ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

Business Continuity: come prevenire i disastri applicando le normative

David D'Agostini, Antonio Piva, Attilio Rampazzo

1. Introduzione

Molti fatti, si pensi per esempio al *black-out* nazionale del 16 settembre 2003 causato da problemi IT e non da mancanza di energia, stanno portando le organizzazioni a porre una particolare attenzione sulla Continuità Operativa conosciuta tra gli addetti ai lavori come *Business Continuity*.

Il D.Lgs 196/2003, meglio noto come Codice della Privacy, recependo i provvedimenti comunitari 96/45/CE e 2002/58/CE ha previsto che il trattamento di dati personali effettuato con strumenti elettronici sia consentito solo se sono adottate procedure per la custodia di copie di sicurezza e il ripristino della disponibilità dei dati ed dei sistemi[1]. La maggior parte dei sistemi IT delle aziende non sono comunque preparati a gestire un blocco delle infrastrutture di business superiore ai sette giorni[2].

Altre normative di settore, emanate sempre negli ultimi anni, prevedono l'adozione di un sistema di continuità operativa. Infatti la *Business Continuity* ormai non risulta solo un'esigenza interna alle organizzazioni, bensì è oggetto di precise richieste settoriali, come per esempio le Linee Guida per la continuità di servizio emanate da Banca d'Italia nel 2004 o le Disposizioni di Vigilanza di Banca d'Italia del 21/3/2007, oppure i quaderni del Centro Nazionale per l'Informatica nella pubblica Amministrazione (CNIPA) sulla continuità operativa nella Pubblica Amministrazione e, infine, la Direttiva Europea per le Infrastrutture Critiche (2008/114/CE dell'8 dicembre 2008).

L'origine della Gestione della Continuità Operativa è spesso ricondotta al *Disaster Recovery* specialmente se si considerano i sistemi IT, ovvero al ripristino dei sistemi IT e delle informazioni dopo un "disastro". Persino i termini "*business continuity*" (continuità operativa) e "*disaster recovery*" vengono spesso confusi: alcune persone li usano per indicare la stessa cosa, per altri significano cose completamente diverse. Altri termini quali: valutazione del rischio, analisi dell'impatto sull'organizzazione (BIA, o *Business Impact Analysis*), gestione delle crisi, gestione degli incidenti, ridondanza, sicurezza, protezione e *governance* sono stati via via aggiunti a questa miscellanea.

Esistono poche norme in tutto il mondo sulla continuità operativa, soprattutto perché è considerata ancora un concetto relativamente nuovo. Tra le norme/leggi/guide che esistono nel mondo, comunque, molte fanno riferimento alla Gestione

[1] Per una completa trattazione si rinvia al numero 2 del giugno 2008, al numero 2 di giugno 2007, al numero 1 di marzo 2004, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

[2] È questo il riscontro emerso da Gartner Group citato in: "La sicurezza condotta dall'IT è destinata a diventare un ricordo?", News Letter Clusit del 28 febbraio 2008.

della Continuità Operativa (GCO o *Business Continuity Management*, BCM), anche se non utilizzano necessariamente la stessa terminologia. Tra queste norme esistenti si annoverano:

- NFPA 1600 della *National Fire Protection Association* degli USA: questo standard è stato sviluppato dalla lotta agli incendi e vede la continuità operativa da una prospettiva di divieto di accesso;
- HB 221 e HB 292/293: lo standard australiano per la BCM e la guida alla gestione della continuità operativa;
- AS/NZS 4360:2004 una norma in comune tra Australia e Nuova Zelanda, abbinabile al HB 436 per una linea guida alla gestione del rischio;
- NIST *special publication*. 800-34 fornisce le istruzioni, i consigli pratici, le considerazioni per implementare e gestire un *Contingency Planning*[3];
- SPRING TR 19: il riferimento tecnico di Singapore per la gestione della continuità operativa, che si occupa soprattutto degli aspetti tecnici dei sistemi BCM;
- *The King II report of Corporate Governance*: queste linee guida sudafricane sulla gestione del rischio considerano la BCM da un punto di vista di *governance* (governo e gestione dei Sistemi informativi);
- *The Civil Contingencies Act 2004*: questa legge è entrata in vigore nel Regno Unito nel 2004 a seguito dell'approvazione reale (*Royal Assent*) e fornisce una guida alla BCM;
- ISO 27002: una norma per i sistemi di gestione della sicurezza delle informazioni che gestisce e minimizza le minacce alle informazioni[4];
- ISO 22399: una linea guida per la consapevolezza e la preparazione agli incidenti e la gestione della continuità operativa.

In Inghilterra a inizio secolo nasce il *Business Continuity Institute* (BCI), il primo organismo al mondo sull'argomento, che offre accreditamento professionale nel campo della continuità operativa e ha oltre 4.000 membri in più di 85 Paesi: nel 2002 il BCI ha emesso le sue prime Linee Guida di Buona Pratica redatte con la collaborazione di molti esperti del settore. Queste Linee Guida hanno fornito l'ossatura sulla quale si sono modellate le prime attività del BSI (*British Standards Intitution*, ente di normazione britannico) nel campo della gestione della continuità operativa, che hanno portato all'emissione di una specifica sulla *Business Continuity* denominata PAS 56. Nel 2006 la pubblicazione della BS 25999-1 che sostituisce la PAS 56, e successivamente nel 2007 la pubblicazione della BS 25999-2 hanno posto le basi per una nuova famiglia di norme per il mondo anglosassone (anche se già riconosciute a livello mondiale) sulla *Business Continuity*.

La Norma BS 25999 è composta da due parti: la prima elenca i "*consigli pratici*" fornendo la guida e gli obiettivi della norma oltre a spiegare esattamente il campo di applicazione della Gestione della Business Continuità; la seconda parte contiene le specifiche a fronte delle quali le organizzazioni possono essere certificate, dettagliando i requisiti per implementare, documentare e migliorare un Sistema di Gestione della *Business Continuity* (o Sistema di Gestione della Continuità Operativa). In buona sostanza: la parte 1 è il "*dovrebbe*", mentre la parte 2 è il "*deve*".

Il lancio della BS 25999-1, il codice di pratica, ha senza dubbio modificato l'opinione diffusa che la Gestione della *Business Continuity* (BCM) non avesse alcun vantaggio rispetto ad altre discipline di gestione. Una nuova norma raramente viene accolta con un entusiasmo, essendo spesso percepita più come "un aggravio burocratico" che come un'opportunità imprenditoriale. Invece quando la bozza iniziale dei "consigli pratici" è stata diffusa pubblicamente per i commenti, il documento è stato scaricato 5.000 volte in tutto il mondo; prima di allora, nella storia ultracentenaria del BSI non si erano mai superate le poche centinaia. Ne è seguita un'enorme quantità di commenti da recepire prima che la norma potesse essere pubblicata. Molti dei commenti erano positivi, anche se una parte era ferocemente contraria ad una qualsiasi forma di norma in questo campo. Analogamente, la BS 25999-2, la norma che dettaglia i requisiti a fronte dei quali un'organizzazione può essere oggetto di *audit* e certificata, ha suscitato un incredibile interesse, così grande che il BSI ha dovuto organizzare un tour mondiale delle città più importanti, impazienti di saperne di più sulla nuova norma.

---

[3] Inteso come il processo attraverso il quale vengno pianificate le azioni da intraprendere in caso di incidenti, in modo che i servizi IT possano continuare a funzionare, o a riprendere a funzionare dopo un interruzione.

[4] Per una completa trattazione si rinvia al numero 3 di settembre 2008, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

Attualmente si sta lavorando in tutto il mondo per ottenere un'accettazione chiara e standardizzata della gestione della *Business Continuity*: è un compito arduo perché ciò che risulta applicabile in un settore o in uno Stato potrebbe non essere accettabile in un altro.
Negli USA, la *National Fire Protection Association* (NFPA) ha emesso un regolamento per la gestione delle emergenze e la risposta ai disastri mentre il *National Institute of Standards and Tecnologies* (NIST) ha emesso una linea guida sulla pianificazione degli eventi nel settore IT.
Non si tratta, tuttavia, di norme e quindi le organizzazioni non possono ottenere la certificazione che tanto desiderano: ne consegue che al momento la BS 25999-2 è l'unica norma che possa certificare un Sistema di Gestione della *Business Continuity*.

2. BS 25999-1:2006 Code of Practice for Business Continuity Management

Come già citato la Norma BS 25999-1 è una linea guida che stabilisce i principi, la terminologia e il processo per la gestione della continuità operativa e del business; la norma stabilisce le attività che risultano necessarie nella progettazione del processo di gestione della continuità operativa e i documenti da produrre e, inoltre, fornisce i passi necessari per mettere in atto il processo della continuità del business.
Questa norma è orientata a tutte le organizzazioni indipendentemente dalla dimensione, settore commerciale o tipologia e fornisce assistenza ai responsabili di gestione del programma della continuità del business. L'approccio si basa sull'analisi del contesto dell'organizzazione dove l'obiettivo è quello di capire quali sono i prodotti/servizi critici e a quali esigenze dei portatori di interessi (degli *stakeholder*) principali a questi sono collegabili; tale prima analisi formale porta a individuare quello che in termini di prodotti e servizi sarà il campo di applicazione del modello.
Il sistema proposto parte dall'analisi del rischio (identificazione, analisi e valutazione), per proseguire con l'individuazione degli aspetti di rischio che superano il livello di soglia valutato accettabile e che hanno influenza sulla *Business Continuity*, ossia la capacità di mantenere i livelli di servizio/prodotto collegati all'evento/crisi ed emergenza in atto. Se i rischi non sono collegabili ai suddetti livelli di servizio non rientrano nel modello di *Business Continuity* e nel relativo approccio sistemico: ciò, ovviamente, deve essere da un lato coerente rispetto al rapporto tra costo e beneficio e dall'altro rispettoso dei requisiti contrattuali, di legge e normativi.
Si devono definire per ogni rischio collegabile alla Gestione della *Business Continuity* tre documenti:
- piano di gestione incidenti (per minimizzare l'evento);
- piano per la *business continuity*;
- programma per il ripristino della situazione normale.

Il contenuto della Norma BS25999-1 è il seguente:
- *Scope and applicabilità*;
- *Terms and definitions*;
- *Overview of business continuity management (BCM)*;
- *The Business Continuity Management policy*;
- *BCM Programme Management*;
- *Understanding the organization*;
- *Determining business continuity strategy*;
- *Developing and implementing a BCM response*;
- *Exercising, maintaining and reviewing BCM arrangements*;
- *Embedding BCM in the organization's culture*.

La metodologia proposta dalla norma è suddivisa in fasi (capitoli): ogni fase, concepita per essere eseguita in sequenza, è costituita da specifiche attività che implicano l'utilizzo di strumenti/tecniche. L'insieme completo delle fasi costituisce il processo di *Business Continuity Management*, contraddistinto dall'essere un processo continuo che evolve nel tempo e recepisce i mutamenti di business, organizzativi e tecnologici delle realtà in cui è applicato.
Il ciclo di vita della Gestione della *Business Continuity* (o Continuità Operativa), rappresentato nella figura 1, comprende sei elementi:
- programma della Gestione della *Business Continuity* (cap. 5);
- comprendere l'attività / analizzare l'organizzazione (cap. 6);
- determinare la strategia della Gestione della *Business Continuity* (cap. 7);
- sviluppare e implementare la Gestione della *Business Continuity* (cap. 8);
- mettere in pratica, mantenere e revisionare la Gestione della *Business Continuity* (cap. 9);
- incorporare la Gestione della *Business Conti-*

FIGURA 1

Il ciclo di vita della Continuità Operativa (BS 25999-1:2006)

nuity nella cultura dell'organizzazione (cap.10). Tutte le fasi (esposte nei capitoli della norma) sono molto importanti nel ciclo di vita, tuttavia si evidenzia che il capitolo 5 rappresenta il cuore, come dice la norma, di tutto il processo di Gestione della *Business Continuity*: il programma deve definire tutti gli aspetti organizzativi necessari ad assicurare che le attività richieste per la realizzazione della *Business Continuity* siano realizzate nei modi e nei tempi richiesti dall'Organizzazione.

Altro capitolo di rilievo è il 10 nel quale viene evidenziato che, per avere successo, la *Business Continuity* deve diventare parte del modo in cui l'organizzazione viene gestita, indipendentemente dalla dimensione/settore. Infatti nel disegno del ciclo di vita del BCM risulta evidente come questa fase avvolga tutta l'attività di Gestione della *Business Continuity*.

Per gli addetti ai lavori, specialmente dell'ambiente IT, abituati a valutare il *Disaster Recovery* o la *Business Continuity* di un sistema IT tramite i due indici *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO), nella nuova norma hanno trovato un nuovo indice: *Maximum Tolerable Period of Disruption* (MTPOD), mentre non è fatto cenno dell'RPO.

L'MTPOD è la durata massima dopo la quale un'organizzazione sarà irrevocabilmente minacciata se la sua operatività non può essere ripresa, mentre l'RPO è il massimo tempo fissato per l'indisponibilità di un prodotto, del servizio o di un'attività, ovvero il tempo entro il quale il prodotto, servizio, attività da proteggere deve essere ripristinato dopo un incidente, con l'attenzione che l'RTO deve essere sempre inferiore all'MTPOD.

3. BS 25999-2:2007 Requisiti Sistema di Gestione della Business Continuity

La BS 25999-2 fornisce le indicazioni e i requisiti per la messa in esercizio di un Sistema di Gestione della *Business Continuity* (o Gestione Operativa) certificabile.

I contenuti della norma sono riassunti nell'indice seguente:

- *Scope and applicability*;
- *Terms and definitions*;
- *Planning the business continuity management system (cap. 3)*;
  - *General*;
  - *Establishing and managing the BCMS*;
  - *Embedding BCM in the organization's culture*;
  - *BCMS documentation and records*;
- *Implementing and operating the BCMS (cap. 4)*;
  - *Understanding the organization*;
  - *Determining business continuity strategy*;
  - *Developing and implementing a BCM response*;
  - *Exercising, maintaining and reviewing BCM arrangements*;
- *Monitoring and reviewing the BCMS (cap. 5)*;
  - *Internal audit*;
  - *Management review of the BCMS*;
- *Maintaining and improving the BCMS (cap. 6)*;
  - *Preventive and corrective actions*;
  - *Continual improvement*.

La BS 25999-2:2007 è strutturata macroscopicamente in 3 blocchi di requisiti:

- dal capitolo 0 al capitolo 2: requisiti introduttivi e di spiegazione della norma (come quasi tutte le norme);
- dal capitolo 3 al capitolo 6: requisiti applicativi del BCMS;
- allegati.

All'interno dei capitoli (detti anche *requisiti* o *clausole*) dal 3 al 6 sono distribuiti i veri e propri requisiti applicativi per il Sistema di Gestione della *Business Continuity* (BCMS).

Lo schema di figura 2, sebbene non esaustivo, fornisce un'indicazione di massima dei capitoli

FIGURA 2
Capitoli dei requisisti della norma con i relativi collegamenti al ciclo PDCA

dei requisisti della norma con i relativi collegamenti al ciclo *Plan-Do-Check-Act* (PDCA – ciclo di DEMING). In buona sostanza il ciclo PDCA è il motore dello standard BS 25999-2:2007 come tutte le norme che hanno preceduto questo standard (ISO 9001:2000, ISO 14001:2004, ISO 20000-1:2005, ISO 27001:2005).
L'infrastruttura di Gestione della *Business Continuity* si basa quindi sul ciclo di continuo di miglioramento *Plan-Do-Check-Act* (Figura 3) applicato in modo continuativo su più livelli dell'organizzazione e sull'approccio sistemico allo scopo di identificare, capire e gestire i processi tra loro correlati contribuendo all'efficacia ed all'efficienza dell'organizzazione nel conseguire i propri obiettivi.
Il capitolo 3 relativo alla fase *PLAN* prevede come stabilire la politica di *Business Continuity*, gli obiettivi, i controlli, i processi e le procedure pertinenti per gestire i rischi e migliorare la *Business Continuity* al fine di produrre risultati conformi alle politiche e agli obiettivi generali dell'organizzazione.
Il capitolo 4 relativo alla fase *DO* prevede di attuare e rendere operativa la politica della *Business Continuity*, i controlli, i processi e le procedure.
Il capitolo 5 relativo alla fase *CHECH* prevede di valutare e, ove applicabile, misurare le prestazioni a fronte della politica della *Business Continuity*, degli obiettivi e delle esperienze pratiche, quindi riportare i risultati alla direzione ai fini del riesame e del miglioramento.
Il capitolo 6 relativo alla fase *ACT* prevede di mantenere attivo, aggiornato e migliorato il BCMS intraprendendo azioni correttive e preventive, basate sui risultati delle verifiche/riesame e sulla rivalutazione del campo di applicazione, della politica e degli obiettivi del Sistema di Gestione della *Business Continuity*.
Ne consegue che un Sistema di Gestione della *Business Continuity* (BCMS) conforme alla BS 25999-2, deve soddisfare i seguenti capisaldi (cfr. requisito 3.1 della norma):
❑ definizione di campo di applicazione, politica ed obiettivi;

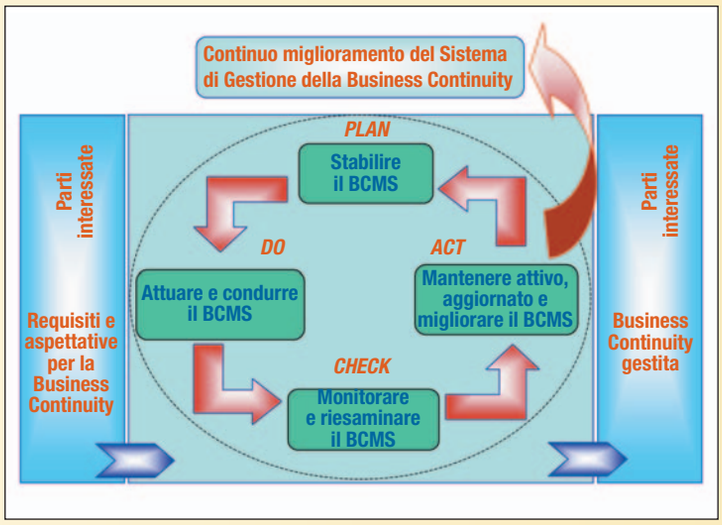

FIGURA 3
Ciclo PDCA come modello di riferimento per la descrizione dei processi e dei requisiti dello standard

❑ allocazione di risorse;
❑ attribuzione di ruoli e responsabilità;
❑ consistenza del sistema documentale e coerenza col campo di applicazione;
❑ accuratezza della *Business Impact Analysis* e del *Risk Assessment*;
❑ preparazione di adeguati piani di *Business Continuity* e di *Incident Management*;
❑ evidenza dell'implementazione del BCMS, sia nelle sue componenti operative (policy, procedure, istruzioni tecniche), che organizzative (*job description, audit* interni, *management review*).
Si rilevano sia l'efficacia del BCMS nel raggiungere gli obiettivi di continuità operativa stabiliti in Politica, sia l'efficienza del medesimo nel migliorare la gestione dei processi operativi nei tre possibili "stati" definiti dalla BS 25999:
• risposta agli incidenti;
• gestione della continuità;
• ripristino della normalità.
In questo ambito deve essere prestata molta attenzione all'esercizio (prova) dei piani di *Bu-*

siness Continuity (requisito 4.4.2 della Norma), il quale consente di essere certi che quanto pianificato trovi un'efficace attuazione in caso di incidente; per essere attendibili e verosimili, i test dei piani devono riprodurre quanto più fedelmente possibile la situazione ipotizzata.

4. Conclusioni

Lo standard BS 25999 risulta ancora giovane e dovrà maturare ulteriormente per la sua accettazione a livello mondiale, per essere con tutta probabilità adottato dall'ISO.
A meno di due anni dalla sua applicazione si contano già numerose aziende, che in tutto il mondo, lo hanno adottato e hanno conseguito la certificazione di BSI tramite accreditamento UKAS[5]: si tratta di circa una cinquantina di soggetti (nella Tabella 1 sono esposte il numero di aziende per nazione) e tra queste anche un'organizzazione italiana[6].

Nazione	n° aziende	n° siti
Brasil	1	1
India	6	61
Italy	1	1
Japan	3	19
Mexico	1	1
Netherlands	1	1
Poland	2	11
South Korea	3	3
Spain	1	1
Sweden	1	1
Taiwan	3	4
UAE	1	24
United Kingdom	21	43
U.S.A.	4	11
Totali	49	182

TABELLA 1
Le certificazioni BS 25999- 2 emesse da BSI sotto accreditamento UKAS, Fonte: BSI Group - United Kingdom (agg. al 20 agosto 2009)

Da ultimo l'ente normatore anglosassone a fine settembre 2008 ha pubblicato la versione draft di una nuova norma con i "consigli pratici per la continuità delle tecnologie dell'informazione e della comunicazione" per organizzazioni sia pubbliche che private. Tale proposta nasce dalla necessità di nuove specifiche di continuità per le organizzazioni con dipendenza dalle tecnologie dell'informazione e della comunicazione (ICT).
La nuova BS 25777, pubblicata recentemente, mira a colmare questa lacuna individuata da BSI, sostituirà la PAS 77 pubblicata nel 2006 per fornire un orientamento sulla continuità IT: per i suoi contenuti andrà a fiancheggiare la BS 25999-1 e integrerà il ciclo di vita del BCM con il nuovo ciclo di vita del BCM in ambiente ICT.
Anche l'ISO, ente internazionale, non è rimasto indietro: acquisendo le esperienze degli enti nazionali (Australia, Israele, Giappone, Inghilterra e Stati Uniti) ha aperto più progetti per nuove norme sull'argomento tra le quali:
- ISO/IEC CD 27031 ICT *readiness for Business Continuity*;
- ISO/PAS 22399:2007 *Societal security - Guideline for incident preparedness and operational continuity management*;
- ISO/CD 22301 *Societal security - Preparedness and continuity management systems – Requirements*.

Bibliografia

[1] BSI BS 25999-1:2006 *Business continuity management. Code of practice*.

[2] BSI BS 25999-2:2007 *Business continuity management. Specification*.

[3] BSI BS 25777:2008 I*nformation and communications technology continuity management. Code of practice*.

[4] BSI PAS 56:2003 - *Guide to Business Continuity Management*.

[5] Ente britannico di accreditamento organizzazioni di certificazione: www.ukas.com

[6] È l'ICCREA, istituto Centrale delle Banche di Credito Cooperativo che ha voluto mettere a frutto il lavoro svolto per aderire alle disposizioni della Banca d'Italia e nel giugno 2008 ha conseguito la certificazione del suo Sistema di Gestione della *Business Continuity*.
Si noti che altri organismi indipendenti di certificazione stanno proponendo la certificazione; infatti sempre in Italia un'altra organizzazione del mondo finanziario la SIA-SSB ha conseguito la certificazione tramite DNV (*Det Norske Veritas*).

[5] BSI PAS 77:2006 - *IT Service Continuity Management. Code of Practice*.

[6] Business Continuity Institute – *GPG 2008 Good Practice Guidelines A framework for Business Continuity mgmt*.

[7] ISO/IEC 27001:2005 - *Security techniques - Information security management systems - Requirements*.

[8] ISO/IEC 27002:2005 – *Information tecnology – Security tecniques – Code of practice for information security management*.

[9] CNIPA - Quaderno n. 28 del 6/2006: *Linee guida per la continuità operativa nella PA*.

[10] CNIPA - Quaderno n. 35 del 8/5/2008: *La continuità operativa nella PA - Casi di studio*.

[11] ISCOM - *Gestione delle emergenze locali*.

[12] Banca d'Italia: *Gestione della continuità operativa*. Bollettino di Vigilanza luglio 2004.

[13] ABI Lab: *Metodologia per la realizzazione del piano di continuità operativa*.

[14] ENISA: *IT & Business Continuity Overview and implementation principles*.

[15] ENISA: *How to raise information security awareness*.

[16] Quaderno n. 28 AICQ – Comitato per la Qualità del Software e dei Servizi IT: *La Gestione della Continuità Operativa: dal Disaster recovery, alla Business Continuity ad un Sistema di Gestione della Business Continuity*.

DAVID D'AGOSTINI avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it

ANTONIO PIVA, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.
E-mail: antonio@piva.mobi

ATTILIO RAMPAZZO, consulente di Sistemi Informativi e Sicurezza delle Informazioni in AlmavivA Finance SpA. Ha maturato un'esperienza più che trentennale nello sviluppo e conduzione di progetti informatici in ambito bancario e finanziario, nei quali la qualità e la sicurezza hanno ricoperto un ruolo determinante. È Vice Presidente del Comitato AICQ "Qualità del Software e dei Servizi IT", valutatore Sistemi di Sicurezza delle Informazioni R.G.V.I. (AICQ_SICEV certificato n.3), socio AIPSI-Associazione Italiana Professionisti Sicurezza Informatica.
E-mail: attilio@rampazzo.it