Forum delle Competenze Digitali

“Competenze nella sicurezza delle informazioni”

1° Rapporto

(marzo 2009)

Introduzione

Il Forum delle competenze digitali è un'Associazione senza scopo di lucro (vedi All.1) che promuove, valorizza ed accresce la diffusione della cultura e delle conoscenze in materia di competenze e professionalità nel settore dell'ICMT (Information, Communication & Media Technology) e delle Tecnologie Digitali. A tal fine il Forum promuove e mantiene rapporti con analoghe istituzioni degli altri Paesi e con la Commissione dell'Unione Europea.

Nell'ambito delle sue iniziative, ha costituito nel maggio 2008 un Gruppo di lavoro (vedi All. 2) , con l'obiettivo di analizzare le competenze specifiche richieste ai professionisti operanti nel comparto della sicurezza delle informazioni e di individuarne le certificazioni.

Il Gruppo ha raccolto ed analizzato la documentazione esistente in materia, a livello nazionale ed internazionale, e ha deciso di procedere per fasi concentrandosi, nella prima fase da giugno 2008 a febbraio 2009, sugli schemi di certificazione. In particolare, ha esaminato le tematiche riguardanti:

1. la ricognizione generale degli schemi di accreditamento e certificazione delle competenze ICT, con riferimento alla sicurezza delle informazioni;
2. l'individuazione di un metodo di mappatura basato sull'analisi delle principali certificazioni oggi presenti sul mercato;
3. la stesura di una lista delle principali certificazioni.

I risultati di tale esame sono oggetto del presente Rapporto redatto dal Gruppo di lavoro e approvato dal Consiglio Direttivo del Forum. Più precisamente in questo Rapporto, la prima tematica è trattata nel 1° Capitolo "La certificazione delle competenze nella sicurezza delle informazioni", curato dal componente del Gruppo Silvano Bari, in cui si analizza:

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

a) la tipologia e le diverse caratteristiche delle attestazioni concernenti le competenze del personale;

b) il processo di accreditamento e certificazione con riferimento alle varie figure coinvolte;

c) le norme e le guide di riferimento;

d) lo stato dell' arte delle certificazioni delle competenze nella sicurezza delle informazioni, distinte per tipologia.

La seconda e la terza tematica sono approfondite nel 2° Capitolo: "Ipotesi di mapping delle certificazioni delle competenze nella sicurezza delle informazioni", redatto con i contributi dei componenti del Gruppo Silvano Bari, Marco Bozzetti, Roberto Ferreri e Maurizio Mapelli, in cui sono illustrate:

a) la proposta di un metodo di mappatura delle certificazioni delle competenze tecniche, in materia di sicurezza delle informazioni;

b) le caratteristiche dei modelli di mappatura presi in esame, e cioè il modello EUCIP (sviluppato da CEPIS) ed il modello eCF (European Competence Framework). Viene, inoltre, illustrato anche il criterio di classificazione ISSA, basato sui campi di applicazione.

Nel 3° Capitolo, infine, è riportata la lista delle principali certificazioni in materia di competenze sulla sicurezza delle informazioni. E' da sottolineare, al riguardo, che la lista non è esaustiva e, comunque, è in continuo divenire e diversificazione.

In questa prima fase il Gruppo di lavoro, focalizzato sulla ricognizione delle competenze richieste dalle certificazioni, non ha approfondito gli aspetti organizzativi e di processo che, unitamente ad un'analisi valutativa delle certificazioni esistenti, saranno oggetto di un secondo Rapporto.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

INDICE

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Capitolo 1

La certificazione delle competenze nella Sicurezza delle Informazioni

1.1 La tutela del patrimonio informativo aziendale

La tutela del patrimonio informativo aziendale è un aspetto di rilevante importanza e criticità tra gli obiettivi aziendali ed ha reso necessario creare all'interno di numerose aziende una vera e propria funzione di Information Security oltre a ruoli specializzati nelle varie analisi e tecniche di prevenzione e riduzione del rischio legato ai crimini informatici. L'accresciuta rilevanza del problema è testimoniata anche dall'attenzione che i Legislatori, gli Organi di vigilanza, le Associazioni di categoria, ecc. hanno posto con l'emissione di leggi e norme che trattano, anche indirettamente, i concetti di Riservatezza, Integrità e Disponibilità delle Informazioni. La conseguente visione "olistica" della Sicurezza delle Informazioni ha portato, anche, ad un rapido mutamento dei "profili" degli addetti, precedentemente solo specialisti tecnici.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Pertanto l'azienda ha necessità di affidarsi a personale specializzato che si occupi a tempo pieno della tutela del patrimonio informativo e che sia in possesso di competenze idonee a gestire con efficacia i vari aspetti della Information Security. Di conseguenza è necessario inquadrare il livello di competenza di tali professionisti al fine di offrire al mercato un rilevatore immediato, oggettivo e garantito della professionalità di coloro che operano in questo ambito, tutelando in particolare le aziende che ricercano professionisti, o si avvalgono di consulenti esterni, dalla offerta di improvvisati esperti di Information Security.
Tutto questo può avvenire attraverso la certificazione delle competenze rilasciata da un Organismo di Certificazione del Personale.

Prima di descrivere specificamente la certificazione delle competenze in materia di Sicurezza delle Informazioni, è opportuno chiarire cosa si intende per "certificazione delle competenze", chiarendo quali sono le forme di attestazione che sul mercato vengono - talvolta impropriamente - definite certificazioni.

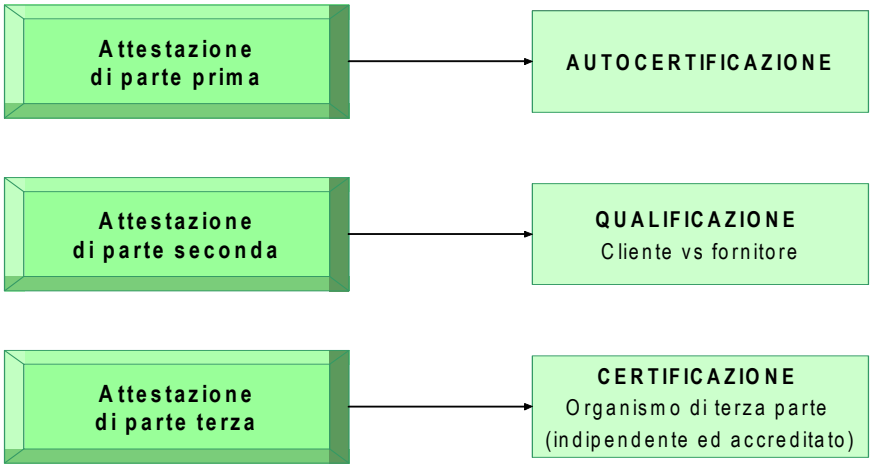
1.2 Le certificazioni delle competenze

Se un'Associazione (che non possiede i requisiti previsti, come vedremo, dalla norma ISO 17024, con particolare riferimento al coinvolgimento delle *parti interessate)* certifica i propri soci, effettua una certificazione "*di prima parte*".
Allo stesso modo, la dichiarazione fatta da un'azienda in merito alla professionalità di un suo dipendente è senz'altro valida ma è chiaramente una dichiarazione di parte e quindi può essere accettata solo con tutte le dovute riserve. In entrambi i casi si tratta di ***attestazioni di prima parte***.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

La qualificazione di un fornitore, fatta da un suo cliente a seguito di opportune valutazioni, è invece una ***attestazione di seconda parte*** (il cliente) verso l'altra parte (il fornitore): ha valore elevato nell'ambito dei loro rapporti di affari, ma minore verso il resto del mercato.

La ***certificazione di terza parte*** delle professionalità attesta che una determinata persona, valutata da una **terza parte indipendente,** secondo regole stabilite da precise norme, possiede i requisiti necessari e sufficienti per operare con competenza e professionalità in un determinato settore di attività.



La certificazione della competenza di una persona rilasciata da un Organismo di Certificazione di persone di terza parte, accreditato e controllato da un Ente di Accreditamento, è la vera certificazione delle competenze ed ha un valore assoluto sul mercato perché garantita, oltre che dall'Ente di Accreditamento, proprio dalla presenza dei rappresentanti delle Parti Interessate del mercato. Questa certificazione rappresenta, pertanto, per il cliente, la garanzia dell'effettiva competenza del professionista e, per la persona certificata, la possibilità di porsi sul mercato con indiscutibile riconoscimento delle proprie capacità.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

1.3 Il processo di accreditamento e certificazione delle competenze del personale in Italia

Vediamo in che cosa consiste, in particolare, il processo di accreditamento e di certificazione.

Innanzitutto, la certificazione è - in generale - un processo composito in cui agiscono, normalmente, vari soggetti e in cui sono definite alcune regole. Il processo di certificazione delle competenze del personale, in Italia, si fonda sui seguenti attori fondamentali:

- **La norma e le guide di riferimento** (UNI CEI EN ISO/IEC 17024:2004, IAF GD 24:2004, Regolamenti tecnici SINCERT).
- **Lo schema di accreditamento** (definito e gestito dall'Ente Accreditatore in base alle norme e guide di cui sopra) cui deve risultare conforme l'Organismo di Certificazione: nel nostro caso il SINCERT ha definito uno schema di accreditamento degli Organismi di certificazione delle competenze di personale denominato "PRS - Certificazione di personale".
- **L'ente Accreditatore**, che definisce le regole per la gestione dello schema di certificazione e che vigila sulla sua corretta applicazione da parte dell'Organismo di certificazione: in questo modo, l'Accreditatore fornisce "credibilità" al Certificatore. Nel nostro caso l'Ente Accreditatore è sempre il SINCERT.
- **Lo schema di certificazione**, che definisce la figura professionale e le competenze che il committente deve possedere per poter essere certificato; lo schema è predisposto, generalmente, dall'Organismo di certificazione stesso e viene riconosciuto dal SINCERT.
- **Il Certificatore**, che rilascia i certificati applicando correttamente lo schema. Fatti salvi i controlli interni, la vigilanza sull'organismo di certificazione è effettuata da SINCERT che controlla anche che l'organismo sia gestito attuando gli indirizzi dati da un comitato di parti interessate, costituito in modo equilibrato tra gli stakeholders.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

- **il Valutatore**, che esegue la valutazione delle competenze del personale e costituisce il braccio operativo del certificatore. Il Valutatore può consistere in personale interno dell'Organismo di Certificazione oppure, più spesso, in consulenti esterni dotati di particolare esperienza.
- **Il Committente della certificazione**, cioè la persona che richiede volontariamente tale atto.

In questo contesto, come detto in precedenza, si definisce “di terza parte” uno schema di valutazione e certificazione nel quale il Valutatore (se presente), il Certificatore e l’Accreditatore siano terza parte indipendente rispetto al Committente della certificazione.

1.4 La norma e le guide di riferimento

Bisogna precisare - anzitutto - che si è in assenza di obblighi di legge, pertanto sia il processo di certificazione della competenza di personale che il processo di accreditamento di un Organismo di certificazione è volontario.
I motivi alla base di una certificazione volontaria da parte di un professionista sono vari e verranno elencati parlando della figura del Committente della certificazione.
Per quanto riguarda il processo di accreditamento, l'Organismo che eroga le certificazioni di competenza del personale può scegliere volontariamente di dimostrare ad un Organismo "super partes" (opportunamente legittimato) il possesso dei requisiti di idoneità (istituzionali, organizzativi, tecnici e morali) che devono ispirare i suoi comportamenti come presupposto essenziale per la credibilità dei risultati forniti.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Un criterio oggettivo ed univoco di qualificazione di detti Organismi, ormai universalmente riconosciuto e condiviso, è rappresentato dalla rispondenza alle apposite Norme e Guide sviluppate su scala internazionale (*norme e Guide EA - European Cooperation for Accreditation in Europa; norme ISO/IEC e Guide IAF - International Accreditation Forum a livello internazionale*).

Nel caso della certificazione di competenza del personale è stata emanata la norma ISO/IEC 17024, "General requirements for bodies operating certification of persons", che stabilisce quali dovrebbero essere le caratteristiche di un Organismo di Certificazione di terza parte indipendente abilitato a certificare la competenza professionale del personale, a prescindere dalla competenza specifica che si vuole certificare. Tali requisiti sono, sostanzialmente, i seguenti:

- Indipendenza
- Trasparenza
- Imparzialità
- Assenza di conflitti di interesse
- Partecipazione nel Consiglio Direttivo dell'Ente di Certificazione delle *"parti del mercato interessate"*
- Equilibrio nelle decisioni (non deve essere possibile che prevalgano interessi particolari)
- Competenza
- Riservatezza
- Individuazione di un Codice Deontologico (da far sottoscrivere ai professionisti prima della certificazione e da far rispettare nel tempo)
- Durata delle certificazioni limitata e controllata nel tempo (e non a vita come per gli iscritti negli albi professionali)

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

- Concessione del rinnovo della certificazione (dopo un limitato periodo di tempo) solo se il professionista:
  - ha curato l'aggiornamento professionale previsto;
  - ha continuato a svolgere, nel periodo di tempo stabilito, l'attività professionale per la quale è stato certificato;
  - ha rispettato il codice deontologico sottoscritto.

1.5 Lo schema di accreditamento e L'Ente Accreditatore

La verifica che un Organismo di Certificazione possieda le suindicate caratteristiche, indicata generalmente con il termine "accreditamento", dovrebbe essere condotta - in stretta aderenza alle prescrizioni della norma citata - da un Ente "super partes" che, a sua volta, abbia una legittimazione ad operare nel campo specifico.
Lo stesso termine "accreditamento" è associato al concetto di terzietà, sia dell'Ente accreditante, sia dell'Organismo richiedente, nonché ad una scelta volontaria dello stesso Organismo richiedente e assume il significato di riconoscimento dell'idoneità dell'Organismo a gestire determinati schemi di certificazione con riferimento alla valutazione delle competenze delle singole persone.

In Italia, il ruolo di Ente "super partes" è svolto dal SINCERT (Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione), Associazione privata senza fini di lucro fondata nel 1991 per iniziativa di UNI (Ente Nazionale Italiano di Unificazione) e di CEI (Comitato

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Elettrotecnico Italiano), con la partecipazione del Ministero dell'Industria, del CNR (Consiglio Nazionale delle Ricerche) e dell'ENEA (Ente per le Nuove Tecnologie, l'Energia e l'Ambiente) [1].

Il SINCERT effettua l'accreditamento degli Organismi di certificazione delle competenze del personale in base alla UNI CEI EN ISO/IEC 17024:2004 e con riferimento alla Guida IAF GD 24:2004 (*IAF Guidance on the Application of ISO/IEC 17024:2003*).

La legittimazione di SINCERT ad effettuare tali accreditamenti risiede nel fatto che ha aderito agli accordi multilaterali EA (European Cooperation for Accreditation,) e IAF (International Accreditation Forum).

A questo proposito bisogna rilevare che gli enti di accreditamento, qualora non siano in possesso di appositi riconoscimenti giuridici, come in questo caso, agiscono sulla base di una delega "de facto" ad essi conferita spontaneamente dal sistema socio-economico; nell'ambito del sistema volontario, quindi, l'esercizio dell'attività di accreditamento è libero, vale a dire non soggetto a specifica regolamentazione ma solo alle leggi generali in materia di attività economiche.

[1] E' da tenere presente che, quale primo concreto passo verso l'unificazione del sistema italiano di accreditamento – e coerentemente con gli impegni assunti in sede di sottoscrizione dell'Accordo di Programma per la costituzione di un Ente Unico Italiano di Accreditamento, a suo tempo siglato da tutte le principali parti interessate sotto l'egida del Ministero delle Attività Produttive – è stata costituita in Roma, in data 21 Maggio 2004, la Federazione Italiana degli Enti di Accreditamento, in sigla FIDEA, i cui Soci Fondatori iniziali sono SINCERT e SINAL – che rappresentano i principali Enti di accreditamento nazionali.
La costituzione della Federazione costituisce un passo fondamentale verso il traguardo finale di creazione dell'Ente Unico di Accreditamento, sia sul piano politico (forte segnale di unificazione in ambito nazionale ed internazionale), sia sul piano operativo (avvio concreto del processo di integrazione, armonizzazione e miglioramento).
Il nuovo Regolamento europeo per l'accreditamento, la vigilanza del mercato e il controllo sui prodotti attribuisce un ruolo di pubblica autorità al futuro Ente unico di accreditamento, qualificandolo come soggetto che, indipendentemente dal proprio status giuridico, opererà in nome e per conto dello Stato.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Il controllo sull'operato degli Enti di Accreditamento, oltre che dall'azione interna di indirizzo e sorveglianza degli stakeholders (fra cui le Pubbliche Amministrazioni), è assicurato tramite opportuni meccanismi di controllo "esterno", rappresentati dalla partecipazione degli Enti di Accreditamento ad apposite Associazioni internazionali e, in tali ambiti, dalla sottoscrizione degli Accordi Internazionali di Mutuo Riconoscimento (MLA) gestiti da dette Associazioni (nel nostro caso, EA e IAF).

Infatti, per essere membri di EA (o IAF) gli Enti di Accreditamento devono fornire evidenza della loro concreta operatività (e questa deve risultare conforme ai requisiti delle Norme e Guide applicabili) e per entrare a far parte degli Accordi di Mutuo Riconoscimento devono essere sottoposti, con esito positivo, ad uno specifico ed accurato processo di valutazione da parte delle stesse Associazioni.

Pertanto, la partecipazione agli Accordi MLA garantisce la competenza ed il rigore procedurale dell'Ente firmatario, nonché l'uniformità del suo modo di operare rispetto a quello degli altri Enti firmatari.

La logica conseguenza è che le certificazioni rilasciate da Organismi accreditati da Enti di Accreditamento che partecipano agli Accordi MLA sono valide e credibili, in quanto sottoposte al controllo di un competente Ente di Accreditamento riconosciuto internazionalmente; inoltre queste certificazioni sono fra loro equivalenti, e come tali accettate e riconosciute da tutti gli Enti partecipanti, in quanto emesse in un contesto di regole comuni e procedure uniformate.

Le certificazioni rilasciate da Organismi non accreditati o accreditati da Enti di Accreditamento che non sono firmatari degli accordi MLA, non offrono le stesse garanzie di valore e di credibilità.

Concludendo, si può quindi affermare che l'accreditamento degli Organismi di certificazione è finalizzato a garantire la loro competenza e di conseguenza il valore e la credibilità dei risultati delle valutazioni di conformità da essi effettuate.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Ad oggi SINCERT ha reso operativi diversi schemi di accreditamento, tra i quali anche quello relativo alle certificazioni delle competenze del personale, denominato:

PRS - Certificazioni di personale

1.6 Lo schema di Certificazione delle competenze del personale e l'Organismo di certificazione

Per ogni figura professionale da certificare, l'Organismo di certificazione delle professionalità, con la collaborazione determinante delle "parti interessate", definisce gli schemi di certificazione comprendenti i requisiti minimi che deve possedere il candidato, le modalità per accedere alla certificazione e quelle per il suo mantenimento e rinnovo. Tali requisiti, devono essere suffragati da riscontri oggettivi, ai fini del conseguimento della certificazione.
La certificazione deve avere una durata limitata e per il rinnovo è indispensabile produrre adeguata documentazione attestante l'attività svolta, la soddisfazione dei clienti e la partecipazione ad attività formative di aggiornamento professionale.
La certificazione assicura quindi non solo che il professionista possieda in un determinato periodo competenze adeguate, ma che le dimostri con continuità. Tali competenze vengono riconosciute da tutto il mercato ed hanno perciò una visibilità più ampia nello spazio e nel tempo attraverso la garanzia della soddisfazione dei clienti e della continuità dell'attività professionale.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

In linea generale, un processo di certificazione deve garantire quattro caratteristiche principali:

1. l'imparzialità *(la valutazione deve essere condotta senza pregiudizi e i valutatori devono dimostrare di non avere interessi di nessun tipo dipendenti dall'esito della valutazione stessa)*;
2. l'oggettività *(la valutazione finale deve essere motivata il più possibile da evidenze oggettive e non da opinioni e valutazioni personali)*;
3. la ripetibilità *(la valutazione della stessa persona effettuata con le stesse modalità e con le stesse evidenze dallo stesso valutatore deve portare allo stesso risultato)*;
4. la riproducibilità *(la valutazione della stessa persona effettuata con le stesse modalità e con le stesse evidenze da un diverso Valutatore deve portare allo stesso risultato).*

E' ovvio precisare che è praticamente impossibile che uno schema di certificazione riesca a soddisfare tutte le caratteristiche descritte in precedenza: tanto per fare un esempio, per quanto riguarda in particolare la verifica delle competenze del personale, la caratteristica della "oggettività" è irrealizzabile proprio per il fatto che la valutazione finale si basa sul giudizio soggettivo del Valutatore.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

1.7 Il Valutatore

Il Valutatore, cioè colui che valuta le competenze del soggetto richiedente e quindi la sua idoneità a conseguire la certificazione di competenza, può essere personale interno dell'Organismo di Certificazione; più spesso, invece, quest'ultimo ricorre a consulenti esterni dotati di particolare esperienza.

In questo caso, la criticità sta nella competenza e nell'approccio etico di tali Valutatori, garanzia che anche in questo caso dovrebbe essere data a sua volta da una apposita certificazione della professionalità di tale figura; in ogni caso, tutto il personale addetto alle attività di valutazione delle competenze del personale in Information Security utilizzato dall'Organismo di Certificazione deve, oltre alla caratteristiche generali definite dalle norme già citate ISO/IEC 17024, IAF GD 24 e dai Regolamenti SINCERT (RT-15 rev. 01), possedere particolari competenze nell'ambito della ICT e, in modo particolare, nella Sicurezza delle Informazioni.

1.8 Il Committente della certificazione

Come già detto in principio, la motivazione alla base della decisione di avviare un processo di certificazione volontaria consiste principalmente nel desiderio di acquisire la consapevolezza della "propria" professionalità, affidando a terzi il compito della verifica, e nell'essere riconosciuto - sia nell'ambito della propria azienda, sia nel proporsi a livello di mercato - come un professionista della Information Security.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

D'altra parte le aziende hanno tutto l'interesse a verificare la competenza - nei vari settori della Information Security - del proprio personale e/o ad avvalersi di servizi professionali altamente qualificati.

Tutto questo è particolarmente valido per le aziende che intendono sottoporsi ad una certificazione volontaria di Sicurezza delle Informazioni, secondo lo schema ISO 27001: tale standard, infatti, prevede che, all'atto della verifica di un Sistema di Gestione della Sicurezza delle Informazioni, sia oggetto di valutazione anche la competenza e il processo formativo del personale che riveste un qualche ruolo nella attuazione delle politiche di sicurezza delle informazioni. Anche se tale verifica si limita a controllare se è stato previsto e/o attuato un processo formativo, e non verifica puntualmente la effettiva competenza del personale, è comunque opportuno che l'azienda si avvalga di personale con competenza certificata nel settore della sicurezza ICT, anche considerando la notevole varietà di "certificazioni" di competenza attualmente disponibili sul mercato.

Altre opportunità derivano dal fatto che lo stesso Organismo di Certificazione, a sua volta, deve assicurarsi che anche il suo personale addetto alle attività di valutazione possieda particolari competenze nell'ambito della ICT e, in modo particolare, nella Sicurezza delle Informazioni.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

1.9 Lo stato dell'arte delle certificazioni delle competenze del personale in Information Security

Certificazioni di terza parte

Al momento SINCERT ha accreditato Organismi di certificazione di competenza del personale in vari settori, ma solo alcuni di essi sono accreditati specificatamente per erogare certificazioni di competenza del personale nel settore della Information Security:

- CEPAS *(Organismo di Certificazione delle Professionalità e della Formazione)* per le figure di ISMS Auditor/Responsabili Gruppo di Audit);
- AICQ-SICEV *(Associazione Italiana Cultura Qualità)* per le figure di Auditor/Responsabile gruppo di audit di Sistemi di gestione per la sicurezza delle informazioni.

A livello internazionale alcune certificazioni sono state sviluppate da $(ISC)^2$ *(International Information Systems Security Certification Consortium),* per quanto riguarda le figure CISSP/SSCP/ISSAP/ISSEP/ISSMP/CAP, e da ISACA *(Information Systems Audit and Control Association)* per quanto riguarda le figure CISA/CISM: queste due organizzazioni operano anche in Italia attraverso le relative affiliazioni nazionali; va ricordato che queste certificazioni sono gestite sotto accreditamento statunitense, emesso da ANAB *(ANSI-ASQ National Accreditation Board),* anch'esso membro IAF e firmatario degli accordi MLA. ANAB è, negli Stati Uniti, l'equivalente di SINCERT in Italia: tra i due enti di accreditamento esiste un accordo di mutuo riconoscimento, essendo ambedue firmatari degli stessi accordi.

Inoltre, una certificazione ASGSI - Auditor di SGSI a norma ISO/IEC 27001 è stata sviluppata da RICEC *(Registro internazionale di certificazione delle competenze, dei prodotti formativi e dei servizi),* ente di certificazione svizzero con filiale a San Marino: questa certificazione è gestita sotto

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

accreditamento svizzero, emesso da METAS-SAS *(Servizio di Accreditamento Svizzero)*, anch'esso membro IAF, membro EA e firmatario degli accordi MLA.
Pertanto, anche quelle suddette sono da considerarsi certificazioni di terza parte.

Certificazioni non di terza parte

Senza accreditamento SINCERT, nel settore Sicurezza delle informazioni ci si può avvalere di altre tipologie di "certificazione": esse non sono formalmente classificabili come certificazioni di terza parte, ma bisogna comunque considerare che la valutazione dell'affidabilità di ciascun tipo di certificazione dovrebbe tenere conto anche delle modalità di attuazione dei requisiti stabiliti dalla ISO17024: questi – infatti - hanno comunque validità generale, anche in assenza di un accreditamento formale dell'Organismo di certificazione.
Queste certificazioni possono essere suddivise in due grandi categorie: le certificazioni "vendor independent" e le certificazioni "vendor specific".

Le certificazioni ***vendor independent*** sono normalmente gestite o riferibili ad associazioni nazionali o internazionali senza scopo di lucro e, sostanzialmente, fondano la loro credibilità sulla maggiore o minore diffusione delle loro certificazioni di competenza, sulla riconosciuta affidabilità dei certificati di competenza emessi e sul comportamento deontologico delle persone che hanno acquisito e mantengono nel tempo quel particolare tipo di certificazione.
Fa parte di questa categoria, ad esempio, uno schema dello stesso CEPAS, che ha attivato una certificazione denominata ISMS Manager/Senior Manager; inoltre, sono da citare le certificazioni KHC *(Know How Certification)*, che ha attivato gli schemi per le figure di Internal Auditor ISMS,

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Provisional Auditor ISMS, Auditor ISMS, Lead Auditor ISMS (basate sulla norma ISO/IEC 27001) e le certificazioni EUCIP erogate, in Italia, da AICA *(Associazione Italiana per l'Informatica e il Calcolo Automatico)*, partner italiano di CEPIS *(Council of European Professional Informatics Societies)*.

Recentemente (2008) AIPSI *(Associazione Italiana Professionisti della Sicurezza Informatica)* ha introdotto una certificazione proprietaria (e italiana): la Localizzazione delle Competenze della Sicurezza Informatica (LoCSI), che, ancora in fase di sviluppo, intende coprire il gap esistente tra le competenze tecnologiche (sempre più di provenienza non nazionale o addirittura non europea, e certificabili con gli altri percorsi esaminati) e quelle normative che determinano sempre di più le decisioni e le scelte nell'ambito della Sicurezza delle Informazioni.

Le certificazioni ***vendor specific*** sono, invece, normalmente erogate da produttori di hardware e software, e sono finalizzate alla formazione di personale specializzato ad operare su specifici prodotti.

La loro affidabilità è legata alla serietà del "vendor": questi, infatti, avendo forti interessi commerciali legati alla vendita dei loro prodotti e alla immagine di sicurezza fornita, è fortemente motivato a far sì che sul mercato siano disponibili un rilevante numero di professionisti abilitati ed esperti nell'utilizzo dei loro prodotti.

Come esempio di questa categoria si possono citare le certificazioni che fanno riferimento alle aziende produttrici quali Microsoft, Symantec, Check Point, Cisco, ecc.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Forum delle Competenze Digitali

Capitolo 2

IPOTESI DI MAPPING DELLE CERTIFICAZIONI DELLE COMPETENZE NELLA SICUREZZA DELLE INFORMAZIONI

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.1 Introduzione

Il documento ha l'obiettivo di presentare un'ipotesi dei criteri di mappatura delle certificazione ICT per la sicurezza digitale secondo gli intendimenti del FORUM DELLE COMPETENZE DIGITALI che ha istituito uno specifico gruppo di lavoro (GdL) per le Competenze nella Sicurezza delle Informazioni, volto a favorire la diffusione della cultura della sicurezza presso gli operatori del settore ICT.

2.2 Gli obiettivi

Il principale obiettivo è quello di definire un metodo per produrre un quadro di riferimento delle principali certificazioni delle competenze nella sicurezza delle informazioni presenti sul mercato, al fine di fornire un criterio di orientamento alle aziende ed ai professionisti, che così potranno individuare quelle maggiormente rispondenti alle loro specifiche esigenze.

Da notare che il metodo proposto è una procedura aperta, nel senso che il quadro di riferimento delle certificazioni potrà essere aggiornato ogni qualvolta sia ritenuto necessario a fronte di specifica esigenze.

Sulla base del metodo proposto sarà, inoltre, possibile elaborare opportune azioni volte alla promozione della cultura della sicurezza dei sistemi ICT per meglio supportare gli obiettivi di business, ed a garanzia degli interessi di coloro che, sempre più, utilizzano le tecnologie informatiche per le attività ed i servizi.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.3 Il contesto organizzativo

Nella realtà degli Enti e delle Aziende italiane, la sicurezza informatica è progettata, attuata, erogata, gestita con diverse modalità e con diversi ruoli, che a grandi linee possono essere così schematizzate:

1. **Lato Domanda (Aziende/Enti utenti)**

a) Nelle grandi organizzazioni esistono:

- esperti di sicurezza informatica all'interno della Unità Organizzativa Sistemi Informativi, con ruoli operativi a tempo pieno (progetto, configurazione, installazione, supervisione acquisti ed interventi di Terze Parti, gestione operativa. Il responsabile della sicurezza informatica, all'interno dei Sistemi Informativi, è chiamato CISO, Chief Information Security Officer;
- competenze di sicurezza informatica per le funzioni di auditing e di controllo, esterne alla Unità Organizzativa Sistemi Informativi;
- competenze di sicurezza informatica nell'ambito dell'Unità Organizzativa "Sicurezza Aziendale/Ente", che si occupa di tutti gli aspetti di "security" e "safety" dal personale dagli edifici, alle risorse, al patrimonio informativo; il responsabile della sicurezza "globale" è chiamato CSO, Chief Security Officer;

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

- competenze di sicurezza informatica nelle Unità Organizzative che si occupano della conformità (Compliance) alle varie normative nazionali ed internazionali, quali la legge sulla privacy, sulla sicurezza sul lavoro, la Legge 231, la 262, ecc. Spesso tali competenze sono all'interno dell'Unità Organizzativa Legale;
- Help-desk e supporto all'utenza

b) Ulteriori considerazioni si possono fare esaminando la situazione nelle Piccole e Medie Imprese, particolarmente significativa - ovviamente – nel quadro dell'economia italiana.

In questo contesto, dove normalmente la funzione ICT è ritenuta, nel migliore dei casi, non strategica (o addirittura solo un costo, purtroppo inevitabile), si verificano due fenomeni importanti:

- la Sicurezza Informatica è già declinata, anche se inconsapevolmente (ma "olisticamente"), nelle sue accezioni di Riservatezza, Integrità e Disponibilità, cioè quelle caratteristiche che, nelle grandi organizzazioni, vengono riassunte nella funzione "Operations";
- le competenze ICT sono richieste solo saltuariamente a figure interne, ma più frequentemente a professionisti esterni (anche inquadrati in Aziende di Servizi ICT).

Di conseguenza, le certificazioni professionali formali (ovviamente sempre accompagnate ad una adeguata expertise) diventano un importante strumento di verifica e selezione delle competenze nel mercato dell'offerta.

Lo stesso criterio è, evidentemente, utilizzabile da organizzazioni più "importanti" quando si rivolgono al corrispondente mercato dei Servizi Professionali.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2. Lato Offerta (Fornitori di prodotti, sistemi, servizi per la sicurezza digitale)

Le competenze sulla sicurezza informatica sono distribuite tra i vari attori che trattano per i clienti i prodotti, sistemi e servizi di sicurezza digitale:

- Forze di vendita
- Supporto tecnico alla vendita ed alla post-vendita
- Progettisti, configuratori ed installatori
- Consulenti
- Gestori di servizi
- Help-desk e supporto all'utenza

L'impiego in azienda di figure professionali certificate è un tema soggetto a forte criticità in quanto condizionato da una serie di fattori, quali:

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

- forte dicotomia tra le competenze richieste dal mercato e quanto sancito nei contratti nazionali, anche per le figure relative alla sicurezza digitale: tale dicotomia è un forte freno, in particolare per le Aziende, nell'adottare le figure definite con specifiche competenze come in Eucip, per le possibilità di rivendicazioni economiche;
- mancanza di definizione a livello contrattuale, e spesso anche a livello di prassi, di "sviluppi di carriera" per le figure tecniche;
- necessità di valutare le posizioni in funzione delle effettive competenze, esperienze, capacità e potenzialità possedute dai candidati.

Va, inoltre, rilevato che le competenze tecniche (e non) richieste dipendono anche, ma non solo, dai processi che il personale deve supportare e nei quali è coinvolto, oltre che dalla struttura organizzativa in cui il personale opera.

La collocazione in azienda del professionista informatico è funzione, oltre che delle competenze tecniche, anche di quelle personali e della posizione che il professionista è chiamato a ricoprire per svolgere determinati ruoli in azienda, facendo riferimento allo specifico processo su cui la sua responsabilità viene esercitata: su questo aspetto la teoria organizzativa pone come riferimento i processi e non l'azienda nel suo complesso e diviene, pertanto, molto importante l'utilizzo della metodologia ITIL.

Dalle posizioni / ruoli che la persona è chiamata a ricoprire è possibile astrarre delle figure / livelli professionali che identificano l'insieme delle funzioni da svolgere nell'ambito dei processi del ciclo di vita dei sistemi informativi.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.4 Oggetto della mappatura

L'insieme delle certificazioni delle competenze nella sicurezza delle informazioni, prese al momento in considerazione dal GdL del Forum, sono riportate nel capitolo 3. Si ricorda, al riguardo, che si tratta di certificazioni di competenze professionali e non di certificazioni di prodotto o di sistema informativo.

Il focus è sulle certificazione "vendor independent", ma eventualmente possono essere mappate anche certificazioni "vendor specific" (CISCO, MICROSOFT, SYMANTEC, …), come definito nella ricerca Harmonise 2007;

Si osserva, inoltre, che non tutte sono "certificazione di terze parti", in base allo standard ISO 17024, e quindi riconosciute dal SINCERT; alcune adottano schemi di accreditamento diversi, basati su altri tipi di accordi internazionali, come nel caso di EUCIP che è definito in ambito CEPIS (vedi Capitolo 1: "La certificazione delle competenze nella sicurezza delle informazioni").

2.4.1 Le competenze tecniche

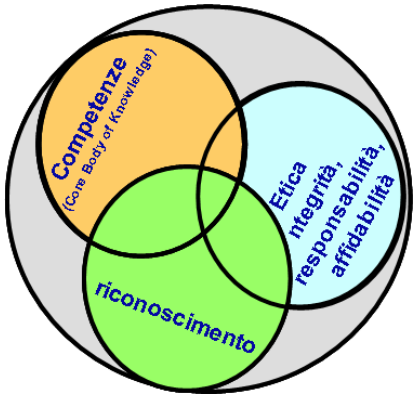
La professionalità ICT è percepita differentemente a secondo dei contesti cui si riferisce; essa è soggetta a una continua e rapida evoluzione delle tecnologie che rende, di fatto, difficile fornirne una definizione univoca e identificarne il corpo di conoscenze condivisibile per una piena comprensione.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Ai fini della mappatura delle certificazioni delle competenze nella sicurezza delle informazioni si può prendere a riferimento il modello descrittivo delle professionalità ICT che, secondo Hughes and Thomson (R. Bellini in "Mondo Digitale", 2008), si basa su tre pilastri:

- le competenze, che dimostrano il possesso rilevante di conoscenze elementari e di capacità appropriate ad una particolare attività o a uno specifico ruolo, integrato da un'esperienza pratica che completa la conoscenza teorica (il saper fare in un contesto dato);

- l'etica, che si riferisce all'assunzione di una personale responsabilità affinché il lavoro e le decisioni siano conformi alle aspettative nel rispetto, anche, di un codice di condotta pubblico (codice etico), definito da istituzioni o comunità professionali in cui siano definiti criteri di integrità, affidabilità e responsabilità;



- il riconoscimento, che è relativo al fatto che la professionalità richiede un impegno a lavorare nell'interesse della società e per lo sviluppo della professione, in modo che vi sia una corretta valutazione da parte del committente e del mercato.

In questa prima fase il GdL si è focalizzato sulla mappatura delle competenze richieste dalle certificazioni relative alla sicurezza delle informazioni. In una seconda fase dell'attività il GdL potrà affrontare l'esame anche degli altri fattori evidenziati.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.4.2 Gli assi di mappatura

Il principale criterio per la definizione degli assi di mappatura è il riferimento a standard europei per la normalizzazione del settore ICT.
In tal senso si propongono gli standard:

- EUCIP di CEPIS per la definizione dei domini di competenza tecnica;
- ISSA (criteri di classificazione per campo di applicazione)

E' da evidenziare, inoltre, il modello eCF (European Competence Framework) per la definizione dei livelli professionali, definito nell'ambito del Programma European eSkill di CEDEFOP: esso rappresenta un vero e proprio modello di interoperabilità e compatibilità tra standard differenti.

Gli assi di mappatura proposti sono:

- asse delle certificazioni: sono gli standard di certificazione della sicurezza da mappare;
- asse dei domini: identifica i domini di competenze tecnica che ogni certificazione copre;
- asse dei livelli professionali: identifica per quali livelli professionali sono necessarie le specifiche certificazioni.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.4.2.1 Le certificazioni

La seguente tabella riporta un esempio delle principali certificazioni della sicurezza finora identificate dal GdL e che vengono a costituire l'asse di riferimento delle certificazioni. Per una lista più completa si rimanda al capitolo 3 "Lista delle certificazioni".

In ragione della loro numerosità si propone di procedere per fasi, operando in un primo momento su quelle maggiormente riconosciute dal settore ICT.
La lista non si intende esaustiva, ed altre certificazioni potranno essere prese in considerazione ed inserite nel seguito.

ente certificatore	CEPIS			ISC2						CEPAS		ISACA		AIPSI	ISECOM-OSSTM			CompTIA	SANS	EC-Council				SCP			
ente di certificazione nazionale	AICA			CLUSIT						CEPAS		AIEA		AIPSI													
certificazione	IS Auditor	Security Aviser	IT Administrator	CISSP	SSCP	ISSAP	ISSMP	ISSEP	CAP	ISMS MANAGER	ISMS AUDITOR	CISA Assurence	CISM SECURITY	LOCSI	OPSA (analyst)	OPSE (expert)	OPST (tester)	CompTIA Security +	(n per area/profilo)	CEH	CHFI	ECSA	LPT	SCP	SCNS	SCNP	SCNA

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.4.2.2 I domini di competenza oggetto delle certificazioni

Per l'asse dei domini tecnici, che sono oggetto delle diverse certificazioni della sicurezza, si fa riferimento al sistema di competenze dello standard EUCIP di CEPIS, che costituisce un framework di competenze tecniche a copertura dei processi di plan, build e operate tipici dei sistemi informativi. Per ogni approfondimento sullo standard si rimanda al sito www.eucip.it

In breve il framework delle competenze EUCIP presenta circa 3.000 unità di competenza elementare (knowledge objects), raggruppate in 155 categorie elettive e 18 aree di competenza. Sulla base di questo framework sono quindi identificati, al momento, 21 profili professionali elettivi, più uno dedicato alla figura di IT Administrator. Di questi, 3 sono i profili certificabili in materia di sicurezza (System Auditor, Security Adviser, IT Administrator) che sono quindi gestiti sull'asse delle certificazioni, come sopra indicato, analogamente alle altre certificazioni.

Dal framework delle competenze tecniche messe a disposizione dallo standard EUCIP sono, quindi, estratti gli elementi caratterizzanti il tema della sicurezza digitale, come struttura iniziale di riferimento su cui basare la mappatura dei diversi domini propri di ogni singola certificazione. In prima ipotesi viene proposta la mappatura a livello di "categorie elementari" , in alternativa si potrà decidere di limitarsi a livello di "aree di competenza" (domini) per semplificare la procedura.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Qualora il dominio interessante una certificazione non sia presente (o non sufficientemente presente) nella struttura iniziale, potrà essere proposta la modifica del set iniziale di domini proposti.

Processi	Aree	sub	domini /categorie elementari
A Plan Knowledge Area : Use and Management of Information Systems	A.1		A.1 Organisations and their Use of IT
		A1.01	Business activity and business process modelling
	A.2		A.2 Management of IT
		A2. 05	Business Continuity Planning
		A2. 06	Key IT Process Control
		A2. 08	IT Governance
	A.3		A.3 Measuring the Value of IT
		A3. 05	IT Security Economics and Business Strategies
		A3. 07	Risk Management
	A.4		A.4 The Global Networked Economy
		A4.01	New technology opportunities and the matching of these to business needs
		A4.02	Package selection and implementation lifecycle
	A.5		A.5 Project Management
		A5.01	Project Management essentials
		A5.02	Estimating for System Development
	A.6		A.6 Presentation and Communication Techniques
		A6. 01	Managing business change
		A6. 06	Audit reporting and communication

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

	A.7		A.7 Legal and Ethical Issues
		A7.01	Health and safety
		A7.02	Business risk and IT security
		A7.03	Data protection
		A7.04	Managing business risk and IT Security
		A7.05	Managing data protection
		A7.06	Access-control policies, models and mechanisms
		A7.07	Risk analysis and management
		A7. 08	Legal aspects of telecommunications
		A7. 09	IS audit process
		A7.10	Gathering evidence through sampling
		A7.11	Compliance evaluation
		A7. 12	IT security assurance

Processi	**Aree**		**domini /categorie elementari**
B Build Knowledge Area : Development and implementation of Information Systems	B.1		B.1 Systems Development Process and Methods
		B1.05	Systems design and implementation
		B1.08	Software engineering principles
		B1.10	"Dry run" application testing
	B.2		B.2 Data Management and Databases
		B2.13	Database Security
	B.3		B.3 Programming
		B3.05	Principles of Testing
		B3.06	Secure programming
	B.4		B.4 User Interface and Web Design
		B4.06	Web-Based Applications

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Processi	Aree		domini /categorie elementary
C Operate Knowledge Area : Operation and Support of Information Systems	C.2		C.2 Operating Systems
		C2.01	Operating Systems
		C2.05	Operating Systems Security
	C.3		C.3 Communications and Networks
		C3.04	IP communications
	C.4		C.4 Network Services
		C4.01	Network Security
		C4.06	Network Attack Prevention
		C4.07	Web Application Security
	C.5		C.5 Wireless and Mobile Computing
		C5.02	Wireless Security
	C.7		C.7 Service Delivery and Support
		C7.03	Change and configuration management
		C7. 04	Quality and performance standard
		C7. 06	Troubleshooting and Problem Prevention
		C7. 07	Service Survey

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.4.2.3 I livelli professionali eCF

Il Quadro europeo delle qualifiche per l'apprendimento permanente (European Qualifications Framework - EQF) è uno strumento per aiutare i datori di lavoro e gli individui a confrontare le qualifiche dei diversi sistemi di istruzione e di formazione dell'Unione Europea.
L'EQF si inserisce nel programma di lavoro Istruzione e formazione 2010, che è parte della Strategia di Lisbona. E' volto a favorire la certificazione delle competenze e la mobilità dei lavoratori, nell'ottica di una maggiore trasparenza, comparabilità e spendibilità delle qualifiche.
In questo ambito il CEN/ISSS Workshop ha sviluppato l'European Competence Framework per l'ICT (versione 1) che correla i livelli professionali ICT con le conoscenze e le abilità acquisibili da percorsi formativi riconosciuti a livello europeo.
Dai livelli eCF è quindi possibile ricondursi al framework EQF per la normazione delle diverse qualifiche di formazione.

Per ogni ulteriore informazione fare riferimento a:

- European e-Competence Framework
  www.ecompetences.eu (see press release)

- European e-Skills and Careers Portal
  http://eskills.eun.org (see press release)

La tabella di pagina seguente riporta la struttura del framework con i 5 livelli professionali da utilizzare per la mappatura delle certificazioni della sicurezza: da notare che ai nostri fini è da usare il riferimento alla colonna che identifica "typical task":

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

livelli eCF	**Typycal task**
e-5 Principal	IS Strategy or programme management
e-4 Lead professional/ Senior manager	IS strategy - Holistic solutions
e-3 Senior professional / Manager	Consulting
e-2 Professional	Concepts /basic principles
e-1 Associate	Support / Services

Oltre ad una stretta relazione con la formazione, il framework proposto consente di collegare i livelli professionali identificati con le posizioni organizzative presenti nei diversi processi ICT che un'azienda intenda adottare.

In altre parole un'azienda è in grado di individuare i ruoli di cui necessita e le posizioni professionali necessarie a ricoprirli. Sulla loro base sarà quindi possibile identificare i livelli professionali e le certificazioni di sicurezza ad essi associati che le persone devono possedere per meglio svolgere le competenze della propria posizione/ruolo.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

EQF levels	EQF Levels descriptions	e-CF Levels	e-CF Levels descriptions	Typical Tasks	Complexity	Autonomy	Behaviour
8	Knowledge at the most advanced frontier, the most advanced and specialised skills and techniques to solve critical problems in research and/or innovation, demonstrating substantial authority, innovation, autonomy, scholarly or professional integrity.	e-5	**Principal** Overall accountability and responsibility; recognised inside and outside the organisation for innovative solutions and for shaping the future using outstanding leading edge thinking and knowledge.	IS strategy or programme management	Unpredictable - unstructured	Demonstrates substantial leadership and independencein context which are novel requiring the solving of issues that involve many interacting factors.	Conceiving, transforming, innovating, finding creative solutions by application of a wide range of technical and / or management principles
7	Highly specialised knowledge, some of which is at the forefront of knowledge in a field of work or study, as the basis for original thinking, critical awareness of knowledge issues in a field and at the interface between different fields, specialised problem-solving skills in research and/or innovation to develop new knowledge and procedures and to integrate knowledge from different fields, managing and transforming work or study contexts that are complex, unpredictable and require new strategic approaches, taking responsibility for contributing to professional knowledge and practice and/or for reviewing the strategic performance of teams.	e-4	**Lead Professional / Senior Manager** Extensive scope of responsibilities deploying specialised integration capability in complex environments; full responsibility for strategic development of staff working in unfamiliar and unpredictable situations.	IS strategy/holistic solutions		Demonstrates leadership and innovation in unfamiliar, complex and unpredictable environments. Addresses issues involving many interacting factors.	
6	Advanced knowledge of a field of work or study, involving a critical understanding of theories and principles, advanced skills, demonstrating mastery and innovation in solving complex and unpredictable problems in a specialised field of work or study, management of complex technical or professional activities or projects, taking responsibility for decision-making in unpredictable work or study contexts, for continuing personal and group professional development.	e-3	**Senior Professional / Manager** Respected for innovative methods and use of initiative in specific technical or business areas; providing leadership and taking responsibility for team performances and development in unpredictable environments.	Consulting	Structured - unpredictable	Works independently to resolve interactive problems and addresses complex issues. Has a positive effect on team performance.	Planning, making decisions, supervising, building teams, forming people, reviewing performances, finding creative solutions by application of specific technical or business knowledge/skills
5	Comprehensive, specialised, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge, expertise in a comprehensive range of cognitive and practical skills in developing creative solutions to abstract problems, management and supervision in contexts where there is unpredictable change, reviewing and developing performance of self and others.	e-2	**Professional** Operates with capability and independence in specified boundaries and may supervise others in this environment; conceptual and abstract model building using creative thinking; uses theoretical knowledge and practical skills to solve complex problems within a predictable and sometimes unpredictable context.	Concepts/Basic principles		Works under general guidance in an environment where unpredictable change occurs. Independently resolves interactive issues which arise from project activities.	Designing, managing, surveying, monitoring, evaluating, improving, finding non standard solutions
4	Factual and theoretical knowledge in broad contexts within a field of work or study, expertise in a range of cognitive and practical skills in generating solutions to specific problems in a field of work or study, self-management within the guidelines of work or study contexts that are usually predictable, but are subject to change, supervising the routine work of others, taking some responsibility for the evaluation and improvement of work or study activities.				Structured - predictable		Scheduling, organising, integrating, finding standard solutions, interacting, communicating, working in team
3	Knowledge of facts, principles, processes and general concepts, in a field of work or study, a range of cognitive and practical skills in accomplishing tasks. Problem solving with basic methods, tools, materials and information, responsibility for completion of tasks in work or study, adapting own behaviour to circumstances in solving problems.	e-1	**Associate** Able to apply knowledge and skills to solve straight forward problems; responsible for own actions; operating in a stable environment.	Support/Service		Demonstrates limited independence where contexts are generally stable with few variable factors.	Applying, adapting, developing, deploying, maintaining, repairing, finding basic-simple solutions

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.5 La profondità di conoscenza ed altri parametri

Oltre agli assi precedentemente descritti nel definire la copertura della certificazione rispetto ai domini/competenze tecniche, potrebbe essere indicato il livello di profondità con cui una certificazione tratta un determinato dominio.

Il criterio che si propone di utilizzare è il seguente:

1 ***introductory*** : conoscenza di base dei concetti;
2 ***incisive*** : buona conoscenza della materia con capacità di applicazione in casi semplici ;
3 ***deep*** : conoscenza approfondita della materia con capacità di applicazione in casi complessi.

Oltre ai parametri utilizzati per la classificazione, è possibile associare alla singola certificazione altre caratteristiche base, che ne qualifichino l'applicazione, come ad esempio la validità temporanea e l'esperienza lavorativa richiesta, che - come detto - potranno essere oggetto di successive valutazioni.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.6 Modalità di presentazione delle mappature

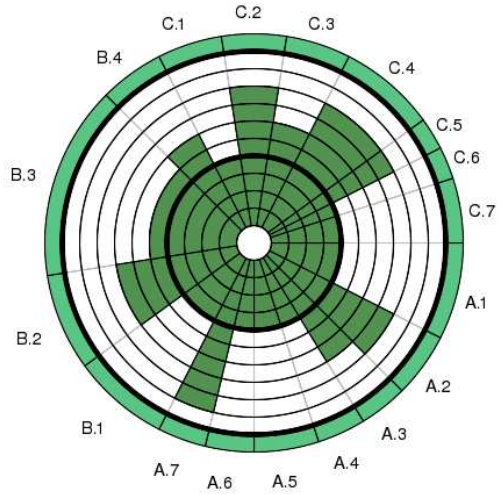
Una prima forma di rappresentazione sono le viste logiche degli assi di classificazione che permettono di correlare tra loro le informazioni sulle certificazioni prese in considerazione.

Inoltre, qualora per ogni certificazione della sicurezza sia stato prospettato il livello di profondità con cui è trattata ogni competenza/dominio, sarà possibile rappresentare un grafico radar con l'indicazione dell'area di copertura delle competenze.

Il radar può essere completato con l'indicazione del livello professionale cui la certificazione si riferisce e con le altre informazioni opzionali eventualmente fornite.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

EUCIP – Security Adviser



	A	Plan Knowledge Area : Use and Management of Information Systems
A.1	A.1	Organisations and their Use of IT
A.2	A.2	Management of IT
A.3	A.3	Measuring the Value of IT
A.4	A.4	The Global Networked Economy
A.5	A.5	Project Management
A.6	A.6	Presentation and Communication Techniques
A.7	A.7	Legal and Ethical Issues
	B	Build Knowledge Area : Development and implementation of Information Systems
B.1	B.1	Systems Development Process and Methods
B.2	B.2	Data Management and Databases
B.3	B.3	Programming
B.4	B.4	User Interface and Web Design
	C	Operate Knowledge Area : Operation and Support of Information Systems
C.1	C.1	Computing Components and Architecture
C.2	C.2	Operating Systems
C.3	C.3	Communications and Networks
C.4	C.4	Network Services
C.5	C.5	Wireless and Mobile Computing
C.6	C.6	Network Management
C.7	C.7	Service Delivery and Support

Livello professionale: e1 - Associate
e2 - Professional

Validità della certificazione: 3 anni
Esperienza richiesta: 36 mesi

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.7 Criterio di classificazione ISSA

Il capitolo riporta a titolo di confronto un altro criterio di classificazione presentato da ISSA sul suo sito; questo si limita a suddividere le certificazioni per la sicurezza digitale in base al campo di applicazione (Fonte: http://www.issa.org/Resources/Industry-Certifications.html):

Information Security

CEH	Certified Ethical Hacker
CIPP	Certified Information Privacy Professional
CISM	Certified Information Security Manager|
CISSP	Certified Information Systems Security Professional
CITRMSR	Certified Identity Theft Risk Management Specialist
CSP	RSA Certified Security Professional
ECSA	EC-Council Certified Security Analyst
GIAC	Global Information Assurance Certification
ISSPCS	International Systems Security Professional Certification Scheme
LPT	Licensed Penetration Tester

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

PCIP	Professional in Critical Infrastructure Protection
Security+	Computer Technology Industry Association (CompTIA)
SSCP	Systems Security Certified Practitioner
Symantec	SPS - Symantec Product Specialist STA - Symantec Technology Architect SCSE - Symantec Certified Security Engineer SCSP - Symantec Certified Security Practitioner

Business Continuity/Disaster Recovery

DRI International

ABCP	Associate Business Continuity Professional
CBCP	Certified Business Continuity Professional
MBCP	Master Business Continuity Professional

BCM Institute

BCCP	Business Continuity Certified Planner
BCCS DRCS	Business Continuity Certified Specialist, Disaster Recovery Certified Specialist
DRCE DRCE	Master Business Continuity Professional, Disaster Recovery Certified Expert

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Audit

CCSA	Certification in Control Self-Assessment
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CSA	Control Self-Assessment

Information Technology/Computing

ACP	Associate Computing Professional
CCP	Certified Computing Professional
CISCO	CCNA/CCNP - Network Installation & Support CCDA/CCDP - Network Engineering & Design CCIP - Communications & Services Cisco Qualified Specialist
CITP	Certified Information Technology Professional (AICPA)
CWNP	Certified Wireless Network Professional
Microsoft	MCP, MCP + Internet, MCP + Site Building MCSD MCSE, MCSE + Internet MCDBA

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

	MCT

Miscellaneous

AHC	Anti-Hacking Certification
AISC	Advanced Information Security Certification
CFE	Certified Fraud Examiner
CHFI	Computer Hacking Forensic Investigator
CPP	Certified Protection Professional
SSEC	Software Security Engineering Certification

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

2.8 Glossario

Per i termini sul processo di certificazione vedasi il capitolo 1: “La certificazione delle professionalità nella sicurezza delle informazioni”.

Per quanto riguarda le definizioni di carattere organizzativo:

- L’asse della **competenze tecniche** acquisito nel tempo e le relative certificazioni, che partono dal ciclo di studi:
  - Formali → Certificate dopo corsi di studi , sono esplicite e talvolta hanno anche valore legale possono essere non sostanziali.
  - Informali → Accumulate con l’esperienza, sono implicite ma sempre sostanziali.
- Le **caratteristiche psicoattitudinali,** insieme **all’autorevolezza** e **all’ etica** della persona costituisco l’insieme delle competenze non “tecniche” determinati per svolgere nel migliori dei modi (efficacemente ed efficientemente) il ruolo che una persona svolge o potrebbe svolgere in un determinato contesto organizzativo e di mercato.
- La **posizione** è uno specifico definito o richiesta nell’organigramma di una Azienda/Ente. E’ (o può/deve essere) regolato da contratti di lavoro ed individua le mansioni che devono essere svolte nello specifico contesto. In termini generali è che quello che il mercato richiede.
- **Figura / livello professionale:** è l’astrazione di una posizione al di fuori dello specifico contesto aziendale/ente per individuare l’insieme dio competenze tecniche e non e le caratteristiche che una persona deve avere.
- **Mansione**: l'insieme dei compiti e delle specifiche attività che il prestatore di lavoro deve eseguire nell'ambito del rapporto di lavoro.
- **Comportamento:** modo di agire e reagire di un oggetto o un organismo messo in relazione con altri oggetti, organismi, o semplicemente con l'ambiente. Il comportamento può essere conscio o inconscio e volontario o involontario.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

- **Etica:** è considerata in questo contesto come "l'insieme di comportamenti buoni, giusti, e moralmente leciti" nello svolgimento delle attività richieste nella posizione che si occupa.
- **Contratto di lavoro** viene stipulato tra un datore di lavoro (persona fisica, giuridica o ente dotato di soggettività) e un lavoratore, necessariamente persona fisica per la costituzione di un rapporto di lavoro.
- **Contratto collettivo nazionale di lavoro (CCNL)** → si veda sito Cnel
- **Rapporto di lavoro**: rapporto giuridico che ha origine dal contratto di lavoro ed è caratterizzato da molteplici situazioni giuridiche, di cui due obbligazioni principali: l'obbligazione in capo al datore di lavoro della retribuzione e l'obbligazione in capo al lavoratore della prestazione lavorativa.
- **Sicurezza delle informazioni**: garanzia di riservatezza, integrità e disponibilità delle informazioni.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Capitolo 3

LISTA CERTIFICAZIONI

rilevate alla data di febbraio 2009

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

3.1 Lista delle certificazioni

La lista fornisce il riferimento delle certificazioni prese al momento in considerazione dal Gruppo di lavoro e suddivise nelle due categorie: “vendor independent” e “vendor specific”.

Le certificazioni di terza parte, secondo lo standard ISO 17024, vengono contrassegnate con un asterisco (*).

3.2 Certificazioni “Vendor Independent”

Italiane

CEPAS *(Organismo di Certificazione delle Professionalità e della Formazione)*

Certificazioni ISMS Auditor/Responsabili Gruppo di Audit (*)
ISMS Manager/ISMS Senior Manager

AICQ-SICEV *(Associazione Italiana Cultura Qualità)*

Certificazioni Auditor/Responsabile gruppo di audit di Sistemi di gestione per la sicurezza delle informazioni (*)

KHC *(Know How Certification)*

Certificazioni Internal Auditor ISMS, Provisional Auditor ISMS, Auditor ISMS, Lead Auditor ISMS

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

AIPSI ***(Associazione Italiana Professionisti della Sicurezza Informatica)***

Certificazioni	LoCSI Localizzazione delle Competenze della Sicurezza Informatica

EUCIP European Certification of Informatics Professionals

Certificazioni	IT Administrator Security Advisor IS Auditor

Estere

(ISC)^2 ***(International Information Systems Security Certification Consortium)***

Certificazioni	CISSP Certified Information Systems Security Professional (*) CISSP - ISSAP focus su Architecture CISSP - ISSEP focus su Engineering CISSP - ISSMP focus su Management SSCP Systems Security Certified Practitioners CSSLP Certified Secure Software Lifecycle Professional

ISACA ***(Information Systems Audit and Control Association)***

Certificazioni	CISA Certified Information Systems Auditor (*) CISM Certified Information Security Manager (*)

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

RICEC ***(Registro internazionale di certificazione delle competenze, dei prodotti formativi e dei servizi)***

Certificazioni	ASGSI - Auditor di SGSI a norma ISO/IEC 27001 (*)

SANS Institute (SysAdmin, Audit, Networking, and Security) / GIAC Global Information Assurance Certification

Certificazioni	GSEC, GCFW, GCIA, GCIH, GCWN, GCUX, GSE, GISF, GSNA, GCFA, GSAE, G7799, GSLC, GCSC

CompTIA

Certificazione	CompTIA Security+

ISECOM - Institute for Security and Open Methodologies (OSSTMM Open Source Security Testing Methodology)

Certificazioni	OPST OSSTMM Professional Security Tester OPSA OSSTMM Professional Security Analist OPSE OSSTMM Professional Security Expert OWSE OSSTMM Wireless Security Expert HHS Security Awareness Instructor

EC-Council

Certificazioni	CEH, HFI

SCP Security Certified Program

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Certificazioni	SCNP, SCNA

ThinkSECURE

Certificazioni	OSSA Organizational Systems Security Analist OSWA Organizational Systems Wireless Auditor OSWAP Organizational Systems Web Application Pentester

Society of Payment-Card Industry Security Professional

Certificazioni	CPISM Certified Payment-Card Industry Security Manager

3.3 Certificazioni "Vendor Specific"

CHECK POINT, CISCO, ISS (Internet Security System), MICROSOFT, RSA Security, SYMANTEC.

In aggiunta alla lista delle certificazioni presentata nella riunione del GDL si segnalano anche le certificazioni "vendor specific" effettuate da SAP:

C_TADMSEC_04Associate	SAP Consultant Certification Technology Consultant SAP NetWeaver - SAP Security (2004)	SAP R/3 4.6C; SAP R/3 Enterprise; SAP Web AS 6.20 / 6.30 / 6.40
P_ADM_SEC_70 Professional	SAP Certified Technology Professional - Security with SAP NetWeaver 7.0	SAP NetWeaver 7.0

E si segnala che molti altri fornitori ICT effettuano corsi certificati nel cui ambito sono trattati, con diverso grado di approfondimento, gli aspetti della sicurezza ICT, in particolare per gli aspetti architetturali e nello sviluppo sicuro del codice.

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

ALLEGATO 1

I Soci del Forum delle competenze digitali

AICA - Associazione Italiana per l'Informazione

AICT - Associazione per la Tecnologia dell'Informazione e delle comunicazioni della Federazione AEIT

AIEA - Associazione Italiana Information Systems Auditors

AIP - Associazione Informatici Professionisti

AIPSI – Associazione Italiana Professionisti Sicurezza Informatica

ALSI - Associazione Nazionale Laureati in Scienze dell'Informazione e Informatica

ANASTAT - Associazione Nazionale Statistici

ANCEI - Associazione Nazionale Cultura Educazione Internazionale

ANIPA - Associazione Nazionale Informatici Pubblici e Aziendali

ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria

ANUIT - Associazione Nazionale Utenti Italiani di Telecomunicazioni

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

APCO – Associazione Professionale Italiana dei Consultenti di Direzione ed Organizzazione

CDTI di Roma - Club Dirigenti delle Tecnologie dell'Informazione di Roma

CLUSIT - Associazione Italiana per la Sicurezza Informatica

Federlazio/Informatica – Associazione piccole e medie imprese del Lazio

Federprofessional - Associazione delle alte professionalità indipendenti

FIDA Inform - Federazione Italiana delle Associazioni Professionali di Information Management

Fondazione FORMIT – Fondazione per la Ricerca sulla Migrazione e Integrazione delle Tecnologie

Fondazione Ugo Bordoni – Ricerca e consulenza nel settore dell'ICT

Infotransport – Associazione per l'Informatica nei Trasporti

INFORAV - Istituto per lo sviluppo e la gestione avanzata dell'informazione

ISCONA – Istituto per la Contabilità Nazionale

ItSMFItalia – il Forum della Gestione dei Servizi Informatici

JAVA Italian Association – La Comunità Java Italiana

SOS - LOGistica - Associazione per la logistica sostenibile

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it

Forum delle Competenze Digitali

ALLEGATO 2

Componenti del Gruppo di lavoro

Francesco ARCIPRETE (Forum delle competenze digitali)

Silvano BARI (AIEA)

Marco BOZZETTI (FIDA Inform)

Roberto FERRERI (AICA)

Matteo FLORA (AIP)

Franco GUIDA (Fondazione U. Bordoni)

Massimiliano MANZETTI (CLUSIT)

Maurizio MAPELLI (AIPSI)

Carlo MAJORANI (Fondazione U. Bordoni)

Marco RECCHIA (ANSSAIF)

Forum delle competenze digitali - c/o Inforav - P.zza Cavour, 19 – 00193 Roma
Tel. 06/3240077 Fax: 06/3234829 E-mail. segreteria@forumcompetenzedigitali.it