

Progetto CSICS

*“Certificazione della Sicurezza ICT nelle Infrastrutture Critiche
e Strategiche”*

Indice

1.	Denominazione del progetto	3
2.	Amministrazioni proponenti	3
3.	Contesto di inquadramento del progetto	3
4.	Descrizione obiettivi generali del progetto.....	4
5.	Descrizione degli obiettivi specifici del progetto	4
5.1	Prima fase	4
5.2	Seconda fase.....	5
6.	Durata temporale del progetto	5
7.	Area geografica di localizzazione dell'intervento	5
8.	Descrizione delle attività per il conseguimento dei risultati attesi	5
8.1	Elenco dei rilasci	6
9.	Impegno delle risorse e piano di finanziamento del progetto	8
9.1	Risorse strumentali.....	8
9.2	Risorse FUB	8
9.3	Risorse umane ISCTI	9

1. Denominazione del progetto

- ACRONIMO: CSICS
- TITOLO: “Certificazione della Sicurezza ICT nelle Infrastrutture Critiche e Strategiche”

2. Amministrazioni proponenti

- Ministero per lo Sviluppo Economico – Istituto Superiore delle Comunicazioni e delle Tecnologie dell’Informazione (ISCTI).
- Fondazione Ugo Bordoni

3. Contesto di inquadramento del progetto

La crescente utilizzazione delle tecnologie ICT in applicazioni sempre più importanti dal punto di vista economico e della tutela dei diritti dei cittadini, tra i quali il diritto alla privacy, ha fatto aumentare negli ultimi anni l’esigenza di disporre di schemi della certificazione della sicurezza dei dispositivi ICT utilizzati nelle predette applicazioni. Questa esigenza si pone poi con requisiti ancor più stringenti quando le tecnologie ICT vengono utilizzate per fornire i cosiddetti servizi essenziali definiti dalla Direttiva europea 2016/1148 del 6 luglio 2016 (nota anche con il nome di Direttiva NIS) concernente la sicurezza delle reti e dei sistemi informativi. In base alla predetta Direttiva tali servizi sono caratterizzati dall’essere essenziali per il mantenimento di attività critiche sociali e/o economiche e dall’impatto potenzialmente devastante sulla loro fornitura che può derivare da incidenti che coinvolgano le reti e i sistemi informativi da cui dipendono. Oggetto di particolare attenzione nella Direttiva NIS sono anche i servizi digitali, offerti da operatori per lo più privati, dal cui corretto funzionamento generalmente dipendono sia i servizi essenziali sia altri servizi di rilevante importanza. Il governo italiano, a seguito della Direttiva NIS, con il DPCM del 17 febbraio 2017 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali) e con il Piano nazionale per la protezione cibernetica e la sicurezza informatica del marzo 2017 ha deciso di adottare un insieme di misure tra le quali l’istituzione presso il Ministero dello Sviluppo Economico di un Centro di Valutazione e Certificazione Nazionale (CVCN) della sicurezza di prodotti, apparati e sistemi ICT destinati ad infrastrutture critiche e strategiche (ICS). I risultati delle attività di studio e approfondimento previste in questo progetto costituiscono un contributo all’istituzione del predetto Centro, per ciò che concerne sia l’avvio in tempi brevi di una fase operativa pilota, sia successivi sviluppi finalizzati ad incrementare progressivamente le capacità operative.

4. Descrizione obiettivi generali del progetto

Il progetto mira ad eseguire uno studio di fattibilità che, sulla base dei requisiti derivanti dalla normativa, nonché dalle esigenze degli stakeholder del settore, individui possibili soluzioni dal punto di vista tecnico, organizzativo e procedurale per la realizzazione di un Centro di Valutazione e Certificazione Nazionale in grado di soddisfare tali requisiti ed esigenze. Gli aspetti economici non saranno oggetto dello studio ma, al fine di ridurre i costi, nella selezione delle soluzioni saranno preferite quelle che si basino in parte su componenti già esistenti che siano in grado di soddisfare un sottoinsieme dei suddetti requisiti. A tal fine lo studio avrà l'obiettivo di individuare preliminarmente quanto già esistente a livello di standard, metodologie, procedure, risorse umane e materiali che appaia idoneo per l'impiego nel contesto di interesse e di verificarne l'effettiva utilizzabilità e le relative modalità di utilizzo. Per favorire la riutilizzabilità di quanto esistente si ipotizzerà, in analogia a quanto avviene normalmente per le attività di valutazione e certificazione della sicurezza ICT, la creazione di uno Schema di Valutazione e Certificazione Nazionale (SVCN) coordinato dal CVCN. Per ciò che concerne componenti che risultino necessarie ma non (o solo in parte) disponibili e/o utilizzabili, lo studio mirerà a definirne i requisiti realizzativi e, ove possibile, a fornire indicazioni utili alla loro implementazione. Tenendo conto dell'esigenza di consentire tale avvio in tempi molto stretti, in modo da permettere al più presto una mitigazione del rischio in un settore così delicato come quello ICS, in una prima fase operativa verranno prese in considerazione soluzioni sperimentali che potranno essere meglio sviluppate nelle fasi successive.

5. Descrizione degli obiettivi specifici del progetto

5.1 Prima fase

La prima fase punta a produrre risultati che costituiscano soluzioni a problemi di carattere tecnico, organizzativo e procedurale che si ritiene debbano essere affrontati per contribuire all'avvio in tempi brevi di una fase operativa pilota. Sarà quindi necessario caratterizzare preliminarmente la fase operativa pilota attraverso la definizione dei diversi aspetti che la differenzieranno dalla piena operatività a regime. Successivamente, tenendo conto della predetta caratterizzazione, si dovrà procedere alla definizione di una o più architetture generali del SVCN e del CVCN, all'individuazione di standard/metodologie esistenti o da sviluppare per la valutazione e certificazione nel SVCN, alla definizione di processi e procedure, alla definizione di linee guida per la certificazione da sviluppare in collaborazione con gli stakeholder del contesto ICS e alla definizione di requisiti per la protezione delle informazioni nel SVCN. Per quanto riguarda la definizione di linee guida per la certificazione nel

contesto ICS, dalla caratterizzazione della fase operativa pilota potrebbe derivare che inizialmente le linee guida per la certificazione vengano sviluppate per le ICS di uno specifico settore (ad esempio quello energetico). Per ciò che concerne invece i requisiti per la protezione delle informazioni nel SVCN è importante evidenziare che Il Piano Nazionale per la protezione cibernetica e la sicurezza informatica emanato dalla Presidenza del Consiglio dei Ministri nel marzo del 2017 definisce una «scala di criticità» articolata su tre livelli. Al livello massimo e a quello minimo corrispondono i contesti della sicurezza nazionale dello Stato e del tessuto produttivo nazionale/cittadinanza, nei quali operano schemi di certificazione già esistenti, coordinati rispettivamente dall'Autorità Nazionale per la Sicurezza (ANS) e dall'Organismo di Certificazione della Sicurezza Informatica (OCSI). Al livello di criticità intermedio corrisponde invece il contesto delle infrastrutture critiche nazionali nel quale dovrà operare l'SVCN coordinato dal CVCN. I requisiti per la protezione delle informazioni nel SVCN potranno quindi essere meno severi di quelli dello schema coordinato da ANS ma dovranno garantire una protezione più elevata di quella relativa allo schema coordinato da OCSI.

5.2 Seconda fase

Dopo aver prodotto i risultati delle attività relative alla prima fase, risultati che potranno contribuire ad avviare la fase operativa pilota, il progetto mirerà ad incrementare gradatamente le capacità operative del SVCN attraverso varie integrazioni da apportare alle soluzioni individuate nella prima fase. A tal fine sono previste due integrazioni nel periodo di esecuzione del progetto le quali, data la complessità del contesto ICS e delle attività di valutazione e certificazione da eseguire nel SVCN, prevedibilmente comporteranno ulteriori sviluppi per coprire tutte le necessità operative del nuovo schema.

6. Durata temporale del progetto

Il progetto avrà una durata di 12 mesi dalla data di sottoscrizione.

7. Area geografica di localizzazione dell'intervento

Italia

8. Descrizione delle attività per il conseguimento dei risultati attesi

Si riporta in modalità grafica la suddivisione del progetto per attività assieme ad un cronoprogramma. La documentazione che verrà prodotta raccoglierà i risultati delle attività svolte.

	Attività	Descrizione
PRIMA FASE Attività che contribuiscono all'avvio della fase operativa pilota	A1	Caratterizzazione della fase operativa pilota del SVCN
	A2	Definizione possibili architetture del SVCN e del CVCN
	A3	Individuazione standard/metodologie da utilizzare nel SVCN
	A4	Requisiti per la protezione delle informazioni nel SVCN
	A5	Definizione linee guida per la certificazione nel settore ICS
	A6	Definizione di processi e procedure all'interno del SVCN
SECONDA FASE Attività che contribuiscono ai successivi sviluppi del SVCN	A7	Prima integrazione delle soluzioni adottate nella fase operativa pilota
	A8	Seconda integrazione delle soluzioni adottate nella fase operativa pilota

Attività/Mese	1	2	3	4	5	6	7	8	9	10	11	12
A1	D1											
A2	D2											
A3	D3											
A4		D4										
A5			D5									
A6			D6									
A7								D7				
A8												D8

8.1 Elenco dei rilasci

Di seguito vengono riportati i rilasci che si prevede di produrre nell'ambito del progetto.

Elenco rilasci		Mese
D1	Caratterizzazione della fase operativa pilota del SVCN	1
D2	Definizione possibili architetture del SVCN e del CVCN	1
D3	Individuazione standard/metodologie da utilizzare nel SVCN	1
D4	Requisiti per la protezione delle informazioni nel SVCN	2
D5	Definizione linee guida per la certificazione nel settore ICS	3
D6	Definizione di processi e procedure all'interno del SVCN	3

D7	Prima integrazione delle soluzioni adottate nella fase operativa pilota	8
D8	Seconda integrazione delle soluzioni adottate nella fase operativa pilota	12

I deliverable da D1 a D6 verranno prodotti nella prima fase del progetto al fine di contribuire all'avvio della fase operativa pilota.

In particolare il deliverable D1 raccoglierà innanzitutto i risultati di un'analisi che dovrà individuare quanto di disponibile e utilizzabile esiste e quanto potrà essere realizzato entro la data di possibile attivazione della fase operativa pilota (tre mesi dopo l'inizio del progetto). Dai risultati di tale analisi saranno poi derivati gli aspetti che caratterizzeranno la fase operativa pilota.

I contenuti di tutti i rimanenti deliverable della prima fase del progetto saranno potenzialmente influenzati dalla caratterizzazione della fase operativa pilota effettuata nel deliverable D1. Nella seconda fase del progetto sono previste due tappe (all'ottavo mese a al dodicesimo mese), in corrispondenza delle quali saranno possibili due incrementi delle capacità operative del SVCN. Per ciascuno di questi incrementi i deliverable da D2 a D6 prodotti nella prima fase potranno subire integrazioni e/o modifiche.

Nel deliverable D2, che includerà le architetture del SVCN e del CVCN, si terrà conto delle particolarità dell'SVCN rispetto ad uno schema di certificazione ordinario, per ciò che concerne sia il contesto di applicazione (ICS) sia le funzioni del CVCN, che non si limitano alla certificazione, bensì includono anche la valutazione.

Nel deliverable D3 saranno individuati gli standard/metodologie di valutazione e certificazione già esistenti e utilizzabili nel contesto ICS, per quanto riguarda sia componenti ICT ordinari sia componenti tipicamente utilizzati in tale contesto. Inoltre saranno illustrate eventuali necessità di sviluppo di nuove metodologie che siano in grado di recepire in modo più efficace e completo le esigenze che vi sono nel contesto operativo di interesse.

Il deliverable D4 raccoglierà i requisiti da soddisfare nel SVCN relativamente alla protezione delle informazioni in esso trattate. Come sopra evidenziato, tali requisiti dovranno essere più stringenti di quelli che valgono nello schema di certificazione coordinato da OCSI, tenendo conto del fatto che la possibile agevolazione nell'esecuzione di attacchi derivante da eventuali violazioni relative alle suddette informazioni può provocare nel caso del SVCN danni considerevolmente più gravi ed il possibile coinvolgimento di un elevato numero di persone.

Il deliverable D5 affronterà il problema dell'individuazione, caso per caso, della modalità di certificazione più idonea. A tal fine il deliverable conterrà linee guida che, tenendo conto delle caratteristiche dell'oggetto da certificare e del suo livello di criticità (da stimare secondo criteri da

concordare con gli stakeholder del settore), forniranno indicazioni relativamente a standard/metodologia di certificazione più idoneo/a, livello di certificazione (se previsto dallo standard/metodologia di certificazione), selezione delle funzionalità di sicurezza da certificare (se prevista dallo standard/metodologia di certificazione), ecc.

Nel deliverable D6 verranno riportate le descrizioni dei processi e delle procedure che regoleranno il funzionamento del SVCN. Conseguentemente verranno illustrate le modalità di esecuzione delle varie attività previste (comprese quelle di accreditamento di entità esterne al CVCN), specificando i ruoli delle entità coinvolte e le interazioni che dovranno avere. Questo deliverable farà riferimento al deliverable D4 per ciò che concerne le modalità di protezione delle informazioni gestite nel SVCN.

Nei delliverable D7 e D8 saranno contenute le integrazioni di quanto definito al termine della prima fase necessarie ad incrementare le capacità operative del SVCN. Tali integrazioni potranno consistere in aggiunte e/o modifiche da fare sui deliverable della prima fase D2-D6 e/o in risultati di analisi utili per il conseguimento del predetto incremento ma non inquadrabili in tali deliverable.

9. Impegno delle risorse e piano di finanziamento del progetto

Il progetto è finanziato dall’Istituto Superiore CTI del Dipartimento per le Comunicazioni, che si avvarrà delle competenze e delle professionalità della Fondazione Ugo Bordoni.

9.1 Risorse strumentali

Nella tabella seguente sono indicate le spese relative agli acquisti della strumentazione necessaria alla realizzazione del progetto di competenza dell’Istituto Superiore delle Comunicazioni e delle Tecnologie dell’Informazione come indicato nell’Art. 6 comma 2 della Convenzione.

Hardware	
Descrizione	Costo (€)
Software	
Descrizione	Costo (€)

Nota: La stima dei costi elencata è da considerarsi al netto dell’IVA

9.2 Risorse FUB

Nella tabella seguente sono indicati gli impegni di spesa della FUB per lo svolgimento del progetto.

Spese FUB (Totale)	Costo
Risorse umane e spese accessorie	230.000,00
Totale	230.000,00

9.3 Risorse umane ISCTI

Nella tabella seguente è indicato il numero di risorse umane dell'Istituto impegnate nel progetto.

Risorse umane ISCTI	1 Funzionario tecnici Area III IGE 1 Funzionario tecnici Area III F5 6 Funzionario tecnici Area III F4 1 Funzionario tecnici Area III F3 1 Funzionario tecnici Area III F2
----------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Firmato da: Rita Forsi
Data: 06/12/2017 19:03:23

SASSANO ANTONIO
07.12.2017 13:23:51 UTC

