

**Migrazione, sviluppo di componenti aggiuntivi della Piattaforma di Early Warning,  
per la rilevazione ed analisi delle nuove minacce informatiche e acquisto nuova licenza applicativo di supporto.**

**Capitolato Speciale d'Oneri  
Capitolato Tecnico All. 1**

## Indice

1.	Premessa .....	3
2.	Ambito di applicazione .....	3
3.	Oggetto della fornitura.....	3
3.1	Fornitura servizi professionali .....	3
3.2	Caratteristiche della Banca Dati storica.....	6
3.3	Fornitura licenze .....	6
4	Requisiti Minimi obbligatori della fornitura.....	8
4.1	Requisiti generali .....	8
4.2	Requisiti di integrazione con l'ambiente operativo del CERT di Poste Italiane .	9
4.3	Requisiti funzionali della piattaforma Early warning .....	10
4.3.1	Componente Repository della piattaforma Early Warning .....	10
4.3.2	Moduli aggiuntivi piattaforma Early Warning .....	12
4.3.3	Componente <i>Web&amp;Documents Reporting Interface</i> piattaforma <i>EW</i> .....	14
4.4	Servizi Professionali .....	15
4.4.1	Figure professionali e <i>skill-mix</i> .....	15
4.4.2	Servizi di Analisi e Personalizzazione Applicativo.....	18
4.4.3	Servizi di supporto al <i>roll-out</i> : <i>Tuning</i> , Collaudo e Certificazione .....	19
4.4.4	Tempi di realizzazione e piano di <i>Roll out</i> .....	21
4.4.5	Installazione finale - Produzione .....	22
4.4.6	Documentazione .....	22
4.5	Garanzia Sviluppo.....	23
4.6	Servizio di manutenzione correttiva nel periodo di garanzia della piattaforma evoluta .....	23
5	Modalità di partecipazione e criteri di aggiudicazione .....	25
5.1	Relazione tecnica .....	25
5.2	Scheda Requisiti minimi .....	26
5.3	Criterio di aggiudicazione.....	26

## 1. Premessa

La Funzione di Tutela Aziendale – Analisi Rischi e Security Intelligence - Business Security Intelligence, ha tra i suoi compiti principali quello di prevenire ed anticipare gli incidenti di natura informatica, assicurando l'analisi e l'elaborazione dei dati disponibili ed il monitoraggio del grado di esposizione dell'Azienda ai rischi interni ed esterni, e individuando e gestendo, di concerto con le funzioni aziendali coinvolte, i fenomeni critici.

In tal quadro, la struttura BSI, si è dotata di una piattaforma di *Early Warning*, che garantisce l'invio delle notifiche relative, alla scoperta di nuove vulnerabilità o codici malevoli, a tutti i referenti delle società del gruppo, con la possibilità di acquisire informazioni relative alle sole tecnologie o prodotti di interesse, secondo i criteri definiti.

## 2. Ambito di applicazione

Allo scopo di innalzare il livello di presidio, ed assicurare quindi maggiore tempestività e analiticità al processo di acquisizione di informazioni necessarie alla valutazione e segnalazione delle nuove criticità aventi impatto sul business aziendale, si ritiene opportuno richiedere prestazioni professionali per lo sviluppo di funzionalità aggiuntive, che consentiranno l'inserimento della piattaforma, nell'ambito delle attività previste dal CERT, e l'acquisto di una licenza per l'integrazione in essa del pacchetto di sicurezza DeepSight Early Warning Gold Pack 8.0 dotata di un numero illimitato di utenze d'accesso.

## 3. Oggetto della fornitura

La gara è ripartita tra forniture di servizi e licenze.

### 3.1 Fornitura servizi professionali

Il sistema di *Early Warning*, oggetto del presente capitolo, dovrà garantire l'invio delle notifiche relative alla scoperta di nuove vulnerabilità o codici malevoli - con la possibilità di acquisire informazioni relative alle sole tecnologie o prodotti di interesse - secondo i criteri definiti dal Responsabile di Progetto di Poste Italiane.



Il citato sistema dovrà, inoltre, assicurare il necessario supporto del personale delle funzioni incaricate della gestione delle criticità e degli incidenti, nella definizione delle opportune contromisure e delle priorità d'intervento, attraverso una dettagliata strategia di prevenzione, mitigazione e contrasto delle minacce, integrata nel CERT (*Computer Emergency Response Team*) aziendale.

### **3.1.1 Configurazione e personalizzazione del servizio**

Dovrà essere possibile gestire profili tecnologici multipli, ovvero liste di prodotti/piattaforme/vendor per le quali si vogliono ricevere segnalazioni di nuove vulnerabilità, in modo da consentire a Poste Italiane di poter ricevere notifiche personalizzate sulla base delle tecnologie di interesse (c.d. *Technology List*).

Dovrà essere possibile, a tal proposito, creare differenti profili di spedizione delle notifiche da collegare con i profili tecnologici, al fine di configurare la notifica sui requisiti definiti dal Team di Progetto di Poste Italiane.

Il servizio dovrà essere disponibile in modalità 24x7 e dovrà consentire di ricevere gli *alert* delle vulnerabilità scoperte e dei *malicious code*, individuati secondo il canale informativo prescelto (email, xml, sms o telefono) e correlato all'*asset* di riferimento.

In particolare nel momento in cui verranno pubblicate nuove vulnerabilità o *malicious code* che soddisfano i criteri di cui sopra, si renderà necessario ricevere una notifica contenente una componente anagrafica, una descrizione della vulnerabilità/*malicious code*, un dettaglio tecnico con relativi sintomi, eventuali *patch/hot-fix* disponibili o *workaround* utili alla mitigazione dell'impatto.

### **3.1.2 Centralizzazione dei data feed e pubblicazione**

In tale specifico ambito, si ritiene necessario consolidare l'aggregazione di fonti informative sicure ed affidabili in un data base conforme agli standard.

La correlazione delle stesse fonti alla *technology list* o all'*asset* (dove presente) forniti da Poste Italiane, nonché ad una lista di sistemi *Business Critical* da monitorare con particolare attenzione. Inoltre dovrà essere garantita la pubblicazione in tempo reale delle notizie su un portale web-based, dove sarà prevista una prima vista di sintesi della minaccia, con particolare riferimento a :

- identificativo univoco della minaccia (CVE ID);
- valutazione a livello globale (cvss2);

- valutazione a livello aziendale, dove possibile;  
(derivante da una correlazione con una *technology list* fornita da Poste Italiane)
- tecnologia, sistema operativo e servizio aziendale impattato;
- severity;

La "Notizia di Sintesi" dovrà avere un *link* diretto alla notizia di dettaglio, con la spiegazione sulla dinamica della minaccia, che riporterà oltre le informazioni sopracitate, anche i necessari interventi di mitigazione (*work-around, patch*), con la possibilità di allegare, secondo la profilatura, documenti in formato pdf per ampliare il dettaglio.

Tale portale dovrà poter essere profilato per poter garantire la consultazione in base al livello di responsabilità aziendale.

### **3.1.3 Tracciatura delle minacce**

Monitoraggio mirato su alcuni applicativi o sistemi *Business Critical* che permette di dare priorità alle attività di mitigazione degli incidenti in ambienti di particolare interesse per l'azienda

### **3.1.4 Informativa Istantanea e feedback**

Ogni minaccia dovrà essere assegnata automaticamente ad uno o a più gruppi in base alla *technology list* o all'*asset*, ove presente, il *ticket* generato deve poter prevedere dei campi a cui possono essere aggiunti i piani di mitigazione previsti per poter far fronte alla minaccia.

In caso di minacce significative dovrà essere gestito il livello di eventuale rischio che il portale dovrà notificare prontamente, via email, ai responsabili preposti, veicolando le seguenti informazioni :

- identificativo univoco della minaccia (CVE ID) ;
- valutazione a livello globale (cvss2);
- valutazione a livello aziendale;  
(derivante da una correlazione con una *technology list* fornita da Poste Italiane)
- tecnologia o sistema impattato;
- severity;
- i *link* alla descrizione estesa sul portale, dove si potranno tracciare, ognuno per le proprie competenze, le attività per porre in sicurezza l'infrastruttura in esame.

Dovrà essere predisposto anche un sistema di notifica via sms, con una sintesi di 160 caratteri del caso in esame.

### 3.1.5 Report

Nel portale dovrà essere prevista una sezione per la reportistica delle minacce, in base alla tecnologia, il tipo e all'impatto sui servizi aziendali.

Inoltre una vista in tempo reale di quelle a più grave impatto, con la tracciatura delle contromisure e dello stato avanzamento lavori

### 3.2 Caratteristiche della Banca Dati storica

Il servizio fornito deve rendere disponibile una banca dati contenente i dati storici riguardanti le varie tipologie di attacco, vulnerabilità e codici malevoli. In aggiunta è richiesto il rispetto dei seguenti requisiti:

- ✓ Eventuale integrazione con altre soluzioni (ad esempio *asset configuration management*) attraverso standard aperti;
- ✓ Accesso mediante *front-end web*;
- ✓ Aggiornamento dei dati in tempo reale;
- ✓ Tipologie di filtri/viste gestite da un “*super-user*” e personalizzabili”;
- ✓ Modalità di notifica via e-mail, sms;
- ✓ Possibilità di accedere ai contenuti secondo ruoli diversi;
- ✓ Possibilità di attribuire il livello di rischio alle minacce in modo personalizzabile dall’utente;
- ✓ Disponibilità di report predefiniti e personalizzabili.

### 3.3 Fornitura licenze

- ✓ Una licenza del servizio di Early Warning “Deepsight Early Warning Services Gold Pack 8.0 25000+ Per Node Sub Lic Band S Essential” per la segnalazione delle nuove minacce, vulnerabilità e codici virali rilevati in rete Internet attraverso la rete di monitoraggio o altri enti qualificati, di durata annuale, comprensiva del servizio di manutenzione, a partire dalla data di accettazione del software oggetto della fornitura.
- ✓ La disponibilità della banca dati storica di Symantec riportante informazioni qualificate ed affidabili riguardanti vulnerabilità, exploit e minacce informatiche, organizzate e strutturate.

- ✓ Software di "Security Intelligence" (Early Warning) per la segnalazione delle nuove minacce, vulnerabilità e codici virali rilevati in rete Internet attraverso la rete di monitoraggio.
- ✓ Software per l'analisi delle vulnerabilità e l'implementazione di una banca dati di informazioni, certificate da enti qualificati ed affidabili, riguardanti exploit e minacce informatiche, organizzate e strutturate.
- ✓ Il servizio DeepSight Early Warning Gold Pack 8.0 prevede:
  - Account illimitati per l'accesso alle informazioni del servizio e alla configurazione delle notifiche ai destinatari dei vari alert.
  - La possibilità di definire liste (gruppi) di tecnologie (sistemi operativi e/o applicativi), in modo da poter catalogare le varie segnalazioni fornite dal servizio.
  - La possibilità di distribuire ad illimitati destinatari le varie segnalazioni in base alla tipologia di alert e alle liste di tecnologie interessate.
  - Le notifiche possono essere inviate via email, XML, RSS oppure SMS.
  - Ridistribuzione delle informazioni, fino alle Società del Gruppo Poste Italiane.
  - Condivisione delle liste tecnologiche.

Le informazioni fornite dal DeepSight Gold Pack 8.0 coprono le seguenti tipologie di dati:

**- Report Base:**

- Livello globale di sicurezza ThreatCon
- Vulnerabilità
- Malicious Code (inclusa documentazione base di reverse engineering, se disponibile)
- Security Risk

**- Report Avanzati:**

- Domain (su particolari domini Internet configurati dal Cliente)
- Port Activity (su particolari porte TCP/UDP configurate dal Cliente)
- Industry Activity (per settore di mercato)
- Network Infection
- Monitoring da honeynet



- Studi di analisi e ricerca sulla sicurezza in generale o su temi specifici valutati di interesse dal team di Intelligence di Symantec
- Servizio di Custom Report

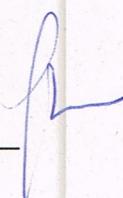
## 4 Requisiti Minimi obbligatori della fornitura

Le caratteristiche elencate nel presente capitolo si intendono minime e obbligatorie, pena la risoluzione del contratto.

Le caratteristiche migliorative rispetto a quanto prescritto non saranno oggetto di valutazione ai fini dell'aggiudicazione.

### 4.1 Requisiti generali

Codice Requisito	Descrizione Requisito
EW_REQ_1.	<p>Come caratteristica generale, valida per tutti i componenti software della fornitura offerta dall'Impresa, si richiede che:</p> <ul style="list-style-type: none"> <li>- la tecnologia di tutti i componenti sia di ultima generazione;</li> <li>- per nessun componente sia stata annunciata, al momento della presentazione dell'offerta, la messa fuori produzione dello stesso o la sospensione del relativo supporto da parte del produttore; nel caso in cui detto annuncio venga effettuato nell'arco dei quattro anni successivi all' aggiudicazione, l'impresa si impegna a garantire a Poste Italiane il supporto di tutte le componenti oggetto della fornitura fino alla scadenza dei quattro anni.</li> </ul>
EW_REQ_2.	<p>Poste Italiane non potrà accettare applicativi <i>software</i> che siano in <i>Beta Test</i> o comunque non ancora ufficialmente rilasciati.</p>
EW_REQ_3.	<p><b><i>Freeware – Shareware – Open Source</i></b></p> <p>Non sono ammessi prodotti <i>Freeware</i>, <i>Shareware</i> ed <i>Open Source</i> con la sola eccezione di componenti di sistema, quali <i>application server</i> e <i>database</i> utilizzabili al solo scopo di gestione temporanea del dato.</p> <p>In questo caso, la componente va garantita come parte organica della soluzione offerta e deve essere certificata dall'impresa, che ne garantisce la completa compatibilità ed integrazione con la piattaforma nonché l'evoluzione tecnologica e la manutenzione nell' ambito della soluzione offerta.</p>



Codice Requisito	Descrizione Requisito
EW_REQ_4.	L'Impresa si impegna a definire un'architettura logica, basata sulle risorse informatiche messe a disposizione da Poste Italiane, che garantisca la completa scalabilità per far fronte, con un'aggiunta di componenti <i>hardware</i> che non modifichino l'architettura indicata e che si integrino con quanto offerto, sfruttando parti di quanto in essa previsto, ad un aumento nella quantità di dati, nel numero di utenti concorrenti e nelle <i>performance</i> , senza la necessità di modificare il <i>software</i> applicativo ed il modello dati.
EW_REQ_5.	Il <i>software</i> sviluppato o integrato nella soluzione offerta deve essere conforme agli standard adottati presso il Sistema Informativo di Poste Italiane; in particolare: <ul style="list-style-type: none"> <li>• le interazioni legate alle analisi statistiche avanzate, legate ad un numero limitato di utenti, dovranno essere effettuate tramite un interfaccia <i>Client</i>. La piattaforma dovrà poi rendere disponibile la possibilità di esportare i risultati di queste analisi in formato <i>WEB</i>;</li> <li>• Le interazioni uomo-macchina per gli utenti finali devono avvenire attraverso una interfaccia utente <i>WEB</i>;</li> <li>• le comunicazioni tra i vari componenti client e server applicativi devono utilizzare il protocollo HTTP o HTTPS.</li> </ul>
EW_REQ_6.	La piattaforma di Early Warning deve prevedere il tracciamento delle attività svolte dagli utenti con diritti di amministrazione.

## 4.2 Requisiti di integrazione con l'ambiente operativo del CERT di Poste Italiane

Ai fini della realizzazione del progetto, risulta determinante l'impegno, da parte dell'Impresa, ad acquisire le competenze e le conoscenze necessarie per la salvaguardia degli investimenti pregressi intrapresi da Poste Italiane, che si concretizzano in una perfetta integrazione della fornitura con il contesto operativo, organizzativo e tecnologico nel quale opera il Sistema Informativo di Poste Italiane.

La piattaforma oggetto di fornitura dovrà quindi garantire i seguenti requisiti di progetto:

Codice Requisito	Descrizione Requisito
EW_REQ_7.	Integrazione della piattaforma di <i>Early Warning</i> con i sistemi già in esercizio (CERT) presso Poste Italiane, e migrazione dell'attuale sistema verso l'ambiente CERT (CAGE), con l'obiettivo di innalzare il livello di <i>performance</i> sia in termini di capacità, che di sicurezza.

Codice Requisito	Descrizione Requisito
EW_REQ_8.	Conformità delle istruzioni operative prodotte nell'ambito del progetto con l'insieme di normative, standard e procedure, già in vigore presso il Sistema Informativo di Poste Italiane.

## 4.3 Requisiti funzionali della piattaforma Early warning

Di seguito sono descritti i requisiti della piattaforma Early Warning che andrà ad integrare e migliorare le funzionalità di quella attuale.

### 4.3.1 Componente Repository della piattaforma Early Warning

Di seguito sono descritti i requisiti minimi relativi al *Repository* Centralizzato del sistema di *Early Warning*, configurabile, scalabile ed estendibile nel tempo.

Codice Requisito	Descrizione Requisito
EW_REQ_9.	La soluzione deve prevedere la connessione verso la base dati del catalogo CIRM, per la gestione, all'interno della piattaforma, degli asset aziendali e delle notifiche relative al <i>service owner</i> a cui esso è associato.
EW_REQ_10.	La soluzione deve prevedere la gestione di profili tecnologici multipli, ovvero liste di piattaforme/vendor/prodotti per le quali si sceglie di ricevere segnalazioni di nuove vulnerabilità.
EW_REQ_11.	Il modulo deve prevedere la gestione degli asset correlati ai loro ambiti di riferimento, per la notifica mirata delle segnalazioni con la conseguente individuazione delle strutture o i servizi maggiormente a rischio, secondo statistiche periodiche.
EW_REQ_12.	Classificazione delle fonti dati in base a metriche stabilite, con la possibilità di ricavare statistiche sul grado di affidabilità delle stesse ed il numero di segnalazioni inviate.
EW_REQ_13.	Normalizzazione dei dati provenienti da fonti informative diverse, con la possibilità di associazione di un grado di "attendibilità".
EW_REQ_14.	Analisi e normalizzazione delle informazioni provenienti da <i>Black Market</i> , <i>Social Network</i> e canali dedicati, oltre che da fonti destrutturate.
EW_REQ_15.	Per la conservazione del dato centralizzato non potranno essere utilizzati tecnologie o prodotti <i>Freeware</i> , <i>Shareware</i> ed <i>Open Source</i> .

Codice Requisito	Descrizione Requisito
EW_REQ_16.	I servizi intesi allo sviluppo applicativo dovranno implementare e personalizzare l'applicativo per una adeguata gestione documentale della reportistica prodotta. In particolare: <ul style="list-style-type: none"> <li>○ gestione del ciclo di vita dei documenti;</li> <li>○ funzioni di ricerca avanza;</li> <li>○ <i>backup</i>.</li> </ul>
EW_REQ_17.	Il modulo deve permettere l'esecuzione di operazioni di <b>manipolazione dati</b> : unione, ordinamento, concatenazione, sottoinsiemi, suddivisioni archivi, aggregazione dati categorici, al fine di considerare anche informazioni esterne al <i>Repository</i>
EW_REQ_18.	La soluzione deve consentire la <b>visualizzazione</b> di grafici e report statistici in una stessa finestra, al fine di poter individuare con facilità la presenza di dati anomali e correlazioni tra le grandezze, mediante appositi <i>tool</i> guidati.
EW_REQ_19.	La soluzione deve rendere disponibili funzionalità di grafica <b>standard</b> (torte, istogrammi, tabelle riassuntive, ecc.).
EW_REQ_20.	Deve consentire la condivisione delle analisi in appositi file di progetto, che possono essere salvati su un server centralizzato o spediti via e-mail, per dare la possibilità a un team di analisti di lavorare in modo condiviso sui modelli di analisi.
EW_REQ_21.	La soluzione deve prevedere la definizione di <b>regole User-Driven</b> , ovvero condizioni e criteri di selezione complessi, al fine di evidenziare eventi rilevanti per la sicurezza.
EW_REQ_22.	I risultati delle esecuzioni delle regole dovranno poter essere <b>rappresentabili in vari formati</b> (Excel, HTML, CSV, XML, file di testo, PDF), in modo da poter pubblicare e distribuire le evidenze delle occorrenze relative all'evento identificato.
EW_REQ_23.	I risultati dell'esecuzione delle regole <b>dovranno poter essere esportati e salvati</b> all'interno del <i>Repository</i> , per la storicitazione delle evidenze e per consentire ulteriori manipolazioni dei dati.
EW_REQ_24.	La soluzione deve prevedere la possibilità di <b>tenere traccia dei cambi avvenuti storicamente</b> , consentendo di riallocare i dati storici in funzione delle evoluzioni avvenute ed effettuare analisi storiche coerenti.
EW_REQ_25.	Il modulo <b>deve poter abilitare report ed analisi sui rischi di Sicurezza e Tutela</b> definiti. Report quali livelli di esposizione di date aree o sistemi.

Codice Requisito	Descrizione Requisito
EW_REQ_26.	<p>In funzione delle evidenze legate agli indicatori, dovrà essere disponibile una componente che consenta di definire <b>criticità</b> (associate ad esempio all'impatto di una vulnerabilità su di un sistema) e <b>piani d'azione</b> volti alla risoluzione di esse.</p> <p>I <i>form</i> di gestione di criticità e piani di azione devono essere personalizzabili mediante campi aggiuntivi per l'inserimento delle informazioni necessarie.</p> <p>Dovrà inoltre essere possibile definire un <b>workflow</b> che autorizzi il supervisore allo svolgimento delle attività di propria competenza.</p>

#### 4.3.2 Moduli aggiuntivi piattaforma Early Warning

Di seguito sono descritti i requisiti minimi relativi ai moduli che integreranno funzionalità aggiuntive al sistema di *Early Warning* attuale.

Codice Requisito	Descrizione Requisito
EW_REQ_27.	<p>Il sistema deve registrare, in un <i>repository</i> ad hoc, le minacce/vulnerabilità rilevate da fonti esterne al CERT di Poste Italiane, o direttamente da fonti interne, classificandole per tipologia, ovvero per tipo di asset impattato, tenendo traccia della fonte della data.</p> <p>Il sistema deve notificare a più utenti finali tramite interfaccia e/o sistema di messaggistica (e-mail) ogni nuova vulnerabilità / minaccia o gruppi di vulnerabilità / gruppi di minacce rilevate per Categorie di Asset dalle varie tipologie di fonti.</p> <p>Il sistema, inoltre, deve erogare in due modalità differenti via web e su supporto elettronico (pdf), sia i bollettini sulle vulnerabilità / minacce, sia i report statistici ad essi relativi.</p>
EW_REQ_28.	Il modulo deve prevedere l'utilizzo di fonti informative per l'identificazione delle nuove minacce non soltanto i dati provenienti da <i>firewall</i> e sonde IDS ma anche dalle <i>honeypot</i> , ossia reti appositamente non protette ed utilizzate per "catturare" le prove di nuove possibili problematiche di sicurezza o forme di attacco.
EW_REQ_29.	La soluzione deve prevedere la classificazione delle fonti dati in base a metriche stabilite, con la possibilità di ricavare statistiche sul grado di affidabilità delle stesse ed il numero di segnalazioni inviate
EW_REQ_30.	Il modulo deve prevedere la valutazione del livello di riservatezza associato alle informazioni contenute in un bollettino creato automaticamente.
EW_REQ_31.	La soluzione deve prevedere la possibilità di creare differenti profili di spedizione delle notifiche da collegare con i profili tecnologici impostati dall'utente.

Codice Requisito	Descrizione Requisito
EW_REQ_32.	<p>Il modulo deve prevedere la profilazione delle utenze e di gruppi di lavoro appositamente costituiti per lo studio delle minacce, che hanno accesso al portale in base al ruolo aziendale_per mostrare dati, documenti o funzioni specifiche a loro destinati.</p> <p>Devono essere previsti i seguenti profili di accesso configurabili da apposita interfaccia amministrativa di <i>Back End</i>:</p> <ul style="list-style-type: none"> <li>• Un profilo di <i>back office</i> per le attività di gestione della piattaforma e uno di gestione creazione bollettini di sicurezza.</li> <li>• Un profilo per l'erogazione di contenuti internamente a BSI/CERT</li> <li>• Un profilo per clienti del CERT per i quali sarà prevista l'erogazione del servizio di <i>Early Warning</i> nell'ambito dell'offerta dei servizi previsti.</li> </ul> <p>In funzione del tipo di clienti che accederanno il servizio dovrà essere possibile definire un profilo di erogazione specifico per cliente e su sua richiesta aderente ad una <i>Technology List</i> di suo interesse. In tal caso la piattaforma notifica solamente gli alert associati e riconducibili alle tecnologie scelte.</p> <p>Inoltre, trattandosi di accessi ad una piattaforma di sicurezza, l'accesso sarà mediato dal sistema di <i>Identity e Access Management</i> aziendale.</p>
EW_REQ_33.	<p>La soluzione dovrà prevedere due aree di erogazione: una privata, riservata interna a BSI e CERT e una pubblica per i clienti esterni.</p> <p>In ciascuna area sono previsti differenti profili di accesso.</p>
EW_REQ_34.	<p>Il modulo deve prevedere la creazione di un sistema a "ticket" per i casi che impattano su una determinata <i>technology list</i> per poi permetterne, successivamente, la tracciatura dello studio effettuato da un <i>team</i> di esperti.</p>
EW_REQ_35.	<p>Predisposizione di una <i>App</i> per l'utilizzo della piattaforma tramite <i>Device</i> e da remoto.</p>
EW_REQ_36.	<p>Il modulo deve prevedere una scrivania di lavoro, dove il <i>team</i> di analisi può condividere documenti o testi, per la creazione di un'analisi strutturata, finalizzata alla diffusione.</p>
EW_REQ_37.	<p>Il modulo deve prevedere la possibilità di creazione dinamica di un bollettino, con l'eventuale possibilità di inserimento di grafici o immagini prese da fonti esterne, proponendo un flusso di informazioni che precompilino il <i>report</i>.</p>
EW_REQ_38.	<p>La soluzione deve prevedere la ricezione di un "flusso di dati" proveniente da fonti interne ed esterne, strutturate o destrutturate, contestualizzate ad ogni vulnerabilità già censita e non, in modo da agevolare l'analisi del <i>team</i> di analisti.</p>

Codice Requisito	Descrizione Requisito
EW_REQ_39.	Il sistema dovrà erogare i contenuti su richiesta, e dovrà prevedere, in funzione della tipologia di utente che è acceduto e per area, differenti tipologie di <i>inquiry</i> , alcune comuni a tutti i profili, altri specializzati per profilo.
EW_REQ_40.	La soluzione deve prevedere un motore di ricerca delle vulnerabilità, che permetterà all'utente di ricercare vulnerabilità per: <i>Asset</i> tecnologico impattato : Sistema Operativo, <i>Application Server</i> , <i>Web Server</i> . Tipologia di vulnerabilità Livello di criticità Data pubblicazione Top 10 <i>Severity</i> Le vulnerabilità richieste saranno restituite in questo caso in formato visuale (pagine html) e potranno essere scaricabili in un formato di intercambio (pdf)

#### **4.3.3 Componente *Web&Documents Reporting Interface* piattaforma EW**

Di seguito sono descritti i requisiti minimi relativi al *Repository* Centralizzato del sistema di *Early Warning*, configurabile, scalabile ed estendibile nel tempo.

Tale modulo deve permettere di organizzare ed accedere a tutte le informazioni prodotte dalla piattaforma, comprendendo sia le informazioni utili al controllo della piattaforma stessa sia quelle derivanti dalle operazioni di correlazione ed analisi.

Codice Requisito	Descrizione Requisito
EW_REQ_41.	La soluzione deve prevedere la gestione di profili tecnologici multipli, ovvero liste di piattaforme/ <i>vendor</i> /prodotti per le quali si sceglie di ricevere segnalazioni di nuove vulnerabilità.
EW_REQ_42.	Il modulo deve prevedere la gestione degli asset correlati ai loro ambiti di riferimento, per la notifica mirata delle segnalazioni con la conseguente individuazione delle strutture o i servizi maggiormente a rischio, secondo statistiche periodiche.

Codice Requisito	Descrizione Requisito
EW_REQ_43.	Gestione documentale condivisa, con possibilità di ricerca avanzata e creazione di reporting di dettaglio, in grado di supportare/orientare le iniziative di pianificazione e le decisioni strategiche operative.
EW_REQ_44.	Creazione di report periodici personalizzati e strutturati secondo piani di visualizzazione definiti, in base alla profilazione del destinatario.
EW_REQ_45.	Il modulo deve consentire la creazione e manutenzione tramite interfaccia web di cruscotti di sintesi o <b>dashboard</b> quale riepilogo dello stato di rischi, valutazioni qualitative, etc. il tutto profilato secondo ruolo e funzione all'interno di Poste Italiane.
EW_REQ_46.	Il modulo deve <b>consentire la creazione tramite interfaccia web di report di dettaglio ed analisi</b> , andando via via più nel dettaglio attraverso <b>drill-down</b> successivi.

#### 4.4 Servizi Professionali

Codice Requisito	Descrizione Requisito
EW_REQ_47.	La fornitura deve prevedere un effort totale di almeno <b>258 gg./uu.</b> , suddiviso per le diverse figure professionali proposte.

##### 4.4.1 Figure professionali e skill-mix

Nella Tabella che segue è riportato il fabbisogno stimato per la fornitura in gara, in base alle Figure Professionali richieste, e il relativo *skill-mix* minimo richiesto:

Scheda Tecnica Servizi Offerti			
Figura Professionale	Fabbisogno Stimato (FTE)	Fabbisogno Stimato (N° gg/uu)	Profilo
Project Manager	0,30	64	Master
Security Specialist	0,88	194	Senior
<b>Totale</b>	<b>1,18</b>	<b>258</b>	

Di seguito si riportano, per ogni profilo e figura professionale: l'esperienza di riferimento, le conoscenze e le competenze professionali richieste.

Codice Requisito	Descrizione Requisito
EW_REQ_48.	I Profili <b>Master</b> devono possedere un'esperienza generale ICT di almeno 10 anni
EW_REQ_49.	I Profili <b>Senior</b> devono possedere un'esperienza generale ICT di almeno 7 anni
EW_REQ_50.	<p><b>Conoscenze generali</b>  Le risorse utilizzate dall'Impresa devono dimostrare di avere maturato esperienze progettuali che coprano le seguenti aree di interesse:</p> <ul style="list-style-type: none"> <li>• progettazione, sviluppo ed esercizio dei sistemi IT</li> <li>• progettazione e realizzazione di progetti di <i>Information Security</i></li> </ul>
EW_REQ_51.	<p><b>Competenze metodologiche</b>  Tutte le risorse messe a disposizione devono possedere le seguenti competenze metodologiche:</p> <ul style="list-style-type: none"> <li>• padronanza delle principali metodologie di sviluppo e collaudo</li> <li>• padronanza delle principali metodologie, tecnologie e prodotti di integrazione sistemi</li> <li>• padronanza delle metodologie di valutazione e reporting delle attività di sviluppo</li> <li>• padronanza delle metodologie di controllo e riduzione del rischio: <ul style="list-style-type: none"> <li>– <i>Risk assessment/management</i></li> <li>– <i>Configuration&amp;quality management</i></li> </ul> </li> </ul>
EW_REQ_52.	<p>Le risorse di Figura professionale <i>Project Manager</i> devono possedere le seguenti caratteristiche:</p> <ul style="list-style-type: none"> <li>• <b>Profilo professionale:</b> <i>Master</i></li> <li>• <b>Seniority professionale:</b> seniority di almeno 7 anni nella definizione, pianificazione e conduzione di progetti in ambito ICT. Il ruolo richiede un bagaglio di esperienze professionali accumulate in almeno 10 anni lavorativi ed esperienze progettuali maturate in realtà aziendali di analoga complessità.</li> <li>• <b>Certificazioni necessarie:</b> <ul style="list-style-type: none"> <li>– ITIL 3</li> </ul> </li> </ul>
EW_REQ_53.	<p>Le risorse di Figura professionale <b>Security Specialist</b> devono possedere le seguenti caratteristiche:</p> <ul style="list-style-type: none"> <li>• Profilo professionale: <i>Senior</i></li> <li>• Formazione scolastica a livello universitario</li> <li>• Seniority professionale: Conoscenza ed esperienza applicativa nell'impiego delle metodologie di progettazione e implementazione di sistemi di almeno 5 anni</li> </ul>

Codice Requisito	Descrizione Requisito
	<p><b>Certificazioni necessarie:</b></p> <ul style="list-style-type: none"> <li>- Microsoft Certified Technology Specialist (MCTS)</li> </ul> <p><b>Attività specifiche del ruolo:</b></p> <ul style="list-style-type: none"> <li>• Referente dei contenuti di <i>Business</i> e dell'analisi degli <i>User Requirement</i></li> <li>• Responsabile della definizione della metodologia di calcolo adottata, degli indicatori di interesse e degli algoritmi di calcolo             <ul style="list-style-type: none"> <li>- Conoscenza delle prassi di gestione del rischio IT</li> <li>- Personalizza gli algoritmi di calcolo</li> <li>- Documenta le procedure di calcolo</li> <li>- Esegue i <i>system test</i></li> <li>- Supporta il collaudo finale del sistema di analisi</li> </ul> </li> <li>• <b>Conoscenze e competenze specifiche:</b> <ul style="list-style-type: none"> <li>- capacità di ideare e sviluppare la soluzione sulla base dei requisiti espressi dal Cliente</li> <li>- conoscenza avanzata delle basi di programmazione sia procedurale sia <i>object-oriented</i></li> <li>- conoscenze specialistiche approfondite tali da poter supportare l'azienda nelle fasi di analisi preliminare, impostazione e sviluppo di progetti complessi e/o nelle valutazioni dell'utilizzo di tecnologie emergenti.</li> <li>- consolidata esperienza pluriennale sull'intero ambiente di configurazione / sviluppo ed esecuzione del prodotto specifico.</li> <li>- conoscenze specialistiche approfondite in amministrazione di sistemi/database con tecnologie specifiche ovvero in specifici campi di applicazione;</li> <li>- capacità autonoma di configurazione e di <i>problem solving</i>.</li> </ul> </li> </ul>
EW_REQ_54.	<p>La fornitura deve essere realizzata da personale in possesso dei requisiti sopra riportati e rispondente allo skill-mix minimo indicato nella Tabella 1.</p> <p>Il criterio guida utilizzato per la classificazione è quello della <i>seniority</i> ovvero l'esperienza professionale maturata: il profilo di livello più alto (<i>Master</i>) corrisponde a quello con la massima esperienza informatica, sia in termini tecnologici, sia in termini di abilità a collegare le evoluzioni dell'informatica stessa al business.</p>
EW_REQ_55.	<p><b>Costituzione Team</b></p> <p>Il <i>Team</i> per l'erogazione dei servizi dovrà essere costituito nella sua globalità al più entro 25 giorni naturali consecutivi dalla stipula del contratto.</p> <p>All'atto della costituzione del <i>Team</i>, Poste Italiane procederà a verificare, anche attraverso colloqui, la corrispondenza delle risorse fornite rispetto ai requisiti richiesti e a quanto indicato dall'Impresa nella documentazione di gara presentata.</p>

Codice Requisito	Descrizione Requisito
	<p>Nel caso in cui una o più risorse del <i>Team</i> risultino non corrispondenti e/o siano ritenute da Poste Italiane non adeguate alle attività da svolgere, l'Impresa è tenuta alla loro immediata sostituzione con altre idonee di livello, profilo, certificazioni ed esperienza analoghi o superiori a quelle richieste ed offerte, senza che ciò comporti costi aggiuntivi per Poste Italiane.</p> <p>Il consolidamento del <i>Team</i> dovrà concludersi al più entro 45 giorni naturali consecutivi dalla stipula del contratto, fermo restando quanto disposto in materia di subappalto (si vedano le Disposizioni contrattuali di riferimento).</p> <p>Trascorso tale termine senza che il <i>Team</i> sia stato consolidato in maniera conforme, Poste Italiane, si riserva la facoltà di risolvere di diritto ai sensi dell'art. 1456c.c. Il contratto, dando corso all'incameramento della cauzione, salvo risarcimento dei maggiori danni.</p> <p>A conclusione delle verifiche positive sarà redatto, dal Responsabile di Progetto incaricato da Poste Italiane, il <i>Verbale di rispondenza</i>, necessario per la prosecuzione della fornitura.</p> <p>L'Impresa si impegna a mantenere la stabilità del <i>Team</i> iniziale durante l'intero periodo di validità contrattuale e ad assicurare la sostituzione al più di <b>una</b> risorsa, per propria decisione o su richiesta di Poste Italiane.</p> <p>E' fatta salva la possibilità per Poste Italiane di verificare, anche in corso d'opera, la corrispondenza delle risorse fornite rispetto ai requisiti richiesti e a quanto indicato dall'Impresa nella documentazione di gara presentata.</p> <p>Nel caso in cui una o più risorse risultino non corrispondenti e/o siano ritenute da Poste Italiane non adeguate alle attività da svolgere, l'Impresa è tenuta a sostituirle, entro 15 giorni naturali consecutivi dalla richiesta, con altre idonee di livello, profilo, certificazioni ed esperienza analoghi o superiori a quelle richieste ed offerte, senza che ciò comporti costi aggiuntivi per Poste Italiane.</p> <p>Le risorse costituenti il <i>Team</i> messo a disposizione dall'Impresa per l'erogazione dei servizi oggetto di Gara presteranno servizio sia presso le sedi dell'Impresa, sia presso le sedi di Poste Italiane (Viale Europa 175, Roma o, se previsto da necessità di progetto, presso le sedi dei Data Center di Poste Italiane dislocate sul territorio nazionale), in funzione di quanto verrà richiesto da Poste Italiane stessa.</p>
EW_REQ_56.	<p><b>Orario di servizio</b></p> <p>Il servizio per le attività oggetto del capitolo sarà erogato dalle 9:00 alle 17:00 dal lunedì al venerdì, per l'intera durata del contratto.</p>

#### 4.4.2 Servizi di Analisi e Personalizzazione Applicativo

In seno alle attività previste dal presente documento, particolare rilevanza detengono le attività di analisi e progettazione della "Nuova piattaforma di Early Warning":

Codice Requisito	Descrizione Requisito
EW_REQ_57.	<p>L' attività progettuale deve coprire le seguenti aree:</p> <ul style="list-style-type: none"> <li>• <i>Project Management</i> tecnico ed organizzativo;</li> <li>• Analisi del contesto e dei requisiti;</li> <li>• Servizi di Installazione e Configurazione della piattaforma;</li> <li>• Integrazione manutenzione ed evoluzione della piattaforma Portale BSI;</li> <li>• Esplorazione ed Analisi dei dati di sicurezza;</li> <li>• Costruzione degli Indicatori;</li> <li>• Esplorazione ed Analisi dei dati;</li> <li>• Integrazione dei servizi di <i>Alerting</i> a disposizione;</li> <li>• Attività di <i>tuning</i>, customizzazione e <i>training</i> della piattaforma;</li> <li>• Formazione del <i>Team</i> di analisti di Tutela Aziendale;</li> <li>• Avviamento all'Esercizio;</li> <li>• Collaudo della piattaforma.</li> </ul>
EW_REQ_58.	<p>Inoltre devono essere forniti anche:</p> <ul style="list-style-type: none"> <li>• manutenzione delle componenti <i>software</i> in fornitura nonché delle componenti derivanti dalle attività di sviluppo: attivata dalla data di collaudo e garantita per la durata di 12 mesi.</li> </ul>

#### 4.4.3 Servizi di supporto al roll-out: Tuning, Collaudo e Certificazione

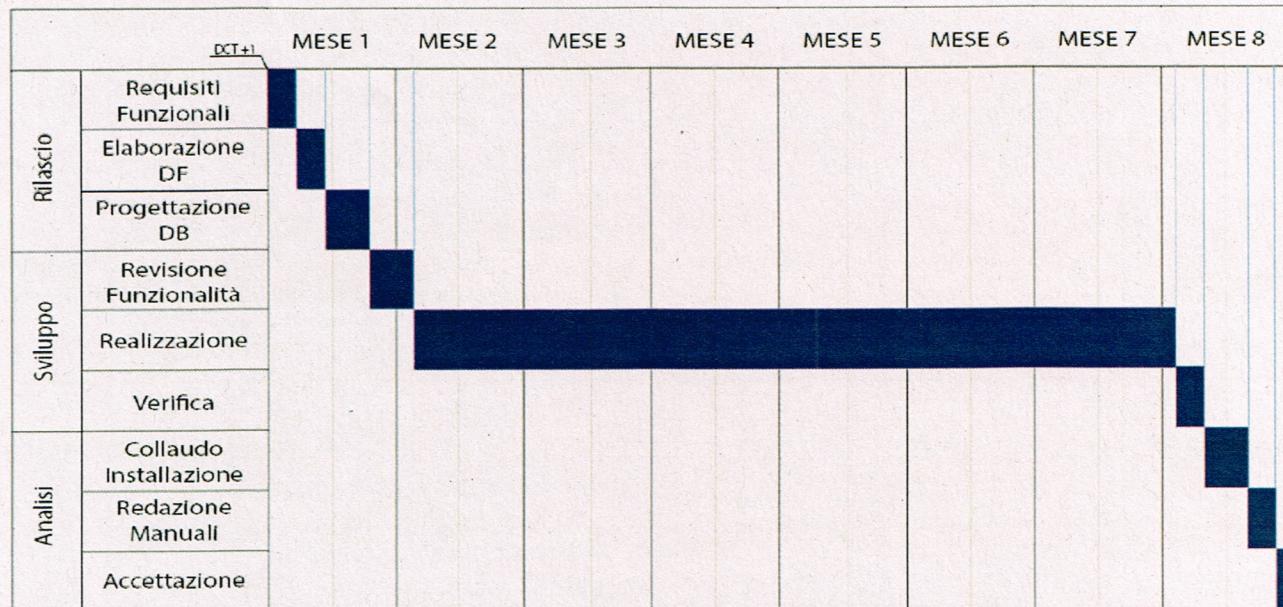
I servizi forniti devono rispondere ai seguenti requisiti.

Codice Requisito	Descrizione Requisito
EW_REQ_59.	<p>Per l'ambiente ditest interno, l'Impresa:</p> <ul style="list-style-type: none"> <li>• deve effettuare l'eventuale installazione del <i>software</i> applicativo</li> <li>• ha in carico la gestione delle configurazioni del <i>software</i> applicativo</li> <li>• deve predisporre i piani tecnici di dettaglio, verificandone la coerenza e l'aggiornamento per la durata dell'intero progetto</li> <li>• deve predisporre un documento con la descrizione delle attività e il relativo effort previsto a carico della struttura di Poste Italiane</li> </ul>
EW_REQ_60.	<p>L'Impresa deve fornire, in occasione della presentazione dei piani di collaudo, l'indicazione di dettaglio della propria metodologia di collaudo e rilascio</p>
EW_REQ_61.	<p>La metodologia di progetto proposta deve prevedere l'effettuazione delle attività di <i>testing</i> articolata su tre livelli: <i>test</i> di sistema, <i>test</i> di integrazione e <i>test</i> unitario. Nel caso del <i>test</i> unitario è sufficiente specificare i <i>test</i> effettuati e la metodologia di applicazione adottata.</p> <p>Nel caso dei <i>test</i> di sistema e dei <i>test</i> di integrazione occorre documentare nel "Piano dei test" i casi di <i>test</i>, previsti e preventivamente concordati con Poste Italiane, nonché il dettaglio degli esiti di applicazione degli stessi.</p> <p>L'accettazione da parte di Poste Italiane del processo e degli esiti dei <i>test</i></p>

Codice Requisito	Descrizione Requisito
	<p>effettuati è propedeutica per avviare la fase di collaudo parziale o globale del sistema.</p> <p>Verrà nominato da Poste Italiane un responsabile unico per tutte le fasi di collaudo.</p> <p>Il collaudo sarà svolto nei tempi previsti da Poste Italiane e con il supporto dell'Impresa, che si dovrà assumere la responsabilità diretta dell'esecuzione delle relative attività.</p> <p>La durata del collaudo sarà specificata tenendo conto anche dell'eventuale periodo di predisposizione dell'ambiente.</p> <p>L'attività verrà svolta in ambienti logistici individuati da Poste Italiane con le modalità indicate dal "Piano di Collaudo" redatto dall'Impresa e approvato da Poste Italiane.</p> <p>Nell'ambito del "Piano di Collaudo" l'Impresa sottoporrà, per l'approvazione, le procedure di collaudo specificando:</p> <ul style="list-style-type: none"> <li>• gli strumenti che intende impiegare</li> <li>• le strutture organizzative dell'Impresa e di Poste Italiane responsabili delle diverse fasi di collaudo</li> <li>• le modalità di registrazione dei dati</li> <li>• Il "Piano" dovrà inoltre essere così articolato: <ul style="list-style-type: none"> <li>◦ designazione, da parte dell'Impresa del proprio rappresentante e delle risorse in possesso delle specifiche competenze ritenute necessarie che lo coadiuveranno nello svolgimento dell'attività</li> <li>◦ pianificazione di dettaglio delle prove di collaudo</li> <li>◦ condizioni di collaudo</li> <li>◦ moduli, report, procedure di alimentazione sottoposti a verifica</li> <li>◦ criteri di gestione dei malfunzionamenti</li> <li>◦ tipologie di test previste</li> <li>◦ condizioni di accettabilità/rifiuto della prova.</li> </ul> </li> </ul> <p>Saranno altresì oggetto di verifica durante il periodo di collaudo oltre al software realizzato, tutti gli altri prodotti della fase realizzativa:</p> <ul style="list-style-type: none"> <li>• analisi di migrazione</li> <li>• disegno di dettaglio</li> <li>• piano dei test e documenti a supporto</li> <li>• manuale operativo di esercizio</li> <li>• piano di roll-out</li> <li>• lista oggetti di consegna</li> <li>• risultati dei tests.</li> </ul> <p>La conformità di quanto sopra verrà sancito attraverso un documento formale di accettazione.</p> <p>Durante la fase di collaudo le attività richieste all'Impresa sono:</p> <ul style="list-style-type: none"> <li>• supporto alla predisposizione dell'ambiente di collaudo: l'attività è volta a dare supporto alle strutture di Poste Italiane che devono predisporre l'ambiente di collaudo quali: definizione e caricamento della base dati, installazione del software applicativo, personalizzazione del software di base</li> <li>• supporto durante l'esecuzione del collaudo: tale supporto dovrà prevedere una illustrazione del sistema realizzato, e, per tutta la durata del collaudo: <ul style="list-style-type: none"> <li>◦ un responsabile del collaudo, cui segnalare i problemi</li> <li>◦ il supporto all'utilizzo delle funzionalità realizzate.</li> </ul> </li> </ul>

Codice Requisito	Descrizione Requisito
EW_REQ_62.	La ditta aggiudicataria s'impegna a fornire supporto per il collaudo e la certificazione della piattaforma in appositi ambienti messi a disposizione da Poste Italiane assistendo il personale di Poste nella verifica dei requisiti richiesti.
EW_REQ_63.	Per gli ambienti di collaudo e certificazione, l'Impresa: <ul style="list-style-type: none"> <li>• fornirà supporto alle strutture di Poste Italiane che devono predisporre gli appositi ambienti per: definizione e caricamento della base dati, installazione del software applicativo, gestione delle configurazioni del software applicativo nei suddetti ambienti</li> <li>• fornirà supporto durante l'esecuzione del collaudo e della certificazione: tale supporto dovrà prevedere una illustrazione di tutte le funzionalità richieste al sistema documentale e, per tutta la durata del collaudo/certificazione: <ul style="list-style-type: none"> <li>○ sarà presente un responsabile del collaudo, cui segnalare i problemi</li> <li>○ sarà fornito supporto al personale di Poste nella verifica delle funzionalità realizzate.</li> </ul> </li> </ul>
EW_REQ_64.	Al termine del collaudo e della certificazione, la conformità ai requisiti richiesti di tutte le funzioni realizzate verrà sancita attraverso un documento formale di accettazione scritto congiuntamente ad un responsabile di Poste Italiane.

#### 4.4.4 Tempi di realizzazione e piano di Roll out



Durante le varie fasi del progetto il fornitore garantire la continuità delle attuali attività di *Security Advisory*, senza causare alcun disservizio nel raggiungimento dei risultati richiesti.

Per garantire la continuità del servizio attualmente erogato, in materia di security alerting, l'Impresa dovrà rispettare la seguente tempistica:

- entro 7 gg. lavorativi dalla data di stipula del contratto dovrà essere attivato il servizio DeepSight Early Warning Gold Pack 8.0.

La realizzazione della piattaforma *Early Warning* dovrà essere attuata sulla base di un piano che prevede, per le tappe fondamentali, tempistiche di seguito riportate (DCT = data costituzione team di sviluppo):

- Una fase d'analisi, ove si analizzano i requisiti funzionali esposti, si elabora un diagramma di flusso dei processi e si progetta il DB
- Una fase di sviluppo che duri circa 6 mesi seguita da una di verifica a cura dell'Impresa
- Segue la fase finale di rilascio della piattaforma *Early Warning* in cui si effettuano test e collaudo finale con la presenza di personale di Poste Italiane, cui verranno dettagliatamente illustrate le varie funzionalità realizzate, seguita dalla redazione dei manuali illustrativi e dalla finale accettazione del sistema documentale.
- Il servizio di manutenzione di *Early Warning* da parte dell'Impresa parte dal giorno successivo all'accettazione del prodotto software da parte di Poste Italiane.
- Le giornate uomo d'impegno complessivo si prevedono ammontare a circa 258 giorni lavorativi, ferma restando la consegna del prodotto *Early Warning* entro 8 mesi dal giorno della firma del contratto.

#### 4.4.5 Installazione finale - Produzione

Codice Requisito	Descrizione Requisito
EW_REQ_65.	La ditta aggiudicataria s'impegna a fornire supporto per l'installazione dell'applicativo nell'ambiente finale di produzione messo a disposizione da Poste Italiane con modalità analoghe a quelle illustrate per l'ambiente di collaudo di cui ai requisiti EW_REQ_63 e EW_REQ_64

#### 4.4.6 Documentazione

Codice Requisito	Descrizione Requisito
EW_REQ_66.	<ul style="list-style-type: none"> <li>• L'impresa si impegnerà a produrre un documento di analisi che descriva le modalità di realizzazione delle funzionalità della piattaforma per rispondere alle indicazioni fornite da Poste Italiane.</li> </ul>
EW_REQ_67.	<ul style="list-style-type: none"> <li>• Deve essere redatto un insieme completo di manuali che preveda:           <ul style="list-style-type: none"> <li>• Manuale Utente</li> <li>• Manuale Gestore Applicativo;</li> <li>• Manuale Amministratore;</li> <li>• Manuale Installatore;</li> <li>• Manuale Manutenzione;</li> </ul> </li> </ul>
EW_REQ_68.	<ul style="list-style-type: none"> <li>• Deve essere consegnato tramite DVD a Poste Italiane il Codice Sorgente in chiaro (non compilato) opportunamente commentato.</li> </ul>
EW_REQ_69.	<ul style="list-style-type: none"> <li>• Deve essere consegnato tramite DVD a Poste Italiane l'applicativo con il Codice Sorgente compilato.</li> </ul>

Codice Requisito	Descrizione Requisito
EW_REQ_70.	<ul style="list-style-type: none"> <li>• Deve essere consegnato a Poste Italiane;</li> <li>• Il Diagramma Entità Relazioni della Base Dati che si implemetterà;</li> <li>• Le tabelle che si implemetteranno</li> <li>• La descrizione delle tabelle e delle relazioni tra le tabelle;</li> </ul>

#### 4.5 Garanzia Sviluppo

Codice Requisito	Descrizione Requisito
EW_REQ_71.	<p><b>Garanzia:</b>            Lo sviluppo del software oggetto di fornitura, nonché le componenti derivanti dalle attività di sviluppo, devono essere garantite e manutenute dalla consegna e per un periodo di 12 mesi a partire dalla data di collaudo positivo.</p>

#### 4.6 Servizio di manutenzione correttiva nel periodo di garanzia della piattaforma evoluta

Codice Requisito	Descrizione Requisito
EW_REQ_72.	<p>Il servizio di manutenzione deve comprendere:</p> <ul style="list-style-type: none"> <li>• <b>Manutenzione correttiva</b>, che assicura il ripristino delle funzionalità a seguito di malfunzionamenti dei componenti software oggetto della fornitura</li> <li>• <b>Manutenzione evolutiva</b>, che assicura il diritto ad acquisire, in modo gratuito e senza limitazioni, le nuove release/versioni dei componenti software oggetto della fornitura.</li> </ul>
EW_REQ_73.	<p><b>Manutenzione correttiva: modalità generali del servizio</b></p> <p>Gli interventi correttivi comprenderanno la diagnosi di tutti i malfunzionamenti segnalati, il ripristino del servizio, la risoluzione completa delle anomalie (comprese le eventuali sostituzioni dei componenti danneggiati e l'aggiornamento della relativa documentazione e manualistica) e le relative comunicazioni al responsabile che ha segnalato l'anomalia stessa.</p> <p>Per ciascun intervento sarà cura dell'Impresa produrre un <i>Rapporto di Intervento</i>.</p> <p>Il suddetto <i>Rapporto di Intervento</i> deve contenere almeno le seguenti</p>

Codice Requisito	Descrizione Requisito						
	<p>informazioni:</p> <ul style="list-style-type: none"> <li>• data e ora di apertura del malfunzionamento;</li> <li>• ticket rilasciato dall' Impresa;</li> <li>• data e ora della risoluzione del malfunzionamento;</li> <li>• sito e nominativo del dipendente o della struttura di Poste Italiane che ha effettuato la richiesta;</li> <li>• tipologia di modulo software soggetto al malfunzionamento;</li> <li>• descrizione del malfunzionamento riscontrato;</li> <li>• eventuale sostituzione del modulo software con uno di caratteristiche funzionali e prestazionali uguali o superiori.</li> </ul> <p>Il ripristino della funzionalità deve essere sottoscritto dall'utilizzatore del componente danneggiato o da altro dipendente di Poste Italiane che certifichi la piena funzionalità delle parti oggetto dell'intervento.</p> <p>Il <i>Rapporto d'Intervento</i> deve essere fornito da colui che ha effettuato l'intervento stesso in duplice copia: una copia deve essere consegnata al dipendente di Poste Italiane che firma il rapporto.</p>						
EW_REQ_74.	<p><b>Manutenzione correttiva: tempi di risposta</b></p> <p>Sarà compito del Referente di Poste Italiane comunicare all'Impresa il malfunzionamento ed assegnare all'anomalia la classe di gravità, utilizzando la casistica illustrata nella tabella seguente.</p> <table border="1" data-bbox="505 1174 1255 1438"> <thead> <tr> <th data-bbox="505 1174 721 1240">Categoria</th><th data-bbox="721 1174 1255 1240">Descrizione</th></tr> </thead> <tbody> <tr> <td data-bbox="505 1240 721 1358">Bloccante</td><td data-bbox="721 1240 1255 1358">Si tratta di un difetto o anomalia che impedisce l' uso dell'applicazione o di una o più funzionalità importanti.</td></tr> <tr> <td data-bbox="505 1358 721 1438">Non Bloccante</td><td data-bbox="721 1358 1255 1438">Malfunzionamenti per cui non è impedito l'uso delle funzioni.</td></tr> </tbody> </table> <p>La risposta alle segnalazioni di anomalie deve avvenire entro 2 ore solari in orario lavorativo (lun-ven 8,30-18,30) dalla segnalazione stessa.</p> <p>L'Impresa dovrà garantire un livello di intervento in funzione della categoria di malfunzionamento, così definita.</p> <p>Per "impedimento all'uso dell'applicazione o delle sue funzioni" si intende una malfunzione vera e propria dell'applicazione o gli effetti che tale malfunzione ha causato alla base dati.</p> <p>In relazione alla tipologia di anomalia rilevata, i tempi di ripristino e risoluzione sono riportati nella tabella al requisito successivo e sono validi sia per anomalie hardware che software.</p> <p>Per Ripristino si intende la disponibilità alla messa in produzione dei componenti del sistema interessati dall' anomalia, tramite una soluzione Quick-Fix.</p> <p>Per Risoluzione si intende la disponibilità alla messa in produzione dei componenti del sistema interessati dall' anomalia con la completa</p>	Categoria	Descrizione	Bloccante	Si tratta di un difetto o anomalia che impedisce l' uso dell'applicazione o di una o più funzionalità importanti.	Non Bloccante	Malfunzionamenti per cui non è impedito l'uso delle funzioni.
Categoria	Descrizione						
Bloccante	Si tratta di un difetto o anomalia che impedisce l' uso dell'applicazione o di una o più funzionalità importanti.						
Non Bloccante	Malfunzionamenti per cui non è impedito l'uso delle funzioni.						

Codice Requisito	Descrizione Requisito													
	<p>risoluzione dell' anomalia stessa.  L'intervento deve concludersi con il perfetto funzionamento della soluzione realizzata.  Il tempo di decorrenza viene misurato a partire dalla data ed ora di segnalazione, formalizzata per iscritto.</p>													
EW_REQ_75.	<p><b>Manutenzione correttiva: tempi di ripristino e risoluzione</b>  I tempi massimi di ripristino del servizio e di risoluzione delle anomalie sono dettagliati nella tabella seguente in giornate lavorative (gg/lav.).</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th colspan="3" style="background-color: #ffffcc;">Tempi massimi dalla segnalazione anomalia</th></tr> </thead> <tbody> <tr> <td rowspan="2">Anomalie Bloccanti</td><td>Ripristino</td><td>2 gg/lav.</td></tr> <tr> <td>Risoluzione</td><td>3 gg/lav.</td></tr> <tr> <td rowspan="2">Anomalie Non Bloccanti</td><td>Ripristino</td><td>3 gg/lav.</td></tr> <tr> <td>Risoluzione</td><td>4 gg/lav.</td></tr> </tbody> </table>	Tempi massimi dalla segnalazione anomalia			Anomalie Bloccanti	Ripristino	2 gg/lav.	Risoluzione	3 gg/lav.	Anomalie Non Bloccanti	Ripristino	3 gg/lav.	Risoluzione	4 gg/lav.
Tempi massimi dalla segnalazione anomalia														
Anomalie Bloccanti	Ripristino	2 gg/lav.												
	Risoluzione	3 gg/lav.												
Anomalie Non Bloccanti	Ripristino	3 gg/lav.												
	Risoluzione	4 gg/lav.												

## 5 Modalità di partecipazione e criteri di aggiudicazione

### 5.1 Relazione tecnica

L'Impresa dovrà presentare una *Relazione Tecnica*, composta da:

- una proposta di dettaglio della propria soluzione di massimo 60 pagine (componenti software offerti e relative illustrazioni funzionali, compresi oggetti software di terze parti essenziali per il funzionamento della soluzione, configurazione minimale della infrastruttura hardware ospitante, performance, affidabilità della soluzione, scalabilità della stessa, etc.), specificando anche le eventuali referenze di analoghe realizzazioni eseguite.
- una dichiarazione dell'impresa in cui sia indicata la conformità dell'offerta a quanto richiesto nei requisiti minimi espressi nel Capitolo 4 del presente documento;
- la Scheda Requisiti minimi redatta come indicato nel paragrafo 5.2 del presente documento;

## 5.2 Scheda Requisiti minimi

L'Impresa deve compilare la Scheda Requisiti minimi sulla base dei requisiti riportati nel capitolo 4 del presente documento (Requisiti minimi obbligatori della fornitura).

Nella colonna "Riferimento documenti" dovranno essere inseriti i documenti, il paragrafo e la pagina della relazione tecnica, da cui si evince che il requisito viene soddisfatto.

Caratteristica richiesta	Riferimento documenti
EW_REQ_1.	
EW_REQ_2.	
EW_REQ_3.	
.....	
EW_REQ_n.	

## 5.3 Criterio di aggiudicazione

L'aggiudicazione avverrà, secondo la disciplina del D.Lgs. 163/06 e successive modifiche ed integrazioni, mediante procedura negoziata e con l'applicazione del criterio del prezzo più basso.