ALLEGATO 4

CAPITOLATO TECNICO – Lotto II

SOMMARIO

1 INTRODUZIONE 3

2 CARATTERISTICHE DELLA FORNITURA 4

3 DESCRIZIONE DEI SERVIZI OGGETTO DEL LOTTO II 5

3.1 SEDI DI FORNITURA 6

4 DESCRIZIONE DELLA FORNITURA 7

4.1 CONTROLLO E VALUTAZIONE DEI LIVELLI DI SICUREZZA 7

4.1.1 Governance della Sicurezza delle Informazioni 7

4.1.1.1 Obiettivi delle fasi 8

4.1.1.1.1 Rilevazione dell'ambito di intervento 8

4.1.1.1.2 Valutazione dello stato della sicurezza 9

4.1.1.1.3 Definizione degli obiettivi di sicurezza e Gap Analysis 9

4.1.1.1.4 Individuazione Progetti di sicurezza e Roadmap 10

4.1.1.1.5 Sviluppo del piano strategico e dei piani di sicurezza 10

4.1.2 Servizi on demand 11

4.1.2.1 Vulnerability Assessment 11

4.1.2.2 Penetration Test Applicativo e Infrastrutturale 12

4.1.2.3 Source Code Auditing 14

4.1.2.4 Deliverables dei Servizi On Demand 14

4.1.2.4.1 Executive Summary 15

4.1.2.4.2 Technical Report 15

4.1.3 Composizione del Team 15

4.2 RESPONSABILE DELLA FORNITURA, ATTIVITÀ ESECUTIVE 19

4.2.1 Startup del servizio 19

4.2.2 gestione dei servizi On Demand 20

4.2.2.1 Richiesta di Servizi On Demand 20

4.2.2.2 Attività esecutive relative a successive attivazioni di servizi On Demand. 20

5 INDICATORI DI QUALITÀ 21

5.1 INDICATORI DI QUALITÀ 22

5.1.1 IQ1: Sostituzione del Responsabile Tecnico della fornitura 22

5.1.2 IQ2: Personale della fornitura inadeguato 23

5.1.3 IQ3: Turn Over del personale 24

5.1.4 IQ4: Qualità della documentazione prodotta 25

6 CERTIFICAZIONI DELL'IMPRESA 26

1 INTRODUZIONE

Il presente Capitolato Tecnico disciplina gli aspetti tecnici della Fornitura dei servizi necessari per l'erogazione dei Managed Security Services per la Corte dei conti (nel seguito indicata per comodità con Cdc) afferenti al **Lotto II - "Controllo e valutazione dei livelli di sicurezza"**.

Nel seguito del documento si ricorrerà più volte ad alcuni termini cui è attribuito il seguente significato:

- **Capitolato Tecnico**, il presente documento,
- **Amministrazione**, la Corte dei conti, "Cdc",
- **Committente**, la CONSIP S.p.A.,
- **Impresa**, l'Impresa aggiudicataria della gara;
- **Fornitura**, quanto indicato nel capitolo 4,
- **Servizio/i,** il servizio o l'insieme dei servizi connessi alla Fornitura in oggetto,
- **MSS,** Managed Security Services,
- **SOC**, Security Operation Center,
- **SaaS**, Security as a Services.

2 CARATTERISTICHE DELLA FORNITURA

Il Committente ha inteso organizzare la presente iniziativa di acquisizione in maniera da rispondere in modo efficiente e flessibile alle esigenze attuali e future dell'Amministrazione in tema di servizi di sicurezza.

L'insieme dei Managed Security Services di cui la Cdc intende avvalersi, è stato suddiviso in due distinte macroattività.
La prima macroattività ha come obiettivo principale la conduzione dei sistemi (gestione e monitoraggio) e l'introduzione di nuovi servizi di sicurezza on demand atti a mantenerne la perfetta efficienza ed il costante allineamento con l'evoluzione tecnologica del mercato ICT coerentemente con gli obiettivi strategici dell'Amministrazione

La seconda macroattività ha come obiettivo il controllo e la valutazione dello stato della sicurezza implementata presso l'Amministrazione e l'attivazione on demand di ulteriori forme di controllo specifiche qualora la Cdc ritenga opportuno approfondire dei contesti specifici della sicurezza del proprio patrimonio informativo.

In considerazione della particolare natura dell'insieme di attività che vanno a costituire i Managed security Services, questi sono stati articolati in due lotti mutuamente esclusivi.

Il presente Capitolato tecnico descriverà l'oggetto di fornitura relativo al **Lotto II - "Controllo e valutazione dei livelli di sicurezza"** costituito da:

- Governance della Sicurezza delle Informazioni per il controllo e la valutazione dei livelli di sicurezza presenti nella Corte dei conti;
- Servizi on demand richiesti a fronte di evoluzioni tecnologiche o all'emergere di nuove esigenze della Corte dei conti.

La durata massima prevista per la fornitura del Lotto II è fissata a 36 mesi a partire dalla data di "Dichiarazione di inizio dei servizi".

3 DESCRIZIONE DEI SERVIZI OGGETTO DEL LOTTO II

Di seguito sono descritti i servizi e le specifiche tecniche ed i requisiti relativi alla **Fornitura del Lotto II**:

- **Controllo e valutazione dei livelli di sicurezza**, secondo quanto descritto al paragrafo **Errore. L'origine riferimento non è stata trovata.** costituita a sua volta da:
  - la **Governance della Sicurezza delle Informazioni,** secondo quanto descritto al paragrafo 4.1.1
  - i **Servizi On Demand**, secondo quanto descritto al paragrafo 4.1.2

Per l'erogazione dei servizi oggetto del presente capitolato tecnico, l'Impresa dovrà definire le seguenti figure professionali:

- **Responsabile del contratto**, ha la responsabilità di gestire e risolvere tutte le problematiche legate al corretto svolgimento del contratto (es. fatturazione, verifica del rispetto dei livelli di servizio, definizione e aggiornamento del Team di cui al paragrafo 4.1.3) nonché l'attivazione di nuovi servizi on demand.
- **Responsabile tecnico** per l'erogazione dei servizi, ha la responsabilità di coordinare dal punto di vista operativo tutte le attività legate ai servizi oggetto del presente capitolato tecnico e di essere il punto di riferimento per l'attivazione dei servizi on demand. Il Responsabile tecnico dovrà inoltre coordinare tutte le attività e produrre resoconti periodici, da presentare per discussione durante i SAL di progetto.

  I SAL, da tenere con cadenza mensile o su esplicita richiesta del Committente/Amministrazione, riguarderanno almeno i seguenti argomenti:
  - dettaglio delle attività svolte e quelle ancora da svolgere;
  - eventuali problematiche insorte;
  - questioni aperte di carattere strategico/metodologico da sottoporre all'attenzione del Committente/Amministrazione.

  A fronte di eventuali problematiche che dovessero presentarsi, il SAL dovrà comprendere anche le relative proposte di risoluzione e la relativa ripianificazione delle attività impattate.

Ogni mese, il responsabile tecnico del servizio, durante i SAL mensili, dovrà presentare al Committente il "Resoconto attività" contenente lo stato della fase in lavorazione e i giorni persona effettivamente impiegati nell'erogazione del servizio al fine di fornire le necessarie informazioni relative alla fatturazione del servizio erogato.

L'impresa dovrà comunicare al Committente il numero di telefono e l'e-mail con le quali contattare tali figure professionali il cui ruolo potrà essere assunto anche dalla medesima persona.

3.1 SEDI DI FORNITURA

Le prestazioni oggetto del presente capitolato dovranno potranno erogate sia presso la sede dell'Impresa, sia presso le sedi di Roma della Cdc a seconda delle esigenze di progetto. Di seguito viene riportato un elenco non esaustivo delle sedi principali della Corte dei conti:

- Roma – via Antonio Baiamonti, n. 25;
- Roma - via Atanasio Soldati, n.80 (La Rustica).

4 DESCRIZIONE DELLA FORNITURA

Di seguito è fornita una descrizione di massima dei servizi costituenti il *Lotto II - "Controllo e valutazione dei livelli di sicurezza"*.

Il Fornitore prende atto che, nel corso dell'erogazione dei servizi, l'introduzione di nuove tecnologie a fronte delle evoluzioni in ambito ICT potrà comportare significative variazioni del contesto tecnologico di inizio fornitura e si impegna ad erogare i servizi richiesti adeguando le conoscenze del personale impiegato nell'erogazione dei servizi o inserendo nei gruppi di lavoro risorse con skill adeguato, senza alcun onere aggiuntivo per Consip/Amministrazione.

I servizi dovranno essere erogati per l'intera durata indicata da Consip operando sia con gli strumenti a supporto delle infrastrutture di Consip e/o dell'Amministrazione sia con strumenti messi a disposizione dal Fornitore in adempimento alle obbligazioni contrattuali; l'uso di questi strumenti/servizi non produrrà oneri aggiuntivi per Consip/Amministrazione.

Tutti gli eventuali strumenti utilizzati a supporto dell'erogazione dei servizio descritti nel presente capitolato sono a totale onere dell'Impresa.

4.1 CONTROLLO E VALUTAZIONE DEI LIVELLI DI SICUREZZA

Nell'ambito dell'insieme di attività che definiscono il *Lotto II - "Controllo e valutazione dei livelli di sicurezza"*, la **Governance della Sicurezza delle Informazioni** rappresenta il servizio fondamentale, volto al miglioramento continuo dei livelli di sicurezza della Corte dei conti. A corredo potranno essere attivati ulteriori **Servizi On Demand** come descritto nei paragrafi successivi.

4.1.1 GOVERNANCE DELLA SICUREZZA DELLE INFORMAZIONI

La **Governance della Sicurezza delle Informazioni** dovrà prevedere un ciclo virtuoso articolato nelle seguenti fasi:

- Rilevazione dell'ambito di intervento in base agli obiettivi strategici dell'amministrazione;
- Valutazione dello stato della sicurezza rispetto agli standard;
- Definizione degli obiettivi di sicurezza e Gap Analysis;
- Individuazione Progetti di sicurezza e Roadmap;
- Sviluppo del piano strategico, in grado di fornire un percorso evolutivo della sicurezza che sia:
    - a supporto degli obiettivi strategici dell'Amministrazione;
    - sinergico con le nuove esigenze evolutive IT;
    - teso al miglioramento continuo dei processi e all'utilizzo ottimale delle risorse.

Tali attività dovranno essere coerenti con gli standard ISO 27001 e ISO 27002.

Tutte le fasi dovranno considerare, in maniera integrata e sinergica, i seguenti aspetti legati

alla sicurezza delle informazioni:

- Governance e Compliance: valutare e adeguare i sistemi e le politiche di sicurezza aziendali con gli obiettivi aziendali, le leggi ed i regolamenti vigenti;
- Threat Management: definire soluzioni di sicurezza in funzione delle minacce esistenti e coerenti con le strategie aziendali, assegnando ai vari elementi da proteggere, la giusta criticità, a difesa della rete, dell'infrastruttura e gestendo vulnerabilità ed incidenti;
- Identity and Access Management: definire i sistemi di gestione dell'identità e di controllo accessi in grado di proteggere i dati, i sistemi e le strutture da accessi non autorizzati;
- Application and Data Security: soluzioni e best practices per l'innalzamento della sicurezza applicativa e dei dati da esse gestiti durante tutto il ciclo di vita dell'applicazione stessa;
- Physical Security: implementare le funzionalità di sorveglianza in modo più flessibile salvaguardando le risorse aziendali.

4.1.1.1 Obiettivi delle fasi

Ogni fase precedentemente descritta dovrà produrre un documento che fornisca un concreto valore aggiunto per l'Amministrazione. Di seguito vengono descritti quali sono gli obiettivi e cosa dovrà essere prodotto in ciascuna fase che compone il servizio di **Governance della Sicurezza delle Informazioni.**
Tale descrizione è puramente a titolo esemplificativo e non esaustivo, l'Impresa potrà proporre il proprio modello di security assessment a patto che sia coerente e rispetti quanto descritto nel presente capitolato.

4.1.1.1.1 Rilevazione dell'ambito di intervento

L'obiettivo di questa fase consiste nel rilevare il contesto strategico, organizzativo, tecnologico e normativo che caratterizza l'operatività dell'Amministrazione in merito ai principali servizi erogati.

Le attività che dovranno essere svolte in questa fase dovranno comprendere l'analisi dei seguenti aspetti:

- Contesto della Missione Istituzionale, piani strategici di evoluzione dei servizi ICT, normative, politiche e direttive aziendali rilevanti per la Sicurezza delle Informazioni;
- Organizzazione, Processi, Sottoprocessi, Servizi della Direzione ICT;
- Organizzazione e processi dei servizi Sicurezza;
- Servizi strategici per l'Amministrazione: obiettivi, utenti, dati, risorse tecnologiche (server, middleware, applicazioni, reti,..)
- Fornitori
- Normative

Tale analisi dovrà produrre un documento che descriva le specificità organizzative e la mappatura tecnologica dei principali servizi dell'Amministrazione. Inoltre tale documento

dovrà contenere gli elementi utili per una corretta strategia di Information Security Governance al fine di indirizzare in maniera strutturata le future iniziative di sicurezza.

4.1.1.1.2 Valutazione dello stato della sicurezza

L'obiettivo di questa fase consiste nel rilevare lo stato attuale della Gestione della Sicurezza delle informazioni rispetto agli standard ISO/IEC 27001 e ISO/IEC 27002, al fine di supportare future attività progettuali che prevedono una corretta definizione degli obiettivi strategici e una puntuale individuazione degli interventi di miglioramento.

Le attività che dovranno essere svolte in questa fase comprendono l'analisi degli aspetti rilevanti rispetto ai domini di sicurezza degli standard ISO precedentemente citati:

- Politiche di Sicurezza
- Organizzazione della Sicurezza delle Informazioni
- Assett Management
- Risorse Umane
- Sicurezza Fisica ed ambientale
- Gestione delle Operazioni e delle comunicazioni
- Controllo degli accessi
- Acquisizione, sviluppo e manutenzione dei sistemi informatici
- Gestione degli incidenti di SIcurezza
- Continuità Operativa
- Compliance

Tale analisi dovrà produrre un documento di assessment contenente lo stato rilevato rispetto agli 11 domini degli standard ISO/IEC 27001 e ISO/IEC 27002 e che metta in evidenza il livello di compliance attuale.

4.1.1.1.3 Definizione degli obiettivi di sicurezza e Gap Analysis

L'obiettivo di questa fase consiste nel fornire supporto all'Amministrazione nella definizione degli obiettivi strategici di Sicurezza in termini di livelli di maturità rispetto ai domini degli standard ISO/IEC 27001 e ISO/IEC 27002.

In base alla definizione di questi obiettivi dovrà essere effettuata una Gap Analysis per individuare le aree di intervento da indirizzare al fine di colmare i gap rilevati.

Le attività che dovranno essere svolte in questa fase comprendono una serie di interviste con i responsabili delle decisioni strategiche dell'Amministrazione per fissare gli obiettivi in termini di livelli di maturità rispetto ai domini di sicurezza degli standard ISO/IEC 27001 e ISO/IEC 27002 ed in particolare inerenti i seguenti aspetti:

- Politiche di Sicurezza
- Organizzazione della Sicurezza delle Informazioni
- Assett Management
- Risorse Umane
- Sicurezza Fisica ed ambientale
- Gestione delle Operazioni e delle comunicazioni

- Controllo degli accessi
- Acquisizione, sviluppo e manutenzione dei sistemi informatici
- Gestione degli incidenti di SIcurezza
- Continuità Operativa
- Compliance

Tale analisi dovrà produrre un documento contente una Gap Analysis che evidenzi, per ciascun dominio ISO, il livello target di maturità da raggiungere, gli scostamenti rilevati e le aree di intervento da indirizzare.

4.1.1.1.4 Individuazione Progetti di sicurezza e Roadmap

L'obiettivo di questa fase consiste nel definire gli interventi di miglioramento atti a colmare il gap evidenziato nella fase di Gap Analysis e realizzare una Roadmap di sviluppo di tali interventi in funzione delle priorità definite dall'Amministrazione.

Le attività che dovranno essere svolte in questa fase comprendono la definizione, per ciascuna area di intervento identificata nella fase di Gap Analysis, degli interventi progettuali individuando e formalizzando i seguenti aspetti:

- obiettivi dell'intervento progettuale;
- attività da svolgere;
- risultati attesi e criteri di completamento;
- ruoli e responsabilità delle risorse coinvolte;
- requisiti organizzativi, di processo e procedurali;
- requisiti tecnologici;
- requisiti di conformità normativa;
- stima di massima dei tempi;
- stima di massima dei costi;
- Servizi strategici dell'Amministrazione impattati;
- Processi Operativi dell'Amministrazione impattati;

Tale fase dovrà produrre un documento che supporti l'Amministrazione nell' assegnazione delle priorità degli interventi di miglioramento. Successivamente dovrà essere realizzata una Roadmap degli interventi tenendo in considerazione i vincoli di sequenzialità tra i diversi interventi e l'allineamento con gli obiettivi strategici della Amministrazione e della funzione ICT.

4.1.1.1.5 Sviluppo del piano strategico e dei piani di sicurezza

L'obiettivo di questa fase consiste nel formalizzare il Piano Strategico della Sicurezza dell'Amministrazione e i Piani di Sicurezza degli interventi di miglioramento identificati e considerati prioritari.

Le attività che dovranno essere svolte in questa fase comprendono lo sviluppo e la validazione dei seguenti documenti:

- Piano Strategico della Sicurezza delle Informazioni dell'Amministrazione
- Piani di Sicurezza degli Interventi di Miglioramento che rientrano nell'arco temporale definito con l'Amministrazione

Il Piano Strategico della Sicurezza dovrà contenere la definizione di alto livello degli obiettivi strategici, in merito alla Information Security Governance ed alla realizzazione del Sistema di Gestione della Sicurezza delle Informazioni di Corte dei Conti, e referenzierà i Piani di Sicurezza e la relativa Roadmap fornendo indicazioni in merito all'attuazione di questi ultimi.
I Piani di Sicurezza dovranno contenere le specifiche attuative degli interventi di miglioramento e costituiranno di fatto l'action plan di dettaglio del Piano Strategico della Sicurezza delle Informazioni.

4.1.2 SERVIZI ON DEMAND

Nell'ambito dei servizi "***on demand***" attivabili nel *Lotto II - "Controllo e valutazione dei livelli di sicurezza"*, è possibile trovare sia servizi a supporto delle attività di *"Governance della Sicurezza delle Informazioni"* sia servizi attivabili su richiesta dell'Amministrazione a fronte di specifiche criticità. Alcuni esempi di servizi "***on demand***" attivabili nel *Lotto II - "Controllo e valutazione dei livelli di sicurezza"* possono essere i seguenti:

- Vulnerability Assessment
- Penetration Test Applicativo e Infrastrutturale
- Source Code Auditing

Tali servizi vengono dettagliatamente descritti nei seguenti paragrafi.

4.1.2.1 Vulnerability Assessment

Il servizio di Vulnerability Assessment deve fornire una panoramica dello stato di sicurezza dell'infrastruttura oggetto di analisi attraverso la raccolta di informazioni concernente i servizi erogati, l'architettura e le configurazioni del sistema.

Queste informazioni dovranno essere confrontate con le vulnerabilità potenziali evidenziate dalla scansione.

Per la raccolta di tali informazioni l'Impresa potrà avvalersi di strumenti automatizzati al fine di rilevare le potenziali vulnerabilità. Gli strumenti dovranno essere configurati in modo da non risultare intrusivi (a meno che non espressamente richiesto e concordato con l'amministrazione).

L'Impresa potrà proporre il proprio modello di Vulnerability Assessment a patto che sia coerente e rispetti quanto descritto nel presente capitolato.

Il servizio di Penetration Test Applicativo e Infrastrutturale dovrà prevedere almeno le seguenti fasi, da considerarsi come requisiti minimi da rispettare:

- Raccolta di informazioni: al fine di raccogliere informazioni sui sistemi oggetto della scansione e sui relativi servizi attivi;
- Individuazione delle vulnerabilità: al fine di collezionare, tramite un set opportuno di strumenti automatizzati e correttamente configurati, una lista delle potenziali vulnerabilità note a cui potrebbero essere soggetti i sistemi analizzati;
- Analisi dei risultati: al fine di individuare tra le vulnerabilità trovate nella fase precedente, i falsi positivi.

4.1.2.2 Penetration Test Applicativo e Infrastrutturale

Il servizio di Penetration Test Applicativo e Infrastrutturale dovrà prevedere una verifica dinamica della sicurezza dei sistemi dell'Amministrazione allo scopo di identificare eventuali vulnerabilità, configurazioni di sicurezza errate, carenze sui livelli di protezione attivi che espongano il contesto ad attacchi interni ed esterni.
La metodologia adottata dovrà fare riferimento alla standard internazionale per l'esecuzione dei test di sicurezza sviluppata dall'ISECOM e alle linee guida per le attività di assessment applicativo definite dall'OWASP.

L'Impresa potrà proporre il proprio modello di Penetration Testing a patto che sia coerente e rispetti quanto descritto nel presente capitolato.

Il servizio di Penetration Test Applicativo e Infrastrutturale dovrà prevedere almeno le seguenti fasi, da considerarsi come requisiti minimi da rispettare:

- **Information Gathering, Mapping e Remote Discovery**: fase svolta al fine di reperire il maggior numero possibile di informazioni sulle piattaforme oggetto di analisi;
- **Service Discovery**: fase svolta con l'ausilio di scanner automatici, specifici per il contesto infrastrutturale, al fine di rilevare potenziali vulnerabilità. Durante questa fase dovranno essere utilizzate anche tecniche di evasione specifiche basate sulla manipolazione dei pacchetti TCP/IP (frammentazione, bad checksum, ordine dei pacchetti, ecc.) o sulle caratteristiche dell'applicazione (ad esempio mediante codifica dei caratteri o utilizzo di servizi criptati). La fase di Service Discovery dovrà adattarsi al contesto infrastrutturale specifico ed alle peculiari vulnerabilità associate allo specifico modello di trasporto.
- **Application Mapping & Data Flow Discovery**: fase svolta al fine di analizzare le informazioni ottenute nelle fasi precedenti al fine di verificare tecniche di attacco basate sulla validazione dell'input dell'utente, sulla gestione delle sessioni e sull'interazione tra i componenti. Le applicazioni saranno analizzate con l'obiettivo di rilevare la tipologia dei dati in transito e le interazioni con i sistemi. Questa fase dovrà analizzare almeno quanto segue:
    - *Configurazione*: identificazione del maggior numero di directory e pagine web al fine di identificare il workflow applicativo. Dovranno essere identificate e rilevate inoltre almeno le seguenti tipologie di vulnerabilità potenziali:
        - Application Fingerprinting
        - Predictable Resource Location
        - URL Redirector Abuse
        - Directory Indexing
        - Improper File System Permissions
        - Information Leakage
        - Insecure Indexing
        - Server Misconfiguration
        - Insufficient Transport Layer Protection
        - HTTP Response Smuggling
        - HTTP Response Splitting
    - *Autenticazione*: analisi delle funzionalità di autenticazione per verificare che al loro interno non siano presenti problematiche di sicurezza in particolare:

        - che le credenziali di accesso fornite dagli utenti viaggino attraverso canali di comunicazioni considerati come sicuri e che siano utilizzati dei meccanismi di protezione tali da non favorire la conduzione di attacchi sofisticati;
        - che siano presenti dei meccanismi di enforcing delle credenziali di accesso cioè se il meccanismo di autenticazione e di provisioning dell'applicazione impedisca agli utenti finali l'utilizzo di determinate password classificate comunemente come deboli
        - che all'interno dell'applicazione siano presenti dei meccanismi di protezione da attacchi al dizionario. Qualora tali meccanismi siano presenti andrà verificato che non siano aggirabili.
    - *Autorizzazione:* verifica della presenza di problematiche di sicurezza legate alla possibilità di elevare i privilegi ed i ruoli delle utenze applicative o di accedere a sezioni dell'applicazione protette aggirando i meccanismi di autenticazione e autorizzazione esistenti.
    - *Validazione dei dati:* verifica della corretta validazione degli input degli utenti al fine di garantire che non siano presenti eventuali criticità di sicurezza. Di seguito una lista esplicativa ma non esaustiva delle più comuni tipologie di vulnerabilità, oggetto della verifica:
        - Accesso abusivo a funzionalità aggiuntive
        - Gestione non controllata degli input
        - Cross-Site Scripting
        - Cross-Site Request Forgery
        - Format String
        - Integer Overflows
        - LDAP Injection
        - Mail Command Injection
        - Null Byte Injection
        - Path Traversal
        - Remote File Inclusion
        - SSI Injection
        - SQL Injection
        - XPath Injection
        - XML Attribute Blowup
        - XML Bombing
        - XML External Entities
        - XML Injection
        - XQuery Injection

- **Simulazione degli incidenti di sicurezza**: su richiesta del Committente/Amministrazione potrà essere inoltre svolta una verifica puntuale di tutte le vulnerabilità segnalate dai tool automatici. Partendo dalle potenziali vulnerabilità dovranno essere portati a termine gli attacchi mediante exploiting, ossia l'esecuzione effettiva dell'attacco e la registrazione della relativa evidenza che ne testimoni la reale possibilità di sfruttamento. Tali evidenze potranno essere degli screenshot o proof of concept (es. l'upload di un file di testo). Ogni variazione sui sistemi dovrà essere indicata in un Report Tecnico con le dovute indicazioni su come rilevarne la presenza ed effettuare la mitigazione e l'eventuale eliminazione.

Potranno essere inoltre richieste attività di brute force sull'autenticazione esposta da "form web". Una volta verificati i livelli di accesso alle informazioni e ai sistemi ottenibili mediante lo sfruttamento delle vulnerabilità identificate, dovranno essere pianificati eventuali scenari di attacco utilizzando sempre le informazioni raccolte nelle fasi precedenti e definendo quindi tutte le possibili **catene di vulnerabilità.**

Il servizio di Penetration Test Applicativo e Infrastrutturale potrà essere richiesto, a seconda dell'esigenze dell'Amministrazione, anche in modalità Black Box.

4.1.2.3 Source Code Auditing

Il servizio di Source Code Auditing prevede una verifica integrale della sicurezza del codice sorgente a partire dal progetto di sviluppo.
Tale attività si basa sull'analisi del flusso di input all'interno della logica delle diverse componenti applicative, così come definito nelle linee guida dell'OWASP.

L'Impresa potrà proporre il proprio modello di analisi del codice sorgente a patto che sia coerente e rispetti quanto descritto nel presente capitolato.

In particolare l'analisi del codice sorgente dovrà essere strutturato almeno sui seguenti controlli:

- Data Flow: verifica della presenza di vulnerabilità che possono riguardare eventuali dati corrotti in ingresso che possono portare ad un comportamento anomalo dell'applicazione.
- Control Flow: verifica dei rischi collegati all'assenza di specifiche sequenze di operazioni che, se non eseguite in un certo ordine, potrebbero portare a violazioni sulla memoria o l'uso scorretto di determinati componenti.
- Semantico: rilevazione di eventuali problematiche legate all'uso pericoloso di determinate funzioni o API (es. funzioni deprecate).
- Configurazioni: verifica dei parametri intrinseci di configurazione dell'applicazione.
- Buffer Validation: verifica della presenza di buffer overflow exploitabile attraverso la scrittura o lettura di un numero di dati superiore alla reale capacità del buffer stesso.

4.1.2.4 Deliverables dei Servizi On Demand

Al termine dell'attività svolte nell'ambito dei Servizi On Demand sopraccitati dovranno essere realizzati due rapporti: uno di stampo tecnico, Technical Report, con tutte le indicazioni necessarie per la comprensione del problema, per la sua classificazione in termini di priorità e per l'identificazione delle strutture aziendali più idonee alla risoluzione, ed un Executive Summary destinato prevalentemente al management ed al personale non tecnico per una comprensione immediata del problema e della sua distribuzione in termini dipartimentali.
Al fine di assicurare la massima confidenzialità delle informazioni trattate, la consegna dei report e delle eventuali evidenze raccolte, dovrà avvenire per mezzo di un canale di comunicazione concordato con i referenti dell'Amministrazione.
Tali informazioni dovranno essere archiviate mediante robuste tecniche di cifratura, e verrà consentito l'accesso solo al personale autorizzato mediante opportuni meccanismi di autenticazione. Dovrà inoltre essere evitata la conservazione su supporti rimovibili, e/o notebook, che sarà limitata al tempo strettamente necessario per le operazioni di

elaborazione e di analisi.

4.1.2.4.1 Executive Summary

L'Executive Summary dovrà illustrare i principali rischi a cui l'azienda è sottoposta a causa delle vulnerabilità riscontrate e dovrà fornire un messaggio incisivo allo scopo di provocare un adeguato livello di reazione da parte del management stesso. Nel documento dovranno essere concentrati e riassunti i risultati esposti nel report tecnico, conservandone la sequenza e la struttura concettuale.
L'Executive Summary dovrà inoltre includere un piano di azione ad alto livello per illustrare, su specifiche classi di priorità (Breve, Medio e Lungo Termine), le macro-categorie di problemi rilevati sui sistemi a perimetro e scandire un opportuno Piano di Rientro.

4.1.2.4.2 Technical Report

Il Technical Report dovrà essere articolato in modo da mantenere una separazione logica tra le differenti piattaforme soggette ad analisi.
Per ogni piattaforma in esame, oltre a fornire una precisa segnalazione delle varie vulnerabilità riscontrate e/o punti deboli del sistema (in termini di porte, servizi e informazioni del sistema, o circa eventuali analisi condotte in ambito locale) dovranno essere riportate anche indicazioni precise sulle possibili soluzioni (in termini di patch, di configurazioni necessarie e suggerimenti migliorativi) al fine di mitigare i rischi potenziali generati dal loro sfruttamento.
Ogni problematica riportata dovrà essere descritta in una sezione specifica di approfondimento tecnico. Tale sezione descrittiva dovrà essere composta almeno da:
Descrizione di dettaglio della problematica rilevata;
Riferimenti a documentazione pubblica per ulteriori approfondimenti tecnici;
Suggerimenti provvisori realizzati dal team di analisi;
Workaround possibili, qualora applicabili;
Soluzioni perimetrali di protezione, qualora applicabili.
Per ogni vulnerabilità tecnica dovrà essere effettuata un'analisi del rischio "tecnica" (basata sullo standard CVSS) che prende in considerazione popolarità e semplicità dell'attacco commisurata al valore del sistema e al grado di compromissione raggiunto.

4.1.3 COMPOSIZIONE DEL TEAM

L'Impresa, per formare il team che si occuperà delle attività previste per il *Lotto II - "Controllo e valutazione dei livelli di sicurezza"* dovrà avvalersi di personale specializzato in attività di security assessment, in possesso di specifiche certificazioni.
Di seguito vengono descritti i requisiti minimi e le certificazioni obbligatorie richiesti per ogni figura professionale:

Auditor Team Leader (Consulente specialista)
Ruolo: ha la responsabilità di coordinare il gruppo di lavoro che svolgerà le attività inerenti le fasi del servizio *Governance della Sicurezza delle Informazioni*. Si occupa di partecipare agli incontri con l'Amministrazione inerenti il recepimento dei requisiti strategici. Valida i deliverable prodotti nelle varie fasi e li presenta all'Amministrazione recependo laddove necessario l'integrazione di nuovi requisiti.

Caratteristiche:

- almeno 7 anni di esperienza nella gestione della protezione delle informazioni;
- conoscenza delle metodologie di Project Management e precedente esperienza nella conduzione di progetti di analoghe caratteristiche presso clienti di grandi dimensioni;
- conoscenza delle metodologie per l'analisi dei requisiti;
- capacità di individuazione dei processi di business critici.

Certificazioni richieste: Certified Information Systems Auditor, *Lead Auditor ISO 27001* e *ITIL Foundation v3*

Ethical Hacker Team Leader (Consulente specialista)
Ruolo: coordina tutte le fasi svolte dal gruppo di lavoro inerenti i Servizi on demand di "*Vulnerability Assessment*" e "*Penetration Test Applicativo e Infrastrutturale*" e si occupa di governare il raggiungimento degli obiettivi.

Caratteristiche:

- esperienza non inferiore ai 7 anni in attività analoghe a quelle oggetto del presente Capitolato Tecnico (di cui al paragrafo 4.1) ;
- conoscenza delle metodologie di Project Management e precedente esperienza nella conduzione di progetti di analoghe caratteristiche presso clienti di grandi dimensioni;
- competenza in attività di analisi di sicurezza e di rete;
- profonda conoscenza delle tematiche della sicurezza;
- buona conoscenza dei sistemi operativi più diffusi per aspetti legati alla gestione della sicurezza;
- esperienza nella gestione della protezione delle informazioni.

Certificazioni richieste: *Certified Information Security Manager* (CISM) e *Certified Etical Hacker* (CEH)

Source Code Auditor (Consulente specialista)
Ruolo: figura altamente specializzata che si occupa di tutte le attività legate al Servizio on demand di *"Source Code Auditing"*.

Caratteristiche:

- esperienza non inferiore ai 7 anni in attività di analisi del codice sorgente (di cui al paragrafo 4.1.2.3) ;
- precedente esperienza nella conduzione di progetti di analoghe caratteristiche presso clienti di grandi dimensioni;
- profonda conoscenza della metodologia OWASP;
- profonda conoscenza delle tematiche della sicurezza;
- profonda conoscenza del linguaggio di markup XML;
- profonda conoscenza delle architetture SOA;
- profonda conoscenza dei linguaggi di programmazione web (es. PHP, ASP, ASP.NET; JSP/Java, altri linguaggi legati ai CGI come Perl, etc);

Certificazioni richieste: *Certified Secure Software Lifecycle Professional* (CSSLP).

Security Architect (Consulente specialista o Sistemista Senior)
Ruolo: si occupa di analizzare le informazioni inerenti le soluzioni di tecnologiche di Sicurezza già in essere, anche attraverso interviste programmate con i responsabili di tali soluzioni al fine di fornire una vista aggiornata al responsabile dell'Amministrazione. Supporta le attività di Gap Analysis con particolare riferimento alle soluzioni tecnologiche di Sicurezza. Effettua una stima di massima delle attività/necessità identificate per colmare i gap evidenziati dal punto di vista tecnologico. Supporta la stesura dei deliverable di progetto relativamente alle componenti tecnologiche.

Caratteristiche:
- almeno 7 anni di esperienza nello sviluppo ed implementazione di soluzioni di Sicurezza IT.

Certificazioni richieste: *Varie. Il Committente/Amministrazione potrà richiedere le opportune certificazioni, anche legate a specifici vendor, a seconda delle necessità e dello scenario tecnologico in esame.*

Senior Security Analyst (Sistemista Senior)
Ruolo: si occupa della conduzione delle attività di analisi delle applicazioni e simulazione degli incidenti di sicurezza, nonché alla certificazione e classificazione delle vulnerabilità in relazione al modello di assegnazione del rischio definito.

Caratteristiche:
- almeno 5 anni di esperienza nella gestione della protezione delle informazioni;
- almeno 3 nella realizzazione di penetration test infrastrutturali o applicativi;
- esperienza nell'analisi delle tipologie dei flussi di traffico di rete, analisi di software considerato come malware (worm/virus et similari);
- esperienza nelle attività di risk analysis, di auditing, penetration testing, hardening infrastrutture;
- esperienza nelle attività di ricerca e sviluppo che gli hanno permesso di identificare all'interno di diversi prodotti vulnerabilità e problematiche di sicurezza;
- conoscenze approfondite dei sistemi operativi Unix e Windows per aspetti legati alla gestione della sicurezza;
- esperienza nella gestione della protezione delle informazioni;
- comprensione dei processi di business a livello IT.

Certificazioni richieste: *OSSTMM Professional Security Tester* (OPST)

Senior Auditor (Sistemista Senior)
Ruolo: pianifica e coordina le attività inerenti le fasi del servizio *Governance della Sicurezza delle Informazioni*. Si occupa di partecipare agli incontri con l'Amministrazione inerenti le interviste per la raccolta di informazioni e recepimento dei requisiti strategici. E' parte attiva nello sviluppo e validazione dei deliverable.

Caratteristiche:
- almeno 5 anni di esperienza nella gestione della protezione delle informazioni;
- conoscenza delle metodologie di Project Management e precedente esperienza nella conduzione di progetti di analoghe caratteristiche presso clienti di grandi dimensioni;

- conoscenza delle metodologie per l'analisi dei requisiti;
- capacità di individuazione dei processi di business critici.

Certificazioni richieste: *Lead Auditor ISO 27001* e *ITIL Foundation v3*

Auditor (Sistemista)
Ruolo: raccoglie ed analizza le informazioni necessarie per la valutazione dei livelli di maturità della Sicurezza. Contribuisce all' identificazione degli interventi necessari per il raggiungimento della conformità, definendo le priorità in base agli obiettivi strategici dell'Amministrazione. Sviluppa i deliverable del servizio *Governance della Sicurezza delle Informazioni*. Supporta il Senior Auditor durante gli incontri per la raccolta di informazioni e recepimento dei requisiti strategici.

Caratteristiche:
- almeno 3 anni di esperienza nella gestione della protezione delle informazioni;
- conoscenza delle metodologie per l'analisi dei requisiti;
- capacità di individuazione dei processi di business critici.

Certificazioni richieste: *Lead Auditor ISO 27001* o *ITIL Foundation v3*

Security Analyst (Sistemista)
Ruolo: svolge le attività di analisi della sicurezza legate alle fasi di Information Gathering e Service Discovery sia legate al Servizio on demand di "Penetration Test Applicativo e Infrastrutturale" (paragrafo 4.1.2.2) sia al Servizio on demand di "Vulnerability Assessment" (paragrafo 4.1.2.1).

Caratteristiche:
- esperienza di almeno 3 anni nella gestione della protezione delle informazioni, di cui almeno 2 in attività di Vulnerability Assessment e Penetration Test.
- competenze in attività di analisi di software malizioso e reverse engineering;
- profonda conoscenza nella gestione e nell'analisi di incidenti informatici attraverso l'analisi di flussi di traffico di rete;
- conoscenze approfondite sulla ricerca di vulnerabilità all'interno di software ed hardware sia open source che commerciale;
- buona conoscenza dei sistemi operativi Unix e Windows per aspetti legati alla gestione della sicurezza;
- buona conoscenza della metodologia *OSSTMM*.

Certificazioni richieste: una qualsiasi certificazione (anche di prodotto) legata alle attività di Vulnerabilty Assessment

Security Consultant (Sistemista Junior)
Ruolo: supportano le varie fasi che costituiscono l'insieme dei servizi oggetto della fornitura.
Caratteristiche: le caratteristiche del consulente verranno valutate di volta in volta, in base alle attività da svolgere, dal Committente/Amministrazione.
Certificazioni richieste: nessuna in particolare.

4.2 RESPONSABILE DELLA FORNITURA, ATTIVITÀ ESECUTIVE

Entro 5 (cinque) giorni solari dalla stipula del contratto, l'Impresa comunicherà alla Consip i nominativi del Responsabile del contratto, del Responsabile tecnico e del Process Manager dei processi che regolamentano le attività svolte presso il SOC remoto.

Le attività esecutive, a carico dell'Impresa, sono strumentali alla corretta messa in opera della Fornitura.

4.2.1 STARTUP DEL SERVIZIO

Lo startup del servizio avverrà a seguito dell'invio, da parte del Committente all'impresa, della lettera di "Dichiarazione di inizio dei servizi" che sarà comunicata, tramite lettera formale, dal Committente/Amministrazione al Fornitore entro il termine di 10 (dieci) giorni solari dalla data di consegna della documentazione di startup del servizio, di seguito descritta.

Nella Dichiarazione di inizio dei servizi sarà contenuto il perimetro iniziale oggetto dei servizi di Governance della Sicurezza delle Informazioni.
Per perimetro iniziale si intende un qualsiasi servizio erogato dalla Cdc sia ai cittadini, sia al personale interno.

L'Impresa dovrà produrre la documentazione di startup, entro un tempo massimo di 20 giorni solari, dalla data di stipula del contratto.

La documentazione di startup del servizio dovrà essere composta dalle seguenti voci:

- Piano tecnico contenente:
  - Modello di Governance della Sicurezza delle Informazioni proposto con il dettaglio di ogni sua fase e una stima di massima dei tempi necessari alla produzione dei deliverables (paragrafo 4.1.1);
  - Metodologie proposte per i servizi On Demand (paragrafo 4.1.2)
- Composizione del Team impiegato in ogni fase della *Governance della Sicurezza delle Informazioni* (mappato sulle figure professionali di cui al paragrafo 4.1.3), il nominativo del Responsabile del Contratto, di cui al precendente capitolo 3 e il nominativo del Responsabile tecnico per l'erogazione dei servizi, di cui al precedente capitolo 3;
- Curricula e relative certificazioni dei componenti del Team proposto per ogni fase della *Governance della Sicurezza delle Informazioni*.
- Curricula e relative certificazioni delle seguenti figure professionali legate ai servizi On Demand di "*Vulnerability Assessment*" e "*Penetration Test Applicativo e Infrastrutturale*" e "Source Code Auditing":
  - Ethical Hacker Team Leader;
  - Source Code Auditor;
  - Senior Security Analyst.

All'avvio di ogni fase dei servizi di Governance della Sicurezza delle Informazioni il

Committente dovrà sottoporre all'approvazione della Consip/Amministrazione il numero di giornate pianificate per ogni risorsa del Team per portare a termine la fase in oggetto.
L'eventuale effort aggiuntivo, in termini di giorni/persona, per portare a temine la fase in oggetto sarà a totale onere dell'Impresa.

4.2.2 GESTIONE DEI SERVIZI ON DEMAND

Il Committente si riserva di attivare ulteriori Servizi On Demand a seguito di sopravvenute esigenze di evoluzione/adeguamento dell'Infrastruttura di sicurezza. Le modalità di gestione delle relative Forniture sono descritte nei paragrafi successivi.

4.2.2.1 Richiesta di Servizi On Demand

Per effettuare una richiesta di servizi On Demand, il Committente comunicherà all'Impresa:

- L'elenco dei nuovi servizi/funzionalità che si intende attivare;
- i tempi massimi delle attività esecutive.

La Richiesta di Servizi On Demand avverrà mediante chiamata telefonica, seguita dall'invio di una e-mail ad un indirizzo indicato dall'Impresa. La data della suddetta e-mail costituirà il riferimento per il rispetto dei tempi esecutivi della Fornitura.

4.2.2.2 Attività esecutive relative a successive attivazioni di servizi On Demand.

L'Impresa, entro 10 (dieci) giorni solari dalla data di ricezione dell'e-mail di richiesta del Committente, dovrà trasmettere una pianificazione delle attività e delle risorse professionali impiegate per la gestione del nuovo servizio.

L'Impresa potrà comunicare eventuali problematiche legate alla disponibilità dei servizi, o alle modalità esecutive, richiedendo al Committente l'estensione dei tempi massimi previsti. Qualora vengano concordate nuove tempistiche massime sulle fasi di realizzazione, queste dovranno essere approvate dal Committente.

La pianificazione, una volta concordata con il Committente, dovrà essere rispettata dall'Impresa pena l'applicazione delle penali previste nel contratto.

La Consip/Amministrazione procederà alla valutazione dell'erogazione del servizio ed, in caso di approvazione dello stesso, l'Impresa produrrà un apposito "Resoconto attività" con l'indicazione del tipo di servizio e dell'impegno (in giorni/persona) effettuato, propedeutico alla relativa fatturazione, di cui al successivo art. 13 S, comma 2; in caso di non approvazione del servizio erogato, l'Impresa dovrà adoperarsi al fine di raggiungere quanto previsto nel piano dei lavori, pena il mancato riconoscimento dell'impegno stimato. L'eventuale impegno aggiuntivo non sarà riconosciuto economicamente, se non diversamente comunicato dalla Consip/Amministrazione.

5 INDICATORI DI QUALITÀ

Di seguito viene descritto un insieme minimo di requisiti di qualità della fornitura e delle relative modalità di verifica e controllo.
Il Fornitore è tenuto, per l'intera durata dei servizi compreso il periodo transitorio, a rendicontare gli indicatori di qualità (IQ).

Si precisa che:

- per periodo di riferimento si intende l'arco di tempo entro il quale sono rilevate le grandezze necessarie per la determinazione dei Requisiti di Qualità. E' specificato per ogni indicatore di qualità (IQx);
- per ore e giorni si intendono ore lavorative e giorni lavorativi;
- per mese, trimestre, semestre, si indica il mese, il trimestre, il semestre di calendario nell'ambito della durata contrattuale.

Ai fini della misurazione degli indicatori di qualità, si precisa che, ad esclusione dei casi espressamente indicati, eventuali centesimi dei valori percentuali rilevati dovranno essere arrotondati ad una unica cifra decimale:

- per difetto se i centesimi sono < 5;
- per eccesso se i centesimi sono >= 5.

Ad esempio:

- 15,06% diventa 15,1%;
- 10,01% diventa 10,0%;
- 10,49% diventa 10,5%;
- 14,98% diventa 15,0%.

5.1 INDICATORI DI QUALITÀ

5.1.1 IQ1: SOSTITUZIONE DEL RESPONSABILE TECNICO DELLA FORNITURA

Aspetto da valutare	Sostituzione del Responsabile unico della fornitura operata su iniziativa dell'Impresa e non a fronte di richiesta di Consip e/o dell'Amministrazione.		
Unità di misura	Responsabili sostituiti	**Fonte dati**	Lettera di sostituzione del Responsabile unico della fornitura da parte del Fornitore
Periodo di osservazione	Semestre precedente la rilevazione	**Frequenza di misurazione**	Semestrale
Dati da rilevare	• Sostituzione permanente del Responsabile unico della fornitura non richiesta da Consip e/o dall'Amministrazione (*Nsostituzioni*)		
Regole di campionamento	Vanno considerate le sostituzioni non richieste da Consip e/o dall'Amministrazione che riguardano il Responsabile unico della fornitura.		
Formula	$IQ1 = Nsostituzioni$		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ1 = 0		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

5.1.2 IQ2: PERSONALE DELLA FORNITURA INADEGUATO

Aspetto da valutare	Personale della fornitura inadeguato		
Unità di misura	Richiesta di sostituzione	**Fonte dati**	E-mail, lettere, verbali
Periodo di riferimento	Semestre precedente la rilevazione	**Frequenza di misurazione**	Semestre
Dati elementari da rilevare	Numero di sostituzioni, richieste formalmente da Consip/Amministrazione, del personale della fornitura (N_Sostit_rich).		
Regole di campionamento	Vanno considerate le sostituzioni richieste da Consip/Amministrazione che riguardano il personale della fornitura nel periodo di riferimento.		
Formula	$\mathrm{IQ2} = N_Sostit_rich$		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ2 <= 2		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

5.1.3 IQ3: TURN OVER DEL PERSONALE

Aspetto da valutare	Turn over del personale: numero di risorse sostituite su iniziativa del Fornitore nel periodo di riferimento.		
Unità di misura	Risorsa sostituita	**Fonte dati**	E-mail, lettere, verbali
Periodo di riferimento	Semestre precedente la rilevazione	**Frequenza di misurazione**	Semestrale
Dati elementari da rilevare	Numero di sostituzioni effettuate su iniziativa del Fornitore nel periodo di riferimento (N_Sostit).		
Regole di campionamento	Nessuna		
Formula	$IQ3 = N_Sostit$		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ3 <= 3		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

5.1.4 IQ4: QUALITÀ DELLA DOCUMENTAZIONE PRODOTTA

Aspetto da valutare	Riemissione dei documenti a seguito di rilievi emessi dal Committente.		
Unità di misura	Punto percentuale	**Fonte dati**	Lettere di notifica al Fornitore di non approvazione del documento. Lettere di consegna della documentazione del Fornitore
Periodo di riferimento	Semestre precedente la rilevazione	**Frequenza di misurazione**	Semestrale
Dati elementari da rilevare	Numero di documenti rielaborati (N_documenti_rielaborati) Numero di documenti consegnati (N_documenti)		
Regole di campionamento	Vanno considerati tutti i documenti consegnati nel periodo di riferimento		
Formula	$\mathrm{IQ4} = \frac{N_documenti_rielaborati}{N_documenti} x100$		
Regole di arrotondamento	La percentuale va arrotondata per eccesso alla prima cifra decimale		
Valore di soglia	IQ4 <= 5,0%		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

6 CERTIFICAZIONI DELL'IMPRESA

L'Impresa dovrà dimostrare, producendo tutta la relativa documentazione (anche in autocertificazione), la sussistenza dei requisiti per il rispetto delle seguenti normative:

- DPR. 27/04/1955 n. 547 e DPR. 07/01/1956, sull'osservanza da parte dei singoli lavoratori delle norme di sicurezza citate e sull'uso dei mezzi di protezione messi a loro disposizione;
- DPR. 19/03/1956 n. 303, Norme Generali per l'igiene del lavoro;
- D.Lgs. 19 settembre 1994 N. 626, attuazione direttive CEE riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro e successivi aggiornamenti;
- Legge n. 46 del 05/03/1990: norme sulla sicurezza degli impianti e relativo DPR 447/91 di attuazione, per quanto attiene alla installazione dei Componenti.

Il mantenimento della validità della certificazione viene richiesto anche per tutto l'arco della durata della manutenzione.
Dovrà essere prodotta tutta la documentazione (anche in autocertificazione) attestante la sussistenza di tutti i suddetti requisiti.

Dovrà inoltre essere prodotta tutta la certificazione (o autocertificazione) circa la sussistenza dei suddetti requisiti per le apparecchiature fornite.