

01	11/01/2010	Inseriti alcuni chiarimenti nel paragrafo 4.1	<i>S. Ronchi R. De Pari</i>	<i>E. Stanghellini</i>	<i>G. Mattana</i>
00	01/09/2009	Completa revisione e nuova numerazione	<i>S. Ronchi R. De Pari</i>	<i>E. Stanghellini</i>	<i>G. Mattana</i>
Rev.	Data	Motivo Revisione	<i>Preparato da Referente Schema + Direttore AICQ SICEV</i>	<i>Verificato da Presidente CGC</i>	<i>Approvato da Presidente AICQ SICEV</i>

<p><b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione</p>	<p><b>REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</b></p>	<p><b>RSI 01</b>  <i>Pag. 2/11</i> <i>Rev.01</i></p>
---	--	--

## INDICE

### 1. SCOPO E CAMPO DI APPLICAZIONE

### 2. DOCUMENTI

- 2.1 Documenti di base
- 2.2 Documenti applicabili
- 2.3 Documenti di riferimento

### 3. DEFINIZIONI E ACRONIMI

### 4. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEI VALUTATORI (VSSI) E DEI RESPONSABILI DEI GRUPPI DI VERIFICA (VSSI RGV) DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI.

- 4.1 Requisiti minimi
- 4.2 Situazioni particolari
- 4.3 Rinnovo della Certificazione

### 5. MATERIE DI ESAME

<p><b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione</p>	<p><b>REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</b></p>	<p><b>RSI 01</b>  Pag. 3/11 Rev.01</p>
---	--	--

## 1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Regolamento ha lo scopo di definire i requisiti minimi per la concessione della certificazione delle competenze delle figure professionali di Valutatore e di Responsabile del Gruppo di Valutazione dei Sistemi di Gestione per la Sicurezza delle Informazioni, per il riconoscimento e il mantenimento delle competenze.

Il presente Regolamento si applica sia ai Candidati che abbiano presentato domande di Certificazione sia ai Valutatori/Responsabili dei Gruppi di Verifica dei Sistemi di Gestione per la Sicurezza delle Informazioni già iscritti ai Registri.

## 2. DOCUMENTI

### 2.1 Documenti di base:

- RS 01 – Regolamento per le Certificazione delle competenze dei Valutatori e dei Responsabili dei Gruppi di Valutazione di Sistemi di Gestione e di Prodotto

### 2.2 Documenti applicabili

- Manuale del Sistema di Gestione per la Qualità di AICQ SICEV e relative Procedure
- ISO/IEC 27001:2005 - UNI CEI ISO/IEC 27001: 2006 Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti

### 2.3 Documenti di riferimento

- UNI EN ISO 19011:2003 Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale
- ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management
- ISO/IEC 27005:2008 - Information technology - Security techniques – Information security risk management
- ISO/IEC 27006:2007 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC Guide 73:2002 – Risk management – Vocabulary – Guidelines for use in standards
- EA 7/03 Guidelines for the accreditation of bodies operating certification/registration of Information Security Management Systems
- ISO/IEC 13335 Information technology -- Security techniques -- Management of information and communications technology security
- CobiT - Control Objectives for Information and related Technology (ISACA)

## 3. DEFINIZIONI E ACRONIMI

Per le definizioni valgono quelle riportate nelle norme UNI EN ISO 19011:2003, ISO/IEC Guide 73:2002 e tutte quelle eventualmente indicate nei Documenti di riferimento.

In particolare i termini audit e verifica ispettiva ed i termini derivati auditor e valutatore sono da considerare completamente equivalenti nel presente Regolamento, anche se nella letteratura e nelle norme alle volte si preferisce utilizzare il primo od il secondo di essi.

<b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione	<b>REQUISITI SPECIFICI PER LA          CERTIFICAZIONE DELLE COMPETENZE DEI          VALUTATORI E DEI RESPONSABILI          DEL GRUPPO DI VALUTAZIONE          DEI SISTEMI DI GESTIONE PER LA          SICUREZZA DELLE INFORMAZIONI</b>	<b>RSI 01</b>  Pag. 4/11 Rev.01
--	--	--

Sono inoltre utilizzati i seguenti acronimi:

AICQ SICEV – Associazione Italiana Cultura Qualità – Sistema di Certificazione e di Valutazione  
 CD – Consiglio Direttivo di AICQ SICEV  
 CGC – Comitato di Garanzia della Certificazione di AICQ SICEV  
 EOQ – European Organization for Quality  
 RGVI – Responsabile del Gruppo di Verifica Ispettiva  
 V.I. – Verifica Ispettiva (Audit)  
 VSSI – Valutatore del Sistema di Gestione per la Sicurezza delle Informazioni

Nota: nei seguenti paragrafi del presente Regolamento quando viene usato il termine “Valutatore” il medesimo include le seguenti figure professionali:

- VSSI – Valutatore di Sistemi di Gestione per la Sicurezza delle Informazioni
- VSSI RGVI – Responsabile Gruppo di Valutazione di Sistemi di Gestione per la Sicurezza delle Informazioni

#### 4. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEI VALUTATORI (VSSI) E DEI RESPONSABILI DEI GRUPPI DI VERIFICA (VSSI RGVI) DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

##### 4.1 Requisiti minimi

Con riferimento a quanto indicato nel paragrafo 5.1 del Regolamento Generale RS 01, vengono di seguito riportati, in forma tabellare, i requisiti minimi per ciascun percorso di certificazione.

REQUISITI MINIMI	VSSI	VSSI RGVI
<b>Grado di istruzione</b>	Istruzione secondaria	
<b>Esperienza di lavoro complessiva</b>	5 anni, di cui almeno 4 anni nel settore Information Technology	
<b>Esperienza di lavoro specifica in ambito Sicurezza delle Informazioni</b>	Almeno 2 anni dei complessivi	Almeno 3 anni dei complessivi
<b>Formazione ed addestramento come auditor</b>	<p>Corso, riconosciuto da AICQ SICEV (o da OdC equivalenti), di 40 ore di formazione e addestramento su audit ISO 27001:2005 (in conformità a UNI CEI ISO/IEC 27001: 2006 Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) con superamento esame finale.</p> <p>In alternativa, ove l'Auditor abbia acquisito una precedente qualifica per la ISO 19011, ovvero una certificazione professionale come Auditor sui Sistemi di Gestione (SGA, SGQ, SGS) da parte di un Organismo di Certificazione del Personale Accreditato, viene accettato il superamento di un corso di 24 ore sulla ISO 27001:2005, comprensivo di specifici aspetti di approfondimento della norma, ma soprattutto delle tecniche di auditing relative.</p>	

<b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione	<b>REQUISITI SPECIFICI PER LA          CERTIFICAZIONE DELLE COMPETENZE DEI          VALUTATORI E DEI RESPONSABILI          DEL GRUPPO DI VALUTAZIONE          DEI SISTEMI DI GESTIONE PER LA          SICUREZZA DELLE INFORMAZIONI</b>	<b>RSI 01</b>  Pag. 5/11 Rev.01
--	--	--

REQUISITI MINIMI	VSSI	VSSI RGVI
<b>Esperienza di audit</b>	Partecipazione a 4 audit completi (di cui almeno 2 di 2° o 3° parte), con il coordinamento di un VSSI RGVI certificato da un Organismo di Certificazione del Personale o qualificato da Organismo di Certificazione di Sistema, per una durata complessiva di almeno 20 giorni. (Nota 1) Almeno 2 audit devono essere stati effettuati nell'ultimo anno.	Partecipazione a 5 audit completi (di cui almeno 2 di 2° o 3° parte che comprendono i 4 audit richiesti per i VSSI), con il coordinamento di un VSSI RGVI certificato da un Organismo di Certificazione del Personale o qualificato da Organismo di Certificazione di Sistema, per una durata complessiva di almeno 20 giorni. In almeno 3 dei suddetti audit completi sul Sistema di Gestione per la Sicurezza delle Informazioni dovrà aver ricoperto il ruolo di auditor. (Nota 1) Almeno 2 audit devono essere stati effettuati nell'ultimo anno.
<b>Lingue Straniere (su richiesta)</b>	Capacità di colloquio e di redazione di elaborati in lingua. Tale conoscenza può essere dimostrata da dichiarazioni rese da Istituti di formazione linguistica pubblici, privati o dalla Società di appartenenza del Candidato. AICQ SICEV si riserva di verificare durante la prova orale le reali conoscenze del candidato.	

**Nota 1:** Per audit completi, validi ai fini della certificazione, si intendono audit secondo la 27001:2006 che coprono tutte le fasi descritte dal punto 6.3 al punto 6.6 della UNI EN ISO 19001, incluse le attività di esame documentale, analisi dei rischi, esecuzione della verifica e stesura del rapporto di audit.

#### 4.2 Situazioni particolari

AICQ SICEV intende riconoscere le grandi professionalità presenti nel mondo della industria e dei servizi, semplificando il processo di certificazione delle competenze, che tuttavia non può prescindere da una valutazione oggettiva.

Per queste tipologie di candidati viene, in prima istanza, riconosciuta l'esistenza delle conoscenze necessarie al ruolo di auditor; i candidati sono quindi esonerati dalla prova scritta. Deve comunque essere sostenuta la prova orale, nel corso della quale la commissione d'esame dovrà valutare e confermare non solo la capacità di sostenere il ruolo di auditor ma anche la consistenza delle conoscenze, e delle esperienze lavorative.

Le situazioni particolari attualmente riconosciute da AICQ SICEV includono:

- Le certificazioni CISA e CISM [ISACA (Information Systems Audit and Control Association & Foundation)], CISSP (ISC)<sup>2</sup>, o Attestato di superamento di Master post universitari con percorsi formativi almeno equivalenti.
- VSSI o VSSI RGVI già certificati secondo altri schemi di certificazione di AICQ SICEV (es: Qualità, Ambiente, Salute e Sicurezza).  
 In questi casi, ma solo per un periodo di tempo limitato dall'entrata in vigore del presente regolamento, (periodo definito dal CGC e inserito nel documento AICQ SICEV "Casi particolari per certificazione/rinnovo certificazione competenze"), sarà possibile ammettere agli esami di certificazione AICQ SICEV Candidati Valutatori che:

<p><b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione</p>	<p align="center"><b>REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</b></p>	<p align="right"><b>RSI 01</b>  Pag. 6/11 Rev.01</p>
---	---	--

- Rispettino i requisiti previsti dal presente Regolamento per quanto concerne:
  - o Grado di Istruzione
  - o Esperienza di Lavoro complessiva
  - o Esperienza di Lavoro specifica
  - o Formazione e addestramento
- Presentino come “Esperienza di Audit” le evidenze oggettive di audit eseguiti anche per altri Schemi di Certificazione(es: Qualità, Ambiente, Salute e Sicurezza)
- VSSI o VSSI RGVI già certificati da altri OdC di personale accreditati, o riconosciuti a livello internazionale.
- VSSI di grande esperienza professionale così definita:
  - almeno 15 anni di esperienza lavorativa complessiva, di cui almeno 8 in gestione di Sistemi di Gestione per la Sicurezza delle Informazioni;
  - almeno 20 audit (comprensivi di quelli in addestramento) per un minimo di 60 giornate di impegno, di cui almeno 10 condotti come responsabile del gruppo di verifica.

A fronte di tali requisiti minimi, è prevista una serie di compensazioni ed equivalenze per quanto riguarda le esperienze professionali e specifiche, come di seguito indicato:

- L'iscrizione a Collegi ed Ordini professionali legalmente riconosciuti da più di tre anni e' ritenuto sostitutivo di un anno di esperienza lavorativa complessiva;
- Ogni gruppo di 10 V.I. complete in più delle 20 viene riconosciuto come sostitutivo di 1 anno di esperienza lavorativa complessiva e specifica, con un massimo di cinque anni;
- Ogni gruppo di 80 ore di corsi di formazione frequentati relativi a discipline inerenti i Sistemi di Gestione per la Sicurezza delle Informazioni viene riconosciuto come sostitutivo di 0,5 anni di esperienza lavorativa specifica, con un massimo di 1 anno;
- Lo stato di Docente Universitario Ordinario, Associato o a Contratto in discipline attinenti i Sistemi di Gestione per la Sicurezza delle Informazioni viene riconosciuto come sostitutivo di un anno di esperienza lavorativa complessiva e specifica;
- Lo stato di docente in corsi per la Sicurezza delle Informazioni riconosciuti da AICQ SICEV viene riconosciuto come sostitutivo di un anno di esperienza lavorativa complessiva e specifica;
- La qualifica di assessor in relazione a modelli di Sistemi di Gestione della Sicurezza delle Informazioni viene riconosciuta come sostitutiva di un anno di esperienza lavorativa complessiva e specifica.

Complessivamente non possono essere sostituiti più di sette anni di esperienza lavorativa complessiva e quattro anni di esperienza lavorativa specifica.

### **4.3 Rinnovo della Certificazione**

Si applica quanto previsto nel paragrafo 11.2 di RG 01 con le seguenti variazioni per quanto concerne il numero di audit eseguiti:

- a) affinché venga rinnovata la certificazione della competenza il VSSI deve avere effettuato nel triennio almeno 2 V.I. (di cui almeno 1 di 2<sup>a</sup> o 3<sup>a</sup> parte), per un totale di almeno 8 giorni;
- b) affinché venga rinnovata la certificazione della competenza il VSSI RGVI deve avere effettuato nel triennio almeno 3 V.I. (di cui almeno 2 di 2<sup>a</sup> o 3<sup>a</sup> parte) di cui almeno 2 svolgendo le funzioni di RGVI e coordinando un gruppo di valutazione per un totale di almeno 9 giorni. Ai fini del calcolo

<p><b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione</p>	<p align="center"><b>REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</b></p>	<p align="right"><b>RSI 01</b>  Pag. 7/11 Rev.01</p>
---	---	--

dei giorni lavorativi, al numero dei giorni di ogni verifica ispettiva, trascorsi in campo, viene aggiunto convenzionalmente N° 1 giorno per la preparazione e 0,5 giorni per documentazione. Nel caso di V.I. di 0,5 giorni verrà aggiunto 0,5 giorni per preparazione e 0,5 giorni per documentazione.

## 5. MATERIE DI ESAME

Oltre alle materie di esame comuni a tutti gli Schemi di Certificazione riportate nel paragrafo 8.11 (argomento: AUDIT) del Regolamento RG 01, i seguenti argomenti sono specifici per lo Schema Sicurezza delle Informazioni:

### 1 Gestione della Sicurezza delle Informazioni

#### 1.1 Principi fondamentali di gestione (Basic Management)

- Processo Decisionale
- Pianificazione
- Organizzazione
- Risorse umane
- Revisione

#### 1.2 Principi di Gestione dei Sistemi per la Sicurezza delle Informazioni:

- L'importanza ed efficacia di un Sistema di Gestione della Sicurezza delle Informazioni nelle Organizzazioni, tenendo conto anche degli aspetti economici e di efficienza, della missione e delle strategie aziendali;
- Uso dei principi di gestione delle Sicurezza delle Informazioni;
- Il ruolo dei ISMS managers (CSO, Security Officer, ITC Security Managers ...) , requisiti funzionali e posizione nell'organizzazione.
- Compatibilità con altri Sistemi di Gestione.

Ed in particolare:

- Sistemi di gestione basati sul Quality Management.
- Criteri di Auditing Interno per l' ICT Security.
- Gestione della configurazione.
- Gestione delle risorse umane per la Security – consapevolezza.
- Organizzazione dei Sistemi Informativi: ruoli, responsabilità, possibili incompatibilità e segregazione negli incarichi ICT.
- Gestione delle modifiche ai Sistemi Informativi.
- Risk Analysis e Risk Assessment.
- Rischi di ICT Security connessi allo sviluppo e/o acquisto di Sistemi Informativi e di Telecomunicazione.
- Rischi ICT Security connessi con la re-ingegnerizzazione dei processi o del relativo SW.
- Rischi connessi alla gestione della documentazione di sistema.
- Sistemi di controllo interno ed elementi di Corporate Governance.
- Rischi per la Security delle Informazioni nella gestione della catena di fornitura.
- Gestione della Security nell' outsourcing ICT.

#### 1.3 Concetti:

Fondamenti di Security, Sicurezza delle Informazioni, Sistemi ITC e Networking, gestione e miglioramento dei processi di Sicurezza, l' SGSI (o ISMS) e le verifiche (auditing).

In particolare:

- Elementi base dell'ICT, dei concetti di sistema e delle reti.
- Fondamentali della Security.
- Criteri di classificazione dei dati trattati.
- Controllo accesso fisico e logico.
- Protezione delle informazioni ed elementi di crittografia.

<p><b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione</p>	<p align="center"><b>REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</b></p>	<p align="right"><b>RSI 01</b>  Pag. 8/11 Rev.01</p>
---	---	--

- Firma elettronica, digitale.
- Virus, Worms, Programmi maligni in genere, Prodotti e tecniche di prevenzione e di contrasto.
- Business Continuity, Disaster Recovery e Crisis Management.
- Penetration tests e relativi aspetti legali.
- ISO 15408/ITSEC limitatamente alla struttura e ai contenuti del Traguardo di Sicurezza (Security Target) e al formalismo utilizzato per la definizione dei requisiti funzionali
- Rischi per l' ICT Security nel Commercio Elettronico e per l'EDI (Elettronic Data Interchange).
- Rischi per l' ICT Security nella Posta Elettronica.
- Rischi per l' ICT Security nelle operazioni bancarie o di trading remote.
- Rischi di ICT Security nei sistemi di gestione integrati ERP.
- Rischi per l' ICT Security nei Sistemi di supporto alle decisioni (DSS).

#### **1.4 Politica della Sicurezza delle Informazioni:**

Sicurezza delle Informazioni come professione e come compito della gestione, gestione attraverso gli obiettivi della Sicurezza delle Informazioni, standardizzazione, reporting e rendiconto e formulazione della politica per la Sicurezza delle Informazioni.

#### **1.5 Concetti organizzativi:**

- Principi organizzativi e procedure e regole rilevanti;
- Strutture organizzative delle responsabilità, mansioni e competenze.

#### **1.6 Definizione della politica:**

- Visione e missione;
- Strategia e politica, obiettivi strategici ed operativi;
- Approccio - sistematico delle organizzazioni di gestione;
- Modelli di gestione, efficacia ed efficienza, gestione dei progetti.

#### **1.7 Impegno del Management:**

- Integrazione di: metodologie e strumenti;
- Gestione tramite i processi;
- Impegno verso i clienti ed ai requisiti cogenti;
- Politica della Sicurezza delle Informazioni, obiettivi della Sicurezza delle Informazioni;
- Riesame della gestione, disponibilità delle risorse.

#### **1.8 Standards e linee guida:**

Standards ISO ed EN e linee guida relative ai fondamenti e terminologia, e le verifiche dei sistemi di certificazione e accreditamento nonché le prescrizioni SINCERT applicabili:

- ISO 19011:2002 - UNI EN ISO 19011:2003 Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale
- ISO/IEC 27001:2005 - UNI CEI ISO/IEC 27001: 2006 Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti
- ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management
- ISO/IEC 27005:2008 - Information technology - Security techniques – Information security risk management
- ISO/IEC 27006:2007 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC Guide 73:2002 – Risk management – Vocabulary – Guidelines for use in standards
- EA 7/03 Guidelines for the accreditation of bodies operating certification/registration of Information Security Management Systems
- ISO/IEC 13335 Information technology -- Security techniques -- Management of information and communications technology security
- CobiT - Control Objectives for Information and related Technology (ISACA) cenni

<p><b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione</p>	<p align="center"><b>REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</b></p>	<p align="right"><b>RSI 01</b>  Pag. 9/11 Rev.01</p>
---	---	--

## **2. Organizzazione della Sicurezza delle Informazioni:**

### **2.1 Organizzazione**

Organizzazione delle deleghe delle responsabilità e coordinamento dei compiti. Compiti e posizione del Comitato della Sicurezza, Security Management, Security Team e ruolo del personale della Sicurezza delle Informazioni.

### **2.2 Meccanismo di coordinamento:**

Obiettivi, struttura, procedure e comitati, documentazione del sistema di gestione per la Sicurezza delle Informazioni

### **2.3 Verifica (auditing):**

Verifiche e revisione dell'organizzazione della gestione del Sistema di Sicurezza delle Informazioni (ISMS o SGSI), verifica dei processi e dei sistemi, principi per le tecniche d'intervista.

## **3. Principi di gestione dei processi**

- Identificazione dei processi
- Pianificazione dei processi
- Gestione dei processi
- Misura e di miglioramento dei processi

## **4. Tecniche di miglioramento della Gestione della Sicurezza delle Informazioni**

### **4.1 Organizzazione di un'indagine :**

Programmazione, previsione e controllo dell'avanzamento.

### **4.2 Motivazione:**

Teorie della motivazione in relazione alla Sicurezza delle Informazioni.

### **4.3 Tecniche:**

Pianificazione delle indagini, specifica/descrizione degli obiettivi, sviluppo ed uso dei modelli, scelta del modello, pensare in modo induttivo e deduttivo, ciclo plan- do-check-act, tecniche di indagine e valutazione.

### **4.4 Progetti e programmi del miglioramento della Sicurezza delle Informazioni:**

Principi e metodi, messa a punto dei gruppi o team per la Gestione della Sicurezza delle Informazioni, coinvolgimento del personale

### **4.5 Benchmarking:**

Regole e tecniche del Benchmarking.

## **5. Gestione delle risorse, delle infrastrutture e degli ambienti**

### **5.1 Analisi dell'esigenza di competenza, di formazione e di addestramento:**

Integrazione dei programmi di formazione interna dall'alto al basso, identificazione del bisogno della formazione a breve ed a lungo termine e definizione ed organizzazione dei programmi di formazione.

### **5.2 Valutazione dell'efficacia dell'addestramento:**

Accertare la consapevolezza, della rilevanza e dell'importanza delle loro attività; mantenere la registrazione di istruzione, di esperienza, dell'addestramento e della qualificazione.

### **5.3 Infrastrutture**

Caratteristiche strutturali dell'edificio e/o locali (certificati di abitabilità, conformità degli impianti tecnologici, rispondenza della progettazione sia dei locali che degli impianti).

Valutazione della protezione degli ambienti da attacchi esterni. Locali sicuri (camere lampertz).

Analisi dei rischi e relative coperture per le minacce dovute ad eventi naturali

<p><b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione</p>	<p align="center"><b>REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</b></p>	<p align="right"><b>RSI 01</b>  Pag. 10/11 Rev.01</p>
---	---	---

Protezioni contro il fuoco e gli allagamenti.

Sicurezza dei Cablaggi (energia elettrica e rete T.D.), infrastrutture di supporto o impianti ausiliari (UPS).

I cablaggi debbono essere protetti con canaline incassate.

Modalità di controllo accesso ai locali, sistemi di allarme e videosorveglianza

Manutenzione delle infrastrutture, impianti e apparecchiature ... e un'organizzazione in grado di riparare i guasti in tempi definiti.

#### **5.4 Ambienti del lavoro**

Messa in sicurezza dei locali (muri adeguati e porte antincendio, porte blindate, porte controllate da apertura con badge o chiave, vetri antiproiettile/ antisfondamento).

Uso di armadi chiusi e/o blindati, casseforti.

Sicurezza in rispetto alla normativa (626 ...)

### **6. Acquisto e subappalto**

#### **6.1 Selezione e riesame:**

Selezioni e riesami dei fornitori e dei subappaltatori per mezzo di verifiche e/o classificazione del fornitore.

#### **6.2 Accordi:**

Accordi (contratti o non) circa la Sicurezza delle Informazioni e le loro conseguenze.

#### **6.3 Partnership:**

Nell'acquisto, nel subappalto in situazioni normali/usuali o non-normali / non usuali e/o nel controllo e nella consegna "just-in-time".

### **7. Analisi e raccolta dei dati, metodi statistici**

#### **7.1 Obiettivo**

Selezione dell'informazione, informazione per diversi livelli, codificazione, processo statistico, presentazione dei dati, procedure e sistemi, selezione e tecniche.

#### **7.2 Reporting**

Tipi di presentazione e valutazione, tecniche di presentazione, requisiti della presentazione per l'alto, medio e basso management e per tutto il personale.

#### **7.3 Metodi statistici**

- Teoria della probabilità
- Stima
- Campione
- Uso/utilità dei metodi statistici, nelle verifiche per la sicurezza delle informazioni, nell'analisi dei difetti e negli studi dei processi
- Metodi statistici basilari come istogramma, torte, diagrammi, e tendenze per la gestione ed il funzionamento dei servizi
- Controllo del processo
- Controllo dei lotti
- Progetto degli esperimenti (DOE)
- Affidabilità

### **8 Controllo della non conformità**

#### **8.1 Controllo di non conformità**

Individuazione, identificazione delle non conformità. Autorità per la risposta sulla non conformità.

<p><b>AICQ SICEV</b> Sistema di Certificazione e di Valutazione</p>	<p align="center"><b>REQUISITI SPECIFICI PER LA CERTIFICAZIONE DELLE COMPETENZE DEI VALUTATORI E DEI RESPONSABILI DEL GRUPPO DI VALUTAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</b></p>	<p align="right"><b>RSI 01</b>  Pag. 11/11 Rev.01</p>
---	---	---

### **8.2 RegISTRAZIONI della non conformità**

Registrazioni della natura delle non conformità e commenti.  
Dati per analisi e attività di miglioramento

### **8.3 Riesame e trattamento della non conformità**

Riesame del non conformità, tendenze e modello di accreditamento, accettazione della disposizione di non conformità, competenze di valutazione delle conseguenze.

## **9 Aspetti Sociali**

### **9.1 Soddisfazione del personale**

Motivazione, premi, e misura della soddisfazione del personale.

### **9.2 Comunicazione**

Comunicazione, posizione e ruolo degli specialisti della Sicurezza delle Informazioni, gestione del cambiamento, partecipazione ai livelli gestionali ed operativi, aspetti motivazionali nella gestione e nell'organizzazione, stile e cultura del management ed identificazione nell'organizzazione.

## **10 Aspetti legali e normative**

### **10.1 Legislazione**

Legislazioni nazionali ed internazionali, leggi, sicurezza, ambiente, analisi dei rischi, responsabilità contrattuale.

Ed in particolare:

- L. 300/1970 Statuto dei Lavoratori
- Privacy D.Lgsvo 196/2003 e misure minime di sicurezza (All. B del Disciplinare Tecnico al D.Lgsvo e modificazioni successive)
- Conoscenze degli aspetti normativi sulla tutela del Segreto di Stato
- Responsabilità Civili, Penali e Amministrative
- Aspetti relativi alla Proprietà Intellettuale e copyright (L. 633/41 – D.Lgsvo 518/92 – L. 248/00 – Reg. 338/01)
- Aspetti contrattuali relativi all'Outsourcing ed agli approvvigionamenti connessi alla Security
- Aspetti connessi alla Sicurezza delle Informazioni per quel che concerne le responsabilità amministrativa delle Società D.Lgsvo 231/2000, normative di settore, normativa nordamericana (Sarbanes Oxley Act)
- Il rischio operativo (Basilea II)
- Crimini Informatici (Lg. 547/1993)
- Aspetti relativi al commercio elettronico (D.Lgsvo 70/2003 art. 14 e segg.)
- Aspetti legali relativi all'antiterrorismo (L.155/2005 cosiddetto Decreto Pisanu)
- Aspetti legali legati alla proprietà industriale (D.Lgsvo 30/2005)
- Aspetti legali e normativi legati all'introduzione della Firma Elettronica e della Firma Digitale (D.Lgsvo 82/2005)

### **10.2 Aspetti normativi**

Norme nazionali ed internazionali, accreditamento e certificazione .