenzione di acquisire KVS.”

### **3.5 VERITAS DESKTOP AND LAPTOP OPTION™ (DLO)**

VERITAS NetBackup e Backup Exec DLO offrono una sincronizzazione e protezione disk-based continua agli utenti in ufficio o in viaggio – oltre che per quegli utenti che archiviano il proprio lavoro su desktop e laptop. IDC stima che circa il 60% dei dati totali risiede al di fuori dei server, questi dati sono generalmente ad uno stadio critico del loro ciclo di vita. DLO copia automaticamente i dati utente sui server o sullo storage di rete esistenti, permettendo un rapido recupero o la sincronizzazione dei dati da parte dell'amministratore o dell'utente in caso di perdita di dati. Una volta che i dati sono stati sincronizzati o salvaguardati dai desktop/laptop sul server NBU o BEWS, il server stesso viene salvaguardato su disco e/o nastro.

### **3.6 VERITAS STORAGE EXEC™ (COMPONENTE DELLA NUOVA "BACKUP EXEC SUITE")**

VERITAS StorageExec è lo strumento di gestione dello storage di Windows che controlla automaticamente l'assegnazione di storage, riducendo i tempi di backup e migliorando i livelli di servizio. VERITAS StorageExec si serve di una gestione policy-based per lo storage su disco residente su Storage Area Network (SAN), Network Attached Storage (NAS) e Direct Attached Storage (DAS) basato su Windows. VERITAS StorageExec identifica i tipi di file non autorizzati (anche se gli utenti più smaliziati ne hanno cambiato l'estensione) e li rimuove dal sistema, filtrando i tipi di file non ammessi quali MP3, giochi, script e virus. Individua e recupera lo spazio su disco sprecato – riducendo in questo modo la quantità di dati da proteggere e la finestra di backup. Consente ai dipartimenti di stabilire delle quote in tempo reale sullo storage Windows condiviso, oltre che ad informare gli utenti sull'utilizzazione del disco tramite rapporti HTML interattivi e notifiche in tempo reale sul raggiungimento delle soglie di quota. Permette inoltre agli utenti di gestire il proprio spazio di storage. Microsoft include la tecnologia Storage Exec di VERITAS per curare la gestione delle quote in Windows Storage Server 2003. Oltre 5.000 aziende in tutto il mondo si servono di VERITAS StorageCentral.

### **3.7 VERITAS OPFORCE™**

OpForce permette all'IT di "copiare" l'immagine di sistema di server in produzione e "replicarla" su dei nuovi server, consentendo il rapido spiegamento e provisioning di server (si tratta di minuti invece che di ore). OpForce è in grado di implementare dei nuovi server in ambienti esistenti o di assegnare dei server sottoutilizzati ad ambienti che necessitano di un numero maggiore di server modificandone l'immagine di sistema operativo in pochi minuti. OpForce automatizza la configurazione dei server, eliminando il fastidioso compito di installazione del sistema operativo, patches, drivers e applicativi. Se un'applicazione dovesse richiedere delle risorse aggiuntive per funzionare efficacemente, OpForce è in grado di incrementare le risorse di server per supportare tale applicazione. OpForce cattura una snapshot contenente tutto l'ambiente software completo di un server esistente e ne costruisce uno nuovo come richiesto. Il reale vantaggio di OpForce è che le sue funzionalità sono indipendenti dall'hardware di server a disposizione.

### **3.8 VERITAS SECURITY SERVICES™**

La funzione primaria di VERITAS Security Services è controllare l'accesso alle informazioni basandosi su regole prestabilite e sulle policy di sicurezza. Il prodotto ha due componenti: autenticazione e autorizzazione. L'autenticazione verifica l'identità della persona e concede le credenziali. L'autorizzazione, se le regole di sicurezza lo permettono, consente l'uso dei prodotti VERITAS. Può costituire un unico punto di accesso (Single Sign On) per tutte le soluzioni di VERITAS evitando di digitare più volte la password per accedere ad ogni prodotto.

### **3.9 VERITAS HIGH AVAILABILITY SOLUTION**

Se i dati sono il bene più prezioso per l'azienda, allora è ovvio che tali dati debbano essere disponibili quando sono richiesti. Oggigiorno, ciò può anche significare una disponibilità pari a 24 ore al giorno, 7 giorni alla settimana e 365 giorni all'anno. Ciò che emerge è che tutte le aziende hanno bisogno di strategie per la data availability e, di fatto, la disponibilità è stata la fonte di maggiore esborso IT negli ultimi cinque anni. Disponibilità significa che bisogna essere in grado di mantenere l'ambiente IT costantemente in funzione. Per esempio, se qualcosa dovesse impedire ad un server di funzionare correttamente, l'azienda dovrebbe trovare una soluzione affinché il proprio business non ne risenta.

#### **VERITAS CLUSTER SERVER (VCS)**

VCS è la soluzione leader di mercato per il clustering di sistemi aperti. VCS mette in cluster (unisce) dei server al fine di offrire un alto livello di disponibilità ad applicazioni e database. In caso di eventuale avaria dell'applicazione, del database o del server, VCS rileva automaticamente l'errore e trasferisce i relativi servizi su di un server funzionante in grado di ospitare tale applicazione o database. VCS risulta essere la soluzione ideale per ridurre il downtime programmato e non, per facilitare il consolidamento di server (grazie ad un'ottimizzazione del numero di server per fare girare il business) e per gestire efficacemente una vasta gamma di applicazioni e database in ambienti eterogenei. VCS ha la potenza e la flessibilità adeguata per proteggere qualsiasi ambiente, da una singola istanza di database mission-critical a grandi cluster multi-applicazioni distribuiti geograficamente. Aumentare l'automazione, offrire funzioni in grado di collaudare i piani di disaster recovery senza interrompere il servizio ed offrire un'intelligente gestione del carico di lavoro permette all'amministratore del cluster di massimizzare le risorse IT a disposizione.

### **VERITAS STORAGE FOUNDATION**

VERITAS Storage Foundation unisce due prodotti leader di mercato, VERITAS Volume Manager (VxVM) e VERITAS File System (VxFS) per offrire una soluzione completa di gestione dello storage online. Con VERITAS Storage Foundation i dischi fisici possono essere raggruppati in volumi logici al fine di migliorare l'utilizzazione dei dischi. Grazie alla virtualizzazione, si è in grado di eliminare il downtime relativo allo storage, di modo che se si hanno tre server a disposizione, ed uno di questi tre è utilizzato al massimo, allora VxVM renderà disponibile lo spazio degli altri due virtualizzandoli o ne bilancerà il carico. In aggiunta VERITAS Storage Foundation offre agli amministratori la flessibilità data dalla possibilità di spostare i dati tra sistemi operativi e array di storage diversi, suddividere i flussi I/O tra path multipli al fine di migliorare le prestazioni, – riducendo l'attesa di I/O (migliorando dunque le prestazioni applicative), e di conseguenza riducendo i ritardi della rete –, e replicare i dati (mirroring) su siti remoti per accrescere la disponibilità e trasferire file poco importanti o datati su di uno storage secondario senza dover modificare la modalità di accesso ai file da parte di utenti o applicazioni.

#### 4. CONCLUSIONI

Veritas consente di rispondere con un approccio sistematico ai requisiti di conformità imposti dalle nuove normative, grazie ad una suite di prodotti integrati e modulari. Le soluzioni multiplatforma di Veritas, grazie alla loro flessibilità e alla loro indipendenza dall'infrastruttura hardware, consentono l'adeguamento delle aziende alle nuove normative (costantemente in evoluzione), riutilizzando l'hardware su cui si ha già investito, e fornendo totale integrazione tra le componenti coinvolte nel trattamento dei dati: backup dei servers, backup dei clients, disaster recovery, archiving, encryption e reporting.

Le aziende che hanno scelto in passato le soluzioni di backup di Veritas, hanno già in casa parte della soluzione Veritas di conformità.

PER MAGGIORI INFORMAZIONI:

Sei invitato a seguire il link del VERITAS Architects Network:

<http://www.veritas.com/van/index.jsp>

Visita inoltre:

[http://www.veritas.com/Products/www?c=home&ln=it\\_IT](http://www.veritas.com/Products/www?c=home&ln=it_IT)

I partner sono inoltre invitati a visitare il VERITAS Partner Network:

<http://www.veritas.com/emea/partnernetwork/home.jhtml>

Oppure contatta direttamente il tuo rappresentate VERITAS.

**VERITAS Software Limited**

EMEA Headquarters  
350 Brook Drive  
GreenPark, Reading, Berkshire, RG2 6UH. UK  
Tel: +44 (0) 870 423 1080

Per maggiori informazioni su VERITAS Software, i suoi prodotti o l'indirizzo dell'ufficio più vicino, contattate la nostra sede centrale o visitate il nostro sito all'indirizzo [www.veritas.com](http://www.veritas.com).