



4tech+ 4you

La newsletter di 4tech+

Edizione Gennaio 2007



In questo numero:

**Information Security e
Broadcasting**

Messaging framework

Profilo di 4tech+

Socio fondatore di

Sh@ng

CONSORTIUM

Information security. Un concetto globale.

Dalla sicurezza delle informazioni
alla certificazione BS7799 - ISO27001

Il cammino per proteggere i dati sensibili delle organizzazioni si gioca a tutto campo, e non concerne solo l'ambito della protezione in senso stretto, in particolare riferita al contesto tecnologico, ma si estende ad altri campi di applicazione rispetto all'azienda e alle sue attività.



Nell'era di Internet, i beni intangibili si affiancano per importanza ai beni materiali e proteggere le informazioni diventa una necessità, proprio come mettere il denaro nei caveau o i gioielli nelle casseforti, oppure il grano nei silos. Ci si aspetterebbe quindi che, contestualmente all'utilizzo del personal computer e della rete, le relative misure di protezione siano state adottate da parte di tutti gli interessati. Non è così: la consapevolezza dell'importanza di proteggere le "informazioni" è solo fenomeno recente e non sempre affrontato nel modo corretto: quando, spinti più dalla necessità che dalla volontà, s'interviene, magari anche solo per salvare l'apparenza, lo si fa a livello tecnologico; si demanda il problema agli specialisti e gli investimenti riguardano soltanto il minimo indispensabile: il firewall, l'antivirus...



Anche dal punto di vista legislativo e normativo la sicurezza dell'informazione è sempre stata trattata come un comparto specialistico dell'Information and Communication Technology, con leggi e regolamenti dedicati (firma elettronica, archiviazione ottica...).

Parimenti, le normative volontarie (gli standard) dedicate alla sicurezza informatica sono sempre state rivolte all'aspetto puramente tecnologico: anche quando si occupavano di processi aziendali, sotto la lente finivano solo quelle del settore IT: vedi, a parte i Common Criteria per la certificazione di prodotti e sistemi, la ISO 13335 che definisce i "GMITS" Guidelines for the Management of IT Security.

Questo anche se da anni, da quel testo fondamentale che è "Computer Crime and Business Information" di James Schweitzer (1986), si era già messo in rilievo che la sicurezza delle informazioni non si ottiene solo affidandola agli specialisti di sistemi informatici, ma assegnando responsabilità, adottando politiche e procedure e facendola diventare oggetto di attenzione del vertice aziendale. Con la conseguenza che trattare di "protezione delle informazioni" non è più una responsabilità degli specialisti, ma diventa oggetto di un sistema di gestione dei processi.

Gestire le informazioni

Come quelli già noti per la qualità (Quality Management System) e per l'ambiente (Environment Management System), ecco l'emergere degli ISMS (Information Security Management Systems), o all'italiana SGSI (Sistemi di Gestione della Sicurezza delle Informazioni).

Negli ultimi anni però, con leggi quali il Testo Unico sulla Privacy, le normative settoriali quali Basilea 2 e persino con la legislazione americana quale il Sarbanes Oxley Act (valido solo per gli USA, ma

con ricadute su tutte le società quotate al NYSE o NASDAQ e sicuramente cogente per le loro affiliate europee), la sicurezza informatica è uscita dal ghetto tecnologico: finalmente il legislatore pone l'accento sul dato più che sul database e sulle modalità di trattamento più che sulla transazione.

In questi ultimi anni la sicurezza informatica è uscita dal ghetto tecnologico: finalmente il legislatore pone l'accento sul dato più che sul database e sulle modalità di trattamento più che sulla transazione.

E, visto che sulla sicurezza delle informazioni s'investe solo quando si è "scottati" direttamente oppure perché allarmati da messaggi multimediali, ma soprattutto quando si è spinti da leggi e norme (e dalle relative sanzioni...), ecco che cresce l'attenzione agli aspetti complessi della sicurezza informatica. Anche se ancora poche organizzazioni si sono dotate di un SGSI formale, molte si accorgono che gli interventi minimi sono solo condizione necessaria, ma assolutamente non sufficiente. L'ISMS, al pari degli altri sistemi di gestione, non è un'entità astratta che ogni organizzazione può interpretare a suo piacimento, ma deve rispondere ad una serie di domande (i "controlli") che la normativa di settore più diffusa, la BS7799, ha identificato da tempo e per prima. La BS7799 (le cui evoluzioni normative saranno trattate più avanti) nasce in Inghilterra, dal British Standard Institute (il corrispondente inglese del nostro UNI) come raccolta di "best practices" (le migliori prassi) in essere presso quelle organizzazioni particolarmente sensibili ed efficaci nella salvaguardia delle informazioni: queste migliori prassi vennero raccolte e codificate nella normativa, emessa per la prima volta nel 1995.



Come premessa, la BS7799 definisce l'Informazione come un bene primario aziendale: per certi versi è solo un'ovvia conseguenza, in un mondo in cui perfino il denaro non è più costituito solo da biglietti e monete, ma ormai è rappresentato da una sequenza di bit. Come però si accennava non è immediato identificare come patrimonio un bene comunque immateriale. L'Informazione può assumere diverse "forme": non solo quella elettronica (comunque quella più sfuggente) ma cartacea, multimediale e perfino verbale. E in qualsiasi forma l'Informazione si presenti, corre dei rischi: di perdita, di manipolazione, di modifica, d'indisponibilità.

E proprio l'approccio per "rischi" è l'ulteriore, innovativa caratteristica della BS7799: la classificazione dell'importanza dell'Informazione deriva da una formale valutazione del rischio secondo le tre fonti per i requisiti di sicurezza:

- i rischi per l'organizzazione e le sue infrastrutture IT (fuga d'informazioni dovute ad accessi indesiderati alla rete, modifiche di parametri o transazioni, distruzione di informazioni in seguito a cancellazione o crash...);
- i requisiti legali, statutari, regolamentari, contrattuali (regole per la licenza e la copia del software, conservazione dei record bilancistici, protezione dei dati sensibili...);
- i processi di business (standard e obiettivi aziendali, metodi informatici per la qualità del prodotto, uso della posta elettronica..).

L'approccio per "rischi" è l'innovativa caratteristica della BS7799

Il processo di analisi dei rischi, e la decisione sul come affrontarli, dà origine alla selezione dei controlli da implementare e che ciascuna organizzazione raggrupperà nella propria Dichiarazione Di Applicabilità.

La parte prima del BS7799 è divenuta già nel 2000 uno standard internazionale ISO (la ISO/IEC 17799). La norma ISO, come negli altri Sistemi della ISO9000 e ISO14000, pone in primo piano gli aspetti gestionali della sicurezza, introducendo il fondamentale concetto di sistema di governo della sicurezza (ISMS) e l'altrettanto fondamentale "ciclo di Deming" (Plan-Do-Check-Act). L'ISMS di un'azienda è costituito dall'assegnazione delle responsabilità, dalla politica di sicurezza aziendale, dalla specificazione dei controlli di sicurezza (logici, fisici, procedurali) necessari per farla rispettare e dal modo in cui questi devono essere realizzati.

Un'azienda che abbia implementato e "impiantato" l'ISMS può richiedere una certificazione formale che ne attesti pubblicamente la bontà. Il certificato viene rilasciato a seguito di un processo di revisione condotto da un'entità indipendente e di riconosciuta competenza ed attesta che l'azienda ha adottato un approccio alla sicurezza dell'informazione sensato, proporzionato al valore dei beni da proteggere e allineato con le migliori pratiche di sicurezza note.

Il metodo della BS7799

Senza pretendere di addentrarsi né nel processo di analisi dei rischi né nell'elencazione dei controlli, è però opportuno ricordare che, anche in assenza di motivazioni forti per la certificazione formale, la metodologia descritta dalla BS7799 è assolutamente valida per qualsiasi organizzazione che sia sensibile al problema di proteggere le proprie informazioni o, a maggior ragione, quelle del cliente o del cittadino.

Si prenda come esempio il Testo Unico della Privacy: una volta che ci si dedichi alla sua parte concreta, il Disciplinare, si verifica l'estrema attinenza tra la vision della BS7799 (che si dedica a tutti i dati) e la 196/2003 (che è ovviamente rivolta alla salvaguardia di un solo subset di dati, anche se importanti come quelli personali e sensibili) e che la metodologia BS7799 è assolutamente coerente con la risoluzione del "problema privacy". Le relazioni tra Documento Programmatico della Sicurezza e Politica/Dichiarazione di Applicabilità sono strette e dimostrabili: in entrambi i casi le "best practices" richiedono la nomina dei responsabili, l'analisi organizzativa, il presidio sui dati, anche non elettronici, e la sicurezza delle aree fisiche...

La BS7799 non deve essere considerata solo per la formalizzazione (audit di terza parte) della certificazione dell'azienda o dell'organizzazione (percorso che è non semplice, e che quindi deve essere valutato con attenzione), ma rappresenta una metodologia assolutamente valida sempre: per esempio come metodo di gap analysis e di verifica formale per un audit interno (di prima parte) o richiesto dal cliente (di seconda parte).

Come detto, la BS7799 è già diventata, nella sua parte prima, normativa dell'ISO. La seconda parte, o per essere più precisi la BSI 7799 2002:2, è quella più operativa, con la descrizione dei controlli (attualmente in numero di centoventisette in dieci sezioni) da implementare, ed è quella di riferimento in questo momento.

Sono però in vista importanti novità: proprio in considerazione dell'importanza che il fenomeno della sicurezza informatica sta assumendo, l'attuale impianto normativo è in corso di revisione, senza stravolgere i principi base, in ambito ISO e il prossimo anno l'attuale BS7799 verrà più conosciuta come ISO 27001. Il set di procedure ISO 27000 avrà quindi la stessa valenza delle attuali ISO 9000 e ISO 140000, a sottolineare l'attenzione che una moderna organizzazione deve porre al tema della protezione delle informazioni.

In considerazione dell'importanza che il fenomeno della sicurezza informatica sta assumendo, l'attuale impianto normativo, senza stravolgere i principi base, è in corso di revisione in ambito ISO e il prossimo anno l'attuale BS7799 verrà conosciuta come ISO 27001.



I “motivi” della BS7799

La BS7799 è normativa volontaria, cioè un'organizzazione decide autonomamente d'implementarla (e l'ambito al quale applicarla) e magari d'intraprendere il processo di certificazione, mediamente un processo lungo e sicuramente non gratuito; ma quali possono esserne le motivazioni?

Proviamo ad identificarne qualcuna:

- La giustificazione dei costi: solitamente il termine sicurezza è direttamente messo in relazione a spese addizionali. È vero che non genera direttamente guadagno, ma il processo di analisi e gestione dei rischi genera, in modo diretto ed automatico, la giustificazione economica per i controlli di sicurezza.
- L'ottimizzazione degli investimenti: l'analisi tecnologica, essenziale al processo, identifica le vere priorità e le possibilità di “commonalities” aziendali.
- L'impatto organizzativo: il processo sicurezza interessa sia il management che il personale. Il management è responsabile di definire il livello di sicurezza/rischio che l'azienda intende accettare (indicazione che coinvolge anche scelte di business). Il reparto IT è responsabile della definizione dei controlli e delle applicazioni. L'analisi dei rischi gioca un ruolo proattivo nei gruppi implicati nel processo, intensificando il livello di comprensione delle necessità e i ruoli, raggruppando funzioni e persone con ruoli eterogenei e mettendole in relazione in termini di analisi del business.
- La creazione di un programma di “security awareness”: l'applicazione del programma di analisi e gestione su larga scala coinvolge in maniera attiva un gran numero di persone, inserendo così il tema sicurezza nell'agenda di molte riunioni aziendali ed incrementando il livello di consapevolezza del problema sicurezza nell'azienda intera.
- La coerenza tra i gruppi: uno dei maggiori risultati ottenuti è l'apporto di coerenza e obiettività nell'approccio alla sicurezza non solo tra diverse applicazioni IT, ma anche tra diverse unità aziendali.
- La protezione dell'immagine aziendale: in un contesto di mercato dove la fiducia del cliente (o la fidelizzazione del consumatore) ha una precisa valenza economica, la salvaguardia del “buon nome” non è più una questione di importanza secondaria.

Sono tutti obiettivi “interni”, raggiungibili col metodo BS7799, però forse sono più le spinte “esogene” ad essere motivanti:

- La protezione del business: quando la sopravvivenza stessa dell'organizzazione dipende esclusivamente o quasi da informazioni proprietarie (brevetti, IPR, progetti, economics...) la cui salvaguardia determina il “vantaggio competitivo” sui concorrenti.
- La conformità alle leggi e alle regole: (italiane: D-Lg 196/2003, richiama il DPR 318 del 28/7/99: “misure minime di sicurezza”; D-Lg L 518/1992 e n. 68/2003 “diritto d'autore”, “tutela del software”; DPR 513/97 “documento informatico e firma digitale”; DPR 445/2000, T.U. sulla documentazione amministrativa; L. 547/93: “criminalità informatica”; D.Lgs114/98: “aste on line”; D.Lgs185/99 “contratti a distanza”; D.Lgs169/99 “tutela banche dati”; e internazionali: Antiterrorismo; Basilea2; Sarbanes Oxley etc) non solo per le conseguenze sanzionatorie, ma, quando il processo di globalizzazione dei mercati e i relativi mutamenti socio/politici impongono ai legislatori una maggiore attenzione alla formalizzazione delle “regole” del mercato (e della comune convivenza), l'azienda moderna deve garantire ai suoi stockholders e stakeholders di operare in conformità alle normative nazionali e internazionali che la riguardano.
- Le richieste delle parti terze: in un mondo collegato o addirittura strettamente integrato in rete, i legami informativi con i clienti e i fornitori o con gli utenti e i cittadini sono così stretti da considerare in qualche caso i “loro” dati più importanti dei “nostri”.

Se quindi si ha l'esigenza di offrire ai cittadini/clienti servizi di sicurezza, di avere una garanzia circa la bontà delle scelte in caso di contenzioso, di avere una forma di tutela circa le scelte di sicurezza di fronte agli obblighi di legge, allora va valutata la necessità di una validazione formale della sicurezza aziendale attraverso un processo di certificazione ufficialmente riconosciuto.

Maurizio Mapelli

- *Segretario Associazione Italiana Per la Sicurezza Informatica [AIPSI]*
- *Senior Consultant 4tech+*



KM4

Il Messaging Kernel di 4tech+

La soluzione per le odierne necessità di messaggistica

Il contesto

Nel corso dell'ultimo decennio gran parte delle comunicazioni si è andata sempre più orientando verso la messaggistica: basti pensare a questo proposito allo sviluppo praticamente esponenziale dei sistemi SMS ed MMS e al loro utilizzo in molteplici, svariati settori di attività.

Lo sviluppo dei sistemi e dei mezzi di trasmissione e di ricezione ha ulteriormente accelerato questa tendenza, richiedendo di fatto una gestione della messaggistica sempre più orientata a caratteristiche di **immediatezza** e di **pervasività**.

Inoltre data la cadenza, pressochè annuale, con cui vengono proposti nuovi formati di trasporto per contenuti multimediali, la **modularità** è diventata una necessità stringente per qualsiasi sistema di supporto alla gestione di tali contenuti.

Verso tale emergente domanda **4tech+** ha realizzato **KM4**, un framework **modulare** e **distribuito**, in grado di offrire **servizi di messaging di base ed avanzati**.

La Modularità

KM4 è in grado di gestire qualunque tipologia di messaggio, dalle e-mail agli SMS o MMS, oltre a poter smistare e ricevere in tempo "utile" messaggi ad hoc, destianti a o provenienti da impianti di rilevamento dati di tipo industriale.

Il framework **KM4** supporta tutti i principali protocolli attualmente disponibili: SMPP, UCP, CIMD, HTTP, MM4, MM7, EAIF, SMTP, Web Services ed altri esistenti o a venire.

I messaggi ed i protocolli sono incapsulati in una struttura completamente agnostica che rende indipendente il servizio sia dalla tipologia del messaggio che dal relativo trasporto. Una tipologia di messaggio, così come di trasporto, viene gestita dal framework come un plugin; è quindi possibile in qualsiasi momento aggiornare o aggiungere nuovi standard o integrare sistemi legacy.

I Servizi

I servizi messi a disposizione da **KM4** sono modulari, ciò significa che in qualsiasi momento è possibile aggiungere una nuova funzionalità, che potrà essere indipendente oppure inserita in un flusso di elaborazione già presente.

La potenza dove serve, quando serve

Modularità e flessibilità sono caratteristiche che permettono di affrontare il mercato garantendo un'elevata velocità di risposta alle richieste prestazionali che il mercato stesso ogni giorno ci pone.

Nel mondo del messaging e più in generale della multimedialità com'è oggi concepita, ci si scontra anche con un altro tipo di problema: gli elevati volumi di traffico che l'odierna base d'utenza esige.

KM4 è un sistema completamente distribuito, in cui ogni servizio è erogato in modo cooperativo da tutti i nodi, logici o fisici, che lo compongono.

L'architettura si basa su una struttura di clustering multinodo, in grado di offrire elevate doti di affidabilità, scalabilità e bilanciamento dei carichi, oltre a garantire prestazioni di tutto rilievo.

Clustering multinodo significa possibilità di "**partire piccoli e crescere in funzione della domanda**", cioè garantire una configurazione sempre adeguata e sempre adeguabile alle necessità elaborative di qualsiasi realtà d'impresa, pur nel completo rispetto della massima attenzione ai costi.

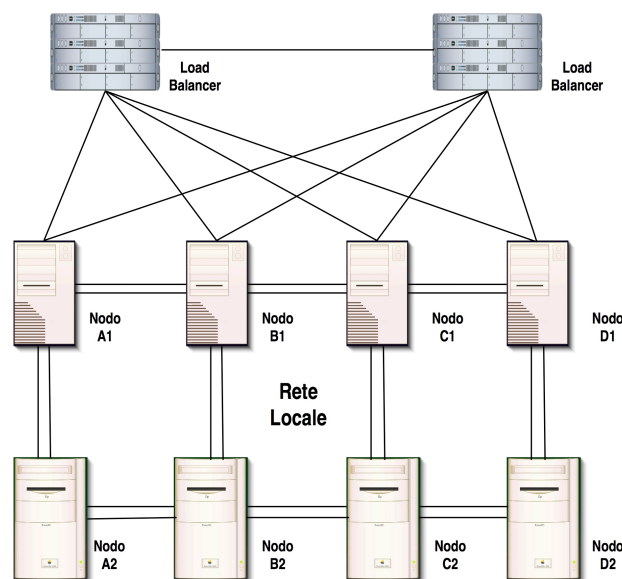


Fig.1 Struttura Clustering Multinodo: i nodi sono interconnessi con svariate modalità, di cui la più semplice ed economica è la Rete Locale (LAN).



La Sicurezza

KM4 supporta, ove il protocollo lo richieda, il trasporto sicuro dei dati via SSL.

Il framework è dotato di un proprio sistema di autenticazione ed accounting. Tale sistema può essere integrato, ove necessario, con sistemi esterni tramite i principali protocolli standard LDAP, RADIUS, DIAMETER, o attraverso l'implementazione di protocolli legacy.

Le Caratteristiche Principali

- **Operating System Independent:**
supporta Linux, Windows e tutti i principali sistemi Unix
- **DataBase Independent:**
supporta tutti i principali RDBMS presenti sul mercato, da PostgreSQL a MySQL, da Oracle a SQL Server
- **Funzionalità Cluster:**
supporto per DataBase in cluster distribuito e IN RAM DataBase

I Servizi Nativi

- **Message Gateway** con funzioni di instradamento dinamico e conversione automatica di formato
- **Message Push**

- **Adaptive Outbound, Throughput Balancing and Control**
- **Inbound Throughput Balancing and Control (Cutoff policies...)**
- **Gestione di Pushing Campaign** tramite schedulazione e liste contatti
- **Gestione Liste Contatti**
- **Gestione Librerie messaggi**
- **Composizione dinamica messaggi (on the fly)** per invii personalizzati
- **Allarmistica di sistema** via trap SNMP o MAIL

Utilizzi possibili (lista parziale)

- **Distribuzione di contenuti multimediali (file audio e video)**
- **Distribuzione di aggiornamenti software**
- **Gestione di campagne marketing via email, SMS/MMS, Web**
- **Comunicazioni interaziendali via terminali di varia natura**
- **Servizi d'informazione finanziaria online**
- **Servizi d'informazione sportiva online**

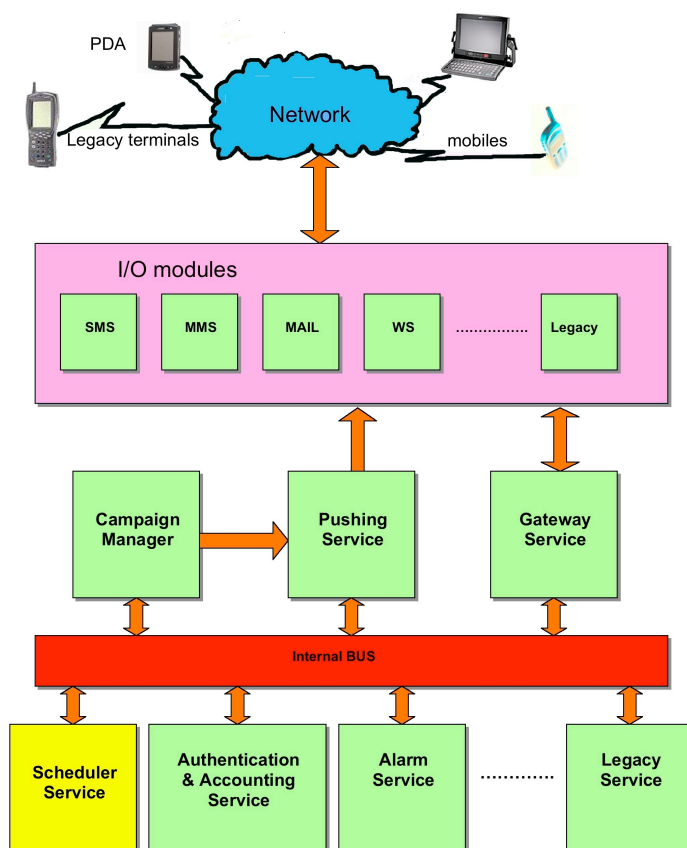


Fig. 2 Schema architetturale del framework **KM4**



Profilo di 4tech+

Caratteristiche salienti di una realtà di spicco nel settore ICT

Un nuovo e diverso approccio

Chi siamo

Quattro esperti ICT, uniti da un forte legame interpersonale, derivante da una solida amicizia e da una profonda stima professionale, conseguita in anni di intensa e fattiva collaborazione, decidono di intraprendere una nuova sfida e, nonostante il momento poco incoraggiante, nel marzo 2004 fondano insieme la Società **4tech+**.

Ai primi soci se ne aggiungono altri, che hanno in comune con quelli fondatori una competenza ultraventennale nel settore informatico e della consulenza operativa, unita ad una cospicua esperienza in posizioni manageriali ed imprenditoriali di alto profilo.

Un altro elemento fortemente qualificante che contraddistingue i soci è la visione di un nuovo e diverso approccio reale alle aspettative di chi sceglie di ricorrere all'uso di consulenza o di capacità progettuali esterne: approccio che, ponendo in primo piano l'etica del rapporto, mira ad individuare e contestualizzare innanzi tutto le esigenze del committente, per poi affrontarne le problematiche emerse con competenze di altissimo livello.

Dove operiamo

Da questo approccio deriva la selezione rigorosa degli ambiti su cui espletare strategicamente la propria attività: **4tech+** pertanto focalizza prevalentemente la sua attenzione su aree **tecnologicamente avanzate**, quali le architetture di rete, la business continuity, la sicurezza logica e biometrica e la gestione documentale, tutte rivolte a primari ambito di mercato.

Il nostro know-how

Business continuity

- Consulenza organizzativa e operativa
- Individuazione, tracciamento e analisi dei processi critici
- Disegno e utilizzo delle strutture di recovery

Sicurezza

- Identity management
- Anti-intrusione e protezione dati sensibili ad ogni livello
- Riconoscimento immagini 2D/3D ed alarming

Gestione documentale

- Archiviazione sostitutiva
- Virtualizzazione dei documenti fiscali
- Razionalizzazione degli archivi esistenti

Reti e tecnologie ICT

- Architetture di Broadcasting wired e wireless
- Sistemi Operativi mainframe, unix, windows
- Middleware, linguaggi e DBMS

Le modalità di erogazione

4tech+ svolge primariamente attività di consulenza e di progettazione.

Tutte queste attività vengono realizzate con l'utilizzo di figure consulenziali dotate di caratteristiche professionali ed attitudinali appropriate alle esigenze.

L'approccio preferenziale è quello team-oriented, ove la garanzia di qualità e di massima efficacia degli interventi è data dalle costanti presenza e supervisione di team leader di alto profilo.

Lo stile di lavoro

4tech+ crede nel successo e lo ricerca attivamente, sia internamente che presso i propri clienti.

Entusiasmo e visione positiva delle situazioni fanno parte del bagaglio culturale e comportamentale di tutti i nostri consulenti e dei nostri specialisti.

L'esperienza ci guida, la passione ci muove

Ogni nuova situazione è vista come una sfida e affrontata con coraggio e serenità, avendo costantemente presenti gli obiettivi del cliente e la messa in comune del patrimonio di esperienza derivante dal disegno e dalla realizzazione di nuove soluzioni, in particolar modo nei confronti dei giovani, che rappresentano il vero patrimonio nostro e dei clienti.

Un network di conoscenze

È una delle grandi ricchezze di **4tech+**, che ci mette in grado di intraprendere con sicurezza le missioni più difficili e critiche.

Le risorse con le le caratteristiche e le conoscenze adeguate esistono e noi sappiamo dove reperirle, grazie a questa vasta rete che si estende in ambiti diversi, da quello informatico a quello professionistico ed accademico.

Qualunque sia l'esigenza, **4tech+** è in grado di indirizzarla e di gestirla al meglio, mettendo in campo le giuste risorse, con le competenze più appropriate.

4tech+

**Knowledge for Advanced Technologies
Network @nd Security Solutions**





***“Simplify,
wherever possible,
the complex.”***