

Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione

Manuale operativo

Dizionario delle Forniture ICT

Classe di Fornitura

Gestione della sicurezza fisica SIF

INDICE

1.	GENERALITÀ SUL DOCUMENTO.....	4
2.	DESCRIZIONE DELLA CLASSE DI FORNITURA.....	4
3.	MODALITÀ DI DEFINIZIONE DELLA FORNITURA	5
3.1.	OBIETTIVI	6
3.2.	UTENZA	6
3.3.	DIMENSIONE, ARCHITETTURA E COMPLESSITÀ	7
3.4.	VINCOLI E REQUISITI.....	7
3.5.	RELAZIONE CON ALTRE CLASSI.....	8
3.6.	STANDARD E NORME.....	8
3.7.	MODALITÀ DI STIMA DEI COSTI ANCHE IN FUNZIONE DELLA QUALITÀ RICHIESTA	8
4.	DESCRIZIONE DELLE ATTIVITÀ E DEI PRODOTTI.....	10
4.1.	ANALISI DEI REQUISITI	13
4.2.	PROGETTAZIONE	14
4.3.	PROGETTAZIONE COLLAUDO	14
4.4.	REALIZZAZIONE DEL SERVIZIO	15
4.5.	REALIZZAZIONE DEL COLLAUDO	16
4.6.	MONITORAGGIO DI SICUREZZA.....	17
4.7.	GESTIONE OPERATIVA DELLE EMERGENZE	17
4.8.	GESTIONE DEI CAMBIAMENTI.....	18
4.9.	GESTIONE OPERATIVA	18
4.10.	RENDICONTAZIONE	19

4.11.	DESCRIZIONE DEI PRODOTTI.....	19
5.	DESCRIZIONE DEI PROFILI PROFESSIONALI COINVOLTI.....	22
6.	INDICATORI/MISURE DI QUALITÀ	27

1. GENERALITÀ SUL DOCUMENTO

Questo documento descrive uno dei lemmi del Manuale operativo “Dizionario delle forniture ICT” delle Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione. Ogni lemma del Dizionario rappresenta una classe di fornitura ICT elementare. Il Dizionario contiene tutte le classi di forniture che si sono ritenute necessarie per rappresentare compiutamente i contratti ICT delle pubbliche amministrazioni. Ogni lemma del Dizionario è autoconsistente e indipendente; esso prevede:

- **la descrizione della classe di fornitura ICT elementare**, che ha lo scopo di definirne univocamente l'ambito di applicazione;
- **l'esplicitazione di “regole” per l'uso della classe di fornitura**, utile a proporre al lettore suggerimenti sull'uso del lemma per la stesura dell'oggetto contrattuale;
- **la descrizione delle attività** relative alla classe di fornitura e dei relativi prodotti, utile al lettore come traccia riutilizzabile per scrivere contratti e capitolati tecnici;
- **una tabella che riassume attività, prodotti e indicatori di qualità**, utile al lettore come quadro sinottico che riassume il legame tra attività e relativi prodotti da queste realizzati ed identifica, in relazione ad entrambi, gli indicatori di qualità adottati per la classe di fornitura;
- **una scheda per ogni indicatore di qualità** (presente nella tabella di cui sopra), utile al lettore come traccia riutilizzabile, per scrivere contratti e capitolati tecnici;
- **un glossario** (ove necessario) specifico per la classe di fornitura.

Nell'ambito della complessa attività di scrittura di contratti e capitolati tecnici, i lemmi possono essere intesi come “ricette contrattuali” di immediato utilizzo mediante processi di copia e incolla, per rappresentare le esigenze della stazione appaltante.

Nell'ottica del riuso, particolare attenzione dovrà essere prestata alle imprescindibili e necessarie attività di specificazione e taratura delle classi di fornitura ICT elementari utilizzate e, successivamente, all'integrazione delle diverse classi di fornitura scelte in un unico e coerente contratto ICT.

La versione digitale di ogni lemma è singolarmente scaricabile dal sito CNIPA in formato editabile (.doc) che ne permette il riutilizzo anche parziale.

Per maggiori informazioni sull'utilizzo integrato delle classi di fornitura e dei processi trasversali si rimanda agli esempi contenuti nel Manuale applicativo “Esempi di applicazione”.

2. DESCRIZIONE DELLA CLASSE DI FORNITURA

La Gestione della sicurezza fisica tratta le misure necessarie per proteggere le aree, i sistemi e le persone che operano sul sistema informativo. I requisiti di sicurezza possono variare considerevolmente in funzione delle dimensioni e dell'organizzazione dello stesso.

Generalmente un sistema SIF si articola nelle seguenti due categorie di servizi:

- **Sicurezza di area**

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze alle informazioni critiche e allo svolgimento dei servizi e dei processi di Information Technology. Le contromisure si riferiscono alla perimetrazione di sicurezza delle sedi e dei locali, alle protezioni perimetrali dei siti, ai controlli fisici degli accessi (realizzati mediante un complesso di controlli e barriere fisiche, all'interno e nei punti di accesso dei locali da proteggere), alla sicurezza della sala macchine rispetto a danneggiamenti accidentali o intenzionali, all'isolamento delle aree ad elevato transito di personale esterno all'organizzazione. Alcuni servizi/sistemi specifici per realizzare la Sicurezza di area sono i seguenti:

- sistemi di video sorveglianza;
- sistemi di allarme perimetrale;
- sistemi di allarme interno;
- servizi di vigilanza;
- servizi di *reception*;
- sistemi di controllo accessi centralizzati.

- **Sicurezza delle apparecchiature**

La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali delle risorse ICT e dei supporti e dall'altro alla sicurezza ambientale demandata principalmente agli impianti di alimentazione e di condizionamento. Alcuni servizi/prodotti specifici per realizzare la sicurezza delle apparecchiature sono i seguenti:

- sistema di climatizzazione;
- sistema rilevamento allarmi ambientali (es. antincendio, antiallagamento);
- impianti di alimentazione elettrica di emergenza.

Pur non costituendo un servizio né un prodotto, alla sicurezza delle apparecchiature contribuiscono anche gli accorgimenti di protezione e posizionamento all'interno dell'area.

I servizi descritti risultano più efficaci se calati all'interno di un processo generale di gestione della sicurezza, definito dall'Amministrazione. In generale quindi, i servizi descritti sono erogati all'interno di un contesto organizzativo e procedurale, che integra la struttura organizzativa esistente, attraverso responsabilità definite e chiari obiettivi alla luce della politica per la sicurezza.

3. MODALITÀ DI DEFINIZIONE DELLA FORNITURA

Una fornitura di Gestione della sicurezza fisica si articola in servizi. Ad ognuno di questi servizi può essere associato un insieme di attività, attraverso le quali si realizza il SIF.

Per esempio, un sistema di rilevamento allarmi ambientali contribuisce principalmente alle attività di monitoraggio, di gestione emergenze e di gestione dei cambiamenti.

Per la descrizione di dettaglio si rimanda al capitolo “Descrizione delle attività e dei prodotti”, di seguito si riporta una tabella riepilogativa.

TIPO DI SERVIZIO/SISTEMA	Attività				
	Monitoraggio e controllo	Gestione delle emergenze	Gestione dei cambiamenti	Gestione ordinaria	Reporting
Sistema di video sorveglianza	✓	✓	✓	✓	✓
Sistema di allarme perimetrale	✓	✓	✓	✓	-
Sistema di allarme interno	✓	✓	✓	✓	-
Servizio di vigilanza	✓	✓	✓	✓	-
Servizio di reception	✓		✓	✓	✓
Sistema di controllo accessi centralizzato	✓	✓	✓	✓	✓
Sistema di climatizzazione	✓	-	✓	✓	-
Sistema di rilevamento allarmi ambientali	✓	✓	✓	-	-
Impianti di alimentazione elettrica di emergenza	✓	✓	✓	-	-

Tabella 1 - Correlazione tra attività e tipo di servizio

3.1. OBIETTIVI

Il sistema SIF provvede a realizzare quei controlli finalizzati a

- proteggere le aree, impedendo accessi non autorizzati, danni e interferenze agli ambienti, danneggiamento delle informazioni e impedimento allo svolgimento dei servizi e dei processi IT;
- proteggere gli apparati mediante la prevenzione di perdite, danni, manomissione degli investimenti e interruzione delle attività;
- prevenire la possibilità di manomissione o di furto delle informazioni e degli strumenti di elaborazione.

3.2. UTENZA

I servizi sono forniti, in modalità differenziate per qualità e livelli di servizio, per i diversi tipi di perimetri in cui sono collocati i sistemi informativi da proteggere e per i diversi tipi di locali in cui sono collocate le risorse (umane ed elaborative) all’interno del perimetro, per esempio:

- uffici di relazione con il pubblico;
- uffici interni;
- sale operatori;

- centri elaborazione dati;
- centri di esercizio degli apparati.

I servizi riguardano diversi tipi di utenza, per esempio:

- personale interno all'Amministrazione (attraverso i referenti per la Sicurezza ed i responsabili ICT);
- consulenti e fornitori;
- visitatori (il pubblico che accede ai locali dell'Amministrazione).

3.3. DIMENSIONE, ARCHITETTURA E COMPLESSITÀ

Le variabili che hanno un impatto su costi, rischi e qualità dei servizi da erogare sono le seguenti:

- tipo dell'ambiente da proteggere:
 - uffici di relazione con il pubblico;
 - uffici interni;
 - sale operatori;
 - centri di esercizio;
 - ambienti di sviluppo e/o di test;
- sensibilità delle informazioni trattate;
- dimensioni delle sedi e dei locali da proteggere.

I costi della fornitura devono tenere conto:

- a) delle risorse necessarie per l'avvio del servizio, nonché dell'acquisto e manutenzione dei prodotti e tecnologie necessarie;
- b) del numero e del tipo di figure professionali necessarie all'erogazione del servizio a regime.

Il costo del punto a) è direttamente proporzionale all'estensione ed al numero delle aree e dei locali da proteggere. Per esempio, per un sistema di video sorveglianza, il costo dipende dal numero e dalla qualità delle telecamere necessarie per sorvegliare i punti critici del perimetro.

Il numero di figure professionali necessarie all'erogazione del servizio di SIF a regime (punto b) è linearmente proporzionale ai seguenti parametri:

- numero dei siti da presidiare;
- tipo di presidio richiesto in base alla fascia temporale (per esempio H24) e qualità di copertura del servizio (presidio fisso o controllo remoto);
- per ogni sito, il numero di attività/prodotti gestiti ed il numero di utenti.

3.4. VINCOLI E REQUISITI

Per usufruire in maniera ottimale dei servizi di sicurezza descritti, l'Amministrazione necessita di un'organizzazione interna e di una politica per la sicurezza in conformità alla

direttiva “Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali” del Ministro per l’Innovazione e le Tecnologie, d’intesa con Il Ministro delle Comunicazioni e successive modifiche ed integrazioni (G.U. n. 69 del 22 marzo 2002) o comunque quanto più possibile in linea con lo standard ISO-17799.

3.5. RELAZIONE CON ALTRE CLASSI

Gli aspetti di gestione della sicurezza trattati nella classe di fornitura SIF sono in stretta relazione, per la natura dei servizi erogati, con gli aspetti complementari discussi nelle classi Gestione della sicurezza logica (SIL) e Business continuity e disaster recovery (DRE).

Inoltre, i servizi di gestione e mantenimento delle condizioni ambientali delle infrastrutture, che di per sé sono pertinenti alla sicurezza fisica, sono trattati nella classe Sviluppo sistemi (SSI), alla quale è necessario fare riferimento per questi aspetti.

Infine, alcuni indicatori di qualità della classe SIF sono mutuati dalle classi di fornitura relative ai processi trasversali, in particolare Documentazione (PGD), Gestione (PGE) e Gestione della configurazione (PGC).

3.6. STANDARD E NORME

ISO/IEC 17799: Information Security Management - Part 1: Code of practice for information security management, 2000

BS7799: Information Security Management - Part 2: Specification for information security management systems, 2000

Ministero per l’Innovazione Tecnologica – La sicurezza Informatica e delle Telecomunicazioni (ICT Security) – Allegato 2, Gennaio 2002

AIPA – Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella Pubblica Amministrazione (Gruppo di Lavoro AIPA-ANASIN-ASSINFORM-ASSINTEL), 1999

Decreto Legislativo 19/9/1994, n. 626 (Attuazione delle direttive 89/391/CEE, 89/654/CEE, 89/655/CEE, 89/656/CEE, 90/269/CEE, 90/270/CEE, 90/394/CEE e 90/679/CEE riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro)

Bibliografia

www.cert.org - uno dei principali punti di accesso alle informazioni sul mondo della sicurezza, contenente articoli, best practices, documenti ed altre risorse fondamentali per l’implementazione di un sistema di gestione della sicurezza.

3.7. MODALITÀ DI STIMA DEI COSTI ANCHE IN FUNZIONE DELLA QUALITÀ RICHIESTA

Numero d’Oggetto/Part Number
MANUALE 4

Ed./Issue
2.0 **10.08.2008**

Com. Mod./Ch. Notice

3.3.2 SIF Gestione della sicurezza
fisica

Nei servizi che prevedono la presenza di personale (come per esempio il servizio di reception e vigilanza), il costo del servizio offerto dipende principalmente dal tempo di copertura.

È possibile ipotizzare quattro tipi di copertura:

- **Normale:** servizio erogato per otto ore, nei giorni feriali dal lunedì al venerdì;
- **H12:** servizio erogato per 12 ore nei giorni feriali dal lunedì al venerdì e 6 ore il sabato;
- **H16:** servizio erogato per 16 ore nei giorni feriali dal lunedì al venerdì e 8 ore il sabato;
- **H24:** servizio erogato 24 ore al giorno, sette giorni su sette.

A titolo indicativo, si fornisce un diagramma che riporta l'andamento del costo rispetto alla finestra temporale di erogazione del servizio (figura 1), la scala delle ascisse va considerata lineare.

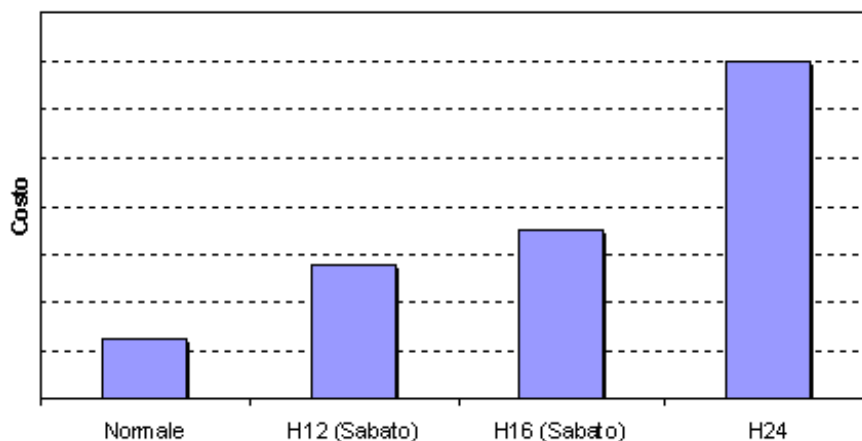


Figura 1 – Relazione tra costo e finestra di erogazione del servizio

Gli altri parametri che influiscono sul costo del servizio, in rapporto alla qualità richiesta, sono il presidio in loco (pionamento), il servizio di ronda con orari di sosta determinati oppure il presidio remoto, per la video-sorveglianza.

Nei servizi che prevedono la fornitura e l'installazione di prodotti (sistemi di allarme perimetrale, allarme interno, sistema di climatizzazione, ecc.), il costo della fornitura, in rapporto alla qualità richiesta, dipende da

- affidabilità delle componenti fornite;
- livello di disponibilità assicurato;
- tipo di assistenza. In questo caso sono da considerare i tempi massimi di intervento e di ripristino assicurati.

4. DESCRIZIONE DELLE ATTIVITÀ E DEI PRODOTTI

Le attività ed i prodotti relativi ai processi organizzativi e di supporto (processi trasversali), e cioè per esempio quelli relativi a gestione, documentazione, gestione della configurazione e assicurazione della qualità non sono descritti in questa scheda. Per la loro descrizione si rimanda pertanto alle schede specifiche.

Nel caso in cui attività o prodotti relativi a questi processi abbiano particolare rilevanza o criticità per la classe, essi sono comunque richiamati, evidenziando gli aspetti rilevanti o critici, rimandando per le caratteristiche generali alla scheda del processo.

Per quanto riguarda i processi trasversali, si segnalano, in particolare, le classi di fornitura Documentazione (PGD), Gestione (PGE), Gestione della configurazione (PGC), che vanno considerate come un indispensabile complemento della classe Gestione della sicurezza fisica. Queste classi infatti trattano i servizi di supporto necessari per mantenere un ambiente di controllo stabile e tale da garantire il soddisfacimento dei requisiti operativi. A queste classi si farà riferimento per l'individuazione delle attività (e dei relativi prodotti ed indicatori), che integrano quanto descritto in questo documento al fine di ottenere una descrizione completa del servizio di Gestione della Sicurezza Fisica.

È importante considerare che una fornitura di Gestione della sicurezza fisica ha normalmente una durata pluriennale e spesso nuove esigenze (variazione del perimetro dei beni da proteggere, evoluzioni tecnologiche o applicative, variazione dei requisiti di sicurezza) possono richiedere significative variazioni alla gestione operativa.

Queste variazioni, oltre richiedere una fase di accettazione (test e collaudo) possono richiedere la riprogettazione della gestione stessa (processi, attività, risorse impiegate, strumenti), che sarà effettuata contemporaneamente alla gestione corrente (si veda a questo proposito l'attività Gestione dei cambiamenti). Ne deriva che tutte le attività possono essere contemporaneamente attive durante il periodo di erogazione del servizio (per esempio, il passaggio in esercizio di un nuovo applicativo che modifica i parametri dimensionali o i requisiti iniziali della fornitura richiede la pianificazione, la riprogettazione e la conseguente nuova realizzazione della gestione).

Questa possibilità va prevista nelle clausole contrattuali della fornitura in quanto ha impatto sui costi.

I servizi svolti nell'ambito della classe di fornitura SIF si articolano su due diverse tipologie di attività. Le attività di progettazione e realizzazione, di natura transiente, finalizzate alla realizzazione del servizio e le attività di gestione, di natura continuativa, le cui interazioni sono illustrate in figura 2.

Il servizio di Gestione della sicurezza fisica è solitamente articolato nelle attività:

- Monitoraggio e controllo
- Gestione delle emergenze
- Gestione ordinaria
- Gestione dei cambiamenti
- Reporting

Queste attività sono organizzate secondo il flusso indicato in figura 2.

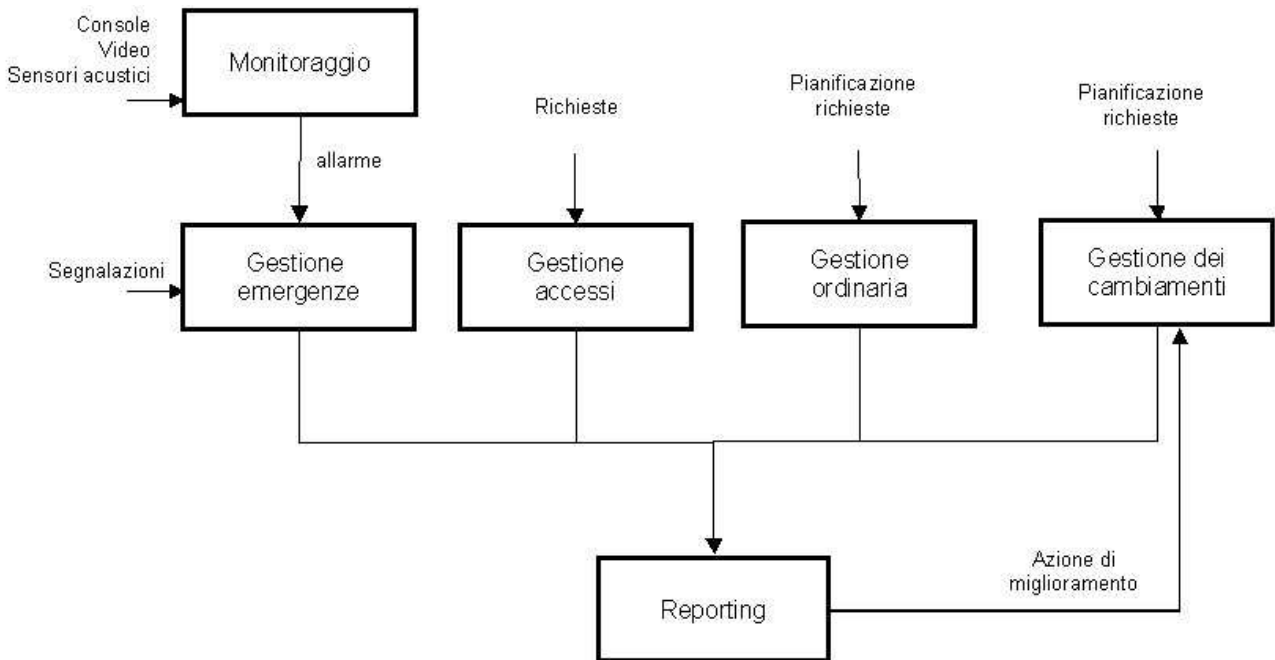


Figura 2: Diagramma di flusso relativo ad un servizio SIF

La seguente tabella riassume le principali attività del ciclo di vita della fornitura, che poi saranno descritte in maggior dettaglio nei paragrafi seguenti. Per ogni attività sono specificati:

- una stima indicativa del peso percentuale di effort richiesto, nell’ipotesi che la fornitura comprenda tutte le categorie di prodotto di pertinenza SIF descritte al paragrafo 4.11, che il servizio di gestione operativa sia erogato con presidio di tipo H 12 e presidio remoto di vigilanza negli orari non coperti in loco. L’incidenza di ciascuna attività è rapportata al totale della tipologia di appartenenza (“progettazione e realizzazione” o “gestione”);
- i prodotti di input e di output;
- i profili professionali EUCIP responsabili dell’esecuzione dell’attività.

ATTIVITA'	% EFFORT	INPUT	OUTPUT	PROFILI PROFESSIONALI RESPONSABILI
Analisi dei requisiti	15%	Capitolato tecnico della fornitura e ulteriori specifiche fornite dall'Amministrazione	Specifica dei requisiti Piano di progetto Piano della Qualità Piano di gestione delle comunicazioni	Consulente per la Sicurezza
Progettazione	35%	Specifiche dei requisiti	Progetto del sistema	Consulente per la Sicurezza
Progettazione collaudo	5 %	Progetto del sistema	Specifica di test Specifica di collaudo	Tecnico di Collaudo e Integrazione di Sistemi
Realizzazione del servizio	40%	Progetto del sistema	Progetto del servizio, Sistema di erogazione del servizio	Consulente per la Sicurezza
Realizzazione collaudo	5 %	Sistema di erogazione del servizio	Rapporto di test Verbale di collaudo	Tecnico di Collaudo e Integrazione di Sistemi
Totale Attività di Progettazione e Realizzazione	100%			
Monitoraggio di sicurezza	35 %	Eventi	Allarme Rapporto monitoraggio sicurezza fisica	Consulente per la Sicurezza
Gestione operativa delle emergenze	10 %	allarme generato dal processo di monitoraggio; allarme pervenuto al servizio di vigilanza .	Rapporto di incidente	Consulente per la Sicurezza
Gestione dei cambiamenti	10 %	Verifiche di necessità	Documento di revisione	Consulente per la Sicurezza
Gestione operativa	35%	Piano per la manutenzione e amministrazione degli strumenti utilizzati Piano per la Gestione degli accessi	Registri di conduzione operativa	
Rendicontazione	10 %	Eventi significativi	Rapporto di sintesi sulla sicurezza fisica	Consulente per la Sicurezza
Totale Attività di Gestione Operativa	100%			

4.1. ANALISI DEI REQUISITI

Questa attività si concretizza in un documento di **Specifica dei requisiti**, articolato in:

- descrizione del servizio e dei relativi processi;
- requisiti contrattuali;
- livello di copertura del servizio che il fornitore si impegna a garantire;
- standard di servizio da assicurare attraverso indicatori di qualità;
- efficacia del servizio;
- requisiti cogenti, in base alle norme in vigore;
- requisiti tecnici, definiti in base alle tecnologie disponibili;
- requisiti di gestione operativa e manutenzione;
- requisiti organizzativi per la gestione del servizio, in termini di struttura gerarchica e modalità operative.

Il documento Requisiti della fornitura tratta ciascuno degli elementi sopra indicati ed ha le seguenti caratteristiche:

- contiene il puntamento alla documentazione contrattuale di riferimento (capitolato, richiesta di offerta, ecc.) per ogni requisito trattato;
- fornisce, per ogni requisito, una descrizione dettagliata, orientata alla progettazione ed alla realizzazione.

Questa attività, così come le altre, è inserita in un piano di lavoro che identifica le attività necessarie per la realizzazione della fornitura e la redazione dei documenti di pianificazione, considerando i vincoli ed i requisiti definiti dal progetto, la necessità di precedenza tra le attività, le responsabilità e le competenze necessarie al gruppo di lavoro che svolge le attività di sviluppo, per garantire il rispetto dei tempi definiti.

Per tutte le attività che non rientrano sotto la diretta responsabilità del fornitore, l'Amministrazione garantisce il corretto svolgimento ed il rispetto dei tempi previsti a piano.

Il prodotto principale di questa attività è il documento **Piano di progetto**.

Viene anche redatto il **Piano della Qualità** che indirizza il controllo di qualità, l'assicurazione di qualità ed il miglioramento della qualità per tutte le fasi del ciclo di vita della fornitura. Il Piano della Qualità contiene la descrizione degli obiettivi di qualità, i controlli e le verifiche, i criteri di entrata/uscita delle varie fasi progettuali e i criteri di accettazione dei prodotti originati dalle attività.

È previsto un **Piano di gestione delle comunicazioni**, in particolare nel caso in cui le attività di gestione assumano caratteristiche di criticità, o quando l'introduzione di modifiche ai sistemi esistenti implichi significative modifiche all'ambiente organizzativo o ai processi dell'Amministrazione o del gestore dei sistemi. Questo piano definisce i criteri di raccolta ed archiviazione delle varie informazioni, il sistema di distribuzione della documentazione, il programma di formazione legato alla comunicazione.

Il Piano di gestione della configurazione descrive le modalità per l'identificazione, la rintracciabilità ed il controllo della configurazione dei sistemi. In questo piano sono individuati gli elementi di configurazione. Questo piano è trattato nel processo di Gestione della Configurazione.

Tutti i piani sono accettati e validati dall'Amministrazione.

4.2. PROGETTAZIONE

Questa attività produce il documento **Progetto del sistema**, con i seguenti contenuti:

- identificazione della architettura di alto livello del sistema riguardante gli elementi infrastrutturali e le procedure previste per la realizzazione di un SIF;
- elaborazione del prototipo del sistema ipotizzato, con la definizione dei flussi di attività;
- descrizione dei flussi di attività in una logica cliente-fornitore, per gestire la relazione come un ciclo o un insieme di cicli di servizio;
- definizione dei dati e dei requisiti degli strumenti necessari per la registrazione e la rendicontazione delle attività del SIF.

Il documento Progetto del Sistema tratta ognuno degli elementi sopra indicati ed ha le seguenti caratteristiche:

- contiene, per ogni elemento, il puntamento alla documentazione contrattuale di riferimento (capitolato, richiesta di offerta, ecc.) per ogni requisito trattato;
- fornisce, per ogni elemento, una descrizione dettagliata orientata alla realizzazione.

4.3. PROGETTAZIONE COLLAUDO

A seguito alla progettazione tecnica del sistema, sono svolte le attività di progettazione di test e collaudo, che sono così caratterizzati:

TEST

- È eseguito durante ed alla fine dello sviluppo.
- Si articola in test di unità, di integrazione e *stress test*. Ogni elemento del test è definito "prova", quindi il test è composto di più prove.
- Ha connotati sia di verifica che di validazione.
- È eseguito in un ambiente di prova.
- È eseguito dal fornitore del servizio, generalmente da un gruppo dedicato (gruppo test e collaudo).
- Necessita di una specifica di test.

COLLAUDO

- È eseguito dopo il completamento dei test ed è orientato all'accettazione formale del servizio.
- Ha connotati di validazione.

- Può articolarsi in due fasi:
 - una prima fase (opzionale) in un ambiente che può essere il target finale, ma non è in esercizio;
 - una seconda fase (sempre necessaria) in condizioni di esercizio.
- È eseguito congiuntamente dal fornitore e dall'Amministrazione, che può delegare una terza parte, scelta per competenza, nel caso in cui il cliente non si possiedano le necessarie capacità tecniche per seguire il collaudo.
- Necessita di una specifica di collaudo, proposta dal gruppo di test e collaudo ed accettata dal cliente.

L'attività di test prevede la definizione delle prove per la verifica del corretto funzionamento del servizio realizzato e l'aderenza ai requisiti.

Per quanto concerne test e collaudo, vengono definiti:

- la pianificazione temporale delle sessioni di prova;
- la definizione di ambienti, strumenti e tecniche per l'esecuzione delle prove;
- le condizioni di accettabilità delle parti messe a disposizione dall'Amministrazione o derivanti dai processi di gestione rilasciati da un precedente gestore;
- le procedure di prova e gli eventuali programmi software da eseguire (dati di input alle prove);
- i risultati attesi;
- i mezzi di prova, gli ambienti ed i metodi;
- i criteri di accettazione;
- i contenuti dei verbali di collaudo.

I prodotti di questa attività sono la **Specifica di test** e la **Specifica di collaudo**. La Specifica di Test è utilizzata dal fornitore per l'esecuzione dei propri cicli di prove, mentre la Specifica di Collaudo è il riferimento per l'Amministrazione al fine di verificare ed accettare la fornitura.

Come indicato al paragrafo 5, la durata pluriennale di erogazione del servizio di Gestione della Sicurezza Fisica fa sì che a seguito dell'introduzione di variazioni (requisiti di sicurezza, perimetro, aspetti tecnologici o applicativi), una parte del servizio debba essere riprogettata (processi, attività, risorse impiegate, strumenti).

Di conseguenza, in questi casi, sono previste nuove attività di test e collaudo, relativamente alle parti modificate.

Mentre l'attività di test è sempre condotta dal fornitore del servizio di Gestione, il collaudo in questi casi può coinvolgere, oltre che l'Amministrazione, anche il fornitore degli applicativi oggetto di modifica.

Le attività di Progettazione Test e Collaudo vanno quindi intese come attività ripetitive, nei casi sopra segnalati.

4.4. REALIZZAZIONE DEL SERVIZIO

Questa attività è articolata nella acquisizione, realizzazione, integrazione e documentazione di:

- componenti infrastrutturali,
- software di gestione,
- procedure di prova (test).

Prodotto di questa attività è il documento **Progetto del servizio** che descrive l'organizzazione, le attività, le responsabilità, i processi necessari all'erogazione del servizio ed i relativi livelli di servizio. Il Piano è soggetto ad approvazione; essendo soggetto ad aggiornamento, sono quindi previste successive approvazioni.

La verifica sul documento è atta ad assicurare la non ambiguità dei requisiti trattati. La verifica è orientata ad accertare che

- per ogni requisito trattato nel documento sia inserito il puntamento alla documentazione contrattuale di riferimento (capitolato/richiesta d'offerta);
- per ogni requisito sia fornita una descrizione orientata alla realizzazione del servizio.

Sulla base del relativo Piano il servizio viene installato, output di questo passo è il **Sistema di erogazione del servizio** di gestione della sicurezza fisica installato.

4.5. REALIZZAZIONE DEL COLLAUDO

La realizzazione del test sull'infrastruttura viene condotta in accordo alla Specifica di Test. Il test prevede l'esecuzione di azioni volte a verificare il corretto funzionamento e la rispondenza del sistema sviluppato alle specifiche ed ai requisiti (prove).

Il prodotto di questa attività è il **Rapporto di test** contenente l'esito delle singole prove di test.

Al termine della realizzazione e dell'eventuale fase di pre-esercizio il servizio viene rilasciato, previo collaudo effettuato da una Commissione di Collaudo nominata dall'Amministrazione.

La Commissione opera con autonoma responsabilità ed ha il compito di verificare che quanto realizzato dal Fornitore sia conforme ai requisiti indicati nel contratto. Sono oggetto di collaudo anche l'infrastruttura degli strumenti di supporto alla gestione e la documentazione.

Il Fornitore supporta la Commissione nell'esecuzione delle prove, nel rilevamento dei risultati, nella stesura del rapporto finale.

Per svolgere le prove di collaudo la Commissione utilizza, a titolo di guida, la Specifica di Collaudo concordata con il Fornitore.

La documentazione di esecuzione delle prove e delle eventuali non-conformità rilevate viene formalizzata nel **Verbale di collaudo** (emesso dalla Commissione di Collaudo). Questo

documento costituisce riferimento per il riciclo delle attività di progettazione finalizzate alla rimozione delle non conformità rilevate.

4.6. MONITORAGGIO DI SICUREZZA

L'attività si realizza per mezzo della continua e consapevole osservazione, all'interno della finestra temporale di erogazione prevista, degli strumenti di rilevazione dei tentativi di accesso, al fine di individuare tempestivamente situazioni di allarme.

Il monitoraggio ha come oggetto:

- il perimetro esterno di sicurezza delle sedi;
- i perimetri interni di sicurezza (ad esempio gli uffici, i locali CED, i magazzini).

Il servizio di vigilanza preposto al monitoraggio si avvale di strumenti, quali ad esempio:

- le console del sistema di allarme perimetrale;
- le console del sistema di allarme interno;
- i monitor della video sorveglianza;
- gli allarmi acustici;
- le console del sistema di controllo accessi centralizzato.

Qualora, a seguito dell'attività di monitoraggio, si evidenziassero delle situazioni sospette, si innesca l'attività di gestione delle emergenze.

Ciascun evento è valutato e verificato. Se la verifica ha esito positivo, è generato un allarme che scatena l'attività di gestione delle emergenze (escalation).

Nell'ambito dell'attività di Monitoraggio e Controllo, saranno effettuati anche interventi di audit, che potranno dare un feedback utile per una revisione del tipo e delle modalità di servizio, nell'ambito della stessa fornitura, o in un ampliamento della fornitura stessa (si veda a questo proposito l'attività di Gestione dei cambiamenti).

Prodotti di questa attività sono

- il singolo evento di allarme;
- il **Rapporto monitoraggio sicurezza fisica**, ossia il documento, prodotto periodicamente, che elenca e descrive gli eventi anomali (comprendendo ogni singolo allarme) che si sono verificati nel corso del periodo di riferimento e le azioni che sono state intraprese, di conseguenza, per affrontare gli eventi anomali.

4.7. GESTIONE OPERATIVA DELLE EMERGENZE

L'attività di gestione delle emergenze ha l'obiettivo di dare risposte concrete e rapide ad eventi critici per la sicurezza fisica.

L'attività è attivata a seguito di una segnalazione o di un evento potenzialmente critico, per esempio:

- un allarme generato dal processo di monitoraggio;
- un allarme pervenuto al servizio di vigilanza.

In funzione della segnalazione pervenuta, il servizio di vigilanza attua le opportune contromisure, secondo le modalità definite nelle Politiche di Sicurezza.

In caso si renda necessaria un'attività di indagine, il servizio di vigilanza può avvalersi delle registrazioni effettuate nel corso del monitoraggio e opportunamente conservate.

Il risultato dell'attività è un dettagliato rapporto (**Rapporto di incidente**) sulle cause e sulle attività svolte per affrontare l'emergenza. Il rapporto sull'incidente riepiloga ed analizza gli eventi al fine di individuare le cause imputabili all'emergenza, documentando:

- il tipo di azione perpetrata,
- le cause all'origine dell'incidente,
- le conseguenze dell'accaduto,
- i tempi e le modalità di rilevazione dell'incidente,
- i tempi e le modalità di ripristino,
- altre anomalie riscontrate.

4.8. GESTIONE DEI CAMBIAMENTI

L'attività di gestione dei cambiamenti ha l'obiettivo di garantire o incrementare il livello di sicurezza previsto, a fronte di modifiche logistiche (per esempio, variazione del numero o della dislocazione del personale o delle risorse ICT, variazione della perimetrazione delle aree di sicurezza) o dell'individuazione di ambiti di miglioramento.

L'attività richiede, da un lato la verifica se sia necessaria una revisione o modifica del servizio di Gestione della sicurezza fisica, dall'altro l'accettazione dei nuovi elementi nell'ambito dei requisiti contrattuali di gestione.

L'attività produce pertanto uno studio di fattibilità del cambiamento, cioè la redazione di un **Documento di revisione**, con le relative specifiche di requisiti e di progettazione.

Qualora debbano essere introdotte modifiche al servizio di Gestione della sicurezza fisica, e queste modifiche esulano dai requisiti contrattuali, viene negoziata una variante contrattuale.

4.9. GESTIONE OPERATIVA

L'attività di gestione operativa ordinaria comprende

- Manutenzione e amministrazione degli strumenti utilizzati, compresa la gestione dei supporti contenenti le evidenze del monitoraggio. In particolare l'attività di manutenzione ha l'obiettivo di garantire il corretto funzionamento degli apparati di

sicurezza ambientale e perimetrale secondo le specifiche tecniche dei Fornitori e quanto previsto dalla Politica per la Sicurezza. L'attività di gestione dei supporti ha l'obiettivo di garantire l'integrità e la disponibilità dei dati acquisiti nell'ambito del monitoraggio, secondo quanto definito dalla Politica per la Sicurezza.

- Gestione degli accessi, con l'obiettivo di garantire l'accesso alle risorse protette, solo al personale autorizzato. Il sistema di gestione di accessi si basa su sistemi di identificazione e processi di autorizzazione definiti nella politica per la sicurezza dell'Amministrazione. L'attività di gestione degli accessi prevede la ricezione, validazione ed evasione delle richieste, producendo opportune credenziali di accesso.

I prodotti dell'attività di Gestione ordinaria sono i **Registri di conduzione operativa**, che consistono in uno o più documenti, descrittivi degli eventi relativi ai diversi tipi di operazione, in cui si articola l'attività di Gestione ordinaria. Per esempio, il documento relativo al sistema di controllo degli accessi riporterà la registrazione delle turnazioni del personale coinvolto nell'attività, degli ingressi dei visitatori, dell'attivazione dei sistemi di controllo automatici, degli interventi di manutenzione sugli apparati, ecc..

4.10. RENDICONTAZIONE

L'attività di reporting ha lo scopo di raccogliere e mantenere la registrazione di eventi significativi per la sicurezza al fine di verificare il superamento/non superamento dei parametri di controllo del servizio e, soprattutto, ad individuare aree di intervento nell'ottica di un miglioramento continuo.

Questa attività è finalizzata a dare informazione di sintesi indirizzate al management, e si differenzia pertanto dai rapporti che vengono prodotti nell'ambito delle attività ordinarie.

L'elaborazione di questi dati consente di produrre periodicamente un **Rapporto di sintesi** sulla Sicurezza Fisica il quali deve

- permettere l'analisi dell'andamento del servizio stesso;
- evidenziare eventuali carenze di sicurezza fisica;
- dare le indicazioni sulle azioni necessarie alla riduzione del rischio.

4.11. DESCRIZIONE DEI PRODOTTI

Per agevolare la comprensione della classe di fornitura ed orientare alla scelta dei prodotti da impiegare per la gestione della sicurezza logica, è opportuno fornirne una breve descrizione.

Video sorveglianza

Il prodotto prevede un sistema di telecamere a circuito chiuso: il controllo del perimetro può essere effettuato con impianti a raggi infrarossi. Le telecamere, con tecnologia "*motion detection*", sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.

Sistema di allarme perimetrale

Dovranno essere previste uscite di sicurezza con sistema di allarme. Il sistema dovrà essere integrato con l'impianto di rivelazione fumi e spegnimento incendi, con il sistema di telecamere, con il sistema di controllo accessi e con gli allarmi tecnologici.

Sistema di allarme interno

Il sistema consiste nell'adozione ed installazione di sensori di rilevamento allocati all'interno dell'edificio. Saranno attivati e disattivati da segnali provenienti dal sistema di controllo accessi.

Servizio di vigilanza

Il servizio consiste nelle seguenti attività:

- presidio armato con personale di vigilanza,
- ronde da parte del personale di vigilanza con unità cinofila, intensificate nelle ore notturne.

Servizio di reception

Il servizio di reception è finalizzato al controllo degli ingressi alle aree riservate. E' consentito l'ingresso solo a persone autorizzate nei locali aziendali, tramite un sistema di registrazione automatico o manuale disposto presso la portineria. L'accesso avviene tramite badge sia per il personale dipendente, sia per i lavoratori interinali (con data di scadenza) che per i visitatori (validità giornaliera). Il rilascio dei badge per il personale non dipendente avviene solamente a seguito di informativa al personale preposto alla reception.

Sistema di controllo accessi centralizzato

Il sistema consiste nella gestione e/o fornitura di un complesso di controlli e barriere fisiche, all'interno e nei punti di accesso dei locali da proteggere. Si può accedere ai locali protetti solo mediante meccanismi di autenticazione basati su credenziali di vari tipi (badge magnetici, smart card, sistemi biometrici, ecc.). Il sistema provvede al mantenimento della funzionalità ed alla gestione delle credenziali fornite agli utenti (per esempio la fornitura e la configurazione smart card).

Il controllo degli accessi fisici restringe i diritti di accesso del personale alle zone che ospitano risorse aziendali informatiche e non (magazzini, aree con dati e/o apparati ad alto rischio, uffici riservati, ecc.).

Gli accessi sono disciplinati da una procedura di carattere generale e da procedure specifiche per ogni singolo sito.

I controlli di accesso fisico alle aree servono a tutte le locazioni che contengono apparati di rete, LAN, impianti elettrici, impianti di condizionamento, telefoni e linee dati, supporti di backup, documenti e qualsiasi altro elemento richiesto per la gestione e manutenzione dei sistemi e non solo alla protezione dei locali contenenti sistemi hardware. Si deve consentire l'accesso alle aree critiche compartimentali, secondo diversi livelli ed esigenze di sicurezza, alle persone autorizzate.

Il personale deve essere informato sulle aree di competenza in termini d'accesso fisico e d'orario.

Deve essere verificata l'efficacia dei controlli di accesso fisico alle aree sia durante il normale orario di lavoro che in altri orari.

Le procedure prevedono regole di sicurezza in grado di disciplinare l'accesso, definendo per il singolo soggetto (per esempio dipendente, consulente, personale di imprese varie) una regola di accesso.

In particolare l'accesso ai Centri di produzione (ad esempio *Data Center*, *Call Center*) viene controllato tramite l'uso di *badge* magnetici/*smart card* personali rilasciati esclusivamente al personale conosciuto.

Il servizio fornisce livelli di controllo di diversa severità, in funzione della sensibilità degli ambienti da proteggere. In particolare, si prevede:

- *Sistema di Controllo Accessi esterno* (tornelli, vetri blindati, porte allarmate). È consentito l'ingresso solo a persone autorizzate nei locali aziendali, tramite un sistema di registrazione automatico o manuale disposto presso la portineria. L'accesso avviene tramite badge sia per il personale dipendente, sia per i lavoratori interinali (con data di scadenza), che per i visitatori (validità giornaliera). Il rilascio dei badge per il personale non dipendente avviene solamente a seguito di informativa al personale preposto alla reception. Tutti coloro che entrano nelle aree riservate devono esporre in maniera visibile il documento identificativo che viene fornito. Tale procedura consente di identificare rapidamente ed efficacemente eventuali trasgressori che tentano di accedere ad aree degli IDC a loro non autorizzate.
- *Sistema di Controllo Accessi interno su aree ad alto rischio*. L'accesso alle sale sistemi è controllato elettronicamente tramite badge e/o lettori biometrici ed è prevista una ulteriore procedura di registrazione degli accessi e identificazione del personale che accede.

Sistema di climatizzazione

Il prodotto consiste in un sistema di controllo del livello di temperatura ambientale e di umidità, concepito per poter smaltire l'energia elettrica trasformata in calore, al fine di garantire, sia in estate che in inverno, le condizioni ambientali volute. Per le specifiche e gli indicatori, si veda la classe di fornitura Sviluppo Sistemi (SSI).

Sistema rilevamento allarmi ambientali

Il prodotto comprende:

- *rivelazione fumo e sistemi antincendio*: consiste nel dotare gli ambienti della sede di rilevatori antifumo e antincendio, con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso. Dovrà essere adottato, come estinguente gassoso, un gas inerte, tollerabile dall'organismo dell'uomo, e pertanto, da un lato permettere l'evacuazione delle persone, dall'altro non danneggiare i sistemi ed è efficace nello spegnimento della fiamma. Gli impianti garantiscono la sola disattivazione della zona oggetto dell'intervento di manutenzione. L'impianto di spegnimento dovrà essere progettato nel pieno rispetto della normativa UNI 9795, che garantisce la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente o calamità naturali ed il continuo funzionamento del resto dell'impianto.
- *anti-allagamento*: al di sotto del pavimento flottante sono installati impianti di allarme anti-allagamento.

Impianti di alimentazione elettrica di emergenza

Il sistema è impiegato per garantire la continuità elettrica. Tutti i quadri che forniscono la corrente elettrica alle apparecchiature delle piattaforme di erogazione sono alimentati da gruppi di continuità. Sono presenti dei gruppi di continuità (UPS) aventi batterie con autonomia di almeno 15-20 minuti a pieno carico; questo intervallo di tempo consente l'attivazione del sistema di emergenza che a sua volta garantisce, senza rifornimento,

un'autonomia di almeno 48 ore e l'asservimento di tutto il complesso. Gli UPS assicurano la continuità a tutti i dispositivi informatici.

5. DESCRIZIONE DEI PROFILI PROFESSIONALI COINVOLTI

Nella tabella seguente (Matrice di Responsabilità Attività – Profilo Professionale) sono riportati per ciascuna attività i profili professionali EUCIP tipicamente coinvolti nello svolgimento dell'attività stessa e nel rilascio dei relativi prodotti, qualificati in termini di:

- responsabile (**R**), è il profilo professionale che esegue l'attività, coordina gli eventuali contributi di altri profili professionali ed è responsabile primario della qualità dei prodotti dell'attività;
- contributore (**C**), è il profilo professionale che contribuisce con competenze specialistiche allo svolgimento di elementi dell'attività e può gestire in autonomia, in accordo con il responsabile, specifiche sotto-attività; i contributori sono suddivisi in due categorie:
 - contributore tipico (**Ct**), il suo contributo all'attività è richiesto nella quasi totalità delle istanze di fornitura, una sua eventuale assenza dovrebbe essere considerata un'eccezione e le relative motivazioni dovrebbero essere esplicitate (peculiarità tecniche od organizzative dell'istanza di fornitura).
 - contributore specifico (**Cs**), il suo contributo all'attività è legato alle specificità dell'istanza di fornitura, la sua presenza, anche se frequente, non può essere considerata tipica.

Il profilo professionale responsabile di tutte le attività di questa classe di fornitura, eccetto quelle relative a test e collaudo, è il Consulente per la Sicurezza.

Per profilo professionale responsabile (o contributore) si deve intendere non una singola persona fisica, ma una famiglia professionale, caratterizzata da competenze comuni, ove coesistono livelli di esperienza, aree di specializzazione e ruoli organizzativi differenziati.

Ad esempio, è possibile, anzi probabile, che lo specialista coinvolto nelle attività di natura progettuale di SIF, dall'analisi dei requisiti sino all'avviamento del servizio, sia distinto da quello responsabile delle successive attività di gestione, pur appartenendo entrambi al medesimo profilo professionale di Consulente per la Sicurezza.

Il Consulente per la Vendita e l'Applicazione di Tecnologie Informatiche contribuisce esclusivamente nella fase di analisi requisiti, come elemento di raccordo tra le fasi di stesura dell'offerta e di avvio del progetto dopo l'aggiudicazione della fornitura.

Il profilo Tecnico di Collaudo e Integrazione di Sistemi, con il contributo del Consulente per la Sicurezza, è responsabile delle attività di progettazione ed esecuzione dei test e del collaudo del servizio (supporto all'Amministrazione per il collaudo).

Gli altri profili che contribuiscono alle attività sono:

- il Progettista di Sistemi informatici, per la definizione dei requisiti, la progettazione e la realizzazione dei sistemi tecnologici di controllo della sicurezza;
- il Sistemista Multipiattaforma, per le attività di progettazione, realizzazione del servizio e gestione operativa, per quanto attiene ai sistemi tecnologici di controllo della sicurezza fisica.

Nel caso vi fossero esigenze di rendicontazione che richiedano sviluppi o personalizzazioni complesse per la gestione dei dati del servizio oppure vi fossero esigenze di comunicazione particolari dei sistemi tecnologici di controllo della sicurezza fisica potrebbe essere necessario il coinvolgimento dei profili rispettivamente di Responsabile di Base di Dati e/o di Responsabile di Rete nelle attività di progettazione e realizzazione del servizio.

Nella tabella “Matrice di Responsabilità Attività – Profilo Professionale” è anche indicata per ciascun profilo professionale, responsabile (R) o contributore tipico (Ct), un’ipotesi di massima del suo impegno (quantità di lavoro, “effort”) nell’attività. Tale impegno è espresso come percentuale, fatto 100 l’impegno totale richiesto dall’attività, ed è quindi una stima del “peso” relativo del profilo professionale nell’esecuzione dell’attività.

Si tratta ovviamente di stime di larga massima ipotizzate a partire da un’astratta istanza di fornitura tipica e che non tengono conto della presenza di eventuali contributori specifici.

Per la stima si è ipotizzato che la fornitura comprenda tutte le categorie di prodotto di pertinenza SIF descritte al paragrafo 4.11, che il servizio di gestione operativa sia erogato con presidio di tipo H 12 e presidio remoto di vigilanza negli orari non coperti in loco.

TABELLA MATRICE DI RESPONSABILITA' ATTIVITA' – PROFILO PROFESSIONALE

Profilo professionale	Attività									
	Analisi dei requisiti	Progettazione	Progettazione collaudo	Realizzazione del servizio	Realizzazione del collaudo	Monitoraggio di sicurezza	Gestione operativa delle emergenze	Gestione dei cambiamenti	Gestione operativa	Rendicontazione
2 – Revisore di Sistemi Informativi						Ct 5%				
4 – Consulente per la Vendita e l'Applicazione di Tecnologie Informatiche	Ct 10%									
11- Tecnico di Collaudo e Integrazione di Sistemi			R 90%	Ct 10%	R 90%					
13- Progettista di Sistemi Informatici	Ct 10%	Ct 20%		Ct 10%				Ct 10%		
15 – Consulente per la Sicurezza	R 80%	R 70%	Ct 10%	R 65%	Ct 10%	R 10%	R 10%	R 90%	R 10%	R 100%
16 -Responsabile di Basi di Dati		Cs		Cs						
17 – Responsabile di Rete		Cs		Cs						
19 – Sistemista Multipiattaforma		Ct 10%		Ct 15%					Ct 10%	
- Personale esecutivo -						Ct 85%	Ct 90%		Ct 80%	
% di effort - totale	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

I profili professionali di riferimento sono quelli definiti dallo schema EUCIP (European Certification of Informatics Professionals) sviluppato dal CEPIS (Council of European Professional Informatics Societies) che, per ciascun profilo, indica le attività tipiche ed il dettaglio delle competenze possedute.

Le sintesi delle competenze dei profili professionali coinvolti nelle attività di questa classe di fornitura sono le seguenti (tra parentesi l' identificativo del profilo):

(2) Revisore di Sistemi Informativi (Information Systems Auditor). Un revisore di sistemi informativi secondo lo standard EUCIP fornisce (riferendo ai più alti responsabili aziendali o agli organi direttivi) un livello indipendente di garanzia su sicurezza, qualità, conformità e valore aggiunto dei sistemi informativi in una particolare organizzazione. Deve dimostrare forti competenze tecniche, indipendenza di giudizio, aderenza all'etica professionale.

(4) Consulente per la Vendita e l'Applicazione di Tecnologie Informatiche (Sales and Application Consultant). Un consulente per la vendita e l'applicazione di tecnologie informatiche secondo lo standard EUCIP deve abbinare alla competenza in una specifica tecnologia (legata al contesto, es. CAD) anche la conoscenza di concetti avanzati di marketing e delle esigenze tipiche dei clienti. E' indispensabile l'efficacia persuasiva nel presentare soluzioni, dimostrazioni pratiche e proposte commerciali.

(11) Tecnico di Collaudo e Integrazione di Sistemi (Systems Integration & Testing Engineer). Un tecnico di collaudo e integrazione di sistemi secondo lo standard EUCIP deve essere molto efficace in varie aree dello sviluppo di sistemi: preparazione della documentazione per l'utente finale, allestimento di sistemi IT, test delle loro funzioni, sia nel complesso che per singoli moduli componenti, identificazione delle anomalie e diagnosi delle possibili cause. E' richiesta anche una conoscenza specifica su come vengono costruite le interfacce tra moduli software.

(13) Progettista di Sistemi Informatici (IT Systems Architect). Un progettista di sistemi informatici secondo lo standard EUCIP assume un ruolo centrale nella progettazione, integrazione e miglioramento di sistemi IT – con particolare riguardo alle architetture software – curandone anche la sicurezza e le prestazioni; oltre ad una vasta competenza dell'ICT (in tutti i campi: software, hardware e reti) e di tecniche di progettazione specifiche, è richiesta la capacità di descrivere un sistema in termini di componenti e flussi logici.

(15) Consulente per la Sicurezza (Security Adviser). Un consulente per la sicurezza secondo lo standard EUCIP deve essere molto efficace nell'identificare i requisiti di sicurezza dei sistemi ICT e nel definire soluzioni affidabili e agevoli da gestire. Ad una competenza dell'ICT ampia e approfondita deve essere abbinata la capacità di interagire con altre funzioni ICT per favorire l'integrazione di tecnologie per la sicurezza all'interno dell'infrastruttura ICT.

(16) Responsabile di Basi di Dati (Database Manager). Un responsabile di basi di dati secondo lo standard EUCIP assume un ruolo centrale tanto nella progettazione di strutture di dati quanto nella gestione ordinaria dei DB; tra i requisiti figurano dunque una profonda competenza in tutti gli aspetti delle tecnologie dei DB, un approccio collaborativo ai contesti di progetto, esperienza nelle tecniche di modellazione dei dati, ma anche l'efficacia nel definire e applicare le procedure e nell'organizzare le operazioni ordinarie.

(17) Responsabile di Rete (Network Manager). Un responsabile di rete secondo lo standard EUCIP deve essere molto efficace nel gestire un sistema informativo di rete di media complessità e nel migliorarne le prestazioni. Deve inoltre saper interagire con i progettisti di reti e con eventuali fornitori esterni in merito a tutte le fasi del ciclo di vita di una rete.

(19) Sistemista Multipiattaforma (X-Systems Engineer). Un sistemista multipiattaforma secondo lo standard EUCIP deve avere una particolare competenza su vari sistemi operativi e sui rispettivi metodi per affrontare i problemi, sull'ottimizzazione delle prestazioni, sulla programmazione a livello di sistema e sull'integrazione tra piattaforme diverse; l'attitudine alla diagnosi e alla risoluzione dei problemi è richiesta per dare supporto su sistemi proprietari o aperti e su configurazioni ibride.

- **Personale esecutivo** (non è compreso nello schema di profili professionali EUCIP).

Operatore vigilanza e reception, gestisce le attività operative connesse al monitoraggio, alla gestione delle emergenze e degli accessi, ha competenze di base sull'utilizzo dei sistemi di controllo sicurezza fisica e ha ricevuto addestramento specifico sulle procedure e relative istruzioni operative di sicurezza (competenze addizionali specifiche nel caso di servizio armato).

6. INDICATORI/MISURE DI QUALITÀ

La tabella Attività/Prodotti/Indicatori associa ad ogni attività e/o prodotto della fornitura gli indicatori di pertinenza descritti nelle schede successive.

NOTA – Per i documenti vanno considerati anche tutti gli indicatori presenti nel Processo di Documentazione.

Tabella 1 - Attività/Prodotti/Indicatori

Attività	Prodotto	Indicatore di qualità				Processo trasversale		
		Caratteristica	Sottocaratt.	acro IQ	Denominazione IQ	cod PT	acro PT	Denominazione PT
Analisi dei requisiti	Specifica dei requisiti	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Progettazione	Progetto del sistema	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Realizzazione del servizio	Progetto del servizio	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Realizzazione del servizio	Sistema di erogazione del servizio	Efficienza	Efficienza temporale	RSC	Rispetto della scadenza contrattuale	6.2.1	PGE	Gestione
Monitoraggio di sicurezza	Rapporto monitoraggio sicurezza fisica	Efficienza	Efficienza temporale	RSC	Rispetto della scadenza contrattuale	6.2.1	PGE	Gestione

Attività	Prodotto	Indicatore di qualità				Processo trasversale		
		Caratteristica	Sottocaratt.	acro IQ	Denominazione IQ	cod PT	acro PT	Denominazione PT
Gestione operativa delle emergenze	Rapporto di incidente	Efficienza	Efficienza temporale	RSC	Rispetto della scadenza contrattuale	6.2.1	PGE	Gestione
Gestione operativa delle emergenze	Rapporto di incidente	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Gestione operativa delle emergenze		Efficienza	Efficienza temporale	TRE	Tempestività di risoluzione dell'emergenza		-	
Gestione dei cambiamenti	Documento di revisione	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Gestione dei cambiamenti		Funzionalità	Adeguatezza	CRAC	Correttezza dell'aggiornamento della configurazione	6.1.2	PGC	Gestione della configurazione
Gestione operativa		Affidabilità	Tolleranza ai guasti	DIS2	Disponibilità del servizio		-	
Gestione operativa	Registro di conduzione operativa	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Rendicontazione	Rapporto di sintesi	Efficienza	Efficienza temporale	RSC	Rispetto della scadenza contrattuale	6.2.1	PGE	Gestione
Rendicontazione	Rapporto di sintesi	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione

Classe di fornitura	GESTIONE DELLA SICUREZZA FISICA
Caratteristica /Sottocaratteristica	Efficienza/Efficienza temporale
Indicatore/Misura	Tempestività di risoluzione dell'emergenza – TRE
Sistema di gestione delle misure	Strumenti di supporto in grado di raccogliere ed elaborare i dati elementari per fornire la misura degli indicatori, quali i sistemi di gestione di trouble ticketing. Per tutti gli eventi considerati nel periodo di osservazione, si misura l'ampiezza del ritardo di risoluzione, ossia la differenza tra il tempo di presa in carico dell'emergenza (evento critico che necessita di una azione di tipo reattivo) ed il tempo di chiusura dell'intervento al netto dell'intervallo di tempo dell'eventuale autorizzazione a procedere che è data dall'interfaccia definita dall'Amministrazione tramite l'interfaccia delegata per i problemi di sicurezza.
Unità di misura	Percentuale
Dati elementari da rilevare	<ul style="list-style-type: none"> • data e orario di presa in carico dell'emergenza. • data e orario di richiesta eventuale autorizzazione • data e orario di arrivo dell'eventuale autorizzazione • data e orario di chiusura intervento (risoluzione dell'emergenza)
Periodo di riferimento	3 mesi
Frequenza esecuzione misure	4 volte l'anno
Regole di campionamento	Si considerano tutti gli eventi relativi al periodo di osservazione, all'interno della finestra temporale definita per l'erogazione del servizio.
Formula di calcolo	<p>Dati necessari:</p> <ul style="list-style-type: none"> • data e ora di presa in carico dell'emergenza (<i>Tie</i>) • data e ora di richiesta eventuale autorizzazione (<i>Tra</i>) • data e ora di arrivo dell'eventuale autorizzazione (<i>Taa</i>) • data e ora di chiusura intervento (risoluzione dell'emergenza) (<i>Tee</i>) <p>Il tempo di risoluzione dell'emergenza viene così calcolato:</p> $TRE = (Tee - Tie) - (Taa - Tra)$ <p>Si calcola quindi la frequenza dei tempi inferiori al valore normale</p> $FN_{TRE} = \frac{N_{tempi}(durata \leq \text{valore normale})}{N_{eventi}} \times 100$ <p>e la frequenza dei tempi inferiori al valore limite</p> $FL_{TRE} = \frac{N_{ritardi}(durata \leq \text{valore limite})}{N_{eventi}} \times 100$
Regole di arrotondamento	<ul style="list-style-type: none"> • La durata dei ritardi va arrotondata al minuto • La frequenza va arrotondata al punto percentuale sulla base del primo decimale - al punto % per difetto se la parte decimale è $\leq 0,5$ - al punto % per eccesso se la parte decimale è $> 0,5$

Obiettivi (valori soglia)	<p>Obiettivi</p> <ul style="list-style-type: none"> • TRE ≤ valore normale con $FN_{TRE} \geq$ frequenza normale • TRE ≤ valore limite con $FL_{TRE} =$ frequenza limite <p>Valori soglia</p> <ul style="list-style-type: none"> • valore normale = 8 ore • valore limite = 48 ore • frequenza normale = 80% • frequenza limite = 100%
Azioni contrattuali	<ul style="list-style-type: none"> • per ogni riduzione dell'1% rispetto all'obiettivo si applica una penale dello 0,5% dell'importo contrattuale del servizio relativo al periodo di riferimento • per ogni evento per il quale si supera il valore limite si applica una penale di importo pari allo 0,2% dell'importo del servizio relativo al periodo di riferimento
Eccezioni	L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di 3 mesi

Classe di fornitura	GESTIONE DELLA SICUREZZA FISICA
Caratteristica /Sottocaratteristica	Affidabilità/ Tolleranza ai guasti
Indicatore/Misura	Disponibilità del servizio – DIS2
Sistema di gestione delle misure	<p>La disponibilità viene misurata contando il numero dei fermi non programmati di sistema e la loro durata, nell'arco della finestra di erogazione del servizio.</p> <p>L'indicatore riguarda la disponibilità <u>del singolo servizio</u>.</p> <p>In sede contrattuale sono indicati i servizi cui applicare l'indicatore con i relativi obiettivi di disponibilità.</p> <p>La finestra di erogazione da considerare è quella contrattuale, per esempio: dal lunedì al venerdì, esclusi festivi: 9.00 - 13.00 e 14.00 - 18.00; oppure: H24: dal lunedì alla domenica.</p>
Unità di misura	Percentuale
Dati elementari da rilevare	<ul style="list-style-type: none"> • Data e ora di interruzione del servizio (al minuto) • Data e ora di riattivazione (al minuto)
Periodo di riferimento	3 mesi
Frequenza esecuzione misure	4 volte l'anno
Regole di campionamento	<p>Vanno considerate le interruzioni non programmate, rilevabili dal log di sistema e/o dai registri di conduzione operativa:</p> <ul style="list-style-type: none"> • interruzioni occorse e risolte nel <u>periodo di osservazione corrente</u> • interruzioni occorse nel <u>periodo di osservazione precedente</u> e risolte in quello <u>corrente</u>.
Formula di calcolo	<p>Dati necessari</p> <ul style="list-style-type: none"> • numero delle interruzioni • durata dell'interruzione • tempo totale = tempo contrattuale di erogazione del servizio nel periodo di riferimento (esclusi i fermi programmati) <p>La disponibilità si rappresenta come</p> $DIS2 = \frac{\text{Tempo}_{\text{totale}} - \sum \text{Durata}_{\text{fermo}}}{\text{Tempo}_{\text{totale}}} \times 100$
Regole di arrotondamento	<p>La percentuale va arrotondata alla frazione decimale di punto percentuale sulla base del secondo decimale</p> <ul style="list-style-type: none"> - per difetto se la parte decimale è $\leq 0,05$ - per eccesso se la parte decimale è $> 0,05$
Obiettivi (valori soglia)	<p>Obiettivi: DIS2 \geq valore contrattuale</p> <p>I valori contrattuali saranno definiti per ogni servizio e saranno compresi tra 99% e 99,9%.</p>
Azioni contrattuali	Per ogni 0,1 % di disponibilità inferiore all'obiettivo si applica una penale di importo compreso tra lo 0,5% e l'1% del corrispettivo relativo al periodo di riferimento per i sotto-sistemi critici e compresa tra lo 0,1% e lo 0,5% per gli altri.
Eccezioni	L'applicazione delle regole contrattuali inizia dopo un periodo di avviamento stabilito contrattualmente