Forensics aziendale, salvaguardia del patrimonio dell'impresa e tutela dei lavoratori

monografia

Antonino Attanasio*

Sommario

Il patrimonio aziendale comprende anche le tecnologie informatiche e assistive. Con l'inserimento lavorativo delle persone con disabilità, l'azienda, come complesso di beni organizzato dall'imprenditore per l'esercizio dell'impresa, acquisisce maggior valore. Questo valore deve essere protetto a vantaggio dei lavoratori, soprattutto di quelli che hanno una disabilità, che devono essere consapevoli dell'importanza dell'uso delle tecnologie. Nel contributo si evidenzia anche il ruolo del *Diversity Manager* che affianca il *Security Manager*.

Strumenti e tecnologie assistive come patrimonio dell'impresa

Il personale delle imprese è composto sia da lavoratori normodotati che da lavoratori con disabilità: la convivenza di queste due categorie di lavoratori ha fatto emergere problemi nuovi e originali rispetto al passato.

L'attenzione alle persone con disabilità nel mondo del lavoro è focalizzata sulle procedure di inserimento lavorativo che, tradizionalmente funzionali all'assolvimento di un obbligo di legge, pongono anche problemi di contemperamento di esigenze potenzialmente in conflitto, come appunto, da un lato, l'esigenza dell'imprenditore di disporre di personale dipendente qualificato da adibire alle mansioni effettivamente necessarie e, dall'altro, l'esigenza del lavoratore con disabilità di svolgere le mansioni per le quali ha acquisito la necessaria competenza, nel rispetto della propria professionalità e dignità; infine emerge l'esigenza, più generale, di tutelare l'integrità del patrimonio aziendale (materiale e immateriale) e la sicurezza aziendale.

Le tecnologie ICT *(Information and Communication Technologies)* costituiscono il «sistema nervoso» di tutte le imprese e la sicurezza del patrimonio informativo e delle infrastrutture ICT è fondamentale per la sopravvivenza stessa delle organizzazioni. In merito si riscontra l'impiego di un'ampia terminologia: *information security, ICT security, business security, corporate security.*

Considerare un lavoratore con disabilità una risorsa fa sì che l'integrazione nell'azien-

* Avvocato e Dottore di ricerca in Economia e Direzione delle Aziende pubbliche.

da non sia più occasionale ma sistematica e l'attenzione ai temi della security aziendale completa il programma di inserimento, qualificandolo: di conseguenza, il dipendente con disabilità è reso partecipe della preservazione dell'integrità degli asset aziendali.

La partecipazione dunque e non la mera fruizione accrescono la security stessa dell'azienda: la fidelizzazione del personale dipendente con disabilità nel rispetto delle policy emanate dall'azienda ha come conseguenza la consapevolezza del rispetto e della salvaguardia dell'integrità del patrimonio aziendale, materiale e immateriale. La security aziendale, a sua volta, non si caratterizza come «segmento organizzativo» isolato, ma rientra nella dinamica del rapporto tra definiti e circoscritti problemi aziendali *(livello micro)* e il loro contesto di riferimento *(livello macro)*.

Tanto premesso, l'inserimento lavorativo delle persone con disabilità ha valorizzato non solo il ruolo delle risorse informatiche e informative aziendali, ma anche quello delle tecnologie assistive. In particolare le tecnologie assistive sono strumentazioni e soluzioni tecniche, hardware e software, che permettono alla persona disabile di accedere alle informazioni e ai servizi erogati dai sistemi informatici, superando o riducendo le loro condizioni di svantaggio; rientrano nella nozione anche le tecnologie ordinarie, cioè non di tipo informatico, funzionali al movimento e alla comunicazione delle persone con disabilità, come pedane, scivoli, carrozzine, scrivanie adattate, ecc.[1]

Le risorse informatiche e informative aziendali, a loro volta, sono costituite dal complesso delle informazioni che risultano disponibili all'azienda a vario titolo (database e archivi cartacei relativi a proprietà intellettuale, know-how, business, informazioni contabili/finanziarie, informazioni sui clienti, sui fornitori e sui partner d'impresa, documentazione di sistema, procedure operative o di supporto, piani di continuità) e dalle risorse hardware.

Queste risorse comprendono anche le risorse di Rete, cioè la posta elettronica, internet, intranet) e fanno parte del patrimonio aziendale, come descritto dall'articolo 2555 del Codice Civile, dal quale emerge che «l'azienda è il complesso dei beni organizzati per l'esercizio dell'impresa». Tale complesso di beni, in origine composto da strumenti e oggetti tradizionali e funzionali all'utilizzo da parte dei lavoratori normodotati, per effetto delle innovazioni tecnologiche e dell'inserimento lavorativo delle persone con disabilità ha acquisito una maggiore caratterizzazione in termini non solo di miglioramento di performance produttive, ma anche di valorizzazione del capitale umano aziendale.

La salvaguardia del patrimonio aziendale: tutela dell'impresa e del lavoratore

Il personale dipendente con disabilità deve ricorrere alle tecnologie assistive, alcune delle quali risultano basate su tecnologie informatiche. L'utilizzo di queste tecnologie e il ricorso agli strumenti informatici aziendali per scopi

[1] Fondamentali sono state le ricerche svolte dalla School of Management del Politecnico di Milano con i due rapporti, entrambi resi pubblici nell'anno 2008, su *ICT Security: quale governance?* e *ICT accessibile e Disabilità: una fotografia della situazione in Italia*. I risultati delle due ricerche sono stati illustrati e commentati allo scopo di individuare lo «stato dell'arte» e, al tempo stesso, le prospettive di soluzione, considerato che il rapporto tra sicurezza informatica e lavoratori con disabilità non è stato esaminato espressamente in nessuno dei due rapporti, riguardando il primo la governance dell'Information Security e il secondo il problema dell'accessibilità dell'ICT per le persone con disabilità.

comunicativi, sia all'interno dell'azienda che all'esterno di essa (si pensi, ad esempio, a una chatline aziendale), pongono il problema della possibile interferenza delle tecnologie usate dal personale dipendente con disabilità con la sicurezza informatica.

Il combinato disposto degli articoli 2087 («Tutela delle condizioni di lavoro») e 2104 («Diligenza del prestatore di lavoro») del Codice Civile costituisce la disciplina fondamentale dell'attività di regolazione all'interno dall'azienda e riguarda due aspetti chiave dell'esercizio dell'impresa: la sicurezza del lavoro e l'esecuzione della prestazione lavorativa.

L'imprenditore, infatti, nell'esercizio dell'impresa è tenuto a adottare le misure che, in base al lavoro, all'esperienza e alla tecnica, sono necessarie per tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro. L'imprenditore, inoltre, impartisce specifiche disposizioni relative all'esecuzione e alla disciplina del lavoro, direttamente o attraverso i propri collaboratori. Tuttavia l'evoluzione tecnologica, la diffusione dell'informatica in azienda e la complessità dei processi produttivi hanno mostrato l'insufficienza delle prescrizioni del Codice Civile e hanno imposto al legislatore una puntuale integrazione della disciplina del processo di regolazione interna all'azienda, mediante l'obbligo dell'adozione di documenti normativi di carattere generale.

Si pensi così, per citare almeno i documenti fondamentali, al Documento di valutazione rischi (art. 28 del D.LGS. 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza nei luoghi di lavoro), al Documento programmatico di sicurezza (art. 34 e All. B, regola 19, D.LGS. 30 giugno 2003, n. 196, in materia di protezione dei dati personali), al Modello di organizzazione e gestione (art. 6 D.LGS. dell'8 giugno 2001, n. 231).

La documentazione normativa di regolazione interna a carattere aziendale, così come disciplinata dal Codice Civile e dalle leggi speciali, può inoltre essere integrata da un'ulteriore regolazione di dettaglio, per effetto di esigenze contigenti e specifiche dell'impresa, in relazione all'attività svolta o all'utilizzo di risorse strumentali.

L'utilizzo, da parte di tutti i componenti dell'organizzazione aziendale, delle risorse informative e informatiche aziendali elencate deve avvenire in conformità alle leggi, ai regolamenti dello Stato e alle normative aziendali interne, allo scopo non solo di eseguire puntualmente la prestazione lavorativa, ma anche di evitare o ridurre al minimo i rischi di indisponibilità, accesso non autorizzato, distruzione o perdita accidentale delle risorse stesse.

Simili rischi possono essere sintetizzati nell'espressione «evento illecito», che è ogni evento, sia interno che esterno all'azienda, che determini una lesione o un pregiudizio grave nei confronti di beni/interessi di cui l'impresa abbia la tutela, la proprietà o anche la disponibilità, per i quali la legge preveda anche l'applicabilità di una sanzione penale.

Occorre prevenire i rischi connessi a un utilizzo di dette risorse per motivi non attinenti allo svolgimento delle mansioni aziendali o, addirittura, per motivi dolosamente diretti a compromettere dati, informazioni e apparecchiature. Si devono quindi predisporre misure preventive di sicurezza idonee, in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati; in particolare la sicurezza fisica è il complesso di sistemi, prodotti e procedure destinato alla protezione delle risorse aziendali, costituite da impianti, ambienti e persone, che sinteticamente costituiscono il patrimonio aziendale.

L'esigenza di disporre di adeguati mezzi di protezione è legata all'intensità di frequentazione delle aree di operatività dell'impresa e al valore dei beni e dei processi produttivi. È diritto dell'imprenditore eseguire forme di controllo cosiddetto «difensivo» sull'esattezza

della prestazione lavorativa e sul corretto uso, da parte del lavoratore, dei beni e servizi aziendali che gli sono stati forniti per l'espletamento delle sue mansioni lavorative.

Il controllo difensivo[2] consiste in attività conseguenti a eventi illeciti, volte ad accertare la responsabilità del fatto e la quantificazione del danno, coordinando le iniziative finalizzate a minimizzare i danni subiti dall'impresa e a contrastare i conseguenti rischi d'immagine, nonché segnalando eventuali debolezze del sistema di controllo interno che abbiano favorito il verificarsi dell'evento illecito.

Il controllo difensivo, consistente nell'acquisizione di tutte le evidenze (documenti, testimonianze, fotografie, registrazioni, ecc.) comprovanti la realizzazione dell'illecito, si conclude con l'elaborazione di una relazione *(report)* funzionale all'adozione dei provvedimenti, cautelativi e/o repressivi, ed eventualmente disciplinari, richiesti dal caso.

Policy, Linee Guida, Regolamenti interni e altri documenti variamente denominati sono gli strumenti dell'impresa con i quali vengono regolamentati i vari aspetti della vita lavorativa, con riferimento al corretto impiego dei sistemi aziendali, all'informazione sulle misure di sicurezza adottate e sull'utilizzo dei dati raccolti all'interno dell'azienda.

La forensics aziendale: definizione, obiettivi e strumenti

La Computer Forensics[3] costituisce il processo più importante nell'ambito delle attività riconducibili ai cosiddetti «controlli difensivi», riconosciuti legittimi a seguito delle sentenze della Cassazione, oltre che della magistratura di merito, e a seguito di provvedimenti di carattere generale e decisioni del Garante per la protezione dei dati personali.

L'informativa diffusa all'interno dell'impresa mediante gli strumenti denominati policy, regolamento interno aziendale, linee guida è sufficiente per legittimare la raccolta e l'utilizzo dei dati relativi alle operazioni di controllo. La policy aziendale è un elemento fondamentale per l'efficacia dell'attività investigativa aziendale. Essa, infatti, contiene i seguenti elementi:

– i riferimenti e richiami agli illeciti informatici, al fine di creare consapevolezza negli utenti;
– le regole a cui il personale e i soggetti terzi che operano con l'azienda devono attenersi nell'uso della strumentazione informatica;
– le modalità e i limiti nella raccolta delle informazioni per le attività interne di gestione e prevenzione delle frodi, in particolare per quanto concerne la raccolta degli elementi probatori;
– le modalità di coordinamento e di collaborazione tra le strutture coinvolte nelle attività di indagine;
– le azioni che possono essere intraprese nei confronti di un soggetto coinvolto in un'attività fraudolenta.

È importante comprendere quali possano essere le motivazioni ricorrenti per le quali dipendenti e dirigenti compiono frodi di varia natura nelle organizzazioni pubbliche o private di appartenenza:

– il desiderio di arricchirsi e/o possedere l'oggetto che, normalmente, non ci si potrebbe permettere, ovvero il desiderio di realizzare con poca fatica le proprie aspirazioni;

[2] G. Costabile, *Information security in azienda*, Forlì, Experta, 2008; Id. (a cura di), *Sicurezza e privacy: dalla carta ai bit,* Forlì, Experta, 2005.

[3] G. Costabile et al., *Computer Forensics aziendale: Fondamenti delle best practice aziendali e ruolo della policy aziendale*. In G. Costabile e A. Attanasio (a cura di), *IISFA Memberbook 2010 Digital Forensics*, Forlì, Experta, 2010.

– l'insoddisfazione e la frustrazione generate dalle condizioni presenti nell'ambiente di lavoro;
– il desiderio di equilibrare inconsapevolmente gli squilibri emozionali di un trattamento di lavoro considerato ingiusto;
– la mancata percezione delle conseguenze legali e amministrative (denuncia, licenziamento, ecc.) dell'eventuale rilevazione della frode commessa;
– l'idea di poter eludere ogni controllo relativo alle azioni commesse in azienda;
– l'errata opinione che una piccola sottrazione non possa interessare a coloro che gestiscono business di ben più elevata portata;
– la mancanza di controlli sistematici nell'azienda e la percezione che le frodi rilevate siano state scoperte per puro caso; da ciò deriva l'idea che il rischio che si sta per correre sia realmente minimo: questo porta a credere che il livello e la qualità del controllo interno siano facilmente superabili.

La Computer Forensics applicata in un contesto aziendale introduce metodologie funzionali ad acquisire, preservare e analizzare i referti (intesi come *digital evidence*) e competenze concernenti le modalità per identificare e analizzare delle prove che coinvolgono svariate tecnologie *(hard disk forensics, network forensics, mobile forensics, ecc.)*.

L'attività deve essere svolta garantendo che l'informazione trattata sia autentica, integra, vera, completa, raccolta legalmente e, se possibile, con metodologie ripetibili, in modo tale da poterla utilizzare in giudizio.

La procedura si articola nei seguenti step:[4]

– implementazione corretta del processo di *Identity Access Management,* in modo da garantire che gli accessi alle risorse aziendali vengano realmente effettuati da persone fisiche ben definite;
– realizzazione di un sistema di *LOG management,* che garantisca l'integrità dei dati e l'impossibilità che questi possano essere modificati manualmente da un amministratore di sistema;
– emissione di una serie di policy o normative interne che determinino i limiti all'uso promiscuo degli strumenti aziendali, in particolare l'utilizzo degli strumenti elettronici (ad esempio, posta elettronica, utilizzo di pc fissi e/o portatili e cellulari/smartphone) assegnati per uso lavorativo, ma concessi in parte anche per uso personale (uso promiscuo);
– ufficializzazione di un gruppo di lavoro per la gestione dei casi/incidenti, composto dal *Fraud Manager* e, se non presente, da un *Risk Manager* o *Internal Audit,* che deve essere affiancato da un tecnico esperto in Computer Forensics (in genere meglio se certificato e con almeno cinque anni di esperienza provata) e di un altro gruppo formato dal personale del settore Risorse Umane e dell'Ufficio Legale che, quando non presente come organo interno, è comunque rappresentato da un Avvocato di fiducia dell'azienda.

Operativamente la Computer Forensics si articola come segue:

– lettera di contestazione e dichiarazione dei dati personali sensibili presenti negli strumenti aziendali che stanno per essere sequestrati;
– incarico per attività di Computer Forensics e autorizzazione al trattamento dei dati personali;
– procedura operativa per identificazione, acquisizione, analisi e documentazione delle digital evidence;
– modello di catena di custodia.

[4] G. Costabile et al., *Computer Forensics aziendale: Fondamenti delle best practice aziendali e ruolo della policy aziendale*, op. cit.

Forensics aziendale e ruolo dei lavoratori con disabilità: il *diversity management*

L'accessibilità dei documenti, dei siti web e di qualsiasi documento elettronico è una garanzia di primaria importanza sul luogo di lavoro, nel rispetto delle regole tecniche funzionali alla realizzazione di documenti digitali accessibili come pdf, rtf, doc, ecc.

Sebbene ciò fino a tempi recenti non sia stato possibile, dal momento che sarebbe stato alquanto complicato e oneroso pensare a una traduzione in Braille di ogni singolo documento, attualmente, grazie ai progressi dell'informatica, questo è praticabilissimo, dato che tutta la documentazione si sta diffondendo attraverso canali telematici in sostituzione della carta, ponendo dei vincoli sia sui formati di interscambio sia sul rispetto dei requisiti di accessibilità.

I soggetti non vedenti sono i primi a essere gravemente colpiti da tale problema, poi vengono le persone dislessiche che, pur vedendo, necessitano comunque di farsi aiutare nella lettura dei documenti da un sintetizzatore vocale; infine occorre considerare le persone con disabilità motorie che, sebbene colpite in maniera molto più lieve rispetto agli altri individui disabili prima citati, hanno il problema di non poter sfogliare i documenti cartacei e quindi necessitano di un'alternativa digitale, anche se, al contrario dei non vedenti, per loro la versione digitale presenta solitamente un minor problema di inaccessibilità, dato che generalmente essa è consultabile senza particolari requisiti poiché l'importante è che l'applicativo preposto a leggere i documenti sia, ad esempio, gestibile tramite programmi di riconoscimento vocale.

Un altro problema è rappresentato dalla poca conoscenza dei requisiti di accessibilità e dalla scarsa attenzione che viene rivolta ad essi da parte di coloro che si occupano di sicurezza informatica. Sono diversi i casi nei quali, infatti, si pongono in essere sistemi di protezione che, di fatto, ostacolano del tutto l'accesso da parte delle persone disabili, come ad esempio i *captcha* che, per evitare la compilazione automatica di formulari da parte di altri programmi appositamente creati, richiedono di inserire caratteri e numeri rappresentati in forma grafica all'interno di un'immagine.

Tale sistema risulta inaccessibile agli *screen reader* e, di conseguenza, le persone non vedenti risultano escluse. Sistemi alternativi non sono stati ancora presi in considerazione, a causa di un'attenzione spesso unidirezionale per la sicurezza in sé, a prescindere dall'effettiva utilità del ricorso a sistemi complessi. Un esempio nel quale le esigenze di sicurezza possono scontrarsi con quelle dell'accesso ai soggetti disabili è proprio rappresentato dalle procedure di autenticazione.

È noto il diffondersi di operazioni di *phishing* e di vari *malware, spyware, trojan* e, in generale, di tutto quel software che viene installato sui computer allo scopo di spiare le attività e transazioni fatte con il pc.

Un metodo sicuro è rappresentato dalle password dinamiche generate da appositi dispositivi hardware portatili: si tratta di chiavette con display che, alla pressione di un pulsante, generano delle sequenze numeriche da usare come password aggiuntive alle credenziali normalmente usate per l'accesso, con la particolarità che queste password così generate sono valide solo per un brevissimo periodo di tempo e possono essere adoperate una sola volta all'interno di tale intervallo temporale. Questi dispositivi, però, se non risultano dotati di una funzione di lettura vocale dei numeri che appaiono sul display, si tramutano in una barriera invalicabile per le persone con disabilità visive.

Un altro problema riguarda i software utilizzati per la firma digitale che non sono accessibili, per cui diviene un problema riuscire a firmare e controllare l'autenticità dei documenti ricevuti. Per quanto riguarda le persone audiolese, l'utilizzo di tecnologie chat interne aziendali consente di comunicare con qualsiasi collega, allegando anche videate di una procedura o qualsiasi file per facilitare la comprensione e, quindi, la soluzione del problema.

Rimangono tuttavia seri problemi di tutela dell'azienda da un lato (concernenti, ad esempio, le comunicazioni esterne all'azienda) e del lavoratore dall'altro (ad esempio, le sessioni chat possono essere monitorate illegittimamente allo scopo di controllare il lavoro del dipendente audioleso).

I progressi che hanno interessato le tecnologie assistive e l'informatica in generale aprono sempre nuove strade di integrazione lavorativa per gli individui disabili. Tuttavia, in riferimento alla policy di sicurezza informatica che deve essere utilizzata all'interno dell'azienda, si può dire che i principali problemi di accessibilità siano dati ancora una volta dalla scarsissima conoscenza di queste tematiche da parte dei sistemisti, che spesso vedono gli ausili software con molta diffidenza, a causa della non conoscenza di essi e dell'assenza di una valutazione del loro impatto, una volta installati sui sistemi informatici in uso nella loro realtà lavorativa.

La non conoscenza del funzionamento e della configurazione di tali programmi genera rapporti distorti tra i sistemisti e l'utente disabile: se quest'ultimo non ha tutte le conoscenze necessarie (relativamente non solo a come si usano gli ausili ma anche a come si installano e si integrano con il restante sistema informatico), i sistemisti devono rivolgersi ai rivenditori degli ausili stessi.

Essendo mediamente basso il livello di conoscenza anche tra gli addetti ai lavori delle problematiche legate all'accessibilità connessa alla sicurezza in ambienti lavorativi medio-grandi, spesso i rivenditori di ausili o le associazioni ed enti di formazione non sono in grado di soddisfare adeguatamente esigenze particolari. Ciò causa delle limitazioni nel contesto lavorativo della persona con disabilità, aggravate dalle legittime esigenze di sicurezza.

Due sono le soluzioni empiricamente adottabili: nel primo caso i sistemisti e i responsabili, per eccesso di cautela, non mettono a disposizione tutti gli ausili e programmi necessari o ne limitano fortemente le possibilità di utilizzo; nel secondo caso è riscontrabile una totale «apertura» e disponibilità in contrasto con le norme elementari di sicurezza, perché i sistemisti e responsabili ICT in genere non possono in nessun modo delegare il loro ruolo alla persona con disabilità.

Occorre quindi mediare tra un ambiente inaccessibile a causa dell'adozione di policy troppo restrittive e un sistema informatico affetto da vulnerabilità, che potrebbero essere evitate se si conoscesse meglio quali sono le vere necessità per ottenere un ambiente accessibile e compatibile con gli ausili.

A parte le principali policy che limitano l'utente nell'installazione del software e nelle modifiche alla configurazione del sistema, queste non creano generalmente problemi se non la necessità di aggiornare il software, cosa che dovrebbe essere pianificata dall'amministratore anche in ragione della compatibilità delle nuove *release* dei programmi maggiormente usati con le tecnologie assistive utilizzate dalla persona disabile, ma questo non viene quasi mai fatto se non dietro protesta del soggetto disabile; di conseguenza la persona disabile ferrata in materia spesso preferisce chie-

dere un account amministratore, in modo tale da eseguire un compito che, in realtà, sarebbe comunque stato di pertinenza del sistemista.

I problemi reali sono solitamente dati da tutte quelle policy che mirano a disabilitare porzioni delle interfacce del sistema operativo o degli applicativi, allo scopo di impedire all'utente di compiere azioni pericolose oppure che, pur non essendo pericolose, potrebbero comunque far confondere un utente non esperto, inducendolo a chiedere l'intervento del tecnico addetto.

La presenza di persone con disabilità nell'organico aziendale e l'utilizzo della tecnologia informatica rendono necessari una definizione, un utilizzo e l'assegnazione delle utenze per l'accesso ai sistemi informativi, allo scopo di garantire il raggiungimento e il mantenimento nel tempo dei seguenti obiettivi di sicurezza aziendale:

– proteggere adeguatamente le risorse informative aziendali, con particolare riguardo ai dati, garantendo alle stesse adeguati livelli di integrità, riservatezza e disponibilità;
– definire/gestire i profili autorizzativi che possono essere attribuiti al personale (utenti interni/utenti esterni) autorizzato ad accedere ai dati aziendali;
– gestire efficacemente gli incidenti di sicurezza.

Nell'ambito del processo di *Identity Management* adottato dall'Azienda, devono essere consentite la definizione dei ruoli organizzativi e dei profili autorizzativi, l'associazione dei ruoli organizzativi ai profili autorizzativi e la gestione dei profili di accesso assegnati.

È fondamentale associare il ruolo del responsabile dell'Information Security a quello del responsabile del Diversity Management (unendoli in una sola persona oppure affiancando due responsabili distinti),[5] in modo tale da gestire la diversità all'interno di un'organizzazione: in primo luogo è necessario riconoscere le disomogeneità interne e legittimare il valore delle differenze, non solo in riferimento alla gestione dei prodotti o ai target di clienti, ma anche con riguardo alle persone che danno il proprio contributo lavorativo in azienda; in secondo luogo occorre valorizzare la strategia dell'Information Security Manager, avendo come principali obiettivi la tutela del dato e dell'informazione, lo sviluppo di una *corporate governance* della sicurezza, la sensibilizzazione della coscienza aziendale sul tema della sicurezza attraverso un maggiore coinvolgimento nelle tematiche di formazione sulla sicurezza e nei progetti di sviluppo del business.

Bibliografia

Bombelli M.C. e Finzi E. (a cura di) (2008), *Oltre il collocamento obbligatorio*, Milano, Guerini e Associati.

Costabile G. (2005), *Information security in azienda*, Forlì, Experta.

Costabile G. (a cura di) (2005), *Sicurezza e privacy: dalla carta ai bit,* Forlì, Experta.

Costabile G., Mazzaraco G., Attanasio A., Graziani M., De Bernardo A. e Marras M. (2010), *Computer Forensics aziendale: Fondamenti delle best practice aziendali e ruolo della policy aziendale*. In G. Costabile e A. Attanasio (a cura di), *IISFA Memberbook 2010 Digital Forensics*, Forlì, Experta.

Costabile G., Mazzaraco G., Attanasio A., Graziani M., De Bernardo A. e Marras M. (2010), *Computer Forensics aziendale: Fondamenti delle best practice aziendali e ruolo della policy aziendale*. In G. Costabile e A. Attanasio

[5] S. Cuomo e A. Mapelli, *Diversity management*, Milano, Guerini e Associati, 2007; M.C. Bombelli e E. Finzi (a cura di), *Oltre il collocamento obbligatorio*, Milano, Guerini e Associati, 2008.

(a cura di), *IISFA Memberbook 2010 Digital Forensics*, Forlì, Experta.
Cuomo S. e Mapelli A. (2007), *Diversity management*, Milano, Guerini e Associati.
School of Management del Politecnico di Milano (2008), *ICT Security: quale governance*? *ICT accessibile e Disabilità: una fotografia della situazione in Italia*, Milano.

Abstract

The Company's assets also include information technology and assistive technologies. Due to the inclusion of persons with disabilities in the work place, the company that corresponds to a series of assets organised by the entrepreneur to engage in business acquires greater value. This value must be protected for the benefit of the workers, above all the workers with a disability, who need to be aware of the use of technologies. The article also highlights the role played by the Diversity Manager who works with the Security Manager.