CIG: 8575348907

Lotto
01

Città metropolitana di Milano

Procedura aperta per l'affidamento dei servizi di vigilanza armata presso i siti in uso a qualsiasi titolo alle Amministrazioni ed Enti non sanitari presenti sul territorio della Regione Lombardia mediante Convenzione ex art. 26 L.488/99 e art.1 Co 499 L.208/2015 suddivisa in Lotti

Territorio della Città Metropolitana di Milano e Province di Monza e della Brianza, Lecco, Como, Sondrio e Varese

Offerta Tecnica

Relazione Tecnica

CIVIS VIGILANZA

VCV VIGILANZA CITTA' DI VARESE

Capogruppo

Indice dei contenuti

A. Struttura Organizzativa, Logistica ed Operativa per la Gestione della Convenzione 1
A.1. Modello organizzativo con cui l'Offerente intende gestire la Convenzione 1
A.1.a Sistema dei ruoli e delle figure professionali 1
A.1.b Modalità di interazione e coordinamento tra le figure chiave dell'organizzazione dell'Offerente con quelle dell'Amministrazione (sia Soggetto Aggregatore, sia Amministrazione Contraente) 8
A.1.c Modalità di predisposizione della reportistica 10
A.2. Struttura logistica con cui l'Offerente intende gestire la Convenzione 13
A.2.a Modalità con cui l'Offerente intende strutturarsi da un punto di vista logistico 13
A.2.b Coerenza fra struttura logistica proposta con la struttura organizzativa. 14

B. Modalità e procedure per la rilevazione delle esigenze e la predisposizione dei PDI e metodologie tecnico – operative per lo svolgimento ed il controllo dei servizi gestionali 15
B.1. Modalità e procedure per gestire i sopralluoghi iniziali 15
B.1.a Organizzazione per gestire i sopralluoghi iniziali 15
B.1.b Modalità e procedure per l'esecuzione dei sopralluoghi 17
B.2. Piano degli Interventi (PDI) 25
B.2.a Organizzazione per la predisposizione del Piano degli Interventi (PDI) 25
B.2.b Procedure e modalità per la predisposizione, definizione del PDI e sua condivisione con l'Amministrazione Contraente 25
B.2.c Struttura del PDI e relativi contenuti 28
B.3. Caratteristiche e modalità operative di gestione del servizio di Call Center 31

C. Metodologie tecnico – operative per lo svolgimento ed il controllo dei servizi operativi 35
C.1. Metodologie tecnico operative per l'esecuzione dei servizi di vigilanza 35
C.1.a Servizi di piantonamento fisso 35
C.1.b Servizio ispettivo / di ronda 38
C.1.c Servizio di teleallarme 39
C.1.d Servizio di televigilanza 42
C.1.e Dotazioni aggiuntive, offerta di sistemi innovativi al personale ed alle vetture 45
C.2. Modalità di gestione della/e Centrale /i Operativa/e 49
C.2.a Piano di remotizzazione dei segnali 49
C.2.b Piano di Remotizzazione 49
C.2.c Soluzioni dedicate agli apparati gateway / router 49
C.2.d Soluzioni dedicate ai canali e alle modalità di trasmissione 50
C.2.e Soluzioni dedicate alla infrastruttura di Centrale Operativa 52
C.3. Turnazione e sostituzione del personale 53
C.3.a Logica territoriale dei nuclei operativi 53
C.3.b Strutturazione in gruppi di lavoro "estesi" 54
C.3.c Modalità di affiancamento in itinere 54
C.3.d Modalità operative di avvicendamento (turnover) per sostituzione 54
C.3.e Modalità operative di prevenzione del turnover 54
C.3.f Modalità operative di gestione delle sostituzioni pianificate e delle assenze non previste 55
C.4. Procedura di verifica dei livelli dei servizi ed azioni volte a migliorarli 56
C.4.a Modello procedurale dell'autocontrollo 56
C.4.b Sistema tracciabile di Customer Satisfaction sui servizi svolti 61
C.4.c Strumenti e contenuti dei controlli del Sistema di Customer Satisfaction 62
C.5. Percorsi formativi e/o di aggiornamento che l'Offerente intende implementare per la corretta erogazione dei servizi 62
C.5.a Piano Formativo e ampliamento delle competenze del personale impiegato 62
C.5.b Ore di formazione minime garantite 67
C.5.c Ciclo di miglioramento continuo per la formazione 68
C.5.d Metodologie didattiche e strumenti utilizzati nell'erogazione dei corsi 68
C.5.e Modalità di verifica della formazione erogata 68
C.5.f Tracciabilità della formazione 68

C.5.g Cronoprogramma della formazione *69*

D. Sicurezza, Ambiente e gestione delle emergenze **69**
D.1. Procedure inerenti la gestione della sicurezza 69
D.1.a Dichiarazione di possesso della certificazione OHSAS 18001 o aggiornamenti successivi *69*
D.1.b Dichiarazione di possesso della certificazione ISO 14001:2015 ..... *69*
D.2. Gestione delle emergenze e di reperibilità 69
D.2.a Sistema di gestione del servizio di reperibilità *69*
D.2.b Sistema di gestione delle emergenze *70*
D.3. Automezzi a ridotto impatto ambientale 73
D.4. Divise delle GPG 74

Indice dell'infografica

Con la presente infografica sono evidenziati specifici elementi distintivi, migliorativi, integrativi dell'Offerta Tecnica.

A. Struttura Organizzativa, Logistica ed Operativa per la Gestione della Convenzione

A.1. Modello organizzativo con cui l'Offerente intende gestire la Convenzione

A.1.a Sistema dei ruoli e delle figure professionali

A.1.a.1 Presentazione dell'Offerente

L'Offerente è costituito dal Raggruppamento Temporaneo di Imprese attualmente aggiudicatario del **Lotto 02** (territorio delle Province di Brescia, Bergamo, Pavia, Lodi, Mantova e Cremona). L'Offerente ha fatto tesoro delle proprie esperienze nella presente Convenzione e della forte presenza dell'Offerente sul territorio del **Lotto 01,** progettando un **servizio ulteriormente migliorato**, in cui inserire alcuni **elementi innovativi** di forte impatto sulla sicurezza, sulla qualità e sulla capacità di governo da parte del Soggetto Aggregatore e delle singole Amministrazioni Contraenti. In particolare, l'esperienza ha permesso di definire una struttura organizzativa contestualizzata sulla realtà e sulle caratteristiche peculiari del Lotto. L'RTI è così composto:

CIVIS S.p.A. (Capogruppo del RTI), fondata nel 1971, è attualmente **presente sul territorio italiano in 35 province coperte: 22 direttamente e 13 tramite società partecipate.** Civis, con **oltre 40.000 Clienti**, è anche assegnataria della **certificazione "Company to Watch"** attribuita da Cerved. A testimonianza dei massimi standard qualitativi raggiunti, il CIVIS agisce con le certificazioni di qualità UNI 10891:2000, UNI EN ISO 14001:2015, UNI EN ISO 45001:2018; UNI EN ISO 9001:2015, ISO/IEC 27001, SA 8000. Inoltre dal 2004 Civis ha anche adottato un Codice Etico secondo un modello di organizzazione e gestione ex D.Lgs. 231/2001. CIVIS S.p.A. è caratterizzata da:

La storia recente di Civis S.p.A. testimonia la vitalità dell'Istituto sul mercato nazionale dei servizi di vigilanza integrata.

Figura 1 Tappe evolutive della crescita di CIVIS negli ultimi anni

Gli amministratori sono Security Manager certificati ai sensi della Norma 10459:2005. Tutti i servizi di vigilanza erogati sull'intero territorio nazionale sono monitorati e coordinati attraverso **le Centrali Operative di CIVIS, attive 24 ore su 24, 365 giorni all'anno, certificate UNI ISO 50518:2014. Civis ha inoltre sviluppato una specifica piattaforma informatica, Civis Security Cloud (CSC), per agevolare il controllo e il governo dei servizi da parte dei Supervisori delle Amministrazioni.** La piattaforma è attualmente utilizzata su numerosi appalti a livello nazionale. Le avanzate funzionalità della piattaforma saranno messe a disposizione del Supervisore al Contratto e del Supervisore di Operativo e permetteranno di monitorare e controllare tutti gli aspetti del servizio, dalla corretta esecuzione delle attività alla conformità della formazione.

VCV (Vigilanza Città di Varese), Istituto di vigilanza fondato nel 1948 e parte del Gruppo Civis, è oggi un marchio riconosciuto in tutto il territorio della Provincia di Varese come **sinonimo di sicurezza, con oltre 2.000 Clienti**. Nel corso del tempo ha ampliato la gamma dei servizi prestati che ora vanno ben oltre le classiche ronde notturne ed includono un elevato livello di **tecnologia e innovazione**. La storia più recente dimostra una ferrea volontà aziendale di crescere sul mercato e dare una risposta a tutte le esigenze di sicurezza.

Evoluzione e crescita di VCV negli ultimi anni

Figura 2 Tappe evolutive della crescita di VCV negli ultimi anni

VCV eroga una pluralità di servizi a Privati ed Aziende: dal teleallarme alla videosorveglianza, dal piantonamento al pronto intervento con la pattuglia armata, dalla scorta valori alla gestione degli stessi. Qualche dato di sicuro interesse:

Oltre **130** Guardie Particolari Giurate impiegate

Oltre **33** Autovetture con localizzazione satellitare

Oltre **13** furgoni con localizzazione satellitare

1 Centrale Operativa 24/24h

511.000 Ronde annue

7.000 Interventi annui su allarme

VCV dedica quotidianamente ingenti energie ed investimenti al costante **controllo del processo di erogazione dei servizi** ed alla verifica della soddisfazione del cliente. Per VCV, inoltre, una completa **formazione**, sotto il profilo legale, tecnico ed operativo, delle proprie risorse costituisce un elemento indispensabile per garantire ai propri clienti personale adeguato alla esecuzione dei servizi affidati.

A.1.a.2 Sistema dei ruoli delle figure professionali costituenti la Struttura Organizzativa

Il modello organizzativo che ospita il sistema dei ruoli è illustrato nel seguente organigramma [→ cfr. Figura 3], strutturato su due livelli:

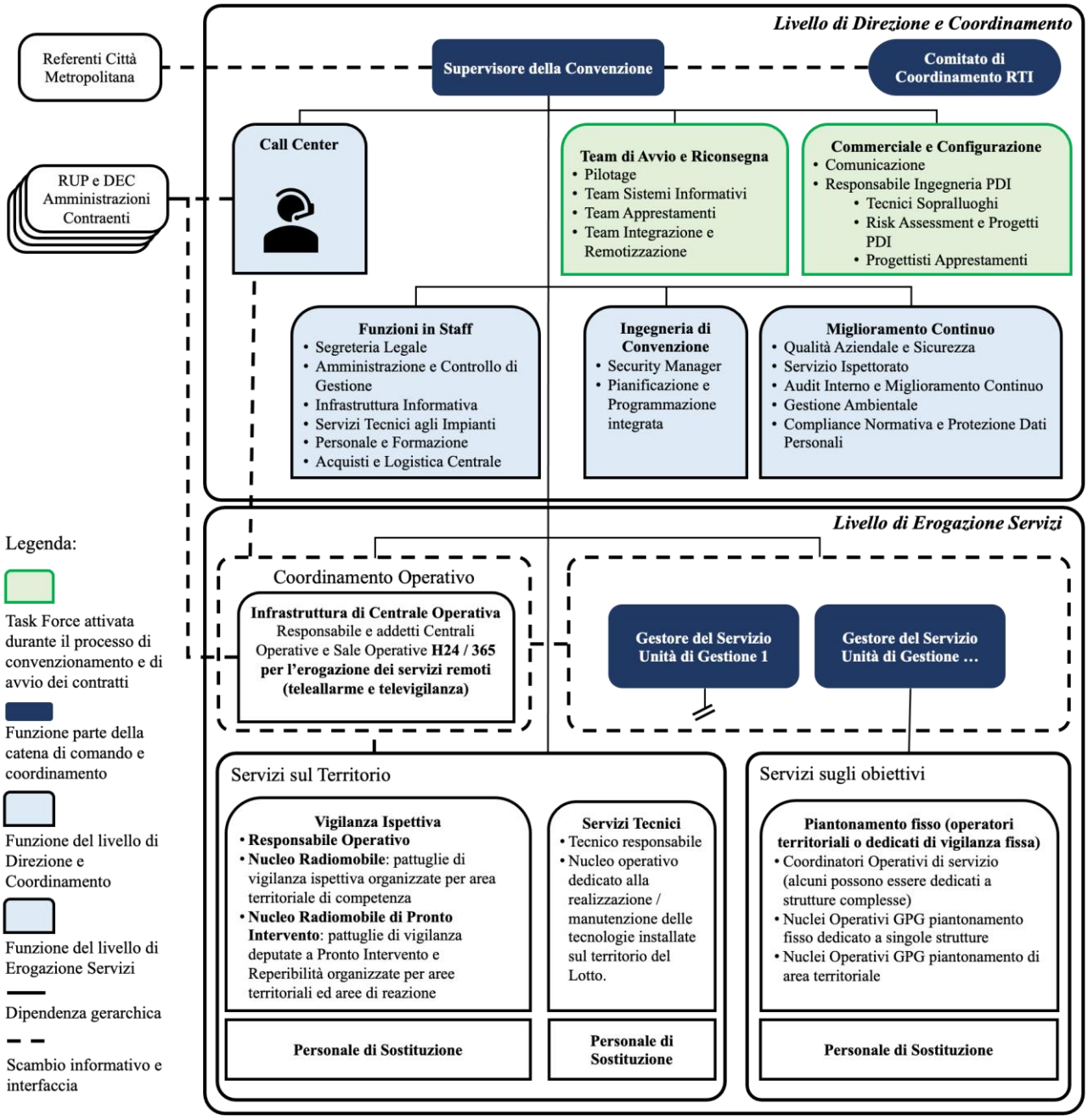


Figura 3 Organigramma organizzativo con evidenza del sistema dei ruoli

- **Livello di Direzione e Coordinamento**, che ospita tutte le competenze per la gestione, il controllo, il coordinamento della Convenzione e dei singoli Contratti attuativi. Questa struttura è trasversale a tutti i contratti attuativi e permette di gestire i processi di supporto, sia di Convenzione sia relativa al singolo ODF, in maniera omogenea. In tal modo

le stesse competenze organizzative procedurali, tecniche sono messe a disposizione in maniera omogenea indipendentemente dalle dimensioni e dai fabbisogni delle Amministrazioni (le Amministrazioni più piccole attingono alle stesse competenze delle Amministrazioni più articolate e di dimensioni maggiori). Ciò garantisce l'omogeneità di tutti i processi trasversali, funzionali alla gestione ed al supporto dei servizi erogati;

- **Livello Erogazione Servizi**, che contiene tutte le figure di coordinamento e di esecuzione dei servizi previsti dalla Convenzione e attivabili da ciascuna Amministrazione Contraente. Questo livello è invece personalizzato affinché l'erogazione dei servizi possa aderire nei tempi e nelle modalità ai *desiderata* delle ciascuna Amministrazione Contraente., e soprattutto in modo tale che il personale sia impiegato sia il più possibile stabile, così da avere la massima familiarità con le peculiarità e le caratteristiche di ciascun obiettivo.

L'organigramma mostra tutte le figure che prendono parte al Servizio, le gerarchie tra esse stabilite e le interazioni che si generano, ovvero i rapporti istituzionali, informativi e di supporto dall'esterno. I due livelli sono concepiti per lavorare in modo strettamente coordinato e sinergico, tramite procedure e avanzate soluzioni di condivisione delle informazioni in tempo reale. Notevole a tal proposito la Funzione ***Infrastruttura Informativa***, responsabile della personalizzazione e dell'integrazione dell'intera infrastruttura tecnologica (Sistema informativo, Portale Web di condivisione con le Amministrazioni, Sistema di Centrale Operativa, dispositivi di campo, impianti, etc.) **Civis Security 4.0**, la quale permetterà la **completa gestione digitale del servizio**. Tale infrastruttura è quindi adattata, all'avvio del singolo OPF, alle specifiche esigenze della singola Amministrazione Contraente.

Figura cardine della struttura organizzativa è il **Supervisore della Convenzione**, che opererà quale supervisore del servizio e referente nei confronti di Città Metropolitana, nonché quale coordinatore:

- Dell'infrastruttura di Centrale Operativa, responsabile dei servizi remoti (televigilanza e teleallarme);
- Delle strutture organizzative dedicate ai servizi sul territorio (vigilanza ispettiva e servizi tecnici all'infrastruttura tecnologica);
- Dei singoli **Gestori del Servizio**, i quali a loro volta sono responsabili nei confronti dei Referenti delle singole Amministrazioni Contraenti e coordinano i servizi erogati direttamente presso gli obiettivi e ad essi dedicati (piantonamento fisso).

Il Supervisore della Convenzione sarà la cerniera di congiunzione tra la Struttura di Governo e la Struttura Operativa nella fase di erogazione dei servizi attraverso il coordinamento delle attività del Gestore del Servizio. Sarà, inoltre, in stretto rapporto con un **Comitato Tecnico di Coordinamento**, costituito dai referenti del RTI, che lo supporterà a livello decisionale in tutte le scelte strategiche necessarie a un corretto svolgimento della Convenzione. Di seguito sono indicate le caratteristiche delle figure del **Livello di Direzione e Controllo**, evidenziando le figure proposte dall'Offerente (Plus) ad elevato valore per la gestione della Convenzione. Sono illustrate qualifica ed esperienza minimi garantiti (Curricula Vitae) che l'Offerente garantirà.

Sono illustrate con il simbolo del "Pollice in su" le figure organizzative che costituiscono un Plus rispetto a quanto richiesto dal Capitolato Tecnico. Esse sono in grado di erogate servizi aggiuntivi o di conferire all'organizzazione competenze integrative e migliorative.

Livello di Direzione e Controllo - Ruolo, qualifica ed esperienza	Plus
Livello di Direzione e Controllo. Contiene le Figure Organizzative dedicate a fornire alla struttura operativa l'appoggio tecnico (know-how) per il corretto avviamento e gestione a regime delle attività, nonché per la creazione di un ciclo di ritorno informativo per il miglioramento continuo dei servizi erogati.	
Supervisore della Convenzione: Tullio Mastrangelo. Il Dott. Mastrangelo ha Esperienza pluridecennale nella gestione di Convenzioni ed appalti di sicurezza integrata. In particolare il Dott. Mastrangelo svolge attualmente il ruolo di Supervisione per la Convenzione in vigore con Città Metropolitana di Milano e ha una solida esperienza come Comandante del Corpo della Polizia Municipale di Milano. Titolo di studio: Laurea. Anni di esperienza: oltre 40 ann i di esperienza	
Team di Avvio e Riconsegna. Permette la corretta implementazione di ciascun contratto attuativo, soprattutto in termini di integrazione fra infrastrutture dell'Offerente e infrastrutture del singolo obiettivo dell'Amministrazione Contraente. Cura anche il Riconsegna, curando la stesura della relazione finale per l'Amministrazione Contraente e tutti i processi di supporto per garantire la continuità gestionale ed operative durante il passaggio di consegne con il nuovo Gestore dei servizi.	
Pilotage. Funzione pensata per le Amministrazioni più complesse, è costituita da figure di supporto e affiancamento nelle fasi iniziali delle attività (periodo massimo di 6 mesi). La fase di start up costituisce infatti la *fase critica* per la corretta impostazione e coordinamento dei servizi fra Amministrazione e Offerente. Funge da facilitatore e fluidificante della fase di avviamento, curando l'interfaccia fra le figure chiave della struttura organizzativa e dell'Amministrazione, la trasmissione dei desiderata dell'Amministrazione e "guida in porto" la fase di avviamento del contratto attuativo. In fase di chiusura, coordina l'intera attività di supporto per il cambio appalto. **Titolo di Studio**: laurea tecnica. **Esperienza:** almeno 5 anni nel settore della vigilanza privata.	
Team Sistemi Informativi. Distaccato dalla Funzione IT del Gruppo CIVIS, il team è formato da ingegneri sistemisti responsabili della personalizzazione della infrastruttura IT necessaria per la gestione basata sui dati della Convenzione e dei singoli contratti attuativi. **Titolo di Studio**: laurea tecnica. **Esperienza:** almeno 5 anni nel settore IT di grandi Istituti di Vigilanza privata.	

Livello di Direzione e Controllo - Ruolo, qualifica ed esperienza	Plus
Team Apprestamenti. Effettua il censimento di dettaglio e la valutazione degli apprestamenti anticrimine, ove previsti i servizi di televigilanza e teleallarme. Valuta, anche in funzione dei Risk Assessment, il migliore assetto delle contromisure tecnologiche per garantire la sicurezza degli obiettivi. **Titolo di Studio**: laurea tecnica. **Esperienza:** almeno 5 anni nel settore delle tecnologie della vigilanza privata.	👍
Team Integrazione e Remotizzazione. La Funzione è composta da personale con specifiche competenze per l'integrazione e centralizzazione degli apprestamenti anticrimine dei singoli obiettivi. In fase di avviamento implementano il progetto di remotizzazione degli apprestamenti, curando la correttezza e completezza **Titolo di Studio**: laurea tecnica. **Esperienza:** almeno 5 anni nel settore delle tecnologie della vigilanza privata.	👍
Commerciale e Configurazione. La funzione è presieduta dal Supervisore della Convenzione e contiene competenze per il *corretto sviluppo commerciale*, la *corretta configurazione dei servizi* in relazione alle *esigenze espresse* da ciascuna Amministrazione Contraente. La Funzione rimane attiva per l'intero periodo di convenzionamento, con diversa entità a seconda dell'andamento della Convenzione	
Comunicazione e Convenzionamento. La funzione è composta da personale della funzione Comunicazione del Gruppo CIVIS, che definisce, implementa e monitora il piano di saturazione della Convenzione. La Funzione è stata pensata per supportare il Soggetto Aggregatore nella comunicazione e nell'indirizzamento dei Referenti delle Amministrazioni Contraenti, e quindi di raggiungere più agevolmente il *plafond* di convenzione. **Titolo di Studio**: laurea in scienze della comunicazione o equipollente. **Esperienza:** almeno 5 anni nel settore della comunicazione	👍
Tecnici Sopralluoghi. Si tratta di personale interno della Funzione IT / tecnologia del Gruppo CIVIS, che possono coordinare professionisti esterni e Società specifiche in funzione dei carichi di lavoro. Essi effettuano l'attività di sopralluogo iniziale, curando in particolare il censimento e la valutazione degli apprestamenti. **Titolo di Studio**: diploma tecnico. **Esperienza:** almeno 8 anni.	👍
Risk Management e Progetti PDI. La Funzione è composta da *Security Manager* interni dell'Offerente, che coordinano *professionisti esterni esperti di analisi del rischio criminoso*, con consolidata esperienza nella effettuazione dei Risk Assessment, funzionali alla redazione ed all'aggiornamento del PDI. Sulla base delle evidenze dell'analisi di rischio, gli esperti predispongono il PDI in maniera tale da aumentare il livello di sicurezza degli obiettivi. **Titolo di Studio**: laurea tecnica e competenze specifiche certificate nell'ambito dell'analisi del rischio di sicurezza. **Esperienza:** almeno 8 anni.	👍
Progettisti Apprestamenti. La Funzione predispone dal punto di vista tecnico il progetto di integrazione e centralizzazione degli apprestamenti anticrimine all'interno della infrastruttura di Centrale Operativa, ove previsto. Il progetto di integrazione e centralizzazione è integrato all'interno del PDI. **Titolo di Studio**: diploma tecnico. **Esperienza:** almeno 5 anni.	👍
Call Center. Il **Call Center** (cfr. paragrafo dedicato) è già attivo poiché impiegato nell'attuale Convenzione. Esso è incaricato della gestione delle comunicazioni che sopraggiungono da parte dell'Amministrazione. Infatti, il Call Center è costantemente in contatto con il Responsabile della Fornitura e con il Gestore del Servizio al fine di trasmettere tempestivamente ogni segnalazione e/o reclamo effettuato dalle Amministrazioni. Il Call Center è composto da addetti operativi in grado di gestire i flussi di chiamata e le richieste d'intervento, attraverso sia l'utilizzo del mezzo telefonico, con un **Numero Verde Dedicato** messo a disposizione della Convenzione che gli altri canali/strumenti quali indirizzi e-mail, fax etc. **Il Call Center è integrato nella infrastruttura di Centrale Operativa al fine di attivare più celermente eventuali risorse in reperibilità e Pronto Intervento.** Numero Verde dedicato: 800 - 909658	
Responsabile Call Center ed Operatore di Call Center / Back Office. Titolo di Studio: diploma tecnico. **Esperienza:** almeno 5 anni nella gestione di flussi di comunicazione.	
Funzioni in Staff. Sono ubicate presso le Sedi Centrali dell'Offerente. Presiedono i processi gestionali e di supporto e forniscono servizi alla struttura organizzativa in ambito legale, gestionale, contabile, gestione del personale, acquisti e logistica, IT e tecnologie.	
Segreteria Legale. Si occupa del supporto legale per tutte le questioni legate alla contrattualistica, alle relazioni sindacali, alle conseguenze civili e penali dell'attività svolta dall'Offerente. **Titolo di Studio**: laurea in giurisprudenza ed iscrizione all'Ordine degli Avvocati. **Esperienza:** almeno 10 anni.	
Amministrazione e Controllo di Gestione. Verifica gli OPF ricevuti dalle Amministrazioni Contraenti. Una volta ricevuto l'OPF, si occupa, poi, della predisposizione della documentazione amministrativa. Cura, inoltre, i rapporti con le Amministrazioni Contraenti, si occupa della fatturazione degli ordinativi di fornitura e gestisce i rapporti amministrativi tra i vari componenti.	
Infrastruttura informativa. E' responsabile della corretta funzionalità dell'infrastruttura informativa per la corretta gestione della Convenzione e dei singoli contratti. La struttura è coordinata da un Responsabile IT che avrà anche il compito di garantire la massima efficienza, la trasparenza del servizio reso e la rapidità dello scambio di informazioni e delle comunicazioni, di standardizzare i modi di operare del personale, assicurare il funzionamento delle infrastrutture a servizio della Centrale Operativa e delle GPG. **Titolo di Studio**: laurea tecnica. **Esperienza:** almeno 5 anni nel settore IT di grandi Istituti di Vigilanza privata.	

Livello di Direzione e Controllo - Ruolo, qualifica ed esperienza	Plus
Servizi Tecnici agli Impianti. E' composta da risorse centralizzate specializzate nella Progettazione, implementazione, gestione e manutenzione degli apprestamenti e dei dispositivi tecnologici installati ed utilizzati dall'Offerente (es. dispositivi di centralizzazione e remotizzazione, sistema di tracciatura NFC / QR Code etc.). La Funzione cura L'esatto inserimento in anagrafica di tutte le dotazioni e apparecchiature impiegate al fine di documentare con precisione le attività e può offrire il medesimo livello di competenze e servizio a tutti gli obiettivi del Lotto, senza distinzione di complessità. **Titolo di Studio**: diploma tecnico. **Esperienza:** almeno 5 anni.	👍
Personale e Formazione. E' composta da personale esperto nella selezione, formazione, valutazione continua e aggiornamento del personale impiegato. Definisce il piano di assorbimento eventuale, ovvero il percorso formativo e di aggiornamento del personale per la corretta erogazione dei servizi. **Titolo di Studio**: diploma di laurea ed esperienza di formazione in ambito di appalti ed in materia di sicurezza sul lavoro ai sensi del D.Lgs. 81/08. **Esperienza:** almeno 8 anni.	👍
Ingegneria di Convenzione. Ubicata presso le Sedi Centrali dell'Offerente, la Funzione è composta da personale con le competenze ed il know-how per il corretto coordinamento e controllo dei servizi.	
Security Manager. E' la figura di riferimento per quanto riguarda la gestione della sicurezza e l'analisi del rischio all'interno del Gruppo Civis. Dotato della qualifica di Professionista della Security ai sensi del D.M. 269/2010, D.M. 115/2014, norma UNI 10459:2015, è preposto alle periodiche analisi di rischio criminoso ed alla progettazione degli apprestamenti anticrimine e dei servizi, nonché della progettazione del servizio in maniera da mitigare lo stato di rischio degli obiettivi. Durante la fase di convenzionamento fa parte della Funzione Risk Management e Progetti PDI. **Esperienza:** almeno 8 anni.	👍
Pianificazione e Programmazione Integrata. Supporta il Supervisore della Convenzione e i Gestori del Servizio nella programmazione dei servizi, in amni era tale da garantire la massima copertura di sicurezza, il puntuale svolgimento dei servizi, la necessaria copertura in caso di attivazione multipla di risorse sul territorio in regime di reperibilità / pronto intervento. Permette di pianificare i servizi in maniera tale che siano robusti a livello dell'intero Lotto, e non solo a livello del singolo obiettivo. **Titolo di Studio**: diploma tecnico. **Esperienza:** Esperienza nella gestione di personale e turnistica per Istituti di Vigilanza privati di almeno 10 anni.	👍
Miglioramento Continuo. Ubicata presso le sedi centrali dell'Offerente, la Funzione presiede le procedure e le soluzioni per far osservare regole e norme per mantenere un ambiente di lavoro idoneo e privo di pericoli.	
Qualità Aziendale e Sicurezza. Implementa e gestisce il processo di ottenimento e rinnovo delle certificazioni del Sistema di Gestione dell'Offerente. Presiede la configurazione del sistema di monitoraggio e controllo sul livello di servizio erogato, nonché sull'obsolescenza della strumentazione utilizzata e dei DPI nell'ambito dei servizi. Include anche la figura del Responsabile del Servizio di Prevenzione e Protezione (RSPP) per le attività oggetto di commessa. La Funzione ha fra l'altro la responsabilità dell'aggiornamento eventuale delle disposizioni di servizio, che debbono essere rispettate a livello di coordinamento e a livello operativo della GPG.	
Servizio Ispettorato. Funzione composta da Guardie Particolari Giurate, con la responsabilità di effettuare controlli specifici sul rispetto del Regolamento di Servizio obbligatorio e delle disposizioni di servizio	
Audit Interno e Miglioramento Continuo. I componenti di questa Funzione effettuano le verifiche di processo e di risultato relative all'intero Sistema di Gestione, quindi anche alle misure di tutela ambientale, sicurezza sul lavoro, etica, tutela dei dati personali, nonché sulle attività di recepimento della Customer Satisfaction, in maniera tale da garantire la costanza ed il miglioramento continuo del livello di servizio erogato. Effettuano la reportistica su tutti i Servizi ed evidenziano eventuali anomalie nell'erogazione degli stessi	👍
Gestione Ambientale. Implementa la sezione di Gestione Ambientale all'interno del Sistema di Gestione, ivi comprese tutte le verifiche con il supporto dell'Auditing Interno e Miglioramento Continuo.	👍
Compliance normativa e protezione dati personali. Data l'importanza della conformità alla normativa per la protezione dei dati personali durante le attività di vigilanza, questa figura si occupa della progettazione, dell'implementazione e dell'aggiornamento di tutte le procedure e soluzioni, metodologiche e tecnologiche, per la protezione dei dati personali in ossequio alle attuali legislazioni e indicazioni sulla tutela dei dati personali durante le attività oggetto di commessa. Presiede le verifiche relative, con il supporto delle figure di Auditing Interno e Miglioramento Continuo.	👍

Il livello **Erogazione Servizi** contiene le figure di comando operativo e tutto il personale operativo, organizzato in maniera da rispondere alle molteplici esigenze delle Amministrazioni in tema di servizi attivati e presenza territoriale. L'organizzazione del livello segue la logica delle **Unità di Gestione**: **ciascuna Unità di Gestione corrisponde a un contratto attuativo, ed è sotto la responsabilità di un Gestore del Servizio**. Ciascun Gestore del Servizio può gestire una o più Unità di Gestione, a seconda dell'estensione dei servizi e della distribuzione territoriale degli obiettivi. Ciascun Unità di Gestione è servita da una struttura di **nuclei operativi**, suddivisi per servizi:

Nucleo operativo Servizi Remoti, che è occupato dall'Infrastruttura di Centrale Operativa. Si occupa del recepimento dei segnali di allarme e dei flussi video, della gestione delle comunicazioni e richieste da parte del personale operativo, della attivazione di risorse per affrontare indisponibilità di personale ovvero emergenze conclamate, indotte da eventi di Security. La struttura di Centrale Operativa *integra le varie gestioni operative all'interno di un'unica struttura integrata*:

ottimizza le prestazioni e aumenta l'efficacia della risposta, ad esempio per il servizio di vigilanza ispettiva e di reperibilità / Pronto Intervento**. Attraverso la Struttura di Centrale Operativa sono infatti coordinati i diversi moduli organizzativi, riferiti ai servizi a sviluppo territoriale e ai servizi identificati ai singoli obiettivi.**

Nucleo operativo Servizi sul Territorio del Lotto. Contiene le competenze per la corretta erogazione di servizi a gestione territoriale, quali servizi di vigilanza ispettiva o servizi tecnici, che permettono la saturazione del personale solo fra più obiettivi / contratti attuativi. La zona territoriale di estensione dei servizi è modulabile, e può coinvolgere dal singolo Comune ad intere province, a seconda della concentrazione di obiettivi sul territorio. I servizi di vigilanza ispettiva sono coordinati da un **Responsabile Operativo**, che si interfaccia con tutti i Gestori del Servizio e, in maniera integrata, mette a disposizione le risorse per i servizi di vigilanza ispettiva ed interventi di pronto intervento / reperibilità. I servizi tecnici sono coordinati da un **Tecnico responsabile**, che coordina le attività sul territorio del Lotto dei tecnici.

Nucleo operativo Servizi sugli obiettivi. Prevede operatori dedicati con presenza continuativa presso gli obiettivi, quali GPG di piantonamento fisso. Il Nucleo, per adattarsi alle esigenze delle varie Amministrazioni, è organizzato secondo una doppia logica. Sono quindi presenti gruppi di lavoro dedicati a obiettivi specifici, in particolare nel caso di obiettivi sensibili o complessi, e gruppi di lavoro dedicati ad aree territoriali, entro le quali possono essere erogati i servizi ai vari immobili, compatibilmente con fasce orarie e vincoli operativi, presenti sul territorio. I gruppi di lavoro sono coordinati da Coordinatori Operativi di servizio.

Questa articolazione progettuale del livello di erogazione servizi ritaglia quindi in maniera naturale l'organizzazione operativa sulla base delle esigenze di ciascuna Amministrazione Contraente e di ciascun obiettivo, ed in più è pensato per ottimizzare le risorse condivise fra le varie Unità di Gestione,

Tutti gli agglomerati organizzativi sono dotati di risorse di sostituzione, in una percentuale più elevata rispetto a quanto richiesto dal D.M. 269/10 Allegato A.

La percentuale riservata dall'Offerente è infatti del **30%, superiore al 20% previsto dal D.M. 269/10.**

Per limitare l'avvicendamento di personale non addestrato e che abbia familiarità presso gli obiettivi ciascun servizio, è inoltre prevista una di **"rotazione programmata"** delle risorse adibite allo svolgimento del servizio con le risorse di sostituzione, che permette di costruire un "*gruppo di lavoro allargato"* con GPG di sostituzione che garantiscono la continuità qualitativa del personale. Nella seguente tabella sono indicate le competenze, le qualifiche e le esperienze del personale all'interno del livello di Erogazione Servizi.

Livello di Erogazione Servizi - Ruolo, qualifica ed esperienza	Plus
Livello di Erogazione dei Servizi. Contiene le Figure Organizzative dedicate al coordinamento e all'erogazione diretta dei servizi sul territorio del Lotto.	
Gestori del Servizio. Costituiscono l'interfaccia unica per tutti i servizi nei confronti delle Amministrazioni Contraenti) con il supporto di tutte le Funzioni della struttura organizzativa. Sono responsabili della gestione e del controllo operativo di tutti i servizi attivati e di tutte le altre responsabilità declinate all'interno del Capitolato Tecnico. Sono previsti due profili di Gestore del Servizio, un profilo Plus e un profilo Ordinario, aventi specializzazioni differenti. Il profilo Plus è stato progettato per la gestione di ODF all'interno dei quali siano contemplate strutture complesse / ad elevata sensibilità. **Qualifica**: GPG con grado minimo di Tenente. Titolo di Studio: laurea o diploma (profilo Plus), diploma (profilo ordinario). Esperienza: almeno 20 anni (profilo Plus), almeno 10 anni (profilo ordinario). I profili "tipo" dei Gestori del Servizio e le loro caratteristiche sono riportati nella documentazione in allegato **[→ Allegati].** Essi sono inoltre elencati nella tabella all'interno del paragrafo A.1.a.3 della presente Relazione Tecnica.	👍
GPG Responsabile di Centrale Operativa. **Qualifica:** Livello: 2 CCNL Istituti e Imprese di Vigilanza Privata e servizi fiduciari.	
GPG di Centrale Operativa. Qualifica: Livello: 3 - 4 CCNL Istituti e Imprese di Vigilanza Privata e servizi fiduciari.	
GPG Responsabile Operativo Vigilanza Ispettiva. Gestisce i servizi di vigilanza territoriali, organizzando la turnistica e i carichi di lavoro in maniera tale da soddisfare le esigenze specifiche di ciascuna Unità di Gestione. Conferisce al personale un'organizzazione territoriale, in maniera tale da ottimizzare gli spostamenti fra obiettivi. Si interfaccia con tutti i Gestori del Servizio e con la Funzione Pianificazione e Programmazione. Permette di adattare la struttura organizzativa all'effettivo fabbisogno dei servizi richiesti dalle singole Amministrazioni e dai singoli obiettivi. **Qualifica**: GPG Livello: 2 CCNL Istituti e Imprese di Vigilanza Privata e servizi fiduciari.	👍
GPG di Vigilanza Ispettiva / Pronto Intervento. Qualifica: GPG con grado di caporale o vigile, Livello 3(s) - 6 CCNL Istituti e Imprese di Vigilanza Privata e servizi fiduciari.	
Tecnico Responsabile servizi tecnici. Gestisce i servizi tecnici sul territorio del Lotto, curando la perfetta copertura in relazione ai fabbisogni dei singoli obiettivi. **Titolo di studio**: diploma tecnico / laurea. **Esperienza**: almeno 10 anni.	👍
Addetti servizi tecnici. Titolo di studio: diploma tecnico / laurea. **Esperienza**: almeno 5 anni.	👍
GPG Coordinatori operativi del servizio di piantonamento fisso. Coordinano, presso gli obiettivi assegnati, gli operatori GPG di piantonamento fisso e supportano i Gestori del Servizio nel coordinamento di punto presso	👍

Livello di Erogazione Servizi - Ruolo, qualifica ed esperienza	Plus
gli obiettivi. Qualifica: GPG con grado minimo di Sergente o Maggiore, Livello 3 – 4(s) CCNL Istituti e Imprese di Vigilanza Privata e servizi fiduciari.	
GPG di piantonamento fisso. È in contatto continuativo con la Centrale Operativa e con il Coordinatore operativo assegnato, oltre che con il Gestore del Servizio. **Qualifica:** GPG con grado di Caporale o di Vigile. Livello 4 - 6 CCNL Istituti e Imprese di Vigilanza Privata e servizi fiduciari.	

A.1.a.3 Curriculum Vitae dei Gestori del Servizio

Si vuole in questa sede "disegnare" il profilo garantito del Gestore del Servizio che sarà impiegato dall'Offerente per la gestione dei servizi di vigilanza armata per il presente Lotto. I profili costituiscono una **sintesi** di curricula reali del personale, allegati all'Offerta Tecnica e indicativi delle caratteristiche minime che l'Offerente intende offrire per il personale che ricoprirà tali ruoli di coordinamento all'interno della Convenzione. I profili di Gestore del Servizio saranno i seguenti:

- **Profilo Plus**, dedicato alla gestione di contratti attuativi che contemplano la presenza di sedi complesse (sedi di Enti di grandi dimensioni / ad elevata sensibilità e/o complessità di servizio);
- **Profilo Ordinario**, dedicato alla gestione dei contratti attuativi che contemplano la presenza di obiettivi ordinari.

Gestore del Servizio	P	O
Formazione		
Formazione. Il Gestore del Servizio dispone di un titolo di studio superiore (laurea o diploma). Ha conseguito preferibilmente anche la certificazione di Security Manager – Professionista della Security di II o III livello UNI 10549. Ha per questo seguito un Master Universitario oppure ha superato un corso universitario con attestazione finale dell'ateneo responsabile oppure da un ente di formazione, entrambi aventi per argomento la gestione della security per materie afferenti alla competenza del profilo.	●	
Formazione. Il Gestore del Servizio dispone di un titolo di studio di scuola superiore (diploma, preferibilmente laurea).		●
Formazione. Ha partecipato a numerosi corsi di formazione in materia di sicurezza (antiterrorismo, psicologia comportamentale, etc.)	●	●
Anzianità lavorativa nel Ruolo		
Anzianità lavorativa nel ruolo. Il Gestore del servizio avrà almeno 20 anni di esperienza professionale continuativa di security nel privato, anche come consulente, o in organismi pubblici di sicurezza, di cui almeno 10 anni di incarichi di livello manageriale (gestione di commesse).	●	
Anzianità lavorativa nel ruolo. Il Gestore del servizio deve avere minimo 10 anni di esperienza professionale continuativa di security, nel privato, anche come consulente, o in organismi pubblici di sicurezza, di cui almeno 5 anni di incarichi di livello non meramente esecutivo.		●

A.1.a.4 Dimensionamento dell'organizzazione dell'Offerente

Nella seguente tabella è proposto il dimensionamento, da intendersi come preliminare e stimato, dell'organizzazione dell'Offerente. Il dimensionamento è proposto in termini di persone impiegate, ed è differenziato nelle fasi di vita della Convenzione (CON: Convenzionamento (da promozione fino ad accettazione ODF); AVV: Avviamento degli ODF; REG: gestione a regime dei diversi ODF. La suddivisione è puramente logica, in quanto la fase di convenzionamento dura per 3 anni, ma permette di rilevare come la struttura organizzativa si modulerà ai diversi carichi di lavoro, per quantità e qualità, nelle diverse fasi della Convenzione.

Funzioni dell'organigramma e sviluppo del dimensionamento	CON	AVV	REG
Livello di Direzione e Controllo			
Supervisore della Convenzione	1	1	1
Team di Avvio e Riconsegna	-	10	-
Pilotage	-	1	-
Team Sistemi Informativi	-	3	-
Team Apprestamenti	-	2	-
Team Integrazione e Remotizzazione	-	4	-
Commerciale e Configurazione	19	-	-
Comunicazione e Convenzionamento	2	-	-
Tecnici Sopralluoghi	12	-	-
Risk Management e Progetti PDI	3	-	-
Progettisti Apprestamenti	2	-	-
Call Center	3	3	-
Responsabile Call Center ed Operatore di Call Center / Back Office	3	3	3
Funzioni in Staff	8	8	8
Segreteria Legale	1	1	1
Amministrazione e Controllo di Gestione	1	1	1

Funzioni dell'organigramma e sviluppo del dimensionamento	CON	AVV	REG
Infrastruttura informativa	2	2	2
Servizi Tecnici agli Impianti	1	1	1
Personale e Formazione	3	3	3
Ingegneria di Convenzione	3	4	3
Security Manager	3	3	2
Pianificazione e Programmazione Integrata.	-	1	1
Miglioramento Continuo	-	9	9
Qualità Aziendale e Sicurezza	-	1	1
Servizio Ispettorato	-	2	2
Audit Interno e Miglioramento Continuo	-	4	4
Gestione Ambientale	-	1	1
Compliance normativa e protezione dati personali	-	1	1
Livello di Direzione e Controllo	**34**	**35**	**23**
Gestori del Servizio	-	3	3
Responsabile di Centrale Operativa	2	2	2
GPG di Centrale Operativa	12	12	12
Responsabile Operativo Vigilanza Ispettiva	1	1	1
GPG di vigilanza ispettiva / ronda e Pronto Intervento	-	27	27
Tecnico Responsabile Servizi Tecnici	-	1	1
Addetti Servizi Tecnici	-	4	4
GPG Coordinatori operativi del servizio di piantonamento fisso	-	7	7
GPG di Piantonamento fisso	-	62	62
Livello di Erogazione Servizi	**15**	**119**	**119**
Totale Struttura Organizzativa	**49**	**154**	**141**

A.1.b Modalità di interazione e coordinamento tra le figure chiave dell'organizzazione dell'Offerente con quelle dell'Amministrazione (sia Soggetto Aggregatore, sia Amministrazione Contraente)

A.1.b.1 Modalità di coordinamento specifiche con Città Metropolitana di Milano

Città Metropolitana avrà un'interfaccia dedicata nel **Supervisore della Convenzione** il quale, essendo profondo conoscitore sia del mondo della vigilanza che della Convenzione, sarà in grado di essere sempre informato sull'andamento dei singoli contratti. Il coordinamento proposto è differenziato nelle fasi di convenzionamento e di fase di erogazione dei servizi:

Fase di convenzionamento

Argomento	Risorse coinvolte	Modalità di coordinamento proposta
Condivisione linee strategiche di saturazione del Lotto	Comitato RTI, Supervisore della Convenzione, Comunicazione e Convenzionamento	Incontro fra figure apicali dell'organizzazione dell'Offerente e Referenti del Soggetto Aggregatore per la condivisione delle linee guida di azione commerciale per la saturazione del Lotto.

Fase di erogazione dei servizi

Durante la fase di erogazione, a disposizione del Soggetto Aggregatore sarà messo a disposizione un utente della piattaforma **Civis Security Cloud**, con i quali sarà possibile accedere a tutta la reportistica e a tutti i dati afferenti i singoli servizi.

Questo strumento aggiuntivo permette al Soggetto Aggregatore di acquisire tutti i dati indipendentemente dalla reportistica e dalle modalità di condivisione proposte dall'Offerente, a testimonianza dell'impegno alla massima trasparenza nella rendicontazione dei servizi effettuati.

In sintesi, le modalità di coordinamento durante la fase di erogazione dei servizi (avviamento degli ODF) sono:

Argomento	Risorse coinvolte	Funzioni coinvolte del Soggetto Aggregatore e modalità di coordinamento proposta
Condivisione dei risultati ottenuti	Supervisore della Convenzione, Miglioramento Continuo	**Referente Soggetto Aggregatore.** Condivisione annuale della reportistica sintetica relativa ai risultati ottenuti. Questo elemento aggiuntivo permette al Soggetto Aggregatore di avere contezza dell'andamento della Convenzione non solo nel momento della sua conclusione, con la Relazione Finale, bensì alla fine di ciascun anno di gestione.
Condivisione dei risultati ottenuti	Supervisore della Convenzione, Miglioramento Continuo	**Referente Soggetto Aggregatore.** Condivisione della reportistica finale (Relazione finale) secondo le modalità indicate dal Capitolato Tecnico

Argomento	Risorse coinvolte	Funzioni coinvolte del Soggetto Aggregatore e modalità di coordinamento proposta
Verifiche Ispettive	Supervisore della Convenzione, Gestori del Servizio, Audit e Miglioramento Continuo	**Referente Soggetto Aggregatore e Organismi (anche terzi) di ispezione.** Piano delle visite ispettive e condivisione della reportistica sintetica relativa ai risultati ottenuti.
Customer Satisfaction	Supervisore della Convenzione, Gestori del Servizio, Audit e Miglioramento Continuo	**Referente Soggetto Aggregatore e Organismi (anche terzi) di ispezione.** Condivisione della reportistica sintetica relativa ai risultati ottenuti.

A.1.b.2 Modalità di coordinamento specifiche con il Referente dell'Amministrazione Contraente

A.1.b.2.1 Interfaccia durante la fase di convenzionamento, avviamento

Le singole Amministrazioni contraenti hanno molteplici interfacce, ognuna in grado di soddisfare le specifiche esigenze, già prima dell'avvio del servizio. Infatti il processo si attiva dal momento in cui le Amministrazioni contraenti emettono un Ordinativo Preliminare di Fornitura (OPF) e la Funzione Commerciale e Configurazione, che ne verifica la piena validità, procede a comunicare all'Amministrazione Contraente la data del sopralluogo. Il Team Sopralluoghi e la Funzione **Risk Management e Progetti PDI**, costituite da diverse professionalità, valuteranno gli specifici rischi e minacce connessi al sito e verificheranno lo stato e le caratteristiche degli edifici in termini di accessi, dei relativi impianti di sicurezza e dispositivi di teleallarme in uso, al fine di redigere il Piano degli Interventi (PDI) che verrà discusso e verificato nei contenuti dall'Amministrazione per definire le basi sulle quali verrà elaborato l'Ordinativo di Fornitura. L'Offerente ritiene essenziale, già durante la fase di convenzionamento, un efficace scambio informativo ed il coordinamento con il Referente dell'Amministrazione Contraente. Di seguito sono elencate le necessità di coordinamento, le Funzioni dell'Offerente coinvolte, le modalità previste.

Necessità di coordinamento	Funzioni coinvolte	Strumento
Fase di convenzionamento		
Comunicazione e promozione della Convenzione, in cui è illustrata l'esistenza della Convenzione, i vantaggi, le modalità di adesione. Questa modalità di coordinamento permette di accrescere il livello di conoscenza della Convenzione e di generare eventualmente un OPF.	• Supervisore Convenzione • Comunicazione Convenzionamento • Call Center	• Contatto telefonico • Riunioni on line / in presenza
Coordinamento per l'organizzazione dei sopralluoghi. Il Call Center dà supporto alla Funzione Commerciale e Configurazione per la gestione dei flussi di richieste e per la calendarizzazione delle attività di sopralluogo.	• Supervisore Convenzione • Funzione Commerciale e Configurazione • Call Center	• Pec / mail • Contatto telefonico
Condivisione e revisione dei PDI. In questa fase è necessario condividere i contenuti del PDI, ed in particolare i contenuti del *Risk Assessment*, che possono comportare una variazione nei contenuti del servizio.	• Supervisore Convenzione • Funzione Commerciale e Configurazione	Sito Soggetto Aggregatore Riunioni (eventuali) pec / mail
Riunione di coordinamento iniziale. Permette di definire il percorso di avviamento dell'appalto, a valle dell'accettazione / firma dell'ODF.	• Supervisore Convenzione • Gestore del Servizio	Riunione on line / in presenza e scambio documenti
Fase di avviamento		
Riunione di coordinamento. Prevede la condivisione del piano di avviamento del OPF(piano organizzativo, piano apprestamenti, piano anagrafica tecnica etc.)	• Supervisore Convenzione • Gestore del Servizio • Team di Avvio e Riconsegna	Riunione on line / in presenza e scambio documenti
Riunioni di aggiornamento sull'andamento del progetto di avviamento e di valutazione della continuità operativa	• Gestore del Servizio • Team di Avvio e Riconsegna	Riunione on line / in presenza e scambio documenti
Condivisione di per comunicazioni, segnalazioni, reclami	• Gestore del Servizio • Call Center	Sistema di Call Center
Condivisione periodica dei dati afferenti il servizio e reportistica (definizione della reportistica di regime).	• Gestore del Servizio	Piattaforma Civis Security Cloud
Condivisione delle non conformità e delle azioni migliorative (riunione del Comitato di Gestione ODF)	• Gestore del Servizio • Miglioramento Continuo	Comitato di gestione ODF

Particolare importanza assume il **Comitato di Gestione ODF**, riunione presidiata dal Gestore del Servizio durante la quale è discusso l'andamento del servizio, sulla base delle eventuali non conformità rilevate e delle azioni migliorative messe in atto. Il Comitato ha *periodicità mensile*, e coinvolge il Referente dell'Amministrazione e le seguenti figure

dell'Offerente, in maniera costante: **(a)** Gestore del Servizio; **(b)** Audit e Miglioramento Continuo, che presenta la reportistica sui livelli di servizio e sulle non conformità; **(c)** Security Manager, in caso di variazioni relative allo stato di rischio degli obiettivi. **(d)** Ulteriori risorse della struttura organizzativa, in dipendenza dagli argomenti e dalla tematica affrontata. Da parte della Stazione Appaltante, invece, è prevista la presenza fissa del Referente (DEC) e la presenza su invito di personale Terzo (es. auditor esterni) o di specifiche Funzioni (Amministrazione, Acquisti, Funzione Security, Responsabile Servizio Prevenzione e Protezione etc.) in dipendenza dalla tematica da affrontate. Il Comitato di Gestione di ODF permette la rapida condivisione delle problematiche e un coordinamento chiaro fra Amministrazione e Offerente. Si possono così condividere le azioni correttive per ciascuna non conformità, e si traccia un vero e proprio piano di miglioramento continuo. Particolare importanza, nel corso degli incontri, è data al monitoraggio delle azioni migliorative / correttive identificate e condivise durante le riunioni precedenti, al fine di verificarne l'efficacia.

A.1.b.2.2 Interfaccia durante la fase di gestione a regime - **OSCURATO**

A.1.b.2.3 Interfaccia durante la fase di riconsegna degli impianti (chiusura di ODF)

Durante la fase di riconsegna, è importante il corretto coordinamento per dare all'Amministrazione Contraente gli strumenti per un passaggio di consegne senza soluzioni di continuità, sia dal punto di vista operativo sia dal punto di vista gestionale.

In questo caso, l'Offerente entro tre mesi dalla fine del contratto attiverà nuovamente il Team di Avvio, ed in particolare la figura del Pilotage, che coordinerà l'intera fase di riconsegna e di interfaccia con l'Amministrazione e con il nuovo Fornitore.

Le modalità e gli strumenti di coordinamento utilizzati sono descritti di seguito, e si intendono aggiuntivi rispetto alle modalità illustrate per la fase di gestione a regime, che continuano ad essere valide.

Necessità di coordinamento	Funzioni coinvolte	Strumento
Fase di riconsegna		
Condivisione del **piano di riconsegna**, sia mediante riunione di condivisione sia mediante piattaforma informativa messa a disposizione dall'Offerente. Il piano contiene la calendarizzazione e le modalità di consegna dell'anagrafica tecnica degli apprestamenti, la condivisione degli eventuali codici, le modalità di riconsegna delle chiavi per i servizi di vigilanza, le modalità di consegna della reportistica finale. *Il coordinamento coinvolge anche i Gestori del Servizio del nuovo Fornitore.*	• Gestore del Servizio • Team di Avvio	• Riunione di condivisione, con frequenza mensile • Sistema Informativo
Riunioni e sopralluoghi di familiarizzazione delle figure di coordinamento operativo, per comprendere e condividere con l'Amministrazione le eventuali peculiarità e criticità dei servizi di cui si richiede l'attivazione.	• Gestore del Servizio	• Riunioni di condivisione
Riunioni di monitoraggio del piano di riconsegna, attraverso la condivisione	• Gestore del Servizio • Pilotage	•
Condivisione della reportistica annuale / finale prevista dal Capitolato Tecnico. In particolare questa modalità mette a fuoco le problematiche, le anomalie, le criticità non risolte e le relative motivazioni, nonché le soluzioni per un continuo miglioramento e le proposte di ottimizzazione dell'ODF.	• Gestore del Servizio • Team di Avvio	

Condividendo la reportistica finale sul singolo ODF, che è un estratto della ultima relazione annuale, l'Offerente può focalizzare il percorso di miglioramento che la nuova Gestione potrà continuare, nell'ottica del miglior servizio per l'Amministrazione Contraente.

A.1.c Modalità di predisposizione della reportistica

La reportistica messa a disposizione dall'Offerente è articolata su diversi piani temporali, che permettono il governo del singolo ODF e dell'intera Convenzione con *cadenza addirittura quotidiana*, se del caso. L'Offerente, grazie alle caratteristiche della propria piattaforma proprietaria CSC, ha messo a punto un sistema di reportistica tempestivo, completo, personalizzabile e facilmente utilizzabile ai fini della rendicontazione, poiché è adattabile alle effettive esigenze di ciascuna figura utilizzatrice e presenta a quest'ultima le informazioni realmente utili al proprio ruolo.

Nella seguente tabella sono messe in relazione le tipologie di reportistica, lo strumento utilizzato, il soggetto che ne fruisce (**[AC]:** Amministrazione Contraente; **[SA]**: Soggetto Aggregatore). In verde sono campite le celle relative alle tipologie di reportistica aggiuntive e integrative, no previste dal Capitolato Tecnico, e che rappresentano un **elemento migliorativo**.

Descrizione della reportistica	Modalità	AC	SA
Reportistica in tempo reale con il potente strumento di reportistica di CSC, Report On Line	Continuo e in tempo reale	Cruscotto real time AC	Cruscotto real time SA

Reportistica mensile, costruita mediante elaborazioni e query di Report On Line e messa a disposizione.	Report mensile	Report mensile AC	Report mensile SA
Reportistica a richiesta, costruita dietro richiesta della Stazione Appaltante	Report costruito su richiesta	-	Report a richiesta
Reportistica annuale	Relazione annuale sui servizi	Relazione annuale AC	-
Report Finale	Report finale	Report finale di ODF	Relazione finale

A.1.c.1 Reportistica in tempo reale con Report On Line OSCURATO

A.1.c.2 Reportistica periodica mensile

L'Offerente intende estendere le richieste di Capitolato Tecnico riguardo la reportistica periodica, e per questo motivo associa alla reportistica mensile per la Stazione Appaltante, già prevista, la reportistica mensile per l'Amministrazione Contraente.

La reportistica mensile è il principale strumento di condivisione e monitoraggio dell'ODF e dell'intera Convenzione. La reportistica destinata all'Amministrazione Contraente è elaborata dal Gestore del Servizio con il supporto dell'Audit e Miglioramento Continuo, sempre con apposite elaborazioni di Report On Line che sono raccolte in un modello di report periodico. La reportistica destinata invece al Soggetto Aggregatore è a cura del Supervisore della Convenzione.

Modalità di messa a disposizione

La reportistica mensile è elaborata a creare un vero e proprio documento di consultazione. Esso è disponibile, in formato elettronico e con tutti gli allegati di dettaglio per le varie sezioni, utili per elaborazioni indipendenti da parte dei soggetti interessati.

La completezza dei dati messi a disposizione è garantita dalla procedura di allineamento dei contenuti e delle viste di sintesi, che sono condivise durante la fase di avvio con il Referente dell'Amministrazione e, a inizio Convenzione, con i Referenti del Soggetto Aggregatore.

Nell'ambito delle riunioni di avviamento, infatti, sono definiti e condivisi i contenuti e il livello di aggregazione / dettaglio di ciascuna singola elaborazione dei report.

Per garantire la trasmissione tempestiva della reportistica, la modalità di pubblicazione e messa a disposizione è completamente automatizzata.

Gli utenti, mediante semplice accesso a CSC, possono scaricare e consultare la reportistica aggiornata nel formato desiderato (di default formato .pdf). In ogni caso, la modalità di coordinamento prevede, ove necessario, l'organizzazione di incontri, sia in persona sia online, che permettono di descrivere e sviscerare ulteriormente i contenuti e le implicazioni della reportistica messa a disposizione.

L'Utente dell'Amministrazione Contraente / del Soggetto Aggregatore ha inoltre a disposizione il cruscotto di reportistica real time, descritto prima, per sviluppare elaborazioni proprie a partire dai dati di reportistica.
Ciò completa le viste e le prospettive dei dati e degli indicatori condivisi.

Contenuti principali della reportistica mensile

Nella seguente tabella sono illustrate le principali sezioni della reportistica messa a disposizione nella reportistica mensile, sia per le Amministrazioni Contraenti sia per il Soggetto Aggregatore.

Reportistica mensile AC	Reportistica mensile SA
• Rendiconto a consuntivo delle attività svolte (numero di ore di piantonamento, minuti di ispezione, etc.) a livello di aggregazione del ODF; • Report su eventuali eventi di security e impatto sulla variazione dello stato di rischio degli obiettivi; • Risultanze del sistema di autocontrollo (valore e trend degli indicatori sul livello di servizio, non conformità, azioni migliorative da intraprendere); • Rendiconto economico progressivo e di periodo dell'ODF, con cruscotto dell'importo eroso, dell'importo contrattuale, degli eventuali atti aggiuntivi approvati etc.; • Tutte le altre eventuali informazioni di reportistica periodica mensile citate nella presente relazione.	• Report progressivo delle Amministrazioni Contraenti che hanno emesso ODF, con data di ricezione ODF e attivazione della convenzione; • Importo delle forniture e dell'eventuale richiesta di riduzione di 1/5 dell'importo della fornitura; • Report con importi fatturati nel periodo e importi fatturati aggregati dall'inizio della Convenzione; • Andamento delle penali e relativo impatto sui singoli ODF; • Andamento generale delle prestazioni eseguite (ore di piantonamento, attività di vigilanza ispettiva etc.); • Report sulle penali ricevute / recepite; • Statistica dei reclami ricevuti dall'Offerente su sito del Soggetto Aggregatore, e relativa reportistica sulle azioni correttive; • Statistica mensile sullo stato di conformità ai livelli di servizio (Statistica degli ODF per impatto delle non conformità e Customer Satisfaction rilevata con sistema di autocontrollo), aggregato a livello dell'intero Lotto.

A.1.c.3 Reportistica a richiesta

La reportistica a richiesta è prevista, come da indicazioni della documentazione di gara, solamente per il Soggetto Aggregatore. Le Amministrazioni Contraenti si interfacciano infatti molto più spesso con l'organizzazione dell'Offerente, che riesce a incorporare nel tempo tutte le richieste di personalizzazione e di approfondimento richieste dai Referenti, senza necessità di richieste specifiche. La reportistica inoltre, prodotta con le medesime modalità viste precedentemente, permette di generare nuovi modelli di report. Se il Soggetto Aggregatore richiede una specifica analisi o un approfondimento (es. andamento dei KPI per uno specifico gruppo di Amministrazioni, trend specifico di saturazione per zona geografica etc.) allora il nuovo report prodotto è messo a disposizione come nuovo "modello" di report e registrato, ove richiesto, all'interno della piattaforma CSC, nel caso il Soggetto Aggregatore ne ravvisasse la necessità.

Il nuovo modello può quindi essere incorporato all'interno della reportistica mensile, arricchendola e rendendo tempestiva e completa la risposta dell'Offerente a fronte delle esigenze del Soggetto Aggregatore.

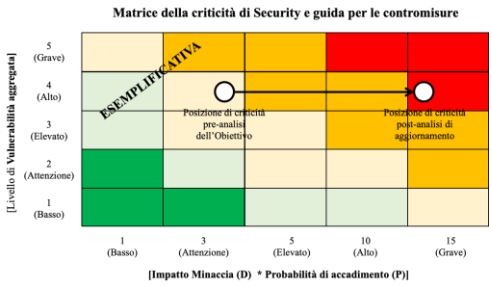
A.1.c.4 Reportistica annuale: Relazione Annuale sui servizi per l'Amministrazione Contraente

La Relazione Annuale è redatto dalla Funzione Reportistica e Miglioramento Continuo. La Relazione Annuale segue una logica di "ritorno informativo", in cui ogni anno le informazioni relative allo stato iniziale e alla gestione annuale sono confrontate attraverso opportuni cruscotti di indicatori. Se ne ricava un'analisi di gap che può essere effettuata per individuare problematiche, criticità e potenziali direttrici di miglioramento ed ottimizzazione dei servizi.

La Relazione annuale sarà messa a disposizione, entro le tempistiche prescritte dal Capitolato Tecnico, con le stesse modalità viste per la reportistica periodica, ossia mediante pubblicazione su piattaforma CSC e mediante avviso / alert su mail ai Referenti dell'Amministrazione Contraente. Ciò permette la completa tracciabilità dei flussi di reportistica all'interno di un ambiente omogeneo e protetto. Di seguito sono illustrati in dettaglio i contenuti della Relazione Annuale, in coerenza con i contenuti indicati dal Capitolato Tecnico, oltre a tutto quanto già previsto dal Capitolato Tecnico stesso.

Struttura della Relazione Annuale

Premessa e convenzioni. In questa sezione sono illustrati i dati principali del Contratto di Fornitura, amministrativi e tecnici. Sono espresse le consistenze degli apprestamenti oggetto del servizio e le caratteristiche dei servizi attivati presso gli Obiettivi, così come espressi all'interno dell'ODF. Tale sezione è importante per la corretta redazione della sezione di scenario in fase di avvio dell'erogazione dei Servizi.



Scenario in fase di avvio dell'erogazione dei servizi. All'interno di questa sezione è descritto lo scenario in fase di avvio dell'erogazione dei servizi, risultato del *Risk Assessment iniziale* effettuato su ciascun Obiettivo incluso nell'OPF. Le informazioni e gli indicatori contenuti in questa sezione costituiscono il p unto di riferimento per le analisi successive, relative al progressivo miglioramento tecnico economico dei servizi erogati dall'Offerente. La sezione costituisce la sintesi dello stato di fatto del rischio criminoso degli Obiettivi analizzati.

L'analisi del rischio criminoso è sempre accompagnata dalla statistica relativa agli eventi criminosi occorsi nel tempo presso gli Obiettivi. Dall'analisi discende l'elenco delle criticità riscontrate, che sono oggetto di un definito piano di intervento per la mitigazione del rischio.

Soluzioni apportate alle criticità riscontrate in fase di avvio. La mappatura delle criticità e la relativa prioritizzazione permette di organizzare la sezione in funzione del quadrante di appartenenza delle stesse sulla matrice delle criticità di Security (figura precedente) e di individuare le soluzioni organizzative, procedurali, tecnologiche, fisiche per mitigare il rischio. Tale approccio permette di monitorare efficacemente l'efficacia di una soluzione rispetto al contesto iniziale i, evidenziando subito lacune, problematiche o anomalie. Analogo approccio può essere impiegato andando a monitorare la diminuzione dell'indice di rischio in funzione delle contromisure adottate.

La sezione viene aggiornata ogni anno, in maniera tale da tenere conto dell'evoluzione dell'efficacia delle soluzioni proposte e, nel caso, permette di apportare variazioni nell'erogazione delle soluzioni proposte.

Problematiche, anomalie, criticità non risolte e relative motivazioni. La sezione illustra le **problematiche e anomalie residue**, che il piano di azione delle soluzioni apportate non è riuscita ad eliminare. Essa costituisce il punto di partenza per le attività da effettuare durante l'anno in corso. Particolare importanza ha la identificazione delle cause della persistenza delle problematiche rilevate alle soluzioni proposte, in modo da definire un percorso di miglioramento. La sezione contiene un'analisi degli indicatori di rischio alla fine del periodo di valutazione, che costituisce il punto di partenza per l'individuazione di punti di miglioramento.

Soluzioni per un continuo miglioramento e proposte di ottimizzazione del ODF. La sezione contiene l'insieme delle soluzioni che si ritiene, alla luce dell'aggiornamento degli indicatori di rischio e delle criticità individuate nell'ambito del documento, possano essere applicate per il miglioramento continuo e l'ottimizzazione del ODF.

Modalità e criteri d'individuazione di problematiche, anomalie e criticità. Durante la gestione del Contratto di Fornitura, l'Offerente adotta, oltre all'analisi statistica degli eventi criminosi ed all'analisi del rischio criminoso, anche una metodologia per l'individuazione di problematiche, anomalie e criticità relative al servizio integrato di vigilanza. E' stato quindi progettato un cruscotto di indicatori che consente di "tenere in rotta" l'evoluzione del Contratto, che fa parte anche del sistema di autocontrollo **[→ cfr. par. c.4].**

La metodologia di monitoraggio permette di coprire efficacemente tutti gli aspetti del servizio, consentendo di rilevare eventuali scostamenti dai valori ottimali durante l'evoluzione del Contratto di Fornitura. Tali indicatori sono calcolati sull'aggregato dell'ODF e per singolo Obiettivo, consentendo di effettuare le verifiche nel caso di situazioni anomale, che possono interessare uno o più Obiettivi.

Modalità e criteri d'individuazione di soluzioni di miglioramento e ottimizzazione. La sezione del documento contiene i riferimenti alle modalità ed ai criteri di individuazione adottati. In particolare, all'interno di tale sezione è effettuata l'analisi di alcuni indicatori relativi alla "prestazione" tecnico - economica dei servizi, evidenziando le possibili dimensioni di miglioramento e quindi l'opportunità di implementazione delle soluzioni proposte nella sezione precedente.

Servizio	Indicatore
Servizi di Vigilanza	
Tasso di saturazione degli operatori di vigilanza fissa, degli operatori di vigilanza ispettiva, degli operatori di vigilanza passiva	Confronto con tasso di saturazione di benchmark tratto dalla base dati dell'Offerente e da esperienze nazionali ed internazionali
Servizi di Manutenzione Apprestamenti	
Evoluzione temporale dell'indice di criticità (funzionale e manutentiva) degli apprestamenti anti-intrusione. L'analisi, effettuata per singola tipologia di apprestamento e per singolo Obiettivo, consente di identificare lo stato di obsolescenza degli apprestamenti e quindi di identificare possibili soluzioni di miglioramento e ottimizzazione per migliorare l'affidabilità degli impianti a supporto dell'attività di vigilanza	Evoluzione dell'indice di criticità globale degli apprestamenti anti-intrusione dell'Obiettivo
Evoluzione temporale dell'indice di criticità (funzionale e manutentiva) degli apprestamenti videosorveglianza. L'analisi, effettuata per singola tipologia di apprestamento e per singolo Obiettivo, consente di identificare lo stato di obsolescenza degli apprestamenti e quindi di identificare possibili soluzioni di miglioramento e ottimizzazione per migliorare l'affidabilità degli impianti a supporto dell'attività di vigilanza	Evoluzione dell'indice di criticità globale degli apprestamenti di video sorveglianza dell'Obiettivo
Evoluzione temporale dell'indice di criticità (funzionale e manutentiva) degli impianti tecnologici di sicurezza. L'analisi, effettuata per singola tipologia di apprestamento e per singolo Obiettivo, consente di identificare lo stato di obsolescenza degli apprestamenti e quindi di identificare possibili soluzioni di miglioramento e ottimizzazione per migliorare l'affidabilità degli impianti a supporto dell'attività di vigilanza	Evoluzione dell'indice di criticità globale degli impinati tecnologici di sicurezza dell'Obiettivo
Tasso di saturazione degli operatori di manutenzione degli apprestamenti	Confronto con tasso di saturazione di benchmark tratto dalla base dati dell'Offerente e da esperienze nazionali ed internazionali

Riepilogo dei precedenti resoconti – Sezione di sintesi dei Resoconti Annuali. SEZIONE AGGIUNTIVA. Questa sezione è presente solamente nel Resoconto Annuale dell'ultimo anno. Al suo interno è proposta una sintesi dell'evoluzione degli indicatori e delle osservazioni effettuate nei precedenti resoconti, sono illustrate criticità, problematiche a/o anomalie residue insieme alle soluzioni proposte per il miglioramento del successivo appalto.

Piano di Continuità. SEZIONE AGGIUNTIVA. Questa sezione è presente solamente nel Resoconto Annuale dell'ultimo anno. Al suo interno sono presenti le procedure e le pianificazioni da mettere in atto per facilitare la continuità del servizio al termine del Contratto di Fornitura, quali:

- Supporto nel passaggio della base dati versi i sistemi del nuovo Fornitore, per la continuità informativa;
- Pianificazione delle riunioni di coordinamento con le Figure organizzative del nuovo Fornitore;
- Pianificazione delle attività di affiancamento operativo fra le risorse dell'Offerente e quelle del nuovo Fornitore (e.g. Gestori del Servizio) per facilitare la presa di coscienza degli assetti operativi degli obiettivi.

A.1.c.5 Relazione Finale

La Relazione Finale costituisce il documento essenziale per condividere con il Soggetto Aggregatore tutte le informazioni a disposizione dell'Offerente, riguardanti l'andamento della Convenzione. E' un potente strumento per evidenziare eventuali elementi di miglioramento e/o di ottimizzazione dei servizi. La Relazione sarà completata entro 3 mesi dalla conclusione dell'ultimo contratto sul Lotto, a cura del Supervisore della Convenzione.

La Relazione sarà accompagnata da una presentazione con un documento di sintesi (presentazione con *Executive Summary*) il quale evidenzierà i punti salienti individuati.

La Relazione Finale sarò costituita dalle seguenti sezioni:

- Principali criticità riscontrate;
- Proposte e soluzioni finalizzate al miglioramento dei servizi nei successivi appalti;
- Proposta di modello di erogazione dei servizi;
- Modalità e criteri di individuazione di problematiche, anomalie e criticità;
- Modalità e criteri di individuazione di soluzioni finalizzate al miglioramento;
- Modalità e criteri di individuazione di nuove Attività e/o Servizi.

A.2. Struttura logistica con cui l'Offerente intende gestire la Convenzione

A.2.a Modalità con cui l'Offerente intende strutturarsi da un punto di vista logistico

L'organizzazione della struttura territoriale prevista è, in conformità alle prescrizioni del D.M. 269/2010, pensata per adattarsi perfettamente alle esigenze dello *stato di fatto* del Lotto (struttura territoriale del Concorrente) e del previsto *percorso di saturazione* dello stesso.

Tutte le strutture saranno adeguatamente potenziate in base alle caratteristiche, all'ubicazione e al carico di lavoro logistica degli obiettivi delle Amministrazioni Convenzionate.

A.2.a.1 Elementi principali della struttura logistica territoriale

Gli elementi principali della struttura logistica territoriale dell'Offerente sono i seguenti:

Sede Centrale di Lotto. La Sede Centrale di Lotto dell'Offerente è ubicata a **Milano**. La sede Centrale ospita tutte le risorse dei livelli organizzativi Direzione e Staff (alto coordinamento) della Convenzione. La Sede Centrale contiene la Centrale Operativa Master di Lotto, ubicata a Milano in Via Piero della Francesca, 45.

Centrale Operativa di Lotto. Rappresenta il punto di convergenza di tutti i flussi informativi afferenti i servizi di vigilanza. Include al suo interno il Call Center, che integra invece le richieste di servizio. E' il punto focale della ***infrastruttura di Centrale Operativa***, di cui fanno parte tutte le Sale Operative sul territorio del Lotto.

Sale Operative territoriali. Rappresentano i *punti di convergenza* dei flussi informativi ed il perno di coordinamento dei servizi a livello locale. Tutte le sale operative sul territorio del Lotto sono ridondanti fra loro e sono in continuo contatto.

Sale Operative di back-up. Sale operative con compiti di back-up all'intera infrastruttura di Centrale Operativa. Possono essere al di fuori del territorio del Lotto e permettono la ridondanza e continuità operativa della struttura di Centrale Operativa. Dell'infrastruttura di Centrale operativa fanno parte i ponti radio, che attualmente garantiscono la copertura sull'intero territorio del Lotto, per tutti i componenti dell'Offerente e tutti i partner che saranno utilizzati nelle attività.

Control Room presso obiettivo (ove presente). Sale di controllo presenti all'interno degli obiettivi e di proprietà dell'Amministrazione Contraente, contenenti i terminali di controllo degli apprestamenti di sicurezza. I segnali provenienti da ciascuna Control Room sono integrati all'interno dell'infrastruttura di Centrale Operativa.

Sedi operative sul territorio. Questi elementi sono punti di supporto per le attività operative e tecniche. Possono essere dotati di sistemi di protezione e conservazione delle chiavi per il servizio di gestione chiavi sul territorio. Sono dotati di postazioni informatiche per il personale e di magazzini per le attività di vigilanza e di manutenzione degli apprestamenti. Durante la fase di avviamento sono utilizzati, insieme alla Sede Centrale di Lotto, per il supporto logistico alle attività di sopralluogo / definizione della corretta configurazione dei servizi. Durante la fase di erogazione costituiscono i *punti di riferimento territoriali* per la logistica delle risorse, delle attrezzature e degli apprestamenti per le zone più lontane rispetto a Control Room, Sale Operative, Centrale Operativa.

Attualmente sono presenti distaccamenti operativi che permettono la copertura dell'intero territorio del Lotto, nella fase di definizione e configurazione dei servizi.

Punti di supporto logistico. Sono attivati sul territorio del Lotto a seconda delle necessità di supporto alle attività. La loro concentrazione varia in funzione della concentrazione territoriale di obiettivi e della distanza dalle sedi operative. Supportano l'erogazione dei servizi presso l'area territoriale di afferenza. Il numero di punti di supporto logistico varia con l'evoluzione della Convenzione.

Automezzi sul territorio per vigilanza ispettiva e Pronto Intervento. Costituiscono i presidi mobili sul territorio, necessari per effettuare le attività di vigilanza ispettiva e di pattuglia per i pronti interventi a servizio della televigilanza e della teleallarme. I mezzi sul territorio fanno capo ai distaccamenti operativi. Il numero di automezzi impiegati varia in funzione delle adesioni e della saturazione della Convenzione.

Automezzi sul territorio per le attività di manutenzione degli impianti tecnologici. Dislocati sul territorio, sono necessari per effettuare le attività di manutenzione degli impianti implementati dall'Offerente. Il numero di automezzi impiegati varia in funzione delle adesioni e della saturazione della Convenzione.

A.2.a.2 Struttura logistica iniziale OSCURATO

A.2.a.3 Modello di evoluzione della struttura logistica OSCURATO

A.2.b Coerenza fra struttura logistica proposta con la struttura organizzativa.

Nella seguente tabella sono illustrate le relazioni fra modello organizzativo e modello territoriale – logistico adottato. Sono infatti evidenziate le ubicazioni delle diverse Funzioni organizzative. E' così possibile apprezzare la coerenza del progetto **organizzativo** e di quello **territoriale** (Nota: **[P]:** elemento di ubicazione principale. **[A]:** elemento di ubicazione di appoggio. **[O]** elemento su cui erogati direttamente i servizi.)

Legame fra funzioni della struttura organizzativa ed elementi della struttura logistica	Sede Centrale di Lotto	Infrastruttura di Centrale Operativa	Sedi Operative	Punti di supporto logistico	Automezzi	Obiettivi
Livello di Direzione e Controllo						
Supervisore della Convenzione	P					
Team di Avvio e Riconsegna						
Pilotage	P		A			
Team Sistemi Informativi	P		A			
Team Apprestamenti	P		A			
Team Integrazione e Remotizzazione	P		A			
Commerciale e Configurazione						
Comunicazione e Convenzionamento	P					
Tecnici Sopralluoghi	P		A			

Legame fra funzioni della struttura organizzativa ed elementi della struttura logistica	Sede Centrale di Lotto	Infrastruttura di Centrale Operativa	Sedi Operative	Punti di supporto logistico	Automezzi	Obiettivi
Risk Management e Progetti PDI	P					
Progettisti Apprestamenti	P					
Call Center						
Responsabile Call Center ed Operatore di Call Center / Back Office	P					
Funzioni in Staff						
Segreteria Legale	P					
Amministrazione e Controllo di Gestione	P					
Infrastruttura informativa	P		A			
Servizi Tecnici agli Impianti	P		A			
Personale e Formazione	P		A			
Ingegneria di Convenzione						
Security Manager	P					
Pianificazione e Programmazione Integrata.	P					
Miglioramento Continuo						
Qualità Aziendale e Sicurezza	P					
Servizio Ispettorato	P		A			
Audit Interno e Miglioramento Continuo	P		A			
Gestione Ambientale	P		A			
Compliance normativa e protezione dati personali	P		A			
Livello di Direzione e Controllo						
Gestori del Servizio			P	A		A
Responsabile di Centrale Operativa		P				
GPG di Centrale Operativa		P				
Responsabile Operativo Vigilanza Ispettiva.	P		A			
GPG di vigilanza ispettiva / ronda e Pronto Intervento			A	A	P	O
Tecnico Responsabile Servizi Tecnici			A	A	P	
Addetti Servizi Tecnici	P		A	A		O
GPG Coordinatori operativi del servizio di piantonamento fisso			A	A		O
GPG di Piantonamento fisso		P	A	A		O

B. Modalità e procedure per la rilevazione delle esigenze e la predisposizione dei PDI e metodologie tecnico – operative per lo svolgimento ed il controllo dei servizi gestionali

Sulla base della propria esperienza, l'Offerente ha definito un efficace approccio organizzativo, metodologico e procedurale per quanto riguarda la raccolta dei dati e la relativa analisi. Esso si articola in due momenti:

- Raccolta dei dati necessari alla definizione dello stato di rischio, attraverso la gestione dei sopralluoghi iniziali;
- Analisi dei dati e progettazione del servizio, le cui risultanze costituiscono in principali contenuti del Piano Dettagliato degli Interventi.

La corretta impostazione della fase di raccolta dei dati è fondamentale, poiché con l'acquisizione dei dati corretti è possibile ottenere una "fotografia" veritiera delle condizioni di rischio di ciascun obiettivo e definire un servizio che sia aderente alle esigenze di quest'ultimo e dell'Amministrazione Contraente in generale.

B.1. Modalità e procedure per gestire i sopralluoghi iniziali

B.1.a Organizzazione per gestire i sopralluoghi iniziali

L'organizzazione dell'Offerente è stata progettata per avere la massima flessibilità e rispondere così alle possibili richieste multiple e contemporanee di effettuazione dei sopralluoghi.

La *Funzione Responsabile* dell'intero processo di valutazione dei rischi e di progettazione dei PDI, del quale l'esecuzione dei *sopralluoghi* è parte fondamentale, è la Funzione **Commerciale e Configurazione**, presieduta dal Supervisore della Convenzione, con le seguenti competenze:

- **Tecnici Sopralluoghi**, incaricati della raccolta dati per le successive analisi dello stato di rischio e la progettazione dettagliata del servizio;
- **Risk Assessment e Progetti PDI**, con le competenze necessarie all'esecuzione delle analisi di rischio e alla progettazione degli elementi di servizio;
- **Progettisti Apprestamenti**, che costituiscono l'area tecnica al servizio del servizio progettato. Consentono di introdurre nella valutazione dello stato di rischio l'effettiva criticità di taluni assetti impiantistici e di individuare le migliori contromisure tecnologiche, aderenti alle necessità effettive dell'Amministrazione Contraente;

L'organizzazione ha *specifici elementi progettuali* ottimizzati per il rispetto dei tempi previsti dal Capitolato, l'esatto recepimento dei fabbisogni e dello stato di rischi, la gestione di richieste multiple e contemporanee.

Prima di tutto, la fase di **raccolta dati** e quella di **analisi e progettazione** sono parallelizzate e assegnate a figure organizzative distinte.

I Tecnici Sopralluoghi possono infatti adattarsi alle richieste di svolgimento dei sopralluoghi sull'intero territorio. La Funzione Risk Assessment e Progetti PDI è organizzata per gruppi di lavoro, ma centralizzati presso la Sede Centrale dell'Offerente a Milano.

Ciò dà la possibilità di ottenere un'organizzazione per la configurazione dei servizi *sufficientemente flessibile* da adattarsi a picchi di carico per le attività di campo / sopralluogo, e con le *competenze centralizzate e omogenee* per la delicata fase di analisi e progettazione.

L'intero flusso di informazioni, anche in tempo reale, è garantito dalla piattaforma Civis Security Cloud (CSC), la quale prevede avanzate funzionalità di gestione documentale, con la possibilità di creare "folder" di analisi aggiornabili in tempo reale con i dispositivi di campo utilizzati dal personale di sopralluogo. **Team Sopralluoghi** e **Risk Assessment / Progetti PDI** si trovano quindi all'interno di un unico grande *"ufficio virtuale"* grazie al quale possono eseguire le attività di **analisi e progettazione in parallelo ai sopralluoghi**, si possono anticipare fasi di lavoro che, con approccio tradizionale, sarebbero in serie l'una all'altra **[→ cfr. Figura 4].**

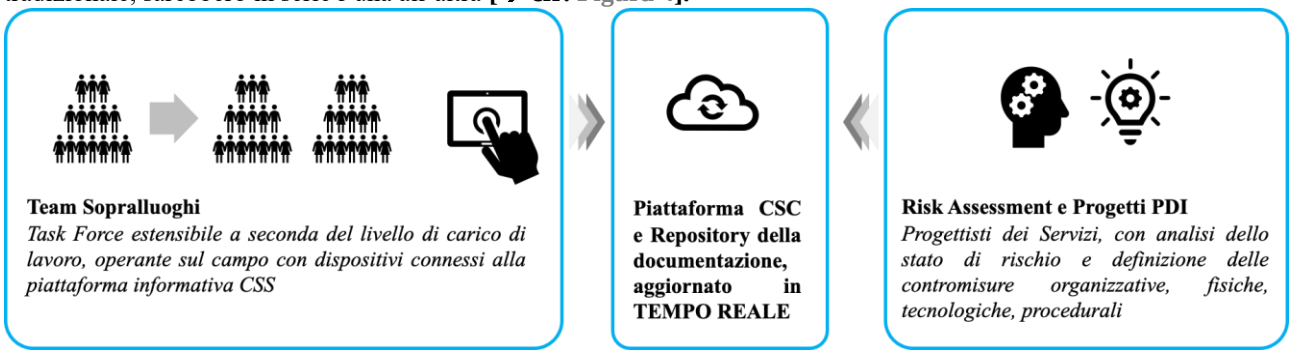


Figura 4 "Ufficio virtuale" con Task Force Sopralluoghi e Risk Assessment e Progetti PDI che condividono i dati necessari alla raccolta dati e alla progettazione dei servizi all'interno della piattaforma informativa CSC.

Il **Team sopralluoghi** è organizzato, come accennato prima, secondo una logica di **task force**. Esso è composto da **coordinatori interni** Civis, che presiedono gruppi di lavoro formati da professionisti interni ed esterni con esperienza, anche grazie alla attuale gestione della Convenzione, nei processi di consultazione istituzionale per le materie oggetto del servizio.

L'organizzazione è quindi elastica, velocemente adattabile a richieste multiple e contemporanee: le figure adibite alla raccolta dati sono infatti pre-selezionate in fase preventiva, all'aggiudicazione della Convenzione.

Esse sono quindi velocemente adattabili, anche con breve preavviso, ad eventuali picchi di carico di lavoro indotti da richieste contemporanee e permettono di rispettare le tempistiche massime richieste dal Capitolato Tecnico per l'esecuzione dei sopralluoghi a valle della notifica di validità degli OPF.

Il **Team sopralluoghi** è inoltre personalizzato in base alle peculiarità del Lotto: esso è **strutturato per zone territoriali di competenza**, in maniera tale da poter coprire omogeneamente tutte le esigenze del territorio del Lotto.

In particolare, la consistenza delle risorse a disposizione (personale, autovetture etc.) sarà organizzata su base provinciale / città metropolitana, sulla base della consistenza di popolazione del Lotto e del numero di Comuni presenti sul territorio. Le zone con maggiore popolazione residente e con un maggiore numero di Comuni sono, dall'esperienza dell'Offerente degli elementi di concentrazione di Amministrazione potenzialmente aderenti e di obiettivi potenziale oggetto dei servizi. Nel caso del Lotto l'organizzazione di massima del Team di Sopralluoghi (in termini di tempo impiegato) derivante da quest'analisi sarà la seguente:

Provincia / Ambito territoriale del Lotto 01	% risorse
Città Metropolitana di Milano	36%
Monza e della Brianza	13%
Lecco	13%
Como	15%
Sondrio	9%

Provincia / Ambito territoriale del Lotto 01	% risorse
Varese	14%

Le risorse professionali del Team Sopralluoghi saranno selezionate considerando che la fase di confronto iniziale con l'Amministrazione Contraente rappresenta un momento di particolare rilevanza al fine della qualità e completezza del servizio di Vigilanza che sarà erogato; come tale non può essere ridotta a una mera raccolta di informazioni circa i siti da monitorare, ma deve configurarsi in un **idoneo processo di ascolto delle istanze e di supporto alle decisioni finalizzato a individuare correttamente le esigenze dell'Ente.**

Il Team sarà quindi composto da figure professionali specializzate nella gestione delle tematiche relative alla sicurezza e alla legalità nei siti urbani sensibili attraverso l'utilizzo delle più avanzate metodologie di Risk Assessment e strumenti dedicati per la mitigazione del rischio criminalità.

Tali figure professionali hanno maturato, nell'ambito della presente Convenzione, una notevole esperienza nelle problematiche riferite a siti strategici, quali le sedi di grandi eventi e manifestazioni, i *main buildings* metropolitani, le aree dismesse e i cantieri edili.

L'Offerente ha quindi sviluppato un know-how specifico nella formulazione di soluzioni per la sicurezza riferite a condizioni anche molto differenziate, affrontando il processo nella sua totalità: dalla raccolta delle informazioni, alla diagnosi dei rischi, alla creazione dei modelli di relazione pubblico- privato, alle tecnologie per il controllo e la sorveglianza degli spazi, ai metodi operativi per la gestione delle emergenze.

Le Funzioni sopra citate sono supportate inoltre dal **Call Center**, attivo fin dal primo giorno di Convenzione.

Durante la fase di convenzionamento / adesione il Call Center svolge attività di supporto al contatto e al coordinamento con i Referenti delle Amministrazioni e dei singoli Obiettivi, in maniera tale da risolvere eventuali interferenze e vincoli all'accesso o all'esecuzione delle attività previste per la raccolta dati. Mantiene in sostanza la *"agenda"* sia degli incontri preliminari con i Referenti delle Amministrazioni e degli obiettivi sia delle attività di sopralluogo specifico.

Il *Call Center* svolge inoltre un'attività di **supporto allo scambio documentale**, e funge da *help desk* nei confronti dei Referenti per la raccolta delle informazioni preliminari.

Ciò permette di risolvere eventuali incoerenze o discrepanze fra programmazione ed esecuzione delle attività, ed anche di gap informativi nella documentazione preliminare ai sopralluoghi.

Ciò consente di rendere questa fase di lavoro molto fluida e priva di soluzioni di continuità, che invece con un approccio tradizionale si verificano puntualmente e pregiudicano il rispetto delle tempistiche e la qualità delle informazioni raccolte.

B.1.b Modalità e procedure per l'esecuzione dei sopralluoghi

I sopralluoghi hanno l'obiettivo di definire lo stato di rischio dei singoli Obiettivi dell'Amministrazione Contraente: esso costituisce la base per una progettazione del servizio di vigilanza integrato effettivamente aderente alle esigenze di sicurezza del singolo obiettivo e di ciascuna zona (c.d. unità di rischio) al suo interno.

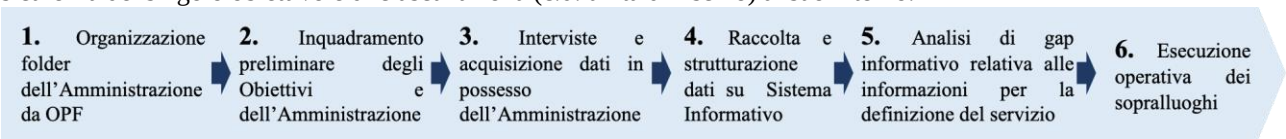


Figura 5 Metodologia per la raccolta dai dati necessari all'analisi del rischio e alla progettazione del servizio

Le singole fasi sono di seguito illustrate in dettaglio, evidenziando le soluzioni progettuali previste dall'Offerente per garantire la conformità quantitativa e qualitativa dei dati necessari per l'analisi di rischio e per la progettazione dei PDI.

1. Organizzazione dossier di raccolta dati

L'Offerente adotta da sempre un approccio preventivo e di anticipazione nell'organizzazione e nell'erogazione dei servizi. Questa metodologia è stata adottata fin dalle fasi preliminari della Convenzione, ossia durante l'acquisizione preliminare dei dati. Essa coinvolge la predisposizione degli OPF.

Aggiunta di campi e allegati all'OPF utili ad anticipazione le informazioni necessarie all'analisi del rischio. Al fine di anticipare l'acquisizione delle informazioni necessarie ad un'accurata progettazione dei servizi, l'Offerente ha previsto specifici contenuti e allegati agli OPF che l'Amministrazione potrà allegare, così da semplificare il processo di valutazione.

Nella seguente tabella sono confrontati i contenuti dell'OPF attuale di Capitolato Tecnico (colonna CT) e di quello proposto dall'Offerente (colonna Progetto).

L'OPF di progetto sarà messo a disposizione per anticipare l'acquisizione delle informazioni per il Risk Assessment:

Sezione	CT	Progetto
Dati generali		
Indirizzo obiettivi oggetto dei servizi di cui è richiesta l'attivazione		●
Presenza e tipologia di unità di rischio (aree / zone) di elevata sensibilità		●
Informazioni sommarie su eventi di security occorsi negli ultimi 5 anni		●

Sezione	CT	Progetto
Presenza di figure dell'Amministrazione destinate alla sicurezza (es. Funzione Security)		●
Servizio di piantonamento fisso		
Indirizzo obiettivo	●	●
Fasce orarie di esecuzione dei servizi	●	●
Giorni di esecuzione dei servizi	●	●
Servizio di vigilanza ispettiva / ronda		
Indirizzo obiettivo	●	●
Numero ronde richieste e relativo minutaggio	●	●
Fasce orarie di esecuzione dei servizi	●	●
Giorni di esecuzione dei servizi	●	●
Servizio di teleallarme		
Indirizzo	●	●
Tavola delle consistenze degli impianti anti-intrusione		●
Eventuali elaborati (schemi di impianto etc.) relativi agli impianti / apprestamenti		●
Servizio di televigilanza		
Indirizzo	●	●
Tavola delle consistenze degli impianti di videosorveglianza (marca, tipo, modello, quantità, anno di installazione)		●

Le informazioni aggiuntive richieste all'interno del modello di OPF non inficiano, ove non disponibili, il processo di acquisizione dei dati e di conseguente analisi.
Nel caso non dovessero essere disponibili, l'Offerente provvederà alla raccolta di tali informazioni durante le fasi successive. Le informazioni preliminari permettono di completare il **dossier di raccolta dati [→ cfr. Figura 6]:**

Figura 6 Informazioni del dossier di raccolta dati, necessari per l'analisi dei rischi e per la progettazione dei servizi

Il dossier di raccolta dati si configura come una "cartella elettronica", accessibile mediante CSC, all'interno della quale sono organizzate le informazioni pervenute e oggetto di successiva raccolta.

Lo scopo della raccolta dati consiste nel raccogliere e strutturare i dati necessari alla **valutazione**, per l'Obiettivo in generale e per le singole Unità di Rischio (i.e. gli asset da sottoporre a controllo, che possono essere tangibili o intangibili) **delle vulnerabilità rispetto alle minacce identificate**. Per vulnerabilità si intende un punto di debolezza in relazione alla minaccia, che può appartenere a tre tipologie:

- **punto di debolezza fisico:** riguarda una condizione di non adeguatezza a contrastare la minaccia, riferita ad elementi dell'Unità di Rischio quali accessi, problematicità logistiche, organizzazione dell'Unità nel contesto dell'Obiettivo (es. ingressi non protetti adeguatamente con infissi anti-effrazione etc..);
- **punto di debolezza tecnologico:** riguarda la non adeguatezza degli apprestamenti di sicurezza anticrimine e degli impianti tecnologici, ma anche l'assetto organizzativo degli stessi (mancata centralizzazione, vetustà, etc.);
- **punto di debolezza organizzativo / procedurale:** relativamente all'Unità di Rischio, definisce un'inadeguatezza del processo di gestione della sicurezza (es. codice di blocco e sblocco di locali ad accesso limitato uguale per tutti e non personalizzato, non adeguata organizzazione dei turni del personale, etc.).

Il metodo di raccolta dati, generale, di seguito personalizzato per il caso dell'Obiettivo selezionato, è completamente supportato dal Sistema informativo e si sviluppa secondo **passi di successivo completamento delle check list di raccolta dati.** Queste ultime costituiscono il principale strumento dell'attività di raccolta dati.
Tutti i dati provenienti da documentazione cartacea ed elettronica, interviste e questionari, attività di sopralluogo "on site" sono articolati e strutturati all'interno delle *check list*, personalizzate per tipologia di Obiettivo. Nel caso dell'Obiettivo

selezionato, la suddivisione delle check list segue l'articolazione per tipologia di informazione / obiettivo cognitivo: sono presenti sezioni – check list focalizzate su:

- Dati generali;
- Sicurezza fisica;
- Sicurezza logica;
- Sicurezza organizzativa;
- Gestione delle situazioni di crisi.

Come prima accennato, la fase di raccolta dei dati è **integralmente supportata dalle funzionalità di "workflow" documentale** (gestione e costruzione condivisa dei documenti) del Sistema informativo **[→ cfr. Figura 10].** Il cuore della fase di raccolta dati è costituito dalle check list o schede dati del dossier di raccolta dati. Per ciascun Obiettivo viene costruito a Sistema informativo un "folder" documentale dedicato, che costituisce un "tavolo di lavoro comune" per il Team e permette di gestire in maniera chiara, trasparente e univoca tutta la documentazione raccolta.

Parallelamente alle attività sopra descritte, l'Ingegneria PDI con il supporto del Call Center **effettua anche le attività di calendarizzazione delle attività di intervista e sopralluogo, definendo un calendario e il relativo programma di impegno delle risorse, al fine di attivare per tempo quanto necessario al gruppo di lavoro.**

I sopralluoghi e le interviste sono programmati a livello centralizzato in maniera tale da minimizzare i disagi ed eventuali criticità per la sicurezza e soprattutto in maniera da ottimizzare il rispetto delle risorse impiegate e da rispettare le tempistiche previste dal Capitolato Tecnico.

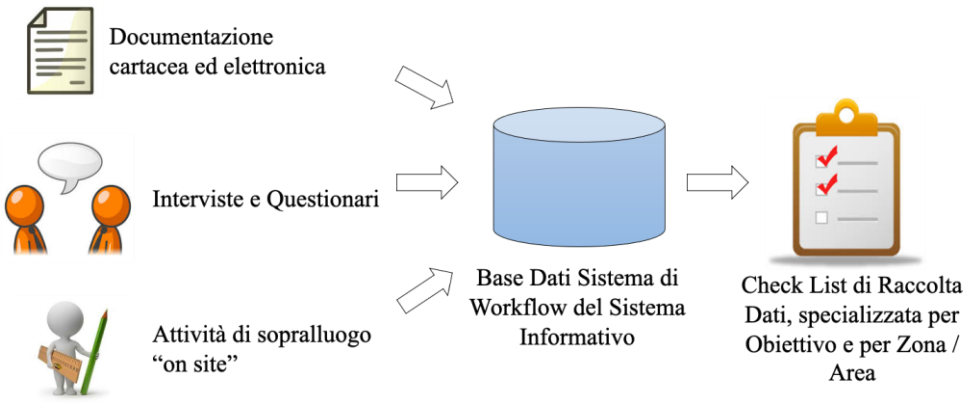


Figura 7 Integrazione della raccolta dati all'interno della piattaforma CSC

1. Organizzazione folder dell'Amministrazione da OPF
2. **Inquadramento preliminare degli Obiettivi e dell'Amministrazione**
3. Interviste e acquisizione dati in possesso dell'Amministrazione
4. Raccolta e strutturazione dati su Sistema Informativo
5. Analisi di gap informativo relativa alle informazioni per la definizione del servizio
6. Esecuzione operativa dei sopralluoghi

2. Inquadramento preliminare degli Obiettivi e dell'Amministrazione e Pianificazione della Raccolta Dati

Durante la fase preliminare, la Funzione Risk Assessment e Progetti PDI svolge l'attività preliminare di inquadramento degli obiettivi. Il primo passo è costituito dall'elaborazione di una **cartografia del territorio di competenza** dell'Amministrazione Contraente.

In preparazione del primo incontro con i Referenti dell'Amministrazione Contraente, a monte o contestuale all'attività di sopralluogo, sarà prodotta una **cartografia** sulla quale saranno evidenziati gli edifici e le aree pubbliche o asservite alle funzioni pubbliche, quali edifici comunali, scuole, parcheggi, parchi, ecc., nonché i principali complessi produttivi, commerciali e ogni altra funzione urbana strategica.

La cartografia sarà utilizzata in occasione dell'incontro con i Referenti dell'Amministrazione quale base di confronto su cui individuare la localizzazione dei siti da ricomprendere nel servizio di Vigilanza.

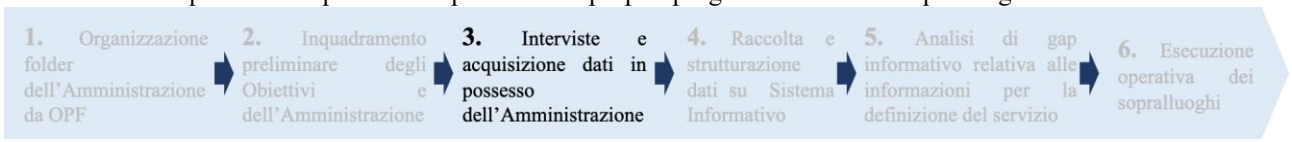
Le basi di riferimento e le informazioni per la predisposizione della cartografia saranno tratte da geo-portali online resi disponibili dalla Regione Lombardia.

Ove disponibili le informazioni preliminari richieste attraverso gli OPF, queste saranno integrate nel dossier di raccolta dati e i relativi indirizzi dei servizi saranno ubicati all'interno della cartografia, aumentando la conoscenza preliminare delle esigenze espresse dell'Amministrazione. Queste saranno quindi confrontate con l'effettiva risultanza del Risk Assessment e con gli effettivi fabbisogni per garantire il livello di sicurezza ottimale agli obiettivi.

Preliminarmente all'avvio delle fasi operative di analisi, viene effettuata una prima attività di pianificazione dell'attività, volta a definire con precisione il responsabile, il perimetro o ambito della stessa, interlocutori primari dell'Amministrazione Contraente (Ufficio Security, Direzione etc.), e quindi acquisire ogni elemento già disponibile e rilevante ai fini del lavoro.

La raccolta dati preliminare è basata soprattutto sulla documentazione resa disponibile da parte dell'Amministrazione attraverso l'OPF e relativi allegati e delle interviste preliminari ai Referenti per la Sicurezza.

I dati raccolti in questa fase preliminare sono strutturati al fine di identificare particolari aree di approfondimento durante le attività di sopralluogo, anche al fine di programmare e dirigere in maniera razionale tali attività. Grazie a questa pre-lavorazione, è possibile già identificare alcuni gap conoscitivi presenti, oggetto di specifica indagine in sede di sopralluogo.
Tutte le informazioni sono riportate all'interno delle check list, che riportano i dati necessari e i dati mancanti per l'analisi. Il Team effettua quindi una rapida analisi per la vera e propria programmazione dei sopralluoghi sull'Obiettivo.



3. Interviste ai Referenti dell'Amministrazione e acquisizione dei dati

A seconda della disponibilità e delle tempistiche, questa fase potrà essere eseguita prima o contestualmente all'esecuzione dei sopralluoghi. L'obiettivo di questa fase è acquisire le informazioni sufficienti a definire:

- Dati statistici sugli eventi criminosi;
- Dati sulla sicurezza fisica (consistenza degli apprestamenti)
- Dati sulla sicurezza tecnologica;
- Dati sulla sicurezza organizzativa;
- Impressioni e percezioni dei Referenti riguardo il livello di rischio;
- Presenza di specifiche unità di rischio all'interno degli obiettivi di cui tenere conto nell'ambito della progettazione del PDI.

Per la prima riunione con l'Amministrazione Contraente sarà proposta la presenza dei referenti dell'Organo esecutivo e dei dirigenti dei servizi tecnici coinvolti. Nel corso della riunione si procederà a raccogliere ogni informazione utile a identificare sulla cartografia georeferenziata i siti e gli immobili a cui rivolgere il servizio di Vigilanza; durante questo confronto gli incaricati dell'Offerente procederanno:

- da un lato, a raccogliere dall'Amministrazione le informazioni relative al *profilo di sensibilità* di ciascun sito / immobile e le aspettative iniziali rispetto alle funzioni di Vigilanza, attraverso opportune interviste strutturate;
- dall'altro lato, a trasferire all'Amministrazione una serie di informazioni e cognizioni riguardo al rischio criminalità tipico delle diverse fattispecie urbane e territoriali, utili a orientare le scelte di configurazione del servizio di Vigilanza, concentrando le risorse sui bersagli realmente esposti.

In particolare, le interviste formuleranno quesiti in relazione a:

- quali sono i siti considerati sensibili e perché (es.: eventi criminosi già avvenuti; attività e funzioni proprie del sito);
- quali sono stati gli eventi criminosi avutisi in passato e con quali caratteristiche (esito dell'evento, modalità di accadimento; date; ecc.);

Con queste informazioni si ha la base di conoscenza per rimodulare eventualmente, laddove necessario, il fabbisogno del servizio richiesto da parte dell'Amministrazione per la mitigazione del rischio.

L'insieme dei contenuti raccolti durante le interviste strutturate costituirà un'apposita sezione del PDI, all'interno della quale saranno debitamente individuati gli elementi che hanno dato luogo ad una rimodulazione del progetto di servizio. In tal modo l'Offerente mantiene una assoluta trasparenza rispetto al processo di configurazione dei servizi, nell'ottica della massima collaborazione con l'Amministrazione,.
Inoltre, Grazie alla capacità di recepimento dei dati, può essere condiviso con i Referenti un calendario di condivisione di informazioni e documenti da aggiungere al dossier di raccolta dati.

4. Raccolta e strutturazione dati sul dossier di raccolta dati

Tutti i dati acquisiti attraverso lo scambio documentale con l'Amministrazione e le interviste strutturate sono inseriti all'interno del dossier di raccolta dati. Il Responsabile dell'Ingegneria PDI coordina questa fase ed effettua il controllo formale di completezza di tutte le informazioni.
La strutturazione dei dati è effettuata dal personale Risk Assessment e Progetti PDI, a livello centralizzato per tutti gli OPF, **applicando così la medesima metodologia.**
All'interno dei folder **sono raccolte tutte le *check list*** le cui lacune saranno oggetto di ***specifica attività di sopralluogo***, in particolare per quanto attiene i siti ad elevata sensibilità.

5. Analisi di gap informativo e programmazione "mirata" dei sopralluoghi

L'Ingegneria PDI effettua l'analisi del dossier di raccolta dati e individua, con il supporto della Funzione Security Manager, l'esistenza di lacune informative riguardanti i dati necessari per una configurazione ottimale del servizio. Sostanzialmente sono comparati i contenuti delle check list di rilevazione con i contenuti già presenti e acquisiti, e sono individuate le informazioni che sarà necessario acquisire in sede di sopralluogo.

L'analisi di gap permette di effettuare, nell'ambito della calendarizzazione stabilita, un dimensionamento ottimale del Team Sopralluoghi, considerando i carichi di lavoro necessari per investigare le aree informative con maggiori lacune.

Il metodo dell'analisi di gap permette sostanzialmente di **modulare la capacità produttiva del gruppo di lavoro** e di conseguire, entro i tempi prescritti dal Capitolato Tecnico, la **massima qualità possibile delle informazioni** per le analisi di rischio e per la progettazione dei servizi.

6. Esecuzione operativa dei sopralluoghi e completamento dei folder informativi

In occasione dei sopralluoghi, ove non già eseguite prima, saranno effettuate le interviste strutturate ai Referenti dell'Amministrazione. Il personale del Team Sopralluoghi avrà, direttamente sul campo, accesso al dossier di raccolta dati e a tutte le check list relative grazie all'utilizzo estensivo di tablet PC connessi alla piattaforma CSC.

I dati di intervista / sopralluogo saranno immediatamente disponibili al gruppo di lavoro di *Risk Assessment* e Progetti PDI, che potrà procedere in parallelo alle attività di sopralluogo con le attività di analisi dei dati, comprimendo le tempistiche di analisi.

Questo approccio è particolarmente efficace per assorbire l'eventuale impatto di richieste multiple e contemporanee, poiché i tempi compressi non inficiano la qualità delle analisi effettuate: parallelizza attività con durata – e impegno e cura – **analoghe a quelle di un approccio più tradizionale, ma con il vantaggio di una maggiore flessibilità.**

La funzionalità di supporto alla compilazione delle check list, Civis Audit, è inoltre dotata di un algoritmo automatico che impedisce la chiusura della documentazione in mancanza di determinati campi.

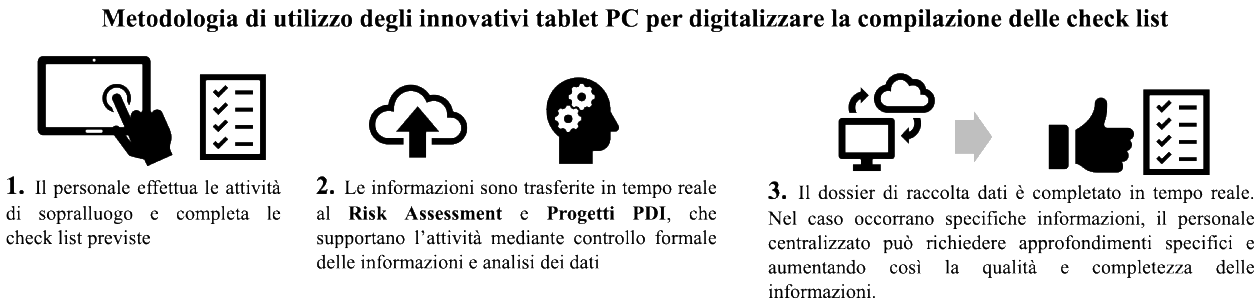


Figura 8 Metodologia di impiego dei tablet PC e della costruzione contestuale del dossier di raccolta dati

All'interno delle check list saranno riportate, in ottemperanza al Capitolato Tecnico, lo stato e le caratteristiche degli edifici e dei relativi impianti di sicurezza e il livello di rischio di ciascun sito desunto dalle interviste con i referenti dell'Amministrazione Contraente. Nel corso dei sopralluoghi saranno verificati e riportati sulla Scheda descrittiva:

- lo stato degli impianti di sicurezza e i dispositivi di teleallarme attualmente in uso;
- lo stato di sicurezza degli accessi agli edifici;
- il profilo generale di rischio degli immobili in relazione alle caratteristiche del contesto (visibilità dalle strade e piazze, illuminazione, ecc.).

Più in particolare, la Scheda descrittiva riporterà informazioni atte a rappresentare l'effettivo grado di vulnerabilità dei siti/immobili in relazione al quale andrà calibrato il servizio di sicurezza. A titolo di esempio si riportano di seguito alcuni contenuti che proponiamo di raccogliere attraverso le schede di sopralluogo, i quali saranno articolati nelle seguenti sezioni generali:

- sicurezza fisica;
- gestione sistemi di sicurezza;
- vigilanza e presidi;
- attività di sensibilizzazione e formazione security.

Di seguito sono illustrati i contenuti di dettaglio, seppur preliminari, delle check list del dossier di raccolta dati:

		n/a	SI	NO
SICUREZZA FISICA				
controllo accessi e presenze				
perimetro esterno delimitato				
controllo accessi e presenze	area esterna			
	area interna			
	area specifica			
sistemi antintrusione videocontrollo videoregistrazione				
sistema antintrusione area esterna				
sistema antintrusione area interna				
sistema tvcc	area esterna			
	area interna			
mezzi di chiusura difese passive				
perimetro esterno	barriera			
	barriera antisfondamento			
accessi ad aree interne	porta			
	porta antisfondamento			
PLANIMETRIE POSIZIONAMENTI APPARECCHIATURE				
Sicurezza				
TVCC				
controllo accessi presenze				

Figura 9 Immagine con contenuti di dettaglio della Check List "Sicurezza Fisica"

	n/a	SI	NO
GESTIONE SISTEMI DI SICUREZZA			
ATTRIBUZIONE MANSIONI			
inserimento sistemi			
procedure inserimento			
disinserimento sistemi			
Procedure disinserimento			
definizione orari e giorni			
on			
off			
definizione modello applicativo apertura e chiusura			
azione seguita da dipendente			
azione eseguita da dipendente con supporto personale non armato			
azione eseguita da dipendente con supporto personale armato			
videocontrollo tvcc da remoto			

Figura 10 Immagine con contenuti di dettaglio della Check List "Gestione Sistemi di Sicurezza"

		n/a	SI	NO
VIGILANZA E PRESIDI				
servizi di guardiania vigilanza telecontrollo				
presidio ingresso				
presidio 24/24				
intervento vigilanza su allarme				
controllo da remoto	antintrusione			
	tvcc			
vigilanza collegamenti remoti				
periferica radio				
periferica gprs				
combinatore telefonico digitale				
id contact				
collegamento sistema di videosorveglianza				
configurazione periferiche				
definizione e redazione delle procedure				
protocollo di gestione con vigilanza				
procedura di sicurezza	per funzione			
	per processi			

Figura 11 Immagine con contenuti di dettaglio della Check List "Vigilanza e Presidi"

	n/a	SI	NO
ATTIVITÀ DI SENSIBILIZZAZIONE E FORMAZIONE SECURITY			
sensibilizzazione formale riunioni			
sensibilizzazione informale one to one			
formazione specifica			
addestramento			
comunicazione di security			
distribuzione elenchi reperibili			
comunicazione formalizzata in tema di security			
sicurezza logica			
definizione delle norme minime di it security			
definizione delle misure di sicurezza non tecniche			
classificazione delle informazioni			
gestione delle emergenze			
formazione ed addestramento del personale in tema di emergenza			
gestione delle comunicazione in caso di emergenza			

Figura 12 Immagine con contenuti di dettaglio della Check List "Attività di sensibilizzazione e formazione security"

			si	no	dettagli
Massima sicurezza	18	sistemi di sicurezza sofisticati con ridondanza sottosistemi			
	17	Forza sul sito di risposta Squadra			
Alto livello	16	Piani e procedure formali contingency			
	15	coordinatore a livello locale			
	14	sistema di illuminazione ad alto livello ; lumen, dell'intero sito			
	13	sistemi di controllo accessi			
	12	Forza sul sito addestrata e con sistemi avanzati di comunicazione ed equipaggiamento			
	11	Allarme perimetrale remotizzato			
	10	CCTV			
Medio Livello	9	disarmato con comunicazioni basica			
	8	barriere perimetrale di alta sicurezza , guardie o cani			
	7	sistema di allarme avanzato e remotizzato			
Basso Livello	6	serrature a doppia mappatura, lucchetti , di buon livello			
	5	barriere fisiche basiche			
	4	sistema di luci semplice			
	3	sistema di allarme locale basico			
Livello minimo	2	semplici sistemi di chiusura , serrature			
	1	semplici barriere fisiche			

Figura 13 Immagine con contenuti di dettaglio della Check List sulle contromisure presenti presso l'obiettivo 1/2

COMPONENTI PER **IMPEDIRE**					
barriere fisiche	**chiusure**		si	no	dettagli
barriere perimetrali	barriere perimetrali				
chiusure ad alta sicurezza	aperture				
finestre blindate	porte blindate				
Volte muri rinforzati					
Forza di siurezza	**sistema di controllo accessi**		si	no	dettagli
livello di equipaggiamento	aree protette				
training	aree vitali				
sistemi					
COMPONENTI PER **RILEVARE**			si	no	dettagli
porte aperture					
perimetro					
aree protette					
aree vitali					
COMPONENTI PER **VALUTARE**			si	no	dettagli
luci	**comunicazione**	**CCTV**			
perimetro	On site	perimetro			
aree protette	Off site	aree protette			
aree vitali		aree vitali			
COMPONENTI PER **NEUTRALIZZARE**			si	no	dettagli
forza di sicurezza on site	forza di risposta / assalto	Coordinamento			
livello di equipaggiamento	livello di equipaggiamento	pianti contingenti			
training	training	esercitazioni			
sistemi	sistemi				

Figura 14 Immagine con contenuti di dettaglio della Check List sulle contromisure presenti presso l'obiettivo 2/2

B.2. Piano degli Interventi (PDI)

Il Piano Dettagliato degli Interventi (PDI) rappresenta il principale strumento di configurazione, pianificazione e descrizione di dettaglio dei servizi richiesti per il singolo ODF.

B.2.a Organizzazione per la predisposizione del Piano degli Interventi (PDI)

La Funzione organizzativa responsabile della predisposizione del Piano degli Interventi p la Funzione Risk Assessment e Progetti PDI. La Funzione è supportata dal **Security Manager** dell'Ingegneria di Convenzione, che si occupa anche del continuo aggiornamento dei PDI in funzione della variazione delle condizioni di rischio degli obiettivi compresi nell'Unità di Gestione.

Le **competenze** sono **centralizzate** all'interno della Sede centrale dell'Offerente, in modo tale da applicare le medesime metodologie di analisi all'intero Lotto e garantire l'applicazione di metodologie omogenee per la mitigazione del rischio.

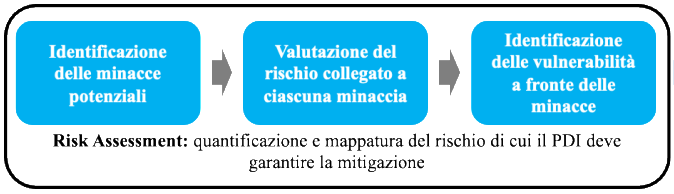
La centralizzazione è resa possibile dalla piattaforma informativa CSC, attraverso la quale è possibile condividere le informazioni e i dati raccolti in tempo reale e in parallelo rispetto alle attività di sopralluogo.

Il Piano degli Interventi è infatti il punto conclusivo di una approfondita fase di analisi dei fabbisogni di sicurezza dell'Amministrazione e di ciascun obiettivo della stessa:

Figura 15 Approccio metodologico alla definizione dei contenuti del PDI da parte di Risk Assessment e Progettazione PDI

B.2.b Procedure e modalità per la predisposizione, definizione del PDI e sua condivisione con l'Amministrazione Contraente

B.2.b.1 Risk Assessment



Il PDI ha l'obiettivo di identificare la configurazione di servizio più aderente alle effettive necessità dell'Amministrazione Contraente, individuando lo stato di rischio e le contromisure, cioè gli elementi del progetto di servizio, che permettono di mitigare il rischio criminoso .

A tal proposito, l'Offerente impiegherà l'efficace strumento del **Risk Assessment**. Esso identifica il livello di rischio per ciascuna minaccia identificata, per ciascun obiettivo vigilato e per ciascuna area dello stesso. La tecnica utilizza la Matrice di Valutazione Preliminare del Livello di Rischio, con l'applicazione della metodologia **UNI ISO 31000 – "Gestione del rischio".**

Sulla base delle informazioni raccolte nel corso della prima riunione con l'Amministrazione Contraente, infatti, nei casi in cui l'individuazione dei siti da monitorare sia risultata incerta, il gruppo di lavoro provvederà a sviluppare internamente un'attività di *Risk Assessment* preliminare finalizzata a definire un quadro del rischio criminalità in relazione ai diversi siti sensibili: sarà valutato il livello di rischio di eventi criminosi nelle aree in esame, assumendo il rischio quale prodotto della probabilità di accadimento degli eventi moltiplicata per la gravità dei danni potenziali.

Tale analisi del rischio, derivata da consolidati standard internazionali di *Risk Assessment*, implica l'individuazione delle potenziali sorgenti di pericolo e delle possibilità che esse si trasformino in danno: le potenziali sorgenti di pericolo saranno individuate da parte di nostro personale specializzato, sulla base della letteratura di settore, in relazione alla morfologia delle aree di studio e delle funzioni in esse insediate, nonché attraverso ogni altra informazione raccolta attraverso l'Amministrazione Contraente.

Tutte le valutazioni del *Risk Assessment* sono effettuate a partire dal dossier di raccolta dati, oggetto della fase di sopralluogo, descritto prima.

L'intero documento è digitalizzato, condivisibile in tempo reale e lavorabile anche da remoto, grazie alla sua integrazione nella base dati della piattaforma informativa CSC.

La gestione completamente elettronica della documentazione relativa ai sopralluoghi effettuati permette di condividere in tempo reale fra tutti gli attori interessati le informazioni. Ciò permette, internamente al gruppo di progettazione, la specializzazione per ambito e quindi la parallelizzazione delle attività di progettazione.

E' quindi possibile, ad esempio, parallelizzare le attività di progettazione dell'organizzazione con le modalità di integrazione e centralizzazione dei segnali di allarme, ovvero con l'implementazione delle soluzioni innovative per la videosorveglianza proposte nella sezione C.1 della presente Relazione Tecnica.

B.2.b.1.1 Metodologia generale del Risk Assessment

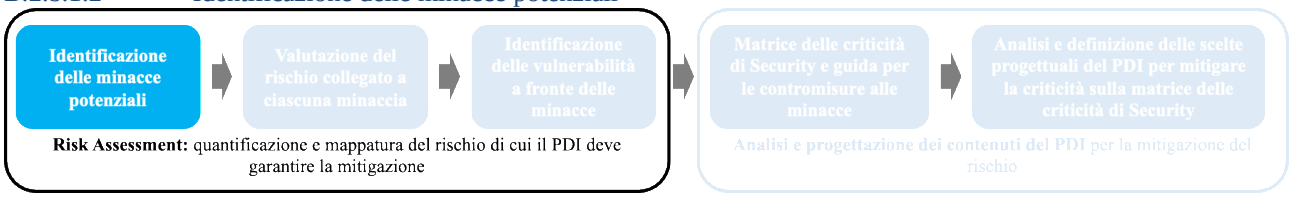
Più in particolare, una volta classificate le strutture in base alla destinazione d'uso verrà esaminato il rischio criminoso a cui si stima possano essere esposte, al fine di valutare e proporre il servizio più adatto alle potenziali esigenze della singola tipologia di Amministrazione, in linea con la normativa **UNI ISO 31000 – "Gestione del rischio".**

Per la valutazione del potenziale rischio criminoso si considereranno differenti fonti del settore, quali: il Codice Penale, per la scelta dei differenti rischi e l'assegnazione del livello di gravità dell'eventuale danno subito; il Rapporto sulla criminalità italiana del Ministero dell'Interno e l'indagine sulla sicurezza dei cittadini (ISTAT), che contiene riferimenti aggiornati per lo studio e la valutazione della probabilità di accadimento di una specifica minaccia, sulla base di numerosi elementi statistici; etc.

La metodologia è basata **sull'identificazione qualitativa degli "elementi" che concorrono a definire il rischio criminoso** per ciascuna **Unità** di **Rischio dell'Obiettivo** ed in forma "aggregata" dell'intero Obiettivo. Tale modalità prevede:

- **L'identificazione delle minacce potenziali** che incombono su unità di rischio / obiettivo (di seguito l'analisi sarà illustrata con riferimento all'intero obiettivo);
- **La valutazione della probabilità "*P*" di accadimento della minaccia specifica,** a partire dai dati raccolti all'interno del dossier;
- **La valutazione del danno "*D*",** cioè della gravità del danno nel caso in cui l'evento si verificasse. quantifica la gravità del rischio associato allo specifico obiettivo, per quanto concerne la singola minaccia
- **La valutazione del peso percentuale** "***r%***", di ciascuna minaccia, ossia il "peso" che ciascuna minaccia ha sugli obiettivi. Ogni atto criminoso ha infatti un peso diverso. È evidente, infatti, che la prevenzione di un attentato richiede un impegno diverso dall'evitare un furto, e questo si riflette anche sull'impegno economico richiesto.

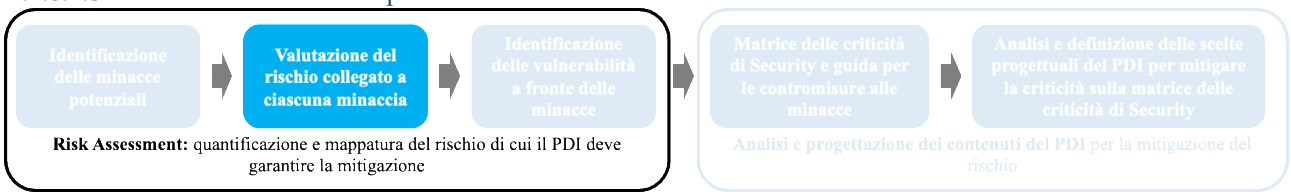
B.2.b.1.2 Identificazione delle minacce potenziali



A partire dai dati raccolti, i diversi siti sono classificati in base alla tipologia di rischio criminoso che può potenzialmente coinvolgere l'obiettivo e, per inciso, le singole Unità di Rischio al suo interno. Si distinguono quindi le seguenti tipologie di rischio criminoso, strutturate per classi:

Classe	Evento / esempio
1	Accattonaggio, "barbonaggio" (come definito dall'Art 669 del CP e art.154 del TULPS)
2	Furto / Rapina di beni tangibili e/o intangibili (es. informazioni, dati etc.), effrazione
3	Atto vandalico / danneggiamento, ingresso non consentito
4	Allagamento doloso, incendio doloso
5	Sabotaggio
6	Attentato

B.2.b.1.3 Valutazione della probabilità di accadimento "P" e del danno "D"



Per ciascun sito, sfruttando le informazioni acquisite, è effettuata la **mappatura delle aree** in funzione della "criticità" (da 1 – bassa criticità, a 5 – massima criticità) in relazione a ciascuna **minaccia.** Classificate le strutture in base alla destinazione d'uso, sarà esaminato il rischio criminoso in linea con la **UNI ISO 31000 – "Gestione del rischio":**

Rischio della minaccia:	=	Probabilità di accadimento	*	Danno (D)
Atti violenti / terrorismo; Effrazione / ingresso di soggetti non autorizzati; Danni / vandalismo; Furto / sottrazione di beni o informazioni; Problema tecnico / impiantistico		Probabilità di accadimento dell'evento afferente la security, a partire dall'esperienza specifica nel servizio di vigilanza presso l'Amministrazione Contraente		Peso attribuito alla gravità del rischio associato alla specifica minaccia, allo specifico sito

Figura 16 Prodotto fra probabilità di accadimento (P) e danno (D) per la definizione del rischio della minaccia (UNI ISO 31000)

Sulla base delle fonti raccolte e della classificazione del rischio così come definito nella **Matrice di Valutazione Preliminare del Livello di Rischio**, sarà quindi assegnato a ciascun sito il livello di rischio criminoso cui è sottoposto.

Le valutazioni sopra descritte saranno lasciate a disposizione dell'Amministrazione Contraente e costituiranno un Decision Support System (DSS) utilizzabile dalla Funzione Security per valutazioni interne all'Amministrazione. Tutti gli stati di rischio nella zona rossa costituiscono le criticità.

I livelli di rischio associati saranno utilizzati per individuare un **R**ischio **G**lobale di ogni categoria di **O**biettivi (**RGO**), dove sarà dato un peso diverso ad ogni atto criminoso, il quale tiene conto del seguente valore di r% (peso percentuale delle classi di minaccia individuate), individuato sulla base delle analisi svolte sulla banca dati CIVIS relativa alla gestione dell'attuale Convenzione:

Matrice di valutazione preliminare del livello di rischio

R = P x D			P = Probabilità di accadimento dell'evento criminoso		
			bassa	media	alta
			1	2	3
D = Peso attribuito alla gravità dell'evento criminoso	basso	1	1	2	3
	medio basso	2	2	4	6
	medio	3	3	6	9
	alto	4	4	8	12
	altissimo	5	5	10	16

Classe	Minaccia	r%
1	Accattonaggio, "barbonaggio" (come definito dall'Art 669 del CP e art.154 del TULPS)	5%
2	Furto / Rapina di beni tangibili e/o intangibili (es. informazioni, dati etc.), effrazione	15%
3	Atto vandalico / danneggiamento, ingresso non consentito	10%
4	Allagamento doloso, incendio doloso	20%
5	Sabotaggio	20%
6	Attentato	30%

Nella figura seguente è riportato un esempio di matrice del Livello di Rischio criminoso per tipologie di immobile / sito, fra le quali sono comprese quelle potenzialmente convenzionabili:

VALUTAZIONE PRELIMINARE DEL LIVELLO DI RISCHIO CRIMINOSO

OBIETTIVI	PESO RELATIVO AL RISCHIO CRIMINOSO						R.G.O.
	30%	20%	20%	10%	15%	5%	
	ATTENTATO	SABOTAGGIO	INCENDIO DOLOSO	ATTO VANDALICO	FURTO/ RAPINA	BARBONAGGIO	
	PROBABILITA' x DANNO						
Sedi uffici	4	0	6	3	3	0	3,2
Caserme esercito	4	0	6	0	0	0	2,4
Carceri e Case Circondariali	4	0	6	0	1	0	2,6
Studentati/complessi immobiliari per studenti	4	0	6	3	3	0	3,2
Caserme VVF	4	0	6	0	0	0	2,4
Ospedali	5	0	6	6	2	1	3,7
ASL/sedi ambulatoriali	4	0	6	0	1	0	2,6
RSA pubbliche accreditate	4	0	6	4	1	0	3,0
Istituto zooprofilattico	4	0	6	4	1	0	3,0
Tribunali ed uffici giudiziari	5	0	6	6	0	0	3,3
Sede polizia locale	4	0	6	0	0	0	2,4
Patrimonio culturale	4	0	6	9	3	1	3,8
Auditorium, Teatro	4	0	6	4	0	0	2,8
Mercati e fiere	5	0	3	4	4	2	3,2
Camere di Commercio	4	0	6	3	3	0	3,2
Centri socio-assitenziali	4	0	6	3	0	0	2,7
Centri per l'impiego	4	0	6	3	0	0	2,7
Impianto sportivo	4	0	3	9	1	0	2,9
Principali parchi pubblici comunali	4	0	6	3	1	3	3,0
Cimitero	4	3	3	2	2	0	2,9
Discariche	4	3	6	0	0	0	3,0
Porti	5	4	6	9	4	2	5,1
Scuola (infanzia, primarie e secondarie)	4	0	6	2	3	0	3,1
Università	4	0	6	3	3	0	3,2
Centri socio assistenziali - CRI	4	0	6	6	0	0	3,0
Enti di ricerca/formazione	4	0	6	4	2	0	3,1
Aeroporti	5	4	6	6	2	2	4,5
Stazioni ferroviarie	5	4	6	9	6	3	5,5
Stazioni metropolitane	5	4	6	9	4	3	5,2

Figura 17 Stralcio della Matrice del livello di rischio criminoso e calcolo del Rischio Globale per Categoria di obiettivo

per ciascuno è definito l'insieme delle debolezze a livello organizzativo, fisico o tecnologico che fungono da base per la definizione delle contromisure organizzative, tecnologiche e fisiche che potranno garantire il miglioramento dello stato di rischio presso i siti.

B.2.b.1.4 Identificazione delle vulnerabilità alle minacce **OSCURATO**

B.2.b.1.5 Analisi e progettazione dei contenuti del PDI **OSCURATO**

B.2.b.1.6 Individuazione delle soluzioni progettuali per la mitigazione dello stato di criticità **OSCURATO**

B.2.b.1.7 Individuazione delle soluzioni progettuali per la mitigazione dello stato di criticità **OSCURATO**

B.2.b.2 Modalità di presentazione e condivisione del PDI

Lo scopo dell'Amministrazione nella valutazione del **PTE** è il perseguimento della convenienza e del pubblico interesse nell'approvazione del Piano Tecnico Economico di Sicurezza Integrata (PTE)**.** Lo scopo è infatti di verificare:

- **L'aderenza tecnica** alle effettive necessità dell'Amministrazione;
- **la convenienza economica**, rispetto alla situazione attuale, dell'adesione ai servizi in Convenzione.

B.2.b.2.1 Logiche di presentazione

La **logica di base** con cui l'Offerente intende proporre e formalizzare i contenuti del PDI è quindi quella di elaborare procedure e strumenti che agevolino al massimo grado i diversi passi di condivisione ed eventuale approvazione del PDI. Per presentare gli interventi progettati in maniera semplice, trasparente, sintetica e comprensibile, l'Offerente produrrà materiale documentale di supporto al PDI in formato grafico, tabellare e descrittivo, tale da rendere altamente comprensibile il valore delle proposte, le loro caratteristiche tecniche, economiche, prestazionali e di mitigazione del rischio criminoso.

B.2.b.2.2 Modalità e procedure di formalizzazione del PDI all'Amministrazione Contraente

In occasione della **prima presentazione** del PDI all'Amministrazione contraente, la documentazione viene rilasciata anche sul **Portale del Soggetto Aggregatore,** secondo le procedure prescritte dal Capitolato Tecnico.

Per quanto riguarda **l'aderenza tecnica della proposta**, si è osservato nella attuale Convenzione che un obbiettivo del PDI è quello di far comprendere con chiarezza i vantaggi tecnici ed economici dei servizi in Convenzione. L'Offerente illustrerà gli aspetti di **convenienza** dei servizi, così come sono proposti, rispetto alla *situazione attuale in assenza di Convenzione*.

La procedura di presentazione prevede quindi di prevedere una sezione di sintesi dal PDI, che illustrerà **i seguenti aspetti:**

- **Presentazione dello stato di fatto e di progetto in termini di Unità di Rischio**, con costi dell'attuale configurazione di servizio, e l'attuale attuale livello di rischio delle Unità di Rischio. La sezione è anche arricchita dalla statistica degli eventi criminosi che hanno eventualmente coinvolto le Unità di Rischio, le quali costituiscono una solida base di confronto per verificare la bontà delle soluzioni di mitigazione del rischio;
- **Presentazione di confronto dei vantaggi economici dell'adesione alla Convenzione.** Questa sezione propone un cruscotto di sintesi che permette di condividere con l'Amministrazione il vantaggio, in termini economici, derivante dall'adesione. Il confronto è puramente economico ed è particolarmente importante per realtà complesse, quali Amministrazioni con notevoli esigenze di sicurezza o che hanno necessità di orientarsi al meglio nei contenuti della Convenzione;
- **Presentazione della configurazione dei servizi di vigilanza proposta**, che illustra le **modulazioni apportate** alla configurazione di servizio inizialmente richiesta dall'Amministrazione per mitigare i livelli di rischio e le eventuali criticità, e quindi di quanto si differenzia la soluzione proposta da quella inizialmente presa in considerazione all'interno dell'OPF.

Grazie a questa metodologia di presentazione, l'Offerente fornisce al Referente dell'Amministrazione Contraente gli strumenti necessari per compiere una scelta razionale, consapevole ed effettivamente aderente alle necessità dell'Amministrazione e dell'Obiettivo gestito.

B.2.c Struttura del PDI e relativi contenuti

Il PDI è stato strutturato come un vero e proprio strumento, nelle mani dell'Amministrazione Contraente, di supporto alle decisioni. La sua struttura è stata quindi pensata in modo da fornire un progressivo grado di dettaglio, ma anche una sintesi semplice e comprensibile capace di razionalizzare e illustrare le caratteristiche tecniche, economiche ed operative del servizio proposto, mettendolo anche a confronto con l'assetto attuale della Amministrazione, ed evidenziandone tutti gli elementi di convenienza qualitativa e quantitativa. A questo fine, rispetto alle specifiche minime di Capitolato Tecnico si prevedono importanti sezioni di sintesi e cruscotti di confronto per fornire un adeguato supporto alle decisioni.

A questo fine, rispetto alle specifiche minime di Capitolato Tecnico si prevedono importanti **sezioni di sintesi** e **cruscotti di analisi** per fornire un adeguato supporto alle decisioni. Con campitura verde sono illustrate le sezioni aggiuntive / integrative ovvero i contenuti integrativi del progetto PDI proposto, rispetto alle prescrizioni minime di Capitolato Tecnico.

Sez.	Plus	Sezione e descrizione
01		**Revisione e status PDI.** La sezione riporta il codice di revisione ed un prospetto per la rintracciabilità di tutte le modifiche intercorse per arrivare alla revisione corrente del documento, comprese eventuali variazioni dei parametri di servizio. La sezione costituisce quindi una "mappa evolutiva" del documento e permette di ricostruire la storia della sua costruzione in maniera chiara e condivisa. Sono specificati gli stati di aggiornamento **anche in funzione di eventuali Atti Aggiuntivi all'ODF.** Sono ben evidenti, inoltre, i riferimenti da contattare per delucidazioni o richieste in merito al PDI.
02		**Informazioni dell'OPF.** La sezione raccoglie tutte le informazioni generali necessarie: **(a)** sedi presso cui il servizio andrà svolto con l'indicazione dell'ubicazione degli immobili; **(b)** sintetica descrizione dei servizi richiesti e delle caratteristiche specifiche per ogni servizio; **(c)** orari di avvio e chiusura dei servizi richiesti; **(d)** informazioni su eventuali rischi specifici; **(e)** procedure interne previste per l'espletamento delle attività richieste; **(f)** altre informazioni recepite dall'Amministrazione attraverso

Sez.	Plus	Sezione e descrizione
		la documentazione aggiuntiva e integrativa proposta dall'Offerente riguardo la struttura e i contenuti dell'OPF **[→ cfr. par. B.1.b]**
03		**Executive Summary.** La sezione è pensata come una sintesi dell'offerta, pensata come una "guida di riferimento" rapido" che sintetizza tutti i punti definiti e analizzati in dettaglio nelle sezioni successive del documento. Al suo interno sono inclusi: **(a)** sintesi dello "stato di fatto", in termini di rischio dell'Obiettivo e statistiche storiche relative agli eventi criminosi occorsi; **(b)** le soluzioni di mitigazione dello stesso proposte in dettaglio all'interno del documento; **(c)** le simulazioni dello stato di rischio a valle delle configurazioni di servizio proposte.
04		**Elenco degli immobili / aree di servizio e tipologia di servizi da erogare.** La sezione contiene i dati identificativi (codifica), localizzativi (indirizzo), funzionali (destinazioni d'uso dell'obiettivo e delle sue parti) degli obiettivi, e l'indicazione dei servizi richiesti per ciascun obiettivo. *Questa sezione attiva o meno ulteriori sezioni del documento **(sez. 05 – 14)**, a seconda della qualità e quantità di servizi richiesti dalla singola Amministrazione Contraente.* La sezione contiene inoltre la descrizione dell'organizzazione e del numero di risorse individuate per l'esecuzione dei servizi. In particolare, questa sezione riporterà l'elenco dei siti (immobili/aree) oggetto del servizio, a ciascuno dei quali sarà associato un codice identificativo che sarà riportato nella scheda descrittiva del sito e sulla Mappa del Rischio allegata al PDI. L'elenco dei siti sarà formulato richiamando l'analoga elencazione contenuta nel fascicolo riepilogativo del Risk Assessment - come confermata dall'Amministrazione Contraente - al fine di garantire la stretta aderenza alle esigenze espresse dall'Ente. La scheda descrittiva del sito, desunta dalle schede compilate in sede di sopralluogo, riporterà il censimento e la descrizione qualitativa e quantitativa degli impianti di sicurezza attualmente in uso.
05		**Nominativo del Gestore del Servizio per il PDI**
06		**Personale impiegato nell'erogazione dei servizi.** La sezione presenta, articolata per servizio attivato, la descrizione del *nucleo operativo dedicato al servizio*: • Elenco generale delle risorse impiegate; • CCNL di riferimento; • Skill professionali e curricula; • Dotazioni personali; • DPI; • Dotazioni speciali; • Formazione di base; • Formazione specialistica; • Piani annuali di aggiornamento professionale.
07		**Modalità di esecuzione.** La sezione descrive in dettaglio le modalità di esecuzione dei servizi, ed in particolare: • Disposizioni di servizio per il personale; • Dotazioni tecniche del personale; • Modalità di programmazione del servizio; • Modalità di esecuzione e coordinamento; • Modalità di monitoraggio, controllo e consuntivazione.
08		**Piantonamento Fisso.** La sezione contiene le seguenti informazioni, per ciascun obiettivo su cui è richiesto il servizio: • Dettaglio delle risorse coinvolte (nucleo operativo) e caratteristiche – skill professionali; • Fasce / turni orari di servizio; • Giorni previsti settimanali di servizio; • Numero di personale GPG necessario per il servizio; • Postazioni di vigilanza fissa per giorno, singola fascia oraria e personale previsto per ciascuna fascia oraria; • Giorni e fasce orarie di apertura e chiusura degli accessi alle strutture. La sezione contiene inoltre un prospetto con le ore annue previste per singolo obiettivo, in funzione dei giorni e fasce orarie prima illustrate.
09		**Vigilanza ispettiva / ronda.** La sezione contiene le informazioni di dettaglio necessarie per l'attivazione del servizio di vigilanza ispettiva: • Obiettivi su cui è attivato il servizio; • Dettaglio delle risorse coinvolte (nucleo operativo) e caratteristiche – skill professionali; • Giorni, fasce orarie e numero di ronde giornaliere da effettuare; • Durata delle singole ronde;

Sez.	Plus	Sezione e descrizione
		• Consistenza degli equipaggi e delle pattuglie. *Per ciascun obiettivo sarà fornito anche, a valle dei sopralluoghi, anche un progetto preliminare dei waypoint di controllo ronda, e dei percorsi alternativi da effettuare per aumentare la imprevedibilità e l'effetto deterrente del servizio di ronda.*
10		**Servizio di Reperibilità e Pronto Intervento.** Sezione che illustra organizzazione e modalità del servizio di pronto intervento, con esplicito riferimento alle modalità di attivazione delle richieste (riferimenti della Centrale Operativa) e alle tempistiche di intervento garantite dall'Offerente.
11		**Procedure di emergenza.** Questa sezione del PDI descriverà le procedure che saranno seguite dal nostro personale operativo nel caso di rilevamento di illeciti, eventi dolosi, etc. Le procedure descritte riporteranno quanto illustrato nella sezione dedicata della presente Offerta tecnica.
12		**Servizi Innovativi / modalità innovative di erogazione dei servizi.** La sezione mostra una tabella sinottica che riassume, per ciascun obiettivo, con l'eventuale attivazione di servizi aggiuntivi / integrativi innovativi, quali ad esempio vigilanza con unità cinofila, vigilanza SAPR etc. Per ciascuna opzione di servizio sono espresse le seguenti informazioni: **(a)** Dettaglio delle risorse coinvolte (nucleo operativo) e caratteristiche – skill professionali; **(b)** Fasce orarie, frequenze, numero di operatori per il servizio; **(c)** Dotazioni specifiche per l'opzione di servizio; **(d)** ulteriori informazioni necessarie a definire il perimetro dei servizi innovativi di vigilanza.
12		**Censimento quali – quantitativo degli impianti.** La sezione contiene i principali dati di consistenza degli apprestamenti, nonché i riferimenti della documentazione tecnica consegnata, la definizione dello stato di funzionalità etc. necessari per la definizione del piano di centralizzazione e remotizzazione e di manutenzione straordinaria / migliorativa.
13		**Piano di integrazione e remotizzazione.** La sezione contiene il piano di centralizzazione e di remotizzazione dei segnali degli impianti per i servizi di teleallarme e teleallarme (ove previsti) **[→ cfr. par. C.2].**
14		**Proposte di manutenzione straordinaria.** Sulla base dei sopralluoghi e del censimento quali – quantitativo degli impianti, la sezione contiene le proposte di manutenzione straordinaria afferenti gli impianti. Per obiettivo e tipologia di impianto sono quindi prodotte tavole sinottiche con riferimento alla tipologia di intervento, quantità oggetto dell'intervento, benefici apportati (es. adeguamento normativo, ripristino della funzionalità, ripristino della copertura di sicurezza etc.) Per ciascun intervento è riportata la stima economica dell'intervento, e gli interventi sono ordinati per livello di priorità e per entità di investimento, così da fornire all'Amministrazione uno strumento di supporto alle decisioni efficace.
15		**Modalità di cambio appalto avvio dei servizi.** La sezione include la pianificazione dell'attività di avvio dei servizi, con la descrizione delle attività del Team di Avvio riferita all'Obiettivo e, in particolare, tutti gli accorgimenti e le procedure per garantire la continuità del servizio nel periodo di transitorio. Saranno evidenziate le procedure di passaggio delle informazioni, le modalità e le tempistiche di scambio dei dati relativi al personale per l'assorbimento, le modalità di implementazione dell'infrastruttura operativa, le modalità di presa in carico degli obiettivi al fine di garantire la continuità del servizio di vigilanza fin dal primo giorno di servizio, senza soluzioni di continuità rispetto all'avvicendamento con il Fornitore attuale (ove diverso dall'Offerente). Per quelle Amministrazioni per le quali l'Offerente risultasse operatore uscente (assenza di avvicendamento), sarà invece presentato un piano di "reboot" o **riavvio di appalto**, finalizzato a garantire la continuità operativa delle attività a fronte dell'implementazione dell'infrastruttura organizzativa, tecnica, procedurale per i servizi in Convenzione.
16		**Parte gestionale.** La sezione contiene i riferimenti a tutte le indicazioni di Capitolato Tecnico relative all'erogazione dei servizi. La sezione contiene inoltre i riferimenti a tutte le procedure di contatto e coordinamento con l'Amministrazione Contraente. Essa descriverà le modalità e procedure attraverso le quali l'Amministrazione Contraente potrà comunicare e interfacciarsi con il nostro team, sia in condizioni ordinarie che in condizioni di emergenza. Le modalità e procedure descritte saranno quelle illustrate nella sezione dedicata della presente Offerta tecnica, le quali saranno espresse in forma di agile consultazione e utilizzo da parte del personale interno dell'Amministrazione Contraente.
17		**Procedure di verifica dei livelli di servizio e azioni migliorative.** In questa sezione del PDI saranno richiamate le procedure per il monitoraggio e il controllo della qualità dei servizi di Vigilanza erogati e le modalità attraverso le quali l'Amministrazione Contraente potrà esprimere le proprie valutazioni (customer satisfaction): tali procedure saranno le stesse presentate nella sezione dedicata della presente Offerta Tecnica, le quali verranno esposte nella forma di "manuale operativo" al fine di un'agile consultazione e utilizzo anche da parte del personale non specializzato interno all'Amministrazione Contraente. In particolare, il manuale operativo illustrerà le modalità di funzionamento di Report On Line, potente funzionalità di reporting di CSC, attraverso la quale l'Amministrazione Contraente potrà,

Sez.	Plus	Sezione e descrizione
		da un lato, formulare i propri feedback in relazione alla qualità del servizio in corso, dall'altro, monitorare l'andamento del livello di rischio criminoso per i propri siti durante il periodo di svolgimento della Vigilanza.
18		**Sezione Economica.** La sezione contiene la quantificazione economica dei servizi attivati, secondo le modalità illustrate nelle sezioni precedenti. Sono evidenziati canoni e prezzi applicati, l'ammontare totale dei singoli servizi attivati e l'ammontare totale del servizio richiesto, con dettaglio per singolo obiettivo e per singolo servizio.
19		Sezione Allegati, che contiene: • **OPF originale**, con tutte le informazioni allegate e la configurazione iniziale dei servizi richiesta dall'Amministrazione Contraente; • **Risk Assessment** con mappa del rischio con individuazione geografica dei siti oggetto del servizio e dei servizi di vigilanza ad essi associati. E' presente la sintesi delle valutazioni fatte sulle singole matrici di criticità della Security con evidenza delle vulnerabilità su cui è stata effettuata la progettazione dei servizi contenuta nel PDI. Costituisce una importante traccia per il supporto alle decisioni dell'Amministrazione Contraente; • **Piano della Sicurezza**, ai sensi del D.Lgs. 81/2008 e s.m.i • **DUVRI** firmato per accettazione.

B.3. Caratteristiche e modalità operative di gestione del servizio di Call Center

B.3.a.1 Raccolta e registrazione dei dati, modalità di risposta alle richieste di informazioni

L'Offerente potenzierà il Call Center già attivo per la gestione dell'attuale convenzione, potenziandolo per migliorare ulteriormente il livello di servizio erogato. Il Call Center sarà quindi attivo fin dal primo giorno di attivazione della Convenzione fino al termine di tutti i contratti di fornitura stipulati e sarà preposto alla gestione delle comunicazioni che sopraggiungono da parte delle Amministrazioni Contraenti. A tale scopo il Call Center sarà costantemente in contatto con il Supervisore del Servizio e con il Gestore del Servizio al fine di trasmettere tempestivamente ogni segnalazione e/o reclamo effettuato dalle Amministrazioni.

Il Call Center è integrato nella struttura di Centrale Operativa, in maniera tale da gestire in maniera unitaria le comunicazioni e le richieste e attivare rapidamente la risposta organizzativa a fronte di emergenze, situazioni anomale, richieste di servizio dei Referenti delle Amministrazioni Contraenti.

Durante la fase iniziale della Convenzione il Call Center ha il ruolo di supportare la Funzione Comunicazione e Convenzionamento, soprattutto per organizzare e coordinare le fasi di sopralluogo e contatto con i Referenti delle varie Amministrazione, e per gestire eventuali richieste multiple. I flussi di dati sono completamente integrati nella piattaforma informativa CSC (Civis Security Cloud) e il contenuto di ciascuna singola richiesta è richiamabile ed elaborabile degli Utenti abilitati grazie alle avanzate funzionalità di reportistica della piattaforma (Report On Line di CSC).

Il Call Center è composto da addetti operativi in grado di gestire i flussi di chiamata e le richieste d'intervento, attraverso sia l'utilizzo del mezzo telefonico, con un **Numero Verde Dedicato** messo a disposizione della Convenzione che gli altri canali/strumenti quali indirizzi email, fax etc. Fulcro dell'organizzazione tecnica- operativa del servizio di Vigilanza è la **Centrale Operativa, attiva 24 ore su 24,** poiché in essa convergono tutte le informazioni necessarie per la supervisione costante del lavoro delle GPG e per la gestione dei sistemi di sicurezza delle Amministrazioni. Pertanto è strutturata per permettere il costante e ininterrotto collegamento con i siti sorvegliati, con le singole Sedi Operative dell'Offerente e con le Centrali Operative delle Forze dell'Ordine. La Centrale Operativa riceve il segnale d'allarme e le segnalazioni d'intervento per potenziali eventi criminosi in atto e provvede a:

- acquisire i dati completi relativi all'Amministrazione e al sito;
- acquisire tutte le informazioni a corollario della richiesta d'intervento;
- inviare in forma automatica la richiesta d'intervento alla Sede Operativa competente per territorio, che provvede tempestivamente ad attivare le pattuglie.

Il Call Center sarà ubicato fisicamente presso la Centrale Operativa della Sede Centrale di CIVIS S.p.A., ubicata a Milano in via Piero della Francesca 45, attiva 24/24h per 365 gg/anno dalla data di attivazione della Convenzione al termine di tutti i contratti di fornitura stipulati, incaricata della gestione delle comunicazioni che sopraggiungono da parte dell'Amministrazione.

Gli addetti del Call Center, si occupano inoltre di rispondere alle varie Amministrazioni interessate ad aderire alla Convenzione o a fornire informazioni in merito ai servizi e alle caratteristiche o alle modalità di adesione, svolgendo anche una funzione di promozione della Convenzione con il supporto dell'Area Comunicazione e Convenzionamento.

Data l'integrazione del sistema di gestione del Call Center nella piattaforma CSC, il servizio di Call Center può gestire flussi di comunicazione multicanale, aggiungendo all'utilizzo del mezzo telefonico (Numero telefonico verde dedicato) altri strumenti/canali di comunicazione quali il Portale Web dedicato, la posta elettronica (indirizzo e-mail dedicato), la messaggistica su telefoni cellulari (SMS), il numero fax dedicato, etc. Il Call Center si configura, quindi, come la prima interfaccia tra Amministrazione Contraente e l'Offerente per lo scambio informativo inerente le richieste o le segnalazioni. Esso ha la caratteristica di tracciare tutte le comunicazioni pervenute con i relativi contenuti.

Esso è pertanto è un ottimo strumento in mano all'Amministrazione per uno scambio di informativo chiaro e trasparente.

Considerando gli ottimi risultati ottenuti nella presente Convenzione, anche per la nuova edizione l'Offerente intende utilizzare un'applicazione **integrata alla piattaforma CSC** per la gestione del sistema di Call Center, considerata oggi uno dei prodotti leader sul mercato della gestione di Call Center.

All'arrivo di una chiamata di Call Center, se il numero è in chiaro il sistema identifica il chiamante e attiva l'applicazione in dotazione all'operatore con le informazioni necessarie per gestire la chiamata in corso. Tale funzionalità si basa sull'identificazione lato Call Center del chiamante o della richiesta che il chiamante specifica attraverso la composizione di codici numerici sulla tastiera del telefono. Identificato il motivo della chiamata la funzionalità di Call Center passa tali informazioni e permette la gestione e registrazione della chiamata. L'operatore può gestire i ticket e i moduli per la registrazione e attivazione delle richieste (es. richieste di pronto intervento, comunicazioni di disagi o lamentele etc.)

In questo modo l'operatore prima di rispondere ha già disponibile il quadro completo della richiesta in corso minimizzando i tempi di risposta e aumentando il livello del servizio.

L'organizzazione dell'Offerente si impegna a garantire la risposta diretta dell'operatore telefonico entro un numero di squilli inferiore rispetto ai 5 squilli (≤ 4 squilli).

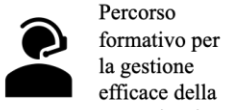
Il sistema è inoltre dotato, grazie all'integrazione con la base dati di CSC, di tutti i dati relativi ai singoli Utenti abilitati che possono generare richieste, quali ticket di reclamo, segnalazioni, richieste etc.

Sulla Home Page di ciascun Utente dell'Amministrazione è presente un **cruscotto di accesso rapido** alle comunicazioni, che permette di compilare i *ticket* online di CSC molto rapidamente: il sistema **completa i campi di identificazione** dell'utente in maniera automatica e velocizza l'acquisizione la raccolta e la registrazione dei dati relativi alla segnalazione.

L'Utente abilitato deve solo concentrarsi sulla descrizione della richiesta. La stessa funzionalità può essere utilizzata anche dal personale di Call Center: con il solo inserimento del nome e cognome del Referente, infatti, il ticket compilato dal personale di Call Center è automaticamente compilato con le informazioni identificative, facendo risparmiare tempo ed eliminando gli errori, specialmente considerando richieste multiple e contemporanee da parte di più Amministrazioni.

Notevole anche l'impegno dell'Offerente per ottimizzare le modalità di risposta alle richieste di informazioni. La correttezza delle modalità di risposta dipende soprattutto, data l'elevata importanza della relazione umana presente, dalla competenza dell'operatore telefonico. L'Offerente ha quindi definito una serie di soluzioni progettuali:

- Ogni Amministrazione / Referente sarà assegnato, ove possibile, costantemente ad una rosa di addetti di Call Center, in maniera tale da sviluppare un rapporto di fiducia e di familiarizzazione che consentirà agli operatori di sapere già, per l'interlocutore, la migliore modalità di approccio, le necessità e le peculiarità dell'Amministrazione;
- Tutti gli addetti di Call Center saranno aggiornati in fase di avvio appalto attraverso un corso pratico di tecniche di reception e comunicazione telefonica, che ha lo scopo di aumentare la capacità di comunicare efficacemente e di utilizzare al meglio il telefono e tutti gli strumenti di comunicazione che costituiscono il Call Center.
- Tutti gli operatori saranno, per tutta la durata dell'appalto, costantemente aggiornati sui contratti in essere e dotati di un apposito strumento che associa al contratto ed al servizio la sede operativa da contattare, in modo tale da smistare sempre correttamente le chiamate;
- Tutti gli addetti saranno inoltre formati alle procedure di definizione della priorità delle richieste, in maniera tale da applicare sempre algoritmi decisionali omogenei alla valutazione delle richieste ed alle segnalazioni.
- Tutti gli addetti al Call Center saranno formati mediante un corso di comunicazione efficace, al fine di affrontare con competenza e professionalità la gestione telefonica dei propri utenti. Obiettivo del corso è quello di far conoscere e apprendere ai nostri operatori tecniche in grado di prevenire l'accumulo di tensioni e di gestire lo stress. Il percorso didattico, più che sulla trattazione teorica, è centrato infatti su esercitazioni guidate e sulla relativa analisi dei feedback per poter, in autonomia, utilizzare strumenti funzionali a gestire stati d'ansia, sintomi o disturbi che spesso condizionano il normale svolgimento della vita lavorativa.



1. Presa di contatto: creare un rapporto favorevole dai primi minuti;
2. Le fasi della comunicazione telefonica: ascoltare, domandare, comprendere, esporre;
3. La cura degli aspetti vocali: sottolineature, tono, ritmo, pause;
4. Usare il linguaggio appropriato con le tecniche neurolinguistiche;
5. Saper "leggere" il cliente e le diverse tipologie di atteggiamento della clientela;
6. Il dialogo telefonico: limiti e peculiarià, la precisione del linguaggio, i vantaggi dell'ascolto assertivo, la
7. tecnica delle domande;
8. Saper gestire le obiezioni: il supporto dell'utilizzo del meta-modello della Programmazione Neuro Linguistica (PNL);
9. Lo sviluppo efficace della telefonata;
10. Esercitazioni sul respiro;
11. Tecniche di rilassamento e gestione dello stress;
12. La fantasia guidata, la visualizzazione e la ristrutturazione cognitiva.

Figura 18 Percorso formativo degli operatori di Call Center per la gestione efficace della comunicazione

Grazie a tutti questi strumenti l'operatore di Call Center potrà far fronte in maniera efficace e soddisfacente alle richieste di informazioni dei Referenti delle Amministrazioni Contraenti.

B.3.a.2 Criteri di valutazione delle segnalazioni pervenute

Per aumentare la copertura di sicurezza delle Amministrazioni Contraenti, l'Offerente intende proporre, come già accennato, a titolo di elemento migliorativo del servizio, un **sistema di reperibilità di primo livello**, gestito dal personale del Call Center, implementato attraverso una **sezione dedicata di CSC**, con *moduli elettronici* o *"ticket"* che permettono al personale di recepire le richieste e di registrare l'esigenza di intervento.

Le funzionalità di gestione dei ticket includono l'approccio *active directory*, ossia il completamento dei dati del richiedente (generalità, ruolo, privilegi di accesso alle procedure di segnalazione, obiettivi di riferimento, etc.) in maniera automatica.

Gli operatori si occupano innanzi tutto della gestione delle richieste d'intervento straordinario provenienti dalle Amministrazioni Contraenti, nonché delle richieste di manutenzione correttiva e straordinaria riguardanti gli impianti anti-intrusione e gli elementi tecnici interessati da eventi di security / safety, che comportano scopertura nel livello di sicurezza assicurato agli obiettivi. A tal proposito risulta essere di fondamentale importanza la giusta associazione del livello di priorità in funzione della richiesta al fine di garantire durante tutta la durata dell'appalto il corretto e continuo funzionamento degli apprestamenti. Al livello di priorità sono infatti associati:

- il relativo tempo massimo d'intervento entro cui il personale raggiunge l'Obiettivo (TMO)
- il tempo massimo di ripristino delle condizioni di sicurezza (TMR)

Pertanto, come illustrato nel precedente paragrafo, gli addetti del Call Center saranno adeguatamente formati in merito alla definizione del livello di priorità in funzione delle varie situazioni che possono verificarsi. Inoltre, come anticipato, sarà predisposta un'apposita procedura per la corretta associazione del livello di priorità in funzione della tipologia di guasto, mal funzionamento o di evento di security comunicato dall'utente chiamante.

Il sistema gestisce una procedura guidata per l'individuazione della tipologia di richiesta e nella valutazione del livello di urgenza:

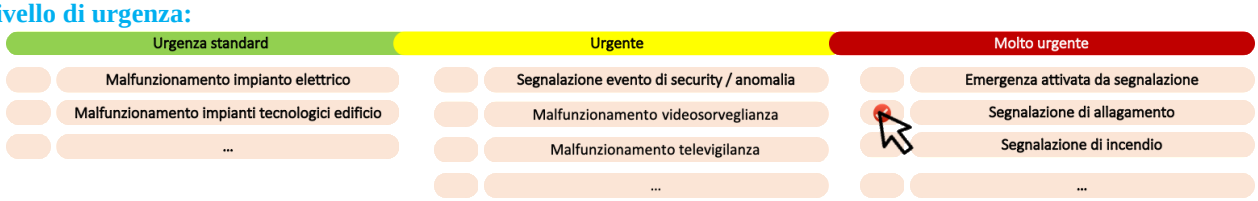


Figura 19 Modalità di valutazione delle segnalazioni / richieste e per l'individuazione dei livelli di urgenza / priorità delle richieste

Questa funzionalità è **integrata dal prontuario**, definito seguendo le indicazioni e prescrizioni dell'Amministrazione Contraente, in particolare per quanto attiene l'integrazione del processo di reperibilità con i **piani di emergenza dell'Amministrazione stessa**.

Le segnalazioni molto urgenti sono gestite direttamente dalla Centrale Operativa, nell'ottica di una gestione specialistica ma rispettosa delle procedure di sicurezza.

All'interno di CSC gli operatori possono accedere alla lista dei reperibili, sia dell'Offerente sia dell'Amministrazione (servizi tecnici e Terzi, quali imprese di manutenzione, pulizie, etc.), in maniera tale da poter attivare con celerità, in base alla segnalazione pervenuta, la competenza più adeguata. All'interno della propria Home Page, l'utente dell'Amministrazione Contraente può accedere sulla propria Home Page alla griglia delle segnalazioni aperte per le quali è stato richiesto un servizio di reperibilità di primo livello, ordinate per priorità e per data. Per ciascuna è fornito il monitoraggio dello stato (aperta, in lavorazione, chiusa, etc.) in maniera tale da fornire il "colpo d'occhio" sullo stato delle richieste.

In particolare, in funzione dello specifico Obiettivo saranno indicati gli apprestamenti in esso installati e l'indicazione dei potenziali accadimenti in funzione del livello di priorità in uno schema facilmente consultabile dall'addetto. Nel caso in cui si verifichi un evento particolare, che esula le conoscenze e l'esperienza dell'operatore o non riportato nella suddetta procedura, l'addetto stesso provvede a contattare immediatamente le Funzioni di Staff e la Funzione Security Management per ricevere tempestivamente il necessario supporto per l'associazione del corretto livello di priorità, lo riporta nell'apposita sezione del Sistema Informatico ed avvia la procedura corrispondente. **Di seguito uno stralcio dell'algoritmo di selezione della priorità per le segnalazioni urgenti [→ cfr.** Figura 19**, afferenti a gusti o anomalie degli impianti tecnologici gestiti dall'Offerente (sistemi di centralizzazione, remotizzazione) e facenti parti delle contromisure tecnologiche necessarie per garantire il livello di sicurezza ottimale agli obiettivi:**

Situazione e descrizione	Potenziali accadimenti (esempi)	TMO	TMR
Urgente con situazione di emergenza. Tipico di situazioni che possono mettere a rischio l'incolumità delle persone e/o possono determinare l'interruzione delle normali attività lavorative.	Mancata disattivazione sistema anti-intrusione. Mancata comunicazione con Centrale Operativa e off line sistemi.	**< 1 ora**	**< 3 ore**
Urgente con avaria di elevata gravità. Tipico di situazioni che possono pregiudicare in modo significativo le condizioni ottimali di svolgimento delle normali attività.	Mancato o difettoso funzionamento di telecamera la cui area di ripresa non sia ridondata / coperta. Mancato o difettoso funzionamento di sensori anti-intrusione.	**< 2 ore**	**< 4 ore**

Situazione e descrizione	Potenziali accadimenti (esempi)	TMO	TMR
Urgente con avaria di media gravità. Tipico di situazioni che possono pregiudicare le condizioni ottimali di svolgimento delle normali attività lavorative	Mancato o difettoso funzionamento di telecamera la cui area di ripresa sia ridondata / coperta. …	**< 4 ore**	**< 6 ore**
Non urgente.	Tutti gli altri casi.	**24 ore**	**48 ore**

B.3.a.3 Procedure di comunicazione delle segnalazioni alle Autorità Competenti

L'Utente dell'Offerente e quello dell'Amministrazione Contraente possono comunicare indifferentemente con il Call Center attraverso fax, telefono, e-mail, mobile, secondo le procedure e i livelli autorizzativi stabiliti.

La gestione delle comunicazioni è realizzata con procedimenti che consentano, in qualsiasi momento, la loro precisa conoscenza e tracciatura, con riferimento alle seguenti informazioni, specifiche in funzione della tipologia di comunicazione:

- Numero della richiesta;
- Data e ora della richiesta;
- Richiedente; ▪
- Numero identificativo dell'OPF;
- Priorità;
- Obiettivo, ambienti ed apprestamenti per i quali è stato richiesto l'intervento;
- Stato della richiesta (aperta, chiusa, assegnata, sospesa etc.);
- Tipi e categorie di lavoro interessate dagli interventi.

A seguito della ricezione della chiamata o della comunicazione attraverso altri canali, l'operatore del Call Center codifica la comunicazione in funzione delle seguenti tipologie:

[A] Richiesta d'intervento di Manutenzione correttiva;
[B] Richiesta di altra Attività Straordinaria;
[C] Richiesta di informazioni relative alle richieste di cui ai punti a) e b);
[D] Sollecito;
[E] Reclamo;
[F] Richiesta di informazioni sui Servizi oggetto della Convenzione/ODF.

L'operatore inserisce quindi la comunicazione in CSC nell'apposito modulo "Gestione richieste d'intervento" compilando tutti campi richiesti e, qualora necessario aprendo il relativo ticket.

Nel caso in cui si tratti di **richiesta di informazioni** (caso c ed f) generalmente sarà direttamente l'operatore in grado di rispondere esaustivamente alla richiesta, in quanto ampliamente formato su tutti gli aspetti della Convenzione e dotato di specifici strumenti di supporto.

In caso di richieste particolarmente tecniche o complesse l'addetto contatta il Gestore del Servizio specifici in funzione dell'OPF connesso alla richiesta, ottiene le informazioni necessarie a soddisfare quanto richiesto dall'utente dell'Amministrazione e lo ricontatta o lo fa ricontattare direttamente dal Gestore.

Nel caso di **richiesta d'Intervento di Manutenzione correttiva**, l'addetto, di concerto con l'Amministrazione Contraente, apre il relativo ticket ed assegna il livello di priorità dell'intervento, in funzione del quale si avvia il relativo **processo autorizzativo** (processo autorizzativo degli interventi urgenti o degli interventi non urgenti). L'addetto provvede subito a contattare il Gestore del servizio agli apprestamenti specifico per quel contratto che a sua volta attiva i reperibili in caso di intervento urgente o provvede all'effettuazione del sopralluogo ed alla redazione del preventivo di spesa con il supporto degli Assistenti di coordinamento tecnico, in caso di intervento non urgente. In particolare, a ogni segnalazione, dopo la presa in carico del problema e la definizione del livello d'urgenza, il Gestore informa direttamente l'Amministrazione Contraente e il tecnico incaricato circa la data e ora di sopralluogo e/o intervento, e assegna la richiesta al tecnico che provvede alla risoluzione della problematica. L'unità competente, concluso tecnicamente l'intervento, effettua la **chiusura del Ticket** fornendo conseguentemente un feedback di conferma della risoluzione della richiesta all'Utente Richiedente, e compila la **Scheda consuntivo Manutenzione correttiva**.

In caso di emergenze che sopraggiungano in orari notturni o durante giorni festivi, il personale del Call Center provvede a chiamare gli addetti dei vari servizi coinvolti (vigilanza attiva, passiva, apprestamenti) reperibili 24/24h, sulla base dell'elenco sempre a disposizione.

Stesso processo si segue nel caso in cui la richiesta d'intervento viene inserita dall'utente dell'Amministrazione Contraente direttamente attraverso il Sistema Informatico, e della quale il Call Center riceve la notifica immediata via mail oltre che a video. In caso di **richiesta di altra Attività Straordinaria**, l'operatore contatta direttamente il Gestore del servizio di competenza in funzione sia dell'Obiettivo (quindi dell'OPF) sia del servizio in relazione al quale è richiesta l'Attività straordinaria e si avvia il relativo **processo autorizzativo delle Attività straordinarie**.

Anche in caso di ricezione di **reclami** o **solleciti** il Call Center contatta immediatamente il Gestore del Servizio competente che provvede a risolvere quanto segnalato dall'Amministrazione. Si precisa che il Gestore del Servizio sarà sempre a conoscenza di tutte le comunicazioni ricevute dal Call Center per gli ODF di sua competenza, attraverso l'invio di un'e-mail contenente tutte le informazioni necessarie connesse alla specifica comunicazione.

B.3.a.4 Strumenti di supporto per l'erogazione del servizio di Call Center

Attraverso il supporto del Sistema Informatico, che registra tutte le informazioni e i dati relativi alle comunicazioni intercorrenti tra Amministrazione Contraente e l'Offerente, è possibile avere a disposizione informazioni strutturate relativamente ai servizi oggetto dell'appalto sotto forma di *dashboard*, tabelle e grafici statistici in funzione dei vari aspetti, come ad esempio:

- tipologia di comunicazione;
- livello di priorità;
- motivo della richiesta.
- esito della Customer Satisfaction "a caldo".

Inoltre, è possibile monitorare lo stato della richiesta attraverso l'apposita sezione (Cruscotto sulla *Home Page* di CSC) che indica in funzione dello specifico ticket lo stato ed il grado di soddisfazione del richiedente mediante la **Customer Satisfaction a caldo** che consente di inserire un giudizio sull'intervento effettuato.

La valutazione dell'intervento è, infatti, sempre l'ultimo step di qualsiasi richiesta, sulla base delle quali fare poi le necessarie analisi statistiche e qualitative.

Il Call Center consente la gestione completa del processo legato alla creazione, gestione e consuntivazione di richieste d'intervento, richieste di altra Attività Straordinaria, solleciti, reclami e richieste d'informazioni, garantendo in particolare:

- la possibilità di inserire la comunicazione ricevuta, con registrazione di tutte le informazioni richieste;
- la possibilità di verificare lo stato degli interventi, con riferimento alla specifica richiesta;
- la gestione della stampa della eventuale Scheda Preventivo / Consuntivo Intervento;
- la possibilità di inserimento di un giudizio sull'intervento effettuato e di segnalazione di avvenuto intervento al richiedente (Customer Satisfaction a caldo);
- l'attribuzione di livelli di priorità alle singole richieste consentendo quindi di gestire le priorità di svolgimento e di monitorare il rispetto dei livelli di servizio attesi;
- la compilazione dei rapporti d'intervento, con eventuali documenti allegati.

Attraverso il Sistema Informatico è quindi possibile gestire tutti i dati relativi allo scambio di comunicazioni tra Amministrazione Contraente e Offerente, nonché tutte le informazioni necessarie alle attività su richiesta.

Infine per quanto riguarda la registrazione audio delle comunicazioni telefoniche, effettuate previa informativa alla controparte e nel rispetto delle disposizioni previste dalla normativa vigente, saranno **rintracciabili direttamente dal Sistema Informatico attraverso apposito link**, così come per tutte le comunicazioni ricevute attraverso un qualunque canale di comunicazione.

C. Metodologie tecnico – operative per lo svolgimento ed il controllo dei servizi operativi

C.1. Metodologie tecnico operative per l'esecuzione dei servizi di vigilanza

C.1.a Servizi di piantonamento fisso

Le procedure e le metodologie operative del servizio sono integrate nella innovativa struttura informativa **Security 4.0** sviluppata dal Gruppo CIVIS. La disponibilità di funzionalità specifiche pensate per documentare e condividere le informazioni sul servizio permettono una gestione digitale del servizio, capace di accrescerne l'efficacia.

C.1.a.1 Integrazione informativa delle procedure e strumenti a supporto OSCURATO

Figura 20 Applicazioni per la digitalizzazione delle procedure

C.1.a.2 Metodologie e procedure operative per la gestione del servizio

Nei seguenti paragrafi sono illustrate le logiche e le modalità di gestione del servizio di piantonamento fisso, attraverso la descrizione della programmazione, esecuzione, coordinamento, monitoraggio, controllo e consuntivazione di ogni singola fase del servizio, nel contesto della digitalizzazione prima illustrato. Esso prevede la presenza costante e continuativa, entro definite fasce orarie e sviluppi di turno, di Guardie Particolari Giurate (GPG) presso l'Obiettivo, con finalità di deterrenza e controllo antintrusione e sorveglianza.

C.1.a.2.1 Fase di programmazione

L'approccio alla programmazione del servizio è **completamente integrato all'interno del Sistema informativo**. A seguito della presa in consegna dell'Obiettivo attraverso la sottoscrizione del primo Verbale di consegna, nel caso di attivazione del servizio di piantonamento fisso, il Gestore del Servizio con il supporto della Funzione Pianificazione e Programmazione programma le attività, predisponendo documenti di pianificazione che identificano l'attività da eseguire e il personale incaricato. La programmazione viene quindi effettuata a livello di singola Unità di Gestione e centralizzato su Lotto, in maniera tale da tenere conto di eventuali saturazioni di risorse condivise all'interno delle aree territoriali (attrezzature, mezzi, etc.) e, soprattutto, da rendere più efficienti le modalità di **"rotazione programmata"** delle risorse adibite allo svolgimento del servizio.

Le modalità operative di programmazione prevedono infatti l'utilizzo del "gruppo di lavoro allargato", costituito da personale titolare e personale di sostituzione, per cui il personale viene fatto progressivamente ruotare.

L'esperienza dimostra infatti che la familiarizzazione delle risorse con l'Obiettivo può portare ad un "rilassamento" delle procedure di sicurezza, aspetto da evitare per mantenere un alto standard di sicurezza dell'Obiettivo. Per garantire personale sempre formato e con un'adeguata conoscenza dell'Obiettivo, tuttavia, si adotta un procedimento **di "rotazione**

diluita", progressiva, variando il nucleo operativo dedicato all'Obiettivo in maniera graduale a seconda delle esigenze fra i vari Obiettivi assegnati al Gestore del Servizio.

La modalità di rotazione progressiva permette di rispettare l'obiettivo della stabilità del gruppo di lavoro, ma al contempo di raggiungere quello di avere a disposizione con continuità personale formato e familiarizzato con gli ambienti e le peculiarità dei vari obiettivi.

Le fasce orarie e le risorse in turno per fascia e postazione sono dei dati di progetto, in quanto rispondono alle esigenze dell'Amministrazione. La procedura di programmazione del servizio tiene conto di:

- postazione di servizio in relazione all'**indice di rischio** (minaccia, vulnerabilità, livello di impatto, ubicazione territoriale dell'Obiettivo);
- fascia oraria di presidio;
- presenza e qualità di apprestamenti tecnologici (control room locale, antintrusione, controllo accessi, TVCC, etc.);
- numero di GPG necessarie a coprire il servizio, con i relativi **vincoli** in termini di **rispetto del CCNL** di riferimento (orari, ore straordinarie, ore di riposo, rischio ambientale, stress psicologico, altre criticità, etc.) e di formazione o competenze in relazione a mansioni e postazioni di servizio (es. utilizzo di attrezzature radiogene, gestione di Control Room, etc.);
- contesto ambientale (aree esterne, locali interni, presenza di grandi afflussi di persone, rischi per la salute nel contesto lavorativo, infrastrutture tecniche, etc.);
- tipologia di attrezzature necessarie, oltre alle normali dotazioni (DPI, sistemi manuali / automatici per l'inoltro chiamate d'emergenza, sistemi speciali di comunicazione, dotazioni specialistiche, etc.);
- tasso di indisponibilità del personale, per ferie, malattie, permessi.

Con **frequenza mensile** il Gestore del Servizio condivide con il Referente dell'Amministrazione il Programma Operativo dei Servizi (POS). Il POS è aggiornato con frequenza settimanale, o ogni qualvolta il Referente faccia una richiesta di variazione.

Le funzionalità di programmazione aggiornano in tempo reale gli ordini di servizio relativi a ciascuna GPG e le trasmettono in tempo reale ai singoli addetti, grazie all'applicazione CIVIS.TEAM.

Oltre alla programmazione "ordinaria", il Gestore del Servizio completa, con il supporto dei Coordinatori operativi GPG di obiettivo, anche la sezione dedicata alle **attività straordinarie** all'interno del POS, attraverso riunioni di coordinamento con i Referenti dell'Obiettivo e dell'Amministrazione Contraente (es. ufficio security dell'Amministrazione contraente). **L'Obiettivo può infatti essere interessato da eventi imprevisti, vincoli operativi, eventi particolari che possono comportare un'estensione delle fasce orarie in cui può essere richiesta la presenza di personale, oppure può subire un'elevazione del livello di rischio, per cui l'Amministrazione può richiedere un maggior numero di personale, ad esempio in particolari fasce orarie.** Il Gestore del Servizio svolge contestualmente la programmazione delle attività straordinarie, verificando che l'importo a consumo abbia la necessaria capienza per le attività di vigilanza fissa richieste. Alla fine del confronto, è disponibile **un POS "in bozza",** da ottimizzare attraverso il **successivo livello di programmazione**. La programmazione a livello centralizzato è effettuata dalla **Funzione Pianificazione e Programmazione,** che centralizza le programmazioni e le richieste di risorse da parte di tutti i Gestori del Servizio. In tal modo è possibile conseguire i seguenti obiettivi:

- **precisa programmazione** delle risorse condivise (dotazioni, attrezzature per l'esecuzione del servizio, competenze del personale) sul territorio del Lotto;
- **rotazione sistematica** delle risorse in maniera tale da limitare la "familiarizzazione" con il sito ed evitare il fenomeno di "rilassamento" delle procedure di sicurezza.

Grazie a quest'approccio alla programmazione, l'Offerente è in grado di offrire una programmazione del periodo del servizio **affidabile** rispetto a eventuali eventi o variazioni. Infatti, il fabbisogno di personale, di dotazioni e/o di attrezzature è analizzato e definito a livello centralizzato, permettendo un più veloce ed efficiente processo di acquisizione di quanto necessario. A questo punto il POS, con la relativa programmazione delle risorse necessarie per la sua esecuzione effettuata a livello centralizzato, può essere proposto al Supervisore.

Nel caso di eventi imprevisti o particolari necessità dell'Amministrazione, la procedura di programmazione è ripetuta, aggiornando il POS con i nuovi dati e i nuovi impegni relativi alle attività straordinarie aggiunte.

L'intero processo di programmazione è completamente supportato dalle funzionalità di pianificazione dei servizi del sistema informativo.

C.1.a.2.2 Fase di esecuzione e di coordinamento del servizio

Durante la fase di **esecuzione e di coordinamento del servizio**, le GPG svolgono le attività previste all'interno del Capitolato Tecnico per quanto concerne i servizi attivati.

Le procedure operative sono accessibili all'interno di **CIVIS TEAM,** ai fini della consultazione anche in casi di particolare urgenza o stress emotivo, sui PC di postazione, tablet PC o smartphone in dotazione.

I dispositivi consentono di accedere da remoto a tutte le sezioni del Sistema informativo e a tutta la documentazione relativa alle procedure operative previste. Le procedure sono ordinate in maniera da essere velocemente consultabili e sono descritte in maniera semplice, così da risultare intellegibili anche in particolari situazioni di stress emotivo. La fase di esecuzione prevede due tipologie di attività, di seguito descritte:

- vigilanza fissa della **Control Room** locale presso l'Obiettivo, ove esistente;

- vigilanza fissa **di presidio** da parte delle GPG.

Di seguito sono illustrati i principali elementi metodologici e procedurali delle due tipologie individuate.

Vigilanza fissa della Control Room locale presso l'Obiettivo

La Control Room locale, ove prevista dall'Amministrazione Contraente, costituisce il punto fisico di controllo e coordinamento dell'intero servizio di vigilanza. L'operatore in turno opera secondo due modalità.

Modalità operative anticrimine. Il personale in turno attiva e verifica l'avvenuto inserimento / disinserimento degli impianti negli orari stabiliti. L'attività prevede il costante controllo dello stato di funzionamento delle periferiche di comunicazione dati (periferiche che permettono il collegamento tra gli impianti di sicurezza e la Centrale Operativa / sale operative dell'Offerente attraverso prove di comunicazione). In particolare, effettua i controlli su presenza/assenza di rete, basso livello di batteria, attivazione/disattivazione, anomalia, etc.). Riguardo gli impianti di videosorveglianza, la procedura operativa prevede il controllo costante, mediante il sistema di videosorveglianza, delle aree a maggiore rischio (parcheggi, accessi, aree/locali sensibili, etc.). Il personale ha anche il compito di rispettare e far rispettare le procedure di acceso alle immagini dei sistemi TVCC sia in funzione "live" che "in registrazione", nel rispetto del D.Lgs. 196/03. Per mantenere alto il livello di attenzione durante il servizio, l'operatore di Control Room ha la responsabilità, fra i compiti pianificati, di effettuare periodicamente l'appello radio alle GPG in servizio sull'obiettivo e di verificare la regolarità e la tempestività operativa del servizio.

Durante l'esecuzione del servizio, le GPG dedicate al servizio compilano il *Registro delle Attività di Control Room*, grazie all'applicazione CIVIS.GATE. Grazie alla gestione digitalizzata è possibile segnalare in maniera chiara e tracciata eventuali anomalie e punti di attenzione al personale dei turni successivi.

All'interno del documento sono infatti registrati tutti gli eventi, le disposizioni, le attività giornalmente svolte, con relativo esito e dettaglio informativo (data, ora, tipo di evento, nominativi del personale coinvolto, esito).

In caso di allarme, il personale di Control Room in turno comunica con le GPG in servizio all'interno della struttura vigilata attraverso i dispositivi di comunicazione in dotazione e, ove necessario, con la Centrale Operativa per richiedere il supporto operativo di autopattuglie esterne in caso di necessità.

Il personale di Control Room fa anche da perno di coordinamento della gestione dell'evento di allarme, supportando la GPG intervenuta. Il personale di Control Room ha la possibilità di ricevere i segnali di allarme in caso di guasto degli impianti di sicurezza, attivando le relative procedure d pianificate in fase di attivazione del servizio. In particolare, il personale attiva immediatamente il Gestore del Servizio ed il Coordinatore operativo, per attivare i servizi di emergenza sostitutivi previsti in caso di guasto/danneggiamento degli impianti di controllo accessi, antintrusione, TVCC.

In caso di eventi di emergenza sanitaria, l'Operatore di Control Room attiva il 118. Ulteriore ruolo di coordinamento è assunto nei confronti di conclamate situazioni di emergenza (incendio, allagamento, catastrofe naturale, incidenti, esplosioni, attentati): la Control Room opera in stretto contatto con il Responsabile del Piano d'emergenza dell'Amministrazione Contraente e richiede l'eventuale intervento dell'Autorità Giudiziaria, delle Forze di Polizia o dei Vigili del Fuoco, ove ritenuto opportuno e indispensabile.

Modalità operative antinfortunistiche. L'attività operativa di Control Room è di supporto anche al Servizio di Sicurezza e Protezione dell'Amministrazione Contraente, in materia di sicurezza nei luoghi di lavoro (D.Lgs. 81/08). In particolare la centralizzazione delle informazioni permette all'operatore di turno di fornire le seguenti prestazioni:

- **gestire le segnalazioni di allarme** provenienti dagli impianti tecnologici di servizio (antincendio, allagamento, allarme ascensori, guasti al sistema di climatizzazione, blackout energetici, guasti ai quadri elettrici, etc.);
- **segnalare eventuali problematiche** e/o danni riscontrati su strutture/dotazioni di protezione quali: estintori, scale di emergenza, maniglioni antipanico, pannelli segnaletici, etc.;
- **fornire supporto operativo**, tramite le autopattuglie, in caso di emergenza (emergenza sanitaria, incendio, allagamento, etc.);
- **contattare il personale in stato di reperibilità**, fuori dell'orario di lavoro e nei giorni festivi, in caso di guasti, manutenzioni straordinarie, etc.

Vigilanza fissa di presidio

La Vigilanza fissa di presidio è supportata dalla Control Room o, se questa non è presente all'interno dell'Obiettivo, dalla Sala Operativa territoriale di competenza dell'Offerente. Le GPG "in campo" hanno la responsabilità di posizionarsi in modo continuativo presso la propria postazione, ove spesso è collocato un terminale di controllo dei sistemi tecnologici di sicurezza (es. ingressi agli edifici o ai parcheggi). Il personale lascia la propria postazione solo in caso di emergenza e solo previa autorizzazione del Coordinatore operativo. Se è presente la Control Room, occorre l'autorizzazione del personale al suo interno e del Coordinatore operativo. Se non è presente la Control Room, occorre l'autorizzazione della Centrale Operativa.

Il personale ha la responsabilità di registrare la propria presenza con la procedura informatizzata di CIVIS WATCH e la scansione dei tag NFC che designano ogni singola postazione di piantonamento degli obiettivi. Lo stesso è fatto nel caso di effettuazione di ronde e/o controlli, designando le aree mediante i tag installati presso i punti di controllo e le aree sensibili degli obiettivi.

Fondamentale è il ruolo nella gestione degli accessi, con movimentazione delle chiavi per l'accesso ai locali, in particolare, per le attività di soggetti terzi, incaricati delle pulizie o delle manutenzioni tecnologiche dell'Obiettivo. All'apertura dell'Obiettivo, la GPG disattiva il sistema antintrusione ed effettua un controllo (bonifica) su tutte le aree ed

i locali esistenti (interni ed esterni) mediante il sistema di videosorveglianza, ove esistente, oppure con un giro di ronda. La GPG ha anche il compito di fornire informazioni ai visitatori (fornitori, operai o tecnici) verificandone l'autorizzazione all'accesso. Durante il proprio turno la GPG ha la responsabilità di gestire gli eventi di allarme rilevati dalla propria postazione o segnalati dalla Control Room / Sala Operativa. In costante contatto radio con la Control Room / Sala Operativa, l'operatore può inoltre operare sull'impianto di videosorveglianza ove presente dalla propria postazione, rispettando le disposizioni in materia di privacy nell'uso dei sistemi TVCC e della documentazione cartacea in genere. Alla chiusura dell'Obiettivo, la GPG attiva il sistema antintrusione. Verifica inoltre che gli ascensori non siano in blocco e che siano tutti liberi. Effettua, poi, periodiche ronde interne dei locali (con frequenze temporali non ripetitive) alternandosi con altre GPG (ove previste), verificando che non vi siano situazioni di pericolo, porte aperte, tentativi di effrazione, allagamenti, principi di incendio.

I passaggi sono documentati attraverso specifiche **letture di controllo presso i tag NFC** mediante gli apparati in dotazione e l'utilizzo dell'app CIVIS WATCH.

In caso di qualsiasi anomalia o allarme, la GPG fa riferimento alla Control Room / Sala Operativa territoriale, in maniera tale da attivare tempestivamente **il supporto per il pronto intervento da parte di autopattuglie esterne**. Grazie all'accesso al sistema informativo attraverso i tablet PC / smartphone, è possibile un collegamento "in tempo reale" con la Control Room / sala operativa territoriale e per la trasmissione d'informazioni, soprattutto immagini di videosorveglianza, che possono informare l'operatore della problematica per poi cercare la maniera migliore di affrontare l'evento che si sta verificando.

L'integrazione della modulistica di servizio all'interno dell'applicazione **CIVIS GATE** consente anche di effettuare la **completa consuntivazione** delle attività direttamente "sul campo", in modo che tutti i dati siano disponibili per le GPGP impiegate nei turni successivi:

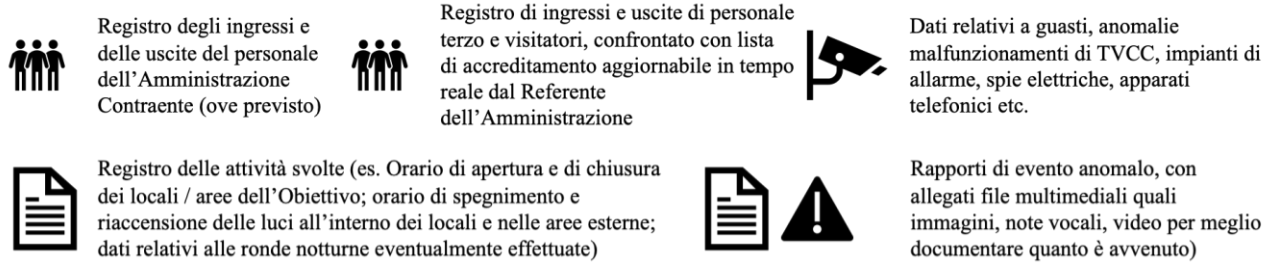


Figura 21 Documentazione del servizio di piantonamento fisso gestibile attraverso l'applicazione CIVIS GATE

C.1.a.2.3 Fase di monitoraggio, controllo e consuntivazione

Grazie alle soluzioni di digitalizzazione del servizio, il processo di controllo e consuntivazione sono automatizzati ed effettuati in tempo reale.

Il tracciamento ed il controllo della conformità delle presenze e delle fasce orarie è effettuato mediante l'elaborazione delle scansioni dei tag NFC attraverso l'applicazione **CIVIS.WATCH**, e attraverso il confronto, effettuato dalla piattaforma informativa CSC, con quanto programmato all'interno del POS [→ cfr. par. C.4].

La verifica interna di processo e di risultato è affidata ai coordinatori operativi ed al Gestore del Servizio, che effettuano attività di verifica relativamente al rispetto delle procedure e della puntualità di effettuazione delle attività richieste, con periodicità quotidiana e controllo a campione sul personale coinvolto. L'intero processo di valutazione e registrazione delle verifiche è completamente supportato e integrato nel Sistema Informativo.

L'Offerente mette infatti a disposizione un'applicazione della Suite CSC, **CIVIS Audit**, pensata per la gestione e compilazione delle check list di autocontrollo. Gestore del Servizio e Coordinatore operativo possono registrare in tempo reale i risultati sulla piattaforma informativa, rendendo le verifiche documentabili, tracciabili e soprattutto condivise in tempo reale con l'Amministrazione Contraente.

L'applicazione è utilizzata in maniera integrata per i controlli di primo livello, eseguiti dalla Funzione Audit e Miglioramento Continuo. In tal modo le modalità di autocontrollo sono speculari alle modalità di controllo: la struttura operativa assimila con l'autocontrollo tutti gli aspetti ed i parametri su cui sarà misurata ai livelli di verifica e monitoraggio successivi (controllo effettuato dalla Funzione Audit e Miglioramento Continuo, controllo effettuato dall'Amministrazione Contraente ovvero dal Soggetto Aggregatore).

C.1.b Servizio ispettivo / di ronda

La vigilanza ispettiva è organizzata con squadre di GPG, a bordo di autovettura radiocollegata, che effettuano controlli ispettivi su tutto il territorio affidato (area). Di norma, il servizio è programmato in maniera tale che una pattuglia rimanga sempre all'interno di una determinata area operativa, in maniera tale da ottimizzare i tempi di spostamento e consentire l'esecuzione di un maggiore numero di attività di ronda sugli obiettivi. Le principali logiche di gestione del servizio riguardano quindi:

- la corretta gestione della **programmazione** dei **percorsi** ispettivi e l'imprevedibilità degli stessi, al fine di aumentare la deterrenza delle ronde;
- la certificazione dei controlli ispettivi effettuati, per la **consuntivazione del servizio,** la presentazione all'Amministrazione Contraente.

C.1.b.1 Integrazione informativa delle procedure e strumenti a supporto OSCURATO

C.1.b.2 Metodologie e procedure operative per la gestione del servizio OSCURATO

C.1.c Servizio di teleallarme

Il servizio di teleallarme consiste nella gestione a distanza di allarmi, segnali e informazioni provenienti da, o diretti verso, gli obiettivi dotati di impianti anti-intrusione e antincendio. Esso è finalizzato all'intervento in loco in caso di allarme. I segnali sono trasmessi alla infrastruttura di Centrale Operativa dell'Offerente ovvero, ove presente, alla Control Room locale dell'obiettivo.

Il servizio di teleallarme viene utilizzato in due distinti contesti di operatività:

- come **attività operativa ad integrazione** di servizi di vigilanza fissa e/o saltuaria;
- come **unica attività operativa** in un contesto di rischio a basso impatto e probabilità medio / alta.

La Centrale Operativa, in funzione 24 ore su 24, dispone per ogni obiettivo collegato in teleallarme di precise informazioni circa le modalità di intervento ed il tipo di controllo da eseguire, ivi comprese indicazioni sulla centrale di allarme dell'utente.

L'infrastruttura di ricezione dei segnali di allarme è ridondante, con impianti di riserva funzionanti in parallelo agli impianti principali e in grado di sostituire *a caldo*, temporaneamente, un singolo sistema temporaneamente in avaria. L'infrastruttura principale di Centrale Operativa, certificata Uni 50518, garantisce la ridondanza anche con la presenza di Centrali Operative di back-up.

Centrale Operativa	Città	Status.
Centrale Operativa di Milano – Via Piero della Francesca, 45	**Milano**	**Principale**
Centrale Operativa di Varese – Via Stoppada, 1	**Varese**	**Principale**
Centrale Operativa di back up all'intera infrastruttura di Vicenza	**Vicenza**	**Back-Up**

C.1.c.1 Integrazione e digitalizzazione delle procedure

CIVIS SUPERVISOR PLATFORM. Anche il servizio di teleallarme è totalmente integrato nella piattaforma **Security 4.0,** grazie all'utilizzo di Civis Supervisor Platform (CSP). CSP, come accennato in precedenza, è una "web application" ingegnerizzata dalla divisione IT di Civis per la ricezione e gestione di tutte le segnalazioni tecnologiche e di Sicurezza provenienti dal "campo" , centralizzando i protocolli di svariate tecnologie abilitanti su di un'unica piattaforma di gestione.

L'architettura modulare ed espandibile di CSP e l'interfaccia web-based sono il valore aggiunto di un vero e proprio Centro Operativo multi-vettoriale e polifunzionale con la caratteristiche di garantire la più assoluta protezione dei dati e la massima tutela della privacy contro possibili intrusioni non autorizzate sia fisiche che informatiche. Gli stati di funzionamento, le segnalazioni di allarme, gli stati di comando di ogni singolo impianto possono essere facilmente integrati all'interno del mondo CSC (Civis Security Cloud) e permettere il governo del servizio basato sui dati.

C.1.c.2 Metodologie e procedure operative per l'esecuzione del servizio

C.1.c.2.1 Programmazione del servizio

La programmazione del servizio può essere distinta in due fasi:

- **Programmazione di start-up del servizio**, che comprende la fase di implementazione del sistema, in particolare per la configurazione e gestione dei segnali riconosciuti;
- **Programmazione operativa del servizio**, che definisce le modalità e le frequenze di effettuazione del servizio.

Programmazione di start-up del servizio

Tale fase discende direttamente dalle risultanze del *Risk Assessment* eseguito durante la fase di redazione del PDI e definisce il programma d'implementazione del sistema di teleallarme e della sua integrazione di Sala Operativa e Centrale Operativa. La programmazione di start-up del servizio tiene conto dei seguenti fattori:

- Tipologia dei segnali da comunicare e gestire (es. **segnali di allarme**: furto / intrusione, rapina / aggressione, manomissione, incendio, uomo a terra, etc.; **segnali variazione di stato**: presenza/assenza rete, caduta vettore di comunicazione, livello batteria, attivazione/disattivazione impianto, etc.);
- Tipologia di comunicatore da utilizzare (in ogni caso sempre in doppia modalità di comunicazione) sulla base del livello di rischio e dei vettori utilizzabili presso l'Obiettivo (es. comunicatore radio bidirezionale + GPRS - backup; comunicatore bidirezionale su rete ADSL+GPRS - backup);
- Tipologia degli apprestamenti tecnologici esistenti: disponibilità di segnali in uscita da collegare al comunicatore, affidabilità del sistema (falsi allarmi), tipologia degli organi di comando (tastiera, badge, radiocomando, etc.);
- Tipologia delle infrastrutture di accesso: sistemi di apertura/chiusura da utilizzare in caso di pronto intervento, livello di accessibilità ai locali interni, etc.;
- Disponibilità di illuminazione di emergenza;
- Disponibilità di reti di comunicazione (PSTN e soprattutto ADSL).

L'ultimo parametro necessario per una corretta pianificazione del servizio è costituito dall'acquisizione dei dati relativi alla gestione del servizio, al fine di definirne le procedure operative. Per ogni obiettivo del servizio viene redatto il Piano di Intervento che contiene:

- Nominativo e recapito telefonico del Responsabile reperibile incaricato dall'Amministrazione Contraente;
- Nominativo e recapito telefonico manutentori reperibili;

- Orari di attivazione/disattivazione dei sistemi di allarme;
- Orari del personale di pulizia (entrata/uscita);
- Elenco nominativo del personale dell'Amministrazione contraente che può permanere all'interno dei locali fuori orario o nei giorni festivi;
- Disposizioni particolari in merito ad aree/locali "sensibili";
- Disposizioni riguardo alle modalità di accesso;
- Copia del Verbale di Consegna Chiavi con relativo numero di sigillo bolgetta;
- Data e orario di attivazione del servizio di teleallarme (decorrenza);
- Procedure di attivazione/disattivazione impianti;
- Prelievo in busta chiusa della "Parola d'ordine" di identificazione utente.

Programmazione operativa del servizio

Il responsabile di Sala Operativa territoriale o altro operatore o capoturno, prima di rendere operativo il servizio di televigilanza, espleta le seguenti attività:

- Redige il modulo denominato **Piano di Intervento di Televigilanza** relativo all'Obiettivo;
- Acquisisce la **parola d'ordine**, le chiavi di accesso ai locali da vigilare (se previsto) e l'eventuale codice o chiave elettronica dell'impianto di sicurezza da porre in plico sigillato (se previsto);
- Codifica l'identificazione dell'Obiettivo;
- Configura sul sistema di centralizzazione allarmi di Centrale Operativa i segnali provenienti dalle periferiche di trasmissione;
- Configura l'anagrafica delle segnalazioni: variazione di stato impianto, allarme furto/intrusione, allarme rapina, allarme aggressione, allarme uomo a terra, manomissione impianto, etc.);
- Configura le procedure di gestione evento in modalità reattiva;
- Configura le procedure di gestione evento in modalità proattiva;
- Configura la frequenza di verifica delle funzionalità di impianto nelle 24 ore (interrogazioni automatiche /manuali);
- Verifica l'archiviazione degli eventi;
- **Redige il piano di intervento su allarme delle autopattuglie:** tempi di intervento, modalità di accesso, gestione chiavi, gestione codici di impianto/sistema, redazione del Rapporto Evento Anomalo. Il Piano di intervento è integrato con quello relativo al servizio di televigilanza, descritto nella sezione successiva, nel caso sia attivato anch'esso;
- Effettua il backup dei dati del sistema MVS (archivio delle segnalazioni e schede utenti) a seguito dell'inserimento del nuovo utente;
- Annota sulla scheda utente del sistema MVS tutte le disposizioni particolari ed i dati riportati nel Piano di Intervento con particolare riferimento agli orari di operatività del servizio e alle disposizioni aggiuntive di sicurezza dell'Obiettivo;
- Annota sul **brogliaccio di Sala Operativa** territoriale tutte le attività tecniche espletate (prove di collegamento, interventi tecnici sulle apparecchiature di Sala Operativa territoriale, nominativo del personale intervenuto, orari di inizio e fine intervento tecnico, inizio e fine prove.

C.1.c.2.2 Esecuzione del servizio

Gli operatori di Centrale Operativa / Control Room effettuano il servizio secondo due modalità, così come previsto dalla programmazione, anche in maniera coordinata:

- **Modalità proattiva** che prevede, in conformità alle procedure, il collegamento con il comunicatore periferico al fine di verificare il funzionamento e lo stato di riposta delle segnalazioni locali. In tal modo, l'addetto verifica anche la presenza di segnali di variazioni di stato (es. taglio della linea telefonica o della alimentazione elettrica, attivazione di jammer, etc.);
- **Modalità reattiva**. Secondo tale modalità, l'addetto valuta le eventuali segnalazioni di allarme ricevute dalla Sala Operativa territoriale. In tale modalità, l'aspetto più delicato è costituito dalla valutazione dei falsi allarmi, in maniera tale da ottimizzare l'impiego di risorse per l'intervento sul posto. In particolare, sono utilizzati algoritmi che valutano l'attivazione di allarmi logicamente connessi ad un evento criminoso (es. apertura finestre, seguita da allarmi dei sensori volumetrici all'interno degli ambienti), considerando il numero minimo di allarmi sopra soglia per la determinazione della veridicità di un evento criminoso in corso. In tal modo, è possibile ridurre gli interventi presso l'Obiettivo.

> Particolare importanza riveste il coordinamento con le risorse destinate ai servizi tecnici in maniera tale che, in presenza di falsi allarmi, sia possibile intervenire prontamente per risolvere eventuali anomalie agli impianti e ai sistemi installati dall'Offerente (apparati di concentrazione e remotizzazione dei segnali).

Il flusso procedurale di coordinamento è illustrato nella figura seguente: i segnali valutati dalle GPG di Control Room, Sala Operativa e/o Centrale Operativa, nel caso evidenzino in maniera chiara falsi allarmi, sono notificati al Call Center, che apre un ticket e consente per attivare i Tecnici di Pronto Intervento, sia dedicati agli apprestamenti anticrimine sia dedicati, eventualmente, ai sistemi di Control Room / Sala Operativa / Centrale Operativa.

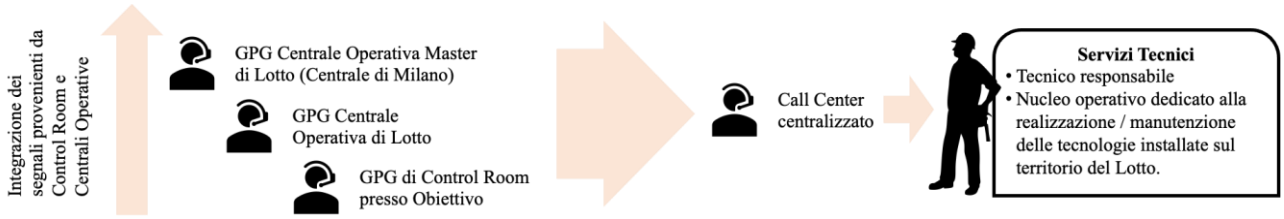


Figura 22 Processo di attivazione dei Servizi Tecnici dell'Offerente per risolvere eventuali avarie e malfunzionamenti

Per l'intervento in seguito a segnalazione di allarme, l'Offerente dispone di autopattuglie radiocollegate dislocate in modo strategico sul Lotto, in grado di coprire interamente il territorio e rispettare i tempi massimi d'intervento garantiti. Per quanto riguarda l'organizzazione specifica del servizio di pronto intervento su allarme, le autopattuglie di pronto intervento si atterranno alle seguenti disposizioni:

- Costante contatto radio con la Centrale Operativa, con **codice di criptazione delle chiamate** in maniera tale da non essere intercettati facilmente da eventuali malintenzionati;
- Conferma radio dell'avvenuta ricezione della richiesta di intervento;
- Conferma radio dell'arrivo presso il sito protetto;
- Registrazione dell'arrivo attraverso la scansione dei tag NFC identificativi dell'obiettivo;
- Verifica delle tecnologie esistenti;
- Rilevazione di eventuali situazioni sospette eventuali situazioni sospette (veicoli, persone, tracce di pneumatici, varchi nella recinzione, vetri rotti, ecc.) e verifica della chiusura delle porte o delle finestre, raggiungibili da terra, relative alla zona dalla quale è partito l'allarme;
- In caso di segni di effrazione, attivazione da parte della Centrale Operativa della pattuglia che ha in dotazione le chiavi del sito (custodite in plico sigillato). Essa infatti può non coincidere con la pattuglia di Pronto Intervento,
- Bonifica esterna e interna del sito mediante utilizzo delle chiavi (custodite in plico sigillato);
- Rilevazione di eventuali anomalie;
- Comunicazione radio in merito all'esito della bonifica;
- Redazione del verbale di intervento su **CIVIS.WATCH**;
- Chiusura dell'intervento su **CIVIS.WATCH**;
- Piantonamento fisso dell'Obiettivo in caso di evento (tentativo di effrazione, danneggiamento, impossibilità a chiudere la struttura, manomissione del sistema tecnologico di sicurezza, ecc.) fino a nuovo ordine o ripristino della normalità;
- Comunicazione telefonica alla funzione reperibile dell'Amministrazione contraente per fornire notizie in merito all'evento;
- Richiesta di intervento del servizio tecnico dell'Offerente per l'eventuale ripristino del sistema tecnologico locale ove si riscontrasse un guasto e/o malfunzionamento dello stesso.

Verbale di intervento

- Data e ora di arrivo dell'allarme, il tipo di allarme, il nome dell'Amministrazione e l'indicazione dell'Obiettivo
- Identificativo pattuglia che è intervenuta ed orario d'intervento
- Esito dell'intervento

All'interno del Verbale di intervento sono contenute le informazioni necessarie a tracciare completamente l'intervento effettuato.

Nel caso in cui la GPG intervenuta non comunichi l'esito dell'operazione o comunque l'operatore di turno non riuscisse a contattarla o richieda l'intervento di un collega di appoggio, la Sala Operativa dovrà informare il Responsabile del Servizio e il Gestore del Servizio e inviare sul posto altre pattuglie, e in caso negativo informare le forze dell'ordine, fornendo tutti i particolari del caso.

Nel caso in cui vengano riscontrate oggettive tracce di reati, la Sala Operativa informerà tempestivamente le Autorità preposte e, una volta che saranno giunte sul posto, la GPG presente fornirà alle stesse la necessaria collaborazione.

Tutte le comunicazioni tra Sala Operativa e GPG di pronto intervento devono essere effettuate con la radio di servizio.

La comunicazione, via radio, permette di rendere circolare, ovvero udibile a tutte le GPG in servizio la comunicazione. Chi ascolta, pur non essendone il diretto destinatario potrebbe intervenire con informazioni che al momento non sono in possesso né della Sala Operativa né della GPG che sta effettuando l'intervento.

Le comunicazioni telefoniche devono essere effettuate solo nei casi in cui non c'è sufficiente copertura con la radio di servizio o per comunicazioni personali o di contenuto complesso e riservato. In particolare per la natura particolarmente delicata del compito svolto, gli operatori della sala operativa vengono attentamente selezionati, hanno un'esperienza specifica nel settore e adeguata formazione per operare in Sala Operativa ed hanno i requisiti psico-fisici ed attitudinali adeguati.

Al termine del turno, l'operatore smontante deve trasmettere al collega che inizia il turno tutte le informazioni necessarie per poter gestire, con cognizione, le attività in corso nonché quelle che si svilupperanno nel corso del suo turno di servizio.

C.1.c.2.3 Esecuzione con soluzioni innovative: Neural Object Detection **OSCURATO**

C.1.d Servizio di televigilanza

Il servizio di televigilanza consiste nel controllo a distanza dell'Obiettivo attraverso il supporto di apparecchiature che trasferiscono le immagini, monitorate direttamente dalla Control Room dell'obiettivo (ove presente) e dalla Centrale Operativa che predispone l'eventuale intervento della GPG di Pronto Intervento in caso di situazioni anomale.
Il servizio di televigilanza è utilizzato nei seguenti contesti di operatività:

- Come attività operativa ad integrazione di servizi di piantonamento fisso e di vigilanza ispettiva / ronda;
- Come unica attività operativa complementare al servizio di teleallarme;
- Come attività operativa di sicurezza, integrata al servizio vigilanza (vigilanza attiva, saltuaria e teleallarme) attraverso l'utilizzo di algoritmi di "videoanalisi".

Le soluzioni di videoanalisi sviluppate e utilizzate dall'Offerente costituiscono un aspetto innovativo dell'infrastruttura di Sala Operativa, e sono particolarmente importanti per ottimizzare il servizio di televigilanza e concentrare l'attenzione degli operatori solo sulle situazioni effettivamente anomale.
Grazie alla possibilità di vedere in tempo reale le immagini trasmesse dal Cliente, l'operatore può acquisire informazioni immediate ed esplicite sulla situazione o sull'evento che si sta verificando presso l'Obiettivo da cui si è ricevuto il segnale d'allarme. L'evoluzione tecnologica presente attualmente, ha permesso, grazie a investimenti costanti, l'installazione di sofisticati sistemi per la ricezione di immagini video remotizzate, le quali permettono la visione in tempo reale del target oggetto di intervento.

C.1.d.1 Integrazione del servizio in Centrale Operativa con il servizio di Teleallarme

Il sistema di videosorveglianza permette di convogliare il servizio di pronto intervento con cognizione di causa eliminando i falsi allarmi ed evitando di impegnare risorse inutilmente. Allo stato attuale è possibile trasmettere in tempo reale senza limiti di distanze qualsiasi ripresa video collegata ad impianti d'allarme specifici.
A tal proposito tulle le società del RTI seguono costantemente le evoluzioni tecnologiche legate allo sviluppo dei sistemi di trasmissioni video, investendo costantemente su tali risorse fino a giungere ad oggi ad avere un sistema di centralizzazione proprietaria che permette il collegamento da qualsiasi apparato di trasmissione dati multimediali. Infatti, è innegabile che l'integrazione del supporto video come sistema integrato ad un impianto d'allarme svolga un ruolo determinante al fine di prevenire e soffocare con tempestività l'atto criminoso.
Anche per il servizio di televigilanza si prevede quindi la totale integrazione nella piattaforma informativa Security 4.0, grazie alla piattaforma *Civis Security platform (CSP)* descritta per il servizio di teleallarme. Essendo multiprotocollo e multi-vettoriale, la piattaforma può gestire ed integrare sia flussi di dati (allarmi, stati di funzionamento) provenienti dagli apprestamenti anti-crimine, sia i flussi video provenienti dagli impianti di video-sorveglianza.

La centralizzazione dei flussi video sarà gestita con un sistema di centralizzazione video *smart*, integrato nella piattaforma CSP (Civis Supervisor Platform) della Centrale Operativa.

Il sistema non si limita a centralizzare passivamente i segnali di videosorveglianza**. In caso di allarme,** il sistema **sottopone, infatti, automaticamente all'operatore gli *alert* per l'accesso alla videosorveglianza**, anche in multi-connessione; l'operatore di Centrale Operativa ha la possibilità di accedere alle immagini dell'area interessata dell'allarme in modalità Live o Play (accesso alle informazioni registrate nei minuti precedenti l'evento).

Il sistema Smart fa cioè lavorare in sintonia, come un unico, efficace strumento, i segnali di allarme e quanto ripreso dalle telecamere.

Ciò permette di discriminare molto velocemente ed efficacemente le situazioni. Il sistema si configura quindi come un **valido supporto al personale di piantonamento ma anche per il controllo di sicurezza presso i siti.**

C.1.d.2 Modalità operative di esecuzione del servizio

C.1.d.2.1 Modalità di programmazione del servizio

Il primo passo riguarda la pianificazione e l'implementazione del sistema di videosorveglianza e il collegamento alla Control Room / Sala Operativa / Centrale Operativa, come illustrato nel seguente diagramma di flusso:

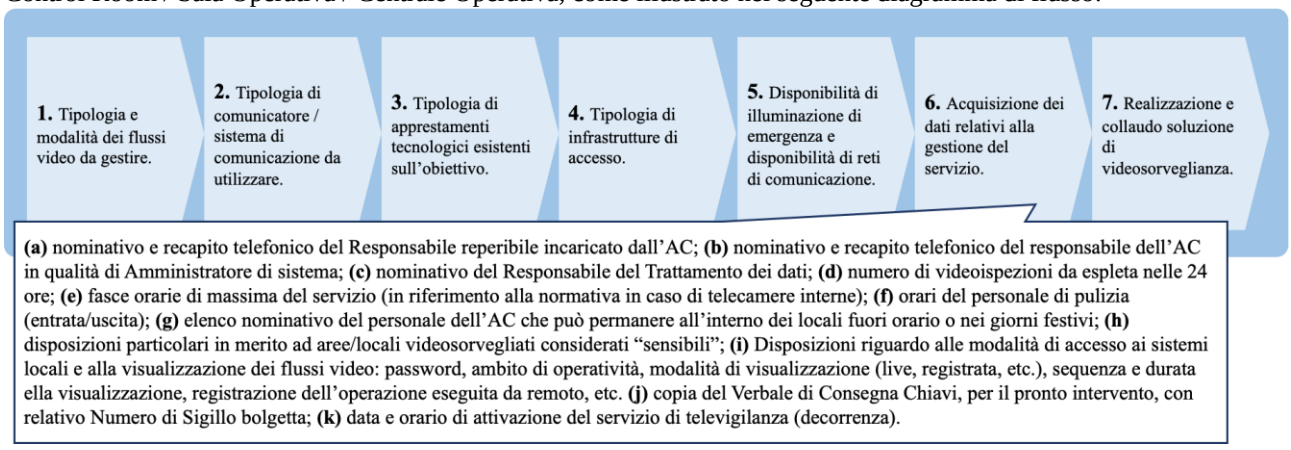


Figura 23 Processo e implementazione del sistema di videosorveglianza e collegamento di Control Room / Centrale Operativa

La fase di pianificazione e programmazione, sotto la responsabilità del responsabile di Sala Operativa territoriale o di altro operatore o capoturno, include le attività descritte nel seguente diagramma di flusso.

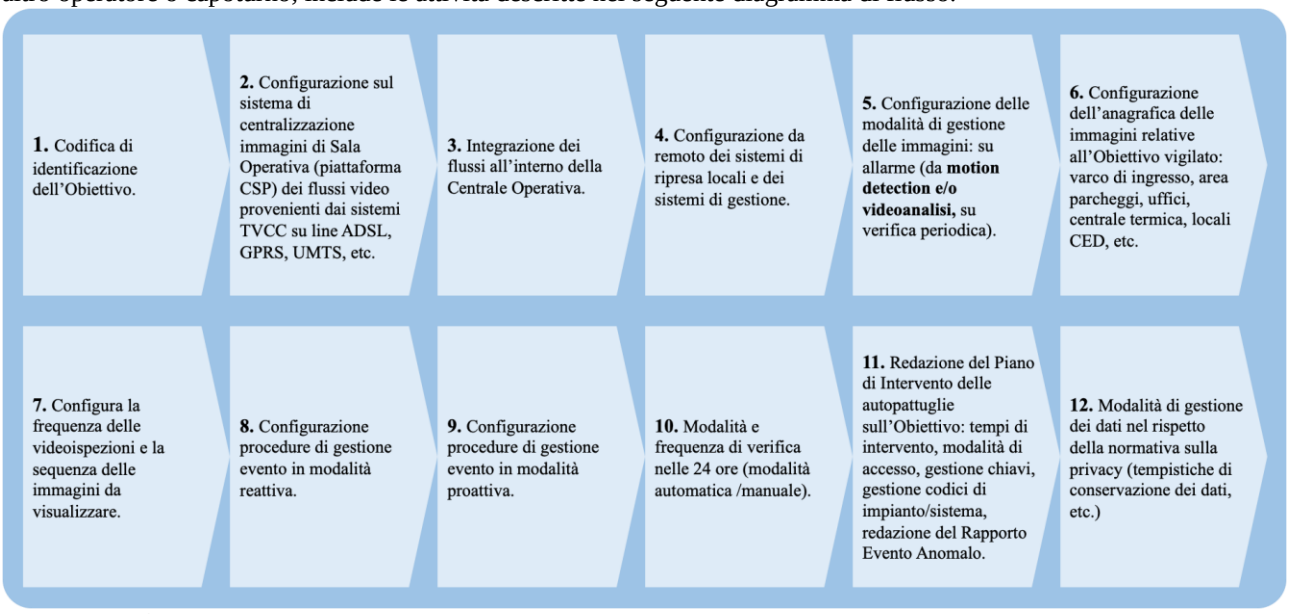


Figura 24 Pianificazione e programmazione del sevizio di Televigilanza

C.1.d.2.2 Modalità di esecuzione e coordinamento del servizio

Durante la fase di esecuzione del servizio, l'operatore della Sala Operativa territoriale / Control Room effettua, secondo le frequenze e le modalità definite dalle procedure di servizio le attività di videosorveglianza.
Tutto il flusso delle immagini e delle informazioni ad esse relative è integrato all'interno della infrastruttura di Centrale Operativa, che fungerà da collettore e integratore di tutti i segnali di remotizzazione provenienti dalle varie Control Room e Sale Operative dell'Offerente sul Lotto, come illustrato nel seguente schema concettuale.

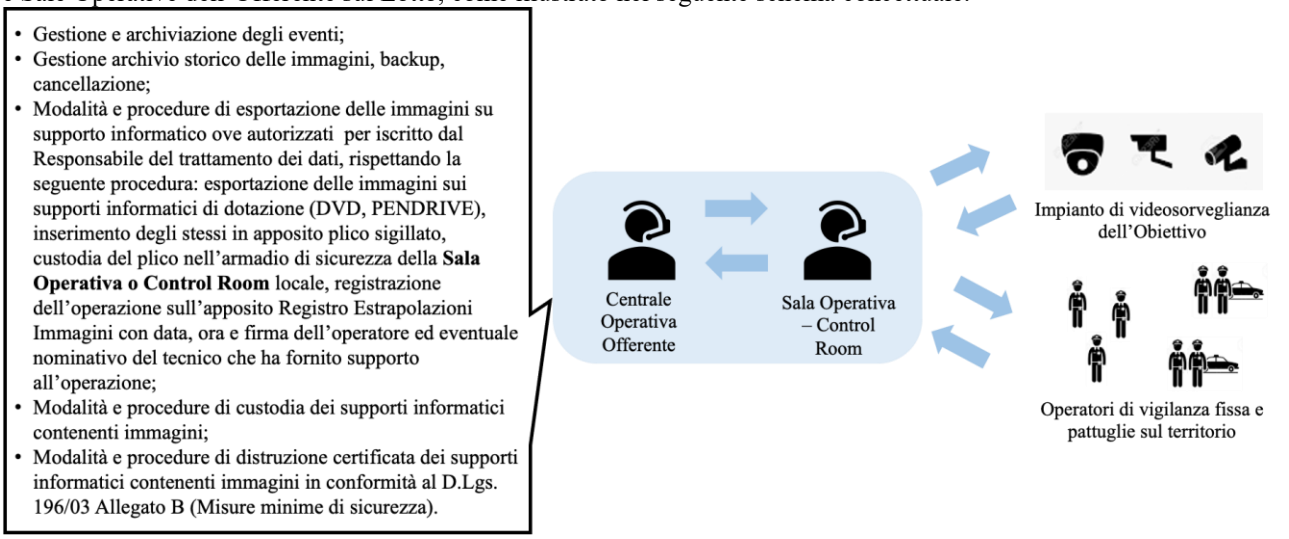


Figura 25 Illustrazione delle modalità di integrazione di tutti i flussi video all'interno dell'infrastruttura di Centrale Operativa

Nel caso di eventi anomali, gli operatori di televigilanza possono attivare gli operatori di vigilanza fissa interni all'Obiettivo, se quest'ultimo ne è dotato, oppure attivare le pattuglie di pronto intervento sul territorio, presenti in maniera tale da coprire i vari OPF di Lotto. La determinazione del tempo massimo d'intervento, in caso di allarme, sarà di **circa 20 minuti**. Le autopattuglie di pronto intervento si atterranno alle seguenti disposizioni:

- Costante contatto radio con la Centrale Operativa;
- Conferma radio dell'avvenuta ricezione della richiesta di intervento,
- Conferma radio dell'arrivo presso il sito;
- Bonifica esterna e interna del sito mediante utilizzo delle chiavi (custodite in plico sigillato);
- Verifica delle tecnologie esistenti;
- Rilevazione di eventuali anomalie;
- Comunicazione radio in merito all'esito della bonifica;
- Redazione del verbale di intervento in doppia copia (una per l'AC);
- Chiusura dell'intervento;

- Piantonamento fisso dell'obiettivo in caso di conclamata emergenza (tentativo di effrazione, danneggiamento, impossibilità a chiudere la struttura, manomissione del sistema tecnologico di sicurezza, ecc.) fino a nuovo ordine o ripristino della normalità;
- Comunicazione telefonica alla funzione reperibile dell'AC per fornire notizie in merito all'evento;
- Richiesta di intervento del servizio tecnico dell'Offerente per l'eventuale ripristino del sistema tecnologico locale ove si riscontrasse un guasto e/o malfunzionamento dello stesso.

I processi di monitoraggio e di consuntivazione sono integrati all'interno della piattaforma Civis Supervisor Platform. Tale attività sarà gestita totalmente dalla Sala Operativa territoriale in quanto:

- Tutti i flussi video trattati sono memorizzati e archiviati sulla piattaforma video di Centrale con relativa data e ora;
- E' possibile avere il report delle visualizzazioni, i controlli di stato, le anomalie di collegamento, le manovre sugli impianti locali (visualizzazione, memorizzazione, archiviazione, esportazione, etc.;
- E' possibile avere il report dei tempi di intervento delle autopattuglie: tempo di percorrenza tra la richiesta di intervento e arrivo presso l'Obiettivo e tempo di durata dell'ispezione;
- E' possibile avere il report in tempo reale della posizione delle autopattuglie tramite il sistema satellitare di bordo GPS (Global Positioning System);
- E' possibile avere il report (dati e immagini) riguardo alla chiusura degli eventi con relativo codificazione degli esiti. Tutta la reportistica è quindi disponibile, grazie all'interfaccia fra sistema di Sala Operativa territoriale e Sistema Informativo, all'interno delle sezioni dedicate del Portale Civis Security Cloud (CSC) dedicato alla gestione della Convenzione. Il Supervisore e/o i Referenti dell'Amministrazione in tal modo hanno la disponibilità continua di una reportistica aggiornata relativa all'attività effettuata.

C.1.d.2.3 Soluzioni tecnologiche per le gestione della connettività

Sulla base della nostra pregressa esperienza maturata in appalti similari, L'Offerente è consapevole che una frequente problematica che si può riscontrare presso le Pubbliche Amministrazioni è la presenza di linee dati insufficienti per poter far transitare le immagini e i segnali necessari a garantire la copertura del servizio di televigilanza.
n tale ambito un'altra esigenza spesso riscontrata è la necessità delle Amministrazioni, per specifiche policy interne, di isolare le proprie reti rispetto a qualsiasi collegamento con l'esterno.

Pertanto, al fine di risolvere tali problematiche e per garantire il collegamento dei sistemi di sicurezza installati presso le Amministrazioni Contraenti con la infrastruttura di Centrale Operativa, l'Offerente propone l'installazione di un sistema di connettività presso la sede oggetto del contratto minimamente invasivo e che consentirà di isolare completamente l'impianto di videosorveglianza dalla rete dati dell'Amministrazione Contraente.

In particolare, l'intervento consisterà semplicemente nell'installazione di un'antenna e di un *router* e nell'effettuazione del cablaggio per collegare gli apparati esistenti alla rete. Tale soluzione consente di garantire all'Amministrazione:

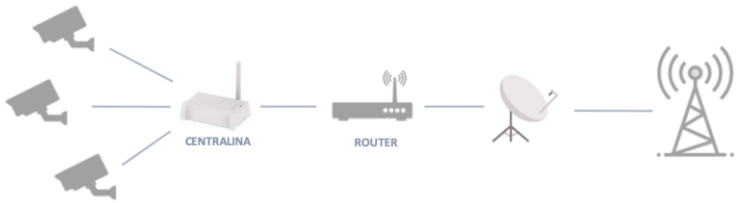


Figura 26 Schema di connettività utilizzato dall'Offerente

- **indipendenza** dalla rete interna grazie all'impiego di una rete di ripetitori radio Hiperlan 2;
- **calibrazione** della banda di traffico in base alle necessità di servizio;
- **infrastruttura** radio basata sulle più innovative tecnologie di mercato, come collegamenti in fibra ottica su tutte le stazioni di diffusione, ridondanti tramite ponte radio;
- **ridondanza** dei nodi principali della rete attraverso collegamenti magliati;
- **monitoraggio continuo** della rete al fine di mantenere livelli ottimali in termini di disponibilità di banda e latenza a garanzia del servizio offerto.

Precisiamo che per ogni Amministrazione Contraente, qualora se ne rilevasse la necessità, gli ingegneri e i tecnici che costituiscono il Team Apprestamenti e il Team Integrazione e Remotizzazione, in fase di redazione del PDI, provvederanno a studiare e progettare la soluzione più adatta e migliore in funzione delle specifiche caratteristiche ed esigenze della sede oggetto del contratto.

Tale sistema è inoltre in grado di garantire la continuità del servizio anche in caso di blackout dei broadband Terresti, in quanto specifiche stazioni di energia e generatori entrano automaticamente in funzione assicurando continuità elettrica ai ripetitori a cui l'Offerente è collegato.

Infine si precisa che con questo sistema l'Offerente può garantire la totale protezione dei dati, aspetto particolarmente importante in conformità a quanto previsto dal GDPR per la tutela dei dati personali, in quanto il canale radio utilizzato prevede una connessione wireless cifrata con protocolli AES e Proprietari, impermeabili e di assoluta sicurezza rispetto a tentativi di intrusione e disturbo.

C.1.d.2.4 Soluzioni tecnologiche innovative per la videosorveglianza **OSCURATO**
C.1.d.2.5 Soluzioni tecnologiche di video analisi e motion detection

La modalità REATTIVA, sarà potenziata da specifici applicativi sistemi avanzati di analisi delle immagini, sollecitando l'attenzione dell'addetto alla Centrale Operativa. A fronte di un evento anomalo infatti si attiverà automaticamente l'apertura di una finestra (pop up) in cui sarà visualizzato il flusso live della camera. L'addetto pertanto, a seguito dell'analisi delle immagini, assumerà la decisione in merito all'attivazione dell'intervento presso la sede.

Televigilanza con sistema avanzato di analisi delle immagini. Tenuto fermo e invariato il sistema di videosorveglianza esistente e di eventuale sviluppo presso gli obiettivi delle singole Amministrazioni Contraenti, l'Offerente possiede tecnologie innovative per supportare le attività di analisi e controllo dei flussi video provenienti dagli impianti di videosorveglianza singoli e/o dalle Control Room degli obiettivi più complessi.

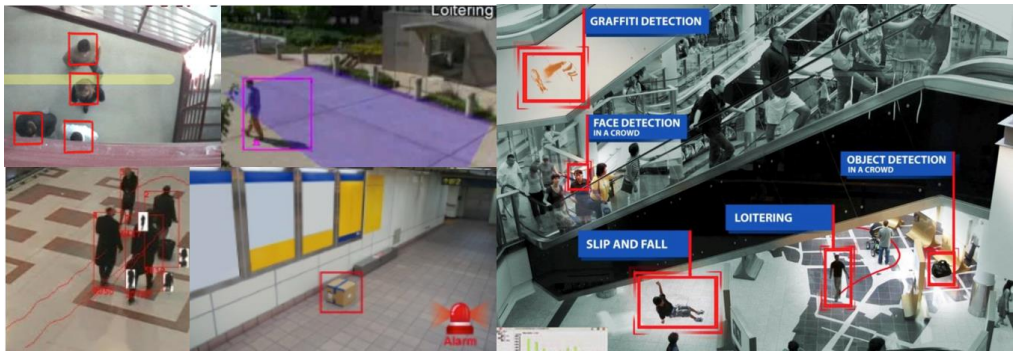
Ove fossero installate videocamere IP, dotate all'interno di un video server, con possibilità di integrazione alla rete ethernet locale o in remoto tramite internet, l'Offerente potrà proporre l'integrazione, previa verifica tecnica, di specifici avanzati sistemi di analisi delle immagini integrati alla Centrale Operativa.

L'analisi video supportata dai sistemi elettronici permette di evidenziare, con completezza ed estrema efficacia, quelle situazioni particolari definite e predeterminate: di comportamenti anomali, fraudolenti o illeciti che possono essere prodromiche ad eventi relativi alla sicurezza quali:

- accesso a zone non consentite;
- la rimozione o l'abbandono di oggetti;
- il vagabondaggio;
- una situazione di panico.

Con l'utilizzo di queste soluzioni innovative è possibile trasformare l'impianto di videosorveglianza da un sistema per la **ricostruzione** di un **evento** attinente la security, in un **sistema attivo di segnalazione e identificazione di situazioni anomale.**

L'Offerente è disponibile alla valutazione tecnico – economica, senza costi per le Amministrazioni Contraenti, per lo studio di ammodernamento degli impianti di videosorveglianza, al fine di poter utilizzare l'avanzata tecnologia di analisi delle immagini di cui è dotata la Centrale Operativa e, previa compatibilità, metterla a disposizione.



Televigilanza con algoritmi di motion detection. Un ulteriore elemento innovativo proposto nella gestione dei flussi video è costituito da **algoritmi** di motion detection di cui è dotata la Centrale Operativa. Grazie alla variazione dei pixel delle immagini (in inglese motion detection), la telecamera è in grado di rispondere in modo intelligente a determinati segnali "catturati" all'interno dell'inquadratura. La soluzione proposta per la motion detection è la **IVS (Intelligent Video Systems) o equivalente**, **un sistema di "motion detection and alarm" in grado di adattarsi a telecamere già presenti ed installate presso le sedi oggetto del contratto, del quale si illustrano i principali punti di forza**:

Ogni telecamera del sistema di sorveglianza diventa parte attiva del sistema e automaticamente identifica gli eventi durante l'analisi continua delle immagini in tempo reale. Avvisa l'operatore della centrale operativa inviando un allarme quando rileva un evento critico trasformando così le telecamere in una squadra di operatori di sicurezza

IVS tiene traccia della traiettoria, infatti tutti gli eventi vengono visualizzati in tempo reale, mentre i dati possono essere registrati per riproduzioni successive

Grazie alla funzionalità di ricerca intelligente, il sistema IVS individua rapidamente i relativi filmati senza dover scorrere l'intera registrazione. I contorni degli oggetti, con codice colore in base allo stato di allarme, si sovrappongono alle immagini per mostrarne la posizione. Fattori quali la proporzione e la prospettiva vengono automaticamente presi in considerazione.

Figura 27 Caratteristiche dei sistemi IVS (Intelligent Video Systems) di motion detection

Il sistema è meno raffinato e potente di quello di analisi intelligente delle immagini, ma è compatibile con tutti i sistemi di telecamere generalmente presenti presso le Amministrazioni. Costituisce quindi una fornitura "minima garantita" a integrazione dei sistemi di videosorveglianza dei siti protetti.

C.1.e Dotazioni aggiuntive, offerta di sistemi innovativi al personale ed alle vetture

Nelle pagine seguenti sono illustrate le **dotazioni aggiuntive** e le **soluzioni innovative** messe a disposizione del personale per l'esecuzione del servizio, evidenziando gli elementi di particolare innovatività, garanzia di sicurezza e di qualità del servizio offerto per l'Amministrazione Contraente. Sono inoltre **esplicitamente definiti i benefici** per l'Amministrazione Contraente. Per maggiore facilità di lettura sono definiti i servizi con le seguenti icone:

 Piantonamento fisso	 Vigilanza ispettiva / ronda	 Teleallarme	 Televigilanza	 Pronto Intervento H24

Di seguito quindi le dotazioni:

Dotazione e soluzioni previste aggiuntive e innovative					
Soluzioni innovative					
Suite Security 4.0 a disposizione degli operatori, per la digitalizzazione dei servizi. Contiene le app sviluppate per il supporto ai servizi e anche una specifica funzionalità di segnalazione "pulsante SOS" attivabile dall'operatore.	●	●	●	●	●
Sistema di gestione chiavi elettronico Key Management, implementato previa verifica tecnica e risk assessment.	●				
Possibilità di installazione di armadi elettronici per la gestione delle chiavi, integrati con il sistema di gestione chiavi Key Management	●				
Sistema di analisi delle immagini NOD che trasforma il sistema di videosorveglianza in **sistema attivo** di segnalazione, implementato previa verifica tecnica e risk assessment.			●	●	
Sistema di videosorveglianza Smart che permette di integrare teleallarme e televigilanza, implementato previa verifica tecnica e risk assessment.			●	●	
Sistemi ed algoritmi di analisi delle immagini, che permettono di evidenziare all'operatore la presenza di situazioni anomale / di rischio.				●	
Dotazioni di squadra presso gli obiettivi					
Sistema di tracciatura del servizio mediante app Civis.Watch e sistema di scansione georeferenziata di tag NFC (NFC/QRCode).	●	●			●
KIT Salute (termometro a raggi infrarossi, DPI operatori, DPI specifici per protezione da virus, defibrillatore semiautomatico Philips HeartStart o equivalente). **Quantità:** 1 per obiettivo.	●				
Megafono per comunicazioni di emergenza. **Quantità:** 1 per postazione.	●				
Specchio veicolare, utilizzato presso le sedi con accessi carrabili. **Quantità**: 1 per obiettivo a seconda delle risultanze del risk assessment. Permette di agevolare l'eventuale ispezione di veicoli per l'accesso a obiettivi particolarmente sensibili	●				
Scanner portatile per la rilevazione di metalli. Individua armi e oggetti metallici. Quantità: 1 per obiettivo Previa necessità da risk assessment, per siti particolarmente sensibili	●				
Tappetino anti-fatica per le postazioni di controllo in piedi. Diminuisce l'affaticamento dell'operatore in piedi. **Quantità**: 1 per postazione	●				
Zaino di emergenza, contenente DPI e dotazioni per il primo intervento. **Quantità:** 1 ogni postazione / veicolo	●				
Dotazioni e attrezzature antincendio, contenute in armadio con anta frangibile. Contiene i DPI previsti per fronteggiare situazioni di incendio , fra cui maschere antigas, protezioni anti calore etc. **Quantità:** 1 ogni postazione / veicolo	●				●
Dotazioni del personale					
Giubbetto antiproiettile ad elevata protezione	●				
Torcia elettrica ad alta potenza con tecnologia LED, per l'illuminazione di emergenza in caso di blackout ovvero di scarsa illuminazione. **Quantità:** 1 ogni postazione / veicolo	●	●			●
Bodycam indossabile da attivare in caso di eventi di rilevanza penale. **Quantità**: 1 ogni postazione di piantonamento		●			●
Smartphone / tablet con integrate le applicazioni specifiche della piattaforma informativa Civis Security Cloud. **Quantità**: 1 ogni postazione fissa / mobile di servizio (postazione di piantonamento fisso o autopattuglia)	●	●	●	●	●
App dedicata alla traduzione simultanea. Disponibile sul dispositivo dell'operatore. Permette la comunicazione in tempo reale, in più lingue. **Quantità**: 1 ogni smartphone.	●				
Dotazioni specifiche delle autovetture di servizio					
Dispositivo di segnalazione GPS installato a bordo dell'autovettura di servizio per la pronta geolocalizzazione dei mezzi in servizio.		●			●
DashCam a bordo vettura, per la ripresa durante interventi in emergenza o su chiamata in regime di Pronto Intervento. Documenta ciò che succede intorno all'automezzo.		●			●
Tablet PC con applicazione CIVIS PATROL per il coordinamento, il controllo e la gestione operativa del servizio di vigilanza ispettiva / ronde. Il tablet permette anche la ricezione delle richieste di **pronto intervento**.		●			●
Zaino di emergenza, con gli stessi contenuti dello zaino di emergenza in dotazione alle postazioni.		●			●
Dotazioni antincendio, con le stesse dotazioni previste per le postazioni.		●			●

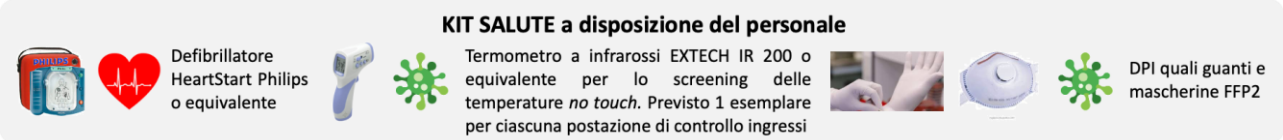
C.1.e.1 Soluzioni Innovative OSCURATO

C.1.e.2 Dotazioni di squadra presso gli obiettivi

Tracciatura del servizio mediante app Civis.Watch e sistema di scansione georeferenziata di tag NFC. Le postazioni di ciascun sito vigilato saranno identificate univocamente con etichette **NFC** (Near Field Communication, un'evoluzione della tecnologia radio RFID). Ciò permetterà la consuntivazione e rendicontazione delle attività effettuate dagli operatori.

Vantaggi per l'Amministrazione Contraente: questa dotazione permette l'automatizzazione delle tracciature, rendendo più chiaro e trasparente il livello di servizio erogato.

KIT SALUTE (termometro a raggi infrarossi, DPI, defibrillatore portatile Philips HeartStart o equivalente). L'Offerente intende dotare tutti gli obiettivi di un kit per la tutela della salute delle persone, anche a valle dell'emergenza Covid-19 verificatasi di recente:



Vantaggi per l'Amministrazione Contraente: le risorse operative, *con adeguata formazione*, utilizzano tale sistema presso gli obiettivi e coprono così non solo la sfera della "sicurezza", ma anche la sfera della "incolumità" delle persone all'interno e all'esterno degli obiettivi. Ciò aumenta la capacità di risposta alle emergenze del personale.

Megafoni elettronici con impugnatura. Il Nucleo è dotato anche di megafoni elettronici con impugnatura, al fine di comunicare più agevolmente in presenza di elevato affollamento o per disciplinare il flusso di persone in caso di situazioni anomale, particolari o di emergenza.

Vantaggi per l'Amministrazione Contraente: l'utilizzo di megafoni facilità la comunicazione durante potenziali situazioni di emergenza, ed in particolare durante le attività di evacuazione.

Scanner portatile 2HHMD (Hand Held Metal Detector) marca CEIA modello PD140 o equivalente. È un dispositivo portatile pensato in back-up / supporto alla dotazione di ciascun presidio. E' capace di rilevare con elevata sensibilità oggetti metallici, magnetici e non magnetici, su persone o cose.

Vantaggi per l'Amministrazione Contraente: il dispositivo aumenta la sicurezza di obiettivi a più elevata sensibilità e permette di individuare oggetti metallici, armi e dispositivi durante eventuali controlli all'ingresso.

Specchi veicolari. L'Offerente prevede l'utilizzo di specchi veicolari, presso tutti gli obiettivi presso cui sia presente personale di vigilanza fissa che debba effettuare controlli su veicoli all'ingresso, di specchi professionali EFIS 1 o equivalenti.

Vantaggi per l'Amministrazione Contraente: il dispositivo aumenta la sicurezza di obiettivi a più elevata sensibilità e permette una più accurata ispezione dei veicoli.

Tappetino anti fatica per GPG operanti in piedi presso le postazioni di controllo. Per tutte le postazioni occupate da questa categoria di lavoratori, l'Offerente ha previsto la fornitura di tappeti anti-fatica. Sono progettati per ridurre la pressione del corpo sui piedi garantendo così una migliore circolazione sanguigna e un miglior beneficio a tutto il corpo all'operatore che passa molto tempo in piedi.

Vantaggi per l'Amministrazione Contraente: la dotazione migliora il *comfort* della GPG in piantonamento, accrescendo la capacità di concentrazione sul proprio ruolo operativo.

Zaino di emergenza. Contiene un **kit di primo soccorso** conformi alla normativa vigente e sempre complete di tutti i prodotti previsti per legge. Contenuto, secondo il DM 388/03:

Contenuti del Kit di Primo Soccorso	
1 Copia Decreto Min 388 del 15.07.03	1 Confezione da 10 cerotti assortiti
2 Paia guanti sterili	1 Rocchetto cerotto adesivo m 5×2,5 cm
1 Disinfettante 125 ml IODOPOVIDONE al 10% iodio PMC	1 Benda di garza m 3,5×10 cm
1 Soluzione fisiologica 250 ml CE	1 Paio di forbici tagliabendaggi cm 14,5DIN
1 Busta compressa garza sterile cm 18×40	1 Laccio emostatico
3 Buste compressa garza sterile cm 10×10	1 ICE PACK Ghiaccio istantaneo monouso
1 Pinza sterile	1 Sacchetto per rifiuti sanitari
1 Confezione di cotone idrofilo	1 Istruzioni MULTILINGUA pronto soccorso

Contiene anche **l'innovativo kit Stop-Bleeding,** sviluppato per fermare efficacemente fuoriuscite di sangue. Il Kit, sviluppato in Israele, è pensato per fermare gravi emorragie durante situazioni di emergenza.

Vantaggi per l'Amministrazione Contraente: consente di aumentare la capacità di risposta ad un'emergenza sanitaria presso l'obiettivo vigilato.

Dotazioni e attrezzature antincendio. Sarà messo a disposizione, qualora non già disponibile, un kit antincendio speciale, dedicato al "servizio prevenzione e primo intervento antincendio" equipaggiato con le seguenti attrezzature:

Contenuti del Kit di Primo Soccorso	
N. 1 estintore portatile a polvere da 6 Kg	N. 2 paia di calzari sfoderati

N. 1 ascia acciaio e N. 1 cesoia	N. 1 Fire Cap (casco antincendio)
N. 1 fire blanket (coperta in fibra per spegnere piccoli incendi e soffocare principi di incendio)	N. 2 paia di guanti con dorso alluminizzato, palmo in fibra aramidica coibentata
N. 2 maschere antigas in gomma policloroprenica completa di filtro	N. 2 torce ricaricabili ad alta luminosità

Vantaggi per l'Amministrazione Contraente: consente di aumentare la capacità di risposta alle emergenze presso l'obiettivo vigilato.

C.1.e.3 Dotazioni del personale

Giubbetto antiproiettile ad elevata protezione (classe minima di protezione IIIa), che permette di offrire all'operatore, ove prevista, una protezione aggiuntiva in caso di conflitto a fuoco.

Vantaggi per l'Amministrazione Contraente: consente di aumentare la sicurezza generale dell'obiettivo.

Torcia elettrica Nitecore MH25GTS. Le Guardie Giurate per i servizi hanno in dotazione, soprattutto per le attività di bonifica e per le eventuali situazioni di emergenza, un'idonea **torcia elettrica** con **tecnologia LED**, munita di accumulatori ricaricabili di grande capacità, che permettono di abbinare una potenza di illuminazione particolarmente estesa ad una prolungata durata di funzionamento.

Vantaggi per l'Amministrazione Contraente: consente di aumentare la sicurezza generale dell'obiettivo e la rilevazione di potenziali minacce.

Bodycam indossabile da attivare in caso di eventi di rilevanza penale. In dotazione a **tutte le risorse in turno** sarà prevista una **microtelecamera** del tipo videocamera indossabile **Body Worn Camera X5 CEDISS o similare**, **indossata e non visibile all'utenza**. Il sistema è attivato rapidamente dall'agente solamente in caso di necessità (situazione di emergenza, presenza di utenza minacciosa etc.) al fine di meglio documentare l'evento ai fini forensi e di indagine. Il dispositivo registra il flusso di immagini in alta risoluzione e anche l'audio della scena.

Vantaggi per l'Amministrazione Contraente: consente di documentare eventi di rilevanza penale e di ricostruire la catena degli eventi, rendendo trasparente l'operato delle GPG sul campo. Tutela inoltre l'Amministrazione poiché testimonia il corretto utilizzo delle procedure da parte del personale in caso di controversie.

Smartphone con applicazione Civis.Watch e altre funzionalità della piattaforma CSC per la digitalizzazione del flusso informativo afferente il servizio. Lo smartphone in dotazione alle risorse è dotato di specifiche funzionalità, quali Civis.Watch e Civis.Gate, che permettono di gestire un vero e proprio "ufficio virtuale" con tutta la documentazione e i flussi di dati relativi ai servizi. Le GPG impiegate nei servizi potranno attraverso lo smartphone inserire verbali e rilievi, sia in forma scritta che in forma fotografica, e di trasmettere tali informazioni al sistema centrale CSC in modo che siano consultabili dal personale di coordinamento e dai Referenti dell'Amministrazione Contraente**. L'utilizzo della modalità elettronica per la gestione della documentazione relativa al servizio permette al cambio turno la condivisione immediata delle informazioni, oltre alla possibilità di avere copia degli atti di registro in modalità on line per l'Amministrazione utilizzando la piattaforma CSC messa a disposizione da Civis.** Lo smartphone è inoltre dotato di **funzionalità panico "SOS"** che lo fanno funzionare come uno strumento di richiesta di aiuto in dotazione al personale.

Vantaggi per l'Amministrazione Contraente: si assicura la gestione elettronica dell'intero appalto.

Applicazione per la traduzione simultanea iTranslate. Sul dispositivo delle GPG sarà messa a disposizione ***iTranslate*****,** l'app di traduzione con dizionario principale, non gratuita, più diffusa al mondo. L'applicazione, sempre disponibile anche in modalità OFFLINE, consente una comunicazione chiara ed immediata in più di 100 lingue. L'app permette inoltre di creare una libreria di frasi per le attività ripetitive delle GPG, così da rendere ancora più efficace e rapida la comunicazione. L'app è bidirezionale: traduce quanto viene digitato o detto dalla GPG nella lingua prescelta, e traduce quanto risposto dall'interlocutore, con efficacia a tutta prova.

Vantaggi per l'Amministrazione Contraente: rende più efficace la comunicazione con utenza e visitatori degli obiettivi, abbattendo la barriera del linguaggio.

Dotazione specifica per l'esecuzione servizio di vigilanza con drone. Per l'esecuzione del servizio l'Offerente utilizzerà droni di ultima generazione, con videocamere professionali e dotate di sistemi IR per le riprese notturne / con scarsa visibilità. Inoltre,

Vantaggi per l'Amministrazione Contraente: la dotazione abilita l'erogazione dei servizi di vigilanza ispettiva con apparati a pilotaggio remoto.

Dispositivo di geolocalizzazione GPS a bordo delle vetture di pattuglia. **Tutti i mezzi utilizzati per le attività di vigilanza ispettiva e pronto intervento sono dotati di apparato GPS di bordo** che trasmette all'infrastruttura di Centrale Operativa, **in automatico e in tempo reale**, la posizione dell'autopattuglia permettendo di ricostruirne gli spostamenti e quindi di controllare i tempi di intervento, la puntualità delle ispezioni rispetto alla programmazione e la situazione generale delle ronde ispettive sul territorio di ubicazione degli obiettivi.

Dash Cam a bordo vettura. Tutti i mezzi utilizzati per le attività di **ronda ispettiva** saranno dotati di "dash cam" vale a dire una videocamera, staccabile, da utilizzare per documentare specifiche situazioni afferenti la security

dalla vettura. Il dispositivo permette di documentare le attività effettuate e **mette a disposizione informazioni aggiuntive per ricostruire eventi di rilevanza penale.**

Tablet PC con accesso a CIVIS.PATROL. Tutti i mezzi utilizzati per le attività di **ronda ispettiva** saranno dotati di tablet PC con accesso alla innovativa web app **CIVIS PATROL**, descritta in precedenza, che permette un continuo scambio di informazioni in tempo reale fra pattuglie sul territorio e Centrale Operativa.

Zaino di emergenza a bordo auto. Contiene un **kit di primo soccorso** conformi alla normativa vigente e sempre complete di tutti i prodotti previsti per legge. Contenuto, secondo il DM 388/03, analogo a quello dello zaino di emergenza presso gli obiettivi.

Dotazioni e attrezzature antincendio. A bordo delle autopattuglie sarà messo a disposizione, qualora non già disponibile, un kit antincendio speciale, dedicato al "servizio prevenzione e primo intervento antincendio" equipaggiato con attrezzature analoghe a quelle componenti il kit antincendio dedicato agli obiettivi

Vantaggi per l'Amministrazione Contraente: la dotazione per le emergenze aumenta la capacità di risposta alle emergenze da parte del personale dell'Offerente.

Unità cinofila. Per aumentare ulteriormente l'efficacia del servizio, l'Offerente prevede l'esecuzione delle ronde – ove ritenuto necessario – anche con unità cinofila.

Vantaggi per l'Amministrazione Contraente: l'unità cinofila permette di tutelare l'incolumità e l'efficacia delle ronde su obiettivi di grande estensione, di rilevanza o in cui l'operatore debba fare lunghi percorsi isolato.

C.2. Modalità di gestione della/e Centrale /i Operativa/e

L'Offerente ha curato in maniera particolare, dal punto di vista organizzativo, procedurale e tecnologico, le soluzioni per garantire la continuità delle trasmissioni bidirezionali dal campo verso l'infrastruttura di Centrale Operativa. La comunicazione dei segnali di teleallarme e di televigilanza, infatti, ha importanza fondamentale per la corretta conoscenza di cosa sta succedendo sull'obiettivo (c.d. *situational awareness*) ed è della massima importanza garantire la continuità.

C.2.a Piano di remotizzazione dei segnali

Uno degli aspetti centrali per i servizi di teleallarme e televigilanza è costituito dalla necessità di garantire la totale affidabilità e continuità dei collegamenti fra apparati di campo (impianti tecnologici di sicurezza di proprietà delle Amministrazioni Contraenti) e Centrale Operativa / Control Room.

Per assicurare la massima affidabilità dei collegamenti, l'Offerente intende effettuare uno **studio dei collegamenti e delle remotizzazioni** per garantire l'affidabilità delle trasmissioni.

L'analisi è effettuata nel periodo subito precedente l'effettivo avvio delle attività e durante il periodo di avviamento dalla Funzione **Team Integrazione e Remotizzazione,** interno al Team di Avvio e Riconsegna. Il risultato dell'analisi è un **Progetto Esecutivo di Remotizzazione**, che consente di remotizzare i segnali senza provocare soluzioni di continuità e soprattutto assicurando che tutti i segnali siano correttamente ridondati sia dal punto di vista fisico (presenza di apparati critici ridondati) che logico (logiche di gestione e programmazione che consentono di sfruttare le ridondanze fisiche in caso di guasto o anomalia). In tal modo durante la fase di avvio si garantisce la ridondanza dei collegamenti con la Control Room degli obiettivi / Centrale Operativa.

Il Progetto Esecutivo di Remotizzazione mette al centro la continuità dei collegamenti e la salvaguardia dei dati sensibili, definendo le linee guida metodologiche da seguire e le specifiche azioni progettuali per singolo impianto.

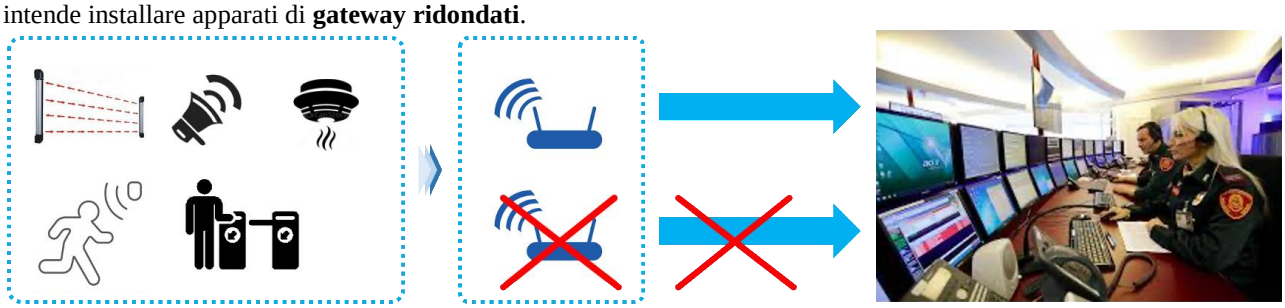
C.2.b Piano di Remotizzazione OSCURATO

C.2.c Soluzioni dedicate agli apparati gateway / router

Tali apparati garantiscono la trasmissione dei segnali provenienti dai combinatori e concentratori delle Centrali verso la Centrale Operativa. Costituiscono quindi un punto molto delicato perché in caso di guasto inibiscono la trasmissione fi più flussi di informazioni e segnali. Se non adeguatamente ridondati costituiscono un **punto unico di guasto**. L'Offerente ha quindi studiato specifiche soluzioni che garantiranno la ridondanza e l'affidabilità del segnale di uscita, sia a livello fisico sia a livello logico.

C.2.c.1.1 Soluzioni per la **ridondanza fisica** degli apparati gateway o router: **gateway ridondati**

Per consentire la continuità della trasmissione anche a fronte di un guasto degli apparati gateway, quindi, l'Offerente intende installare apparati di **gateway ridondati**.



Grazie alla ridondanza fisica dei gateway / router il sistema di comunicazione è immune ai guasti ed alle anomalie e assicura il **costante e continuo scambio di dati con la infrastruttura di Centrale Operativa dell'Offerente**

Figura 28 Approccio di ridondanza fisica dei Gateway / Router

Con questa scelta impiantistica, **l'infrastruttura fisica è robusta a fronte di eventuali guasti o anomalie di funzionamento.**

C.2.c.1.2 Soluzioni per la ridondanza logica degli apparati o router: **gateway ridondati con protocollo HRSP Cisco o equivalenti**

La semplice duplicazione del dispositivo router, che assicura la connessione all'esterno con la Centrale Operativa, è condizione necessaria ma non sufficiente per la robustezza delle trasmissioni, poiché gli indirizzi IP delle interfacce sono solitamente "statici"; gli host non sono in grado di passare automaticamente all'altro router in caso di guasto del loro default gateway, perché essi non sono capaci ad apprendere la topologia di rete tramite i protocolli di instradamento del livello rete.

L'Offerente gestirà quindi i flussi di dati verso la Centrale Operativa mediante apparati ***gateway* ridondati con protocollo HRSP Cisco o equivalenti. Essi hanno una logica di gestione che permette di sfruttare al meglio la presenza di gateway ridondati.**

L'HSRP (Hot Standby Router Protocol) è un protocollo che permette di assegnare un unico indirizzo in grado di "spostarsi" sempre sull'apparato funzionante, svincolando gli indirizzi IP dalle singole interfacce fisiche e di associarli invece a gruppi di interfacce, consentendone la raggiungibilità anche in caso di guasto.

Ciò garantisce automaticamente che ogni apparato mantenga la connettività con la Centrale Operativa attraverso il proprio default gateway anche in caso di guasto di uno dei router ridondanti.

Le soluzioni di ridondanza utilizzate sono quindi innovative, sia a livello fisico (architetture con ridondanza di apparati) sia a livello di logiche di gestione degli stessi (protocolli innovativi di gestione delle comunicazioni *fault tolerant*).

C.2.d Soluzioni dedicate ai canali e alle modalità di trasmissione

La principale preoccupazione dell'Offerente è quella di garantire non solo la ridondanza di elementi essenziali per la corretta trasmissione, ma anche la ridondanza di **canali di trasmissione** a disposizione di tali apparati. In mancanza di rete fissa, ad esempio, un gateway deve comunque essere in grado di comunicare con la Centrale Operativa e garantire la continuità di trasmissione dei segnali. Per ottenere questo risultato, le linee guida previste descritte di seguito.

C.2.d.1.1 Soluzioni per la ridondanza fisica dei canali di trasmissione a disposizione

Nel contesto del progetto di remotizzazione, la principale preoccupazione dell'Offerente è quella di garantire non solo la **ridondanza di apparati** essenziale per la corretta trasmissione, ma anche la rid**ondanza di canali di trasmissione a disposizione di tali apparati.**

In mancanza di rete fissa, ad esempio, un gateway deve comunque essere in grado di comunicare con la Centrale Operativa e garantire la continuità di trasmissione dei segnali. Per ottenere questo risultato, le linee guida previste sono le seguenti:

- **Utilizzo di trasmettitori radio in VHF / UHF bidirezionali con tecnologia IRS** (Integrated Radio System) e **canali di comunicazione ridondati**. Questa tecnologia permette di riunire in un unico elemento parte logica di elaborazione e parte radio. L'apparato selezionato permette di avere a disposizione, come back-up della trasmissione radio principale, sia la **linea telefonica** (protocollo Contact-ID) sia la **linea cellulare** (GSM /GPRS). In tal modo è assicurata la ridondanza di canali di comunicazione da e verso la Centrale Operativa. Inoltre, Al fine di incrementare la sicurezza delle comunicazioni, l'apparato può ricevere e inviare alle periferiche segnalazioni su una frequenza radio alternativa a quella primaria;
- **Collegamento dei combinatori telefonici con doppia tecnologia**, sia Rete cellulare GSM/GPRS sia su rete commutata. In tal modo è possibile sfruttare uno dei due canali a disposizione in caso di assenza di indisponibilità di uno dei due. I canali sono indipendenti fra loro e quindi garantiscono un elevato livello di ridondanza fisica;
- **Utilizzo di connessione di rete con sistema a doppia linea (linee dedicate)** su rete ad alta velocità (es. ADSL/HDSL/MPLS). Questa soluzione permette di avere a disposizione due potenziali "strade" per la gestione dei flussi di dati, con back-up per le comunicazioni verso la Centrale Operativa.

Trasmettitori radio in VHF / UHF bidirezionali con tecnologia IRS (Integrated Radio System)

L'Offerente intende utilizzare trasmettitori radio in VHF/UHF ad elevate prestazioni, quali quelli della Sicep IRS-8B **(o con caratteristiche similari)** con **tecnologia IRS (Integrated Radio System) o equivalenti.** Questa tecnologia utilizza una scheda capace di contenere, **in un unico elemento, logica di elaborazione e parte radio.** Questa consente i seguenti vantaggi:

- maggior controllo dei parametri di ricezione/trasmissione radio da parte del processore;
- assoluta affidabilità del dispositivo;
- elevate prestazioni tecnico / funzionali.

La periferica è caratterizzata da 8 ingressi – 8 uscite, espandibili a 32 IN-OUT, ed è dotata di tre canali di servizio (rete, tamper e batteria). Di seguito sono illustrate alcune delle caratteristiche peculiari, che valgono come caratteristiche minime garantite.

Multiprotocollo. L'apparato è versatile e multiprotocollo. Consente infatti di selezionare diversi protocolli di comunicazione (es. Sicep Alta Velocità, Sicep Bassa Velocità, Compatibili e cripto). Tale peculiarità consente di utilizzare, con estrema versatilità, il protocollo più idoneo al tipo di installazione da effettuare con un unico dispositivo. La periferica bidirezionale IRS-8B può essere utilizzata sia come trasmettitore che come comunicatore/ripetitore (REP).

Smart Repeater Network. L'unità IRS-8B mantiene ed integra la funzione di REP (ripetitore digitale) al fine di estendere il raggio di azione delle periferiche installate. Il collegamento in cascata fra più unità IRS-8B costituisce infatti un sistema di "ripetitori intelligenti" (SRN, Smart Repeater Network) che consente di apprendere tutti i cambiamenti, di instradare le segnalazioni dei dispositivi radio in maniera automatica e di scegliere il percorso migliore per trasmettere le informazioni in Centrale Operativa, rendendo la rete molto flessibile e robusta ad eventuali malfunzionamenti o attacchi.
Test dinamico della batteria. I dispositivi IRS effettuano un monitoraggio costante sulla tensione della batteria ed un controllo periodico sulla capacità effettiva della stessa, in modo tale da avere una diagnosi corretta sull'efficienza dell'accumulatore installato.
Semplicità di programmazione. Configurazione degli apparati mediante terminale portatile e software per PC Sicep Connect con collegamento seriale RS232 o USB. Attraverso pagine di programmazione dinamiche è possibile configurare e verificare istantaneamente tutte le attività dell'apparato: funzionamento dispositivo, qualità del segnale in ricezione, efficienza antenna, temperatura di funzionamento, livello batteria tampone, frequenze di trasmissione e ricezione, protocollo di comunicazione, etc.
Sinottico interattivo. Il software di programmazione Sicep Connect consente una visualizzazione istantanea di tutti i parametri operativi della periferica:

- Stato attuale parametri radio: stato trasmissione, stato ricezione, segnale valido, livello di segnale in ricezione, livello ultima segnalazione, potenza diretta, potenza riflessa dall'antenna e temperatura relativa al finale radio;
- Stato attuale periferica: livello batteria, *tamper* contenitore, tamper RS485, anomalia RS485, taglio antenna e presenza linea telefonica.

Le configurazioni possono essere effettuate inoltre da remoto, direttamente in Centrale Operativa.
Storico eventi. Le periferiche IRS sono in grado di registrare su un proprio storico tutti gli eventi (quali variazione ingressi, attivazione uscite, stato batteria, ecc.) con relativa data e ora ed una dettagliata descrizione. Il numero massimo di eventi memorizzabile è di 512 (al termine, sovrascrivibili) consultabili tramite software per PC Sicep Connect.
Back-up su linea telefonica o su rete GSM/GPRS. L'apparato selezionato permette di avere a disposizione, come back-up della trasmissione radio principale, sia la linea telefonica (protocollo Contact-ID) sia la linea cellulare (GSM /GPRS).

In tal modo **è assicurata la ridondanza di canali di comunicazione da e verso la Centrale Operativa.**

Seconda frequenza radio. Al fine di incrementare la sicurezza delle comunicazioni, l'apparato può ricevere e inviare alle periferiche segnalazioni su una frequenza radio alternativa a quella primaria.

C.2.d.1.2 Soluzioni per la ridondanza logica dei canali di trasmissione a disposizione: modalità di gestione della tecnologia multi-canale

Il collegamento multicanale con **back–up su rete GPRS/GSM** rappresenta allo stato attuale il massimo livello di evoluzione e di sicurezza nei collegamenti bidirezionali alle centrali operative. I sistemi radio tradizionali sono infatti vulnerabili: l'eventuale sabotaggio o anomalia di funzionamento sono rilevati solo in seguito a mancata risposta alla interrogazione ciclica, che avviene con periodicità pre-definita (in genere ogni ora).

La logica di gestione di **apparati multivettore** comporta invece la presenza di un modulo di gestione delle comunicazioni del sistema **interroga continuamente la periferica e rileva immediatamente l'eventuale disconnessione, attivando il canale di riserva.**

Inoltre, l'esistenza nel medesimo dispositivo della funzione di back-up su rete GPRS – con integrato il sistema di antisabotaggio "anti – jamming", eleva ulteriormente il grado di affidabilità di trasmissione di questa periferica bidirezionale.
Oltre a questi aspetti, le periferiche multivettore utilizzate dall'Offerente sono dotate di una "scatola nera" per la memorizzazione locale di tutti gli eventi, scaricabile da centrale e memorizzabile su HD.
I segnali saranno registrati regolarmente e con continuità in Centrale Operativa con data e ora su memoria storica dei sistemi telematici. Saranno :

- identificazione dell'impianto;
- tipo di allarme riscontrato;
- tipo di evento;
- data e ora dell'evento;
- tipo di provvedimento adottato;
- esito dell'evento.

Il monitoraggio di tutti i periferici avviene in modo ridondante: dalla Centrale Operativa con procedure automatiche dell'applicativo software (sorveglianza di rete, polling ciclici) e attraverso l'auto-diagnosi locale effettuata dal periferico stesso (controllo disponibilità della rete, polling periodici verso le centrali, controllo campo e mascheramento segnale GSM/GPRS, manomissione apparato, mancanza rete di alimentazione primaria e secondaria).
L'operatore in Centrale ha inoltre tutte le informazioni necessarie per eseguire ciò che la procedura di trattamento dell'evento ha previsto, sia in fase di verifica dell'evento, che nel corso dell'intervento, agevolandolo nella corretta attivazione delle contromisure stabilite dai protocolli d'intervento concordati con l'Amministrazione Contraente: attivazione pattuglie, FF.OO., VV.F., soccorso medico, squadre tecniche, etc.
L'operatore è in grado da qualsiasi postazione di: ricevere eventi ed allarmi; effettuare letture (livelli e volumi); gestire attivazioni (accensioni impianti o sistemi), anche in modo automatico attraverso fasce orarie di controllo; gestire video

server, con la visualizzazione delle immagini in live; esercitare attività di monitoraggio continuo sulla funzionalità degli apparati; monitorare i vettori di collegamento e la loro disponibilità; inviare comunicazioni – manuali e/o automatiche – al cliente, attraverso SMS, Fax, e-mail; estrapolare dati in formato elettronico, per interazione con altri sistemi informativi aziendali (commerciale, amministrativo, ispettorato, etc.).

C.2.e Soluzioni dedicate alla infrastruttura di Centrale Operativa

Per garantire la continuità operativa di gestione dei segnali provenienti dai sistemi di campo, il progetto di servizio prevede l'interconnessione ridondata delle Centrali Operative, a formare un'infrastruttura di Centrale Operativa ridondata e quindi *fault tolerant*.

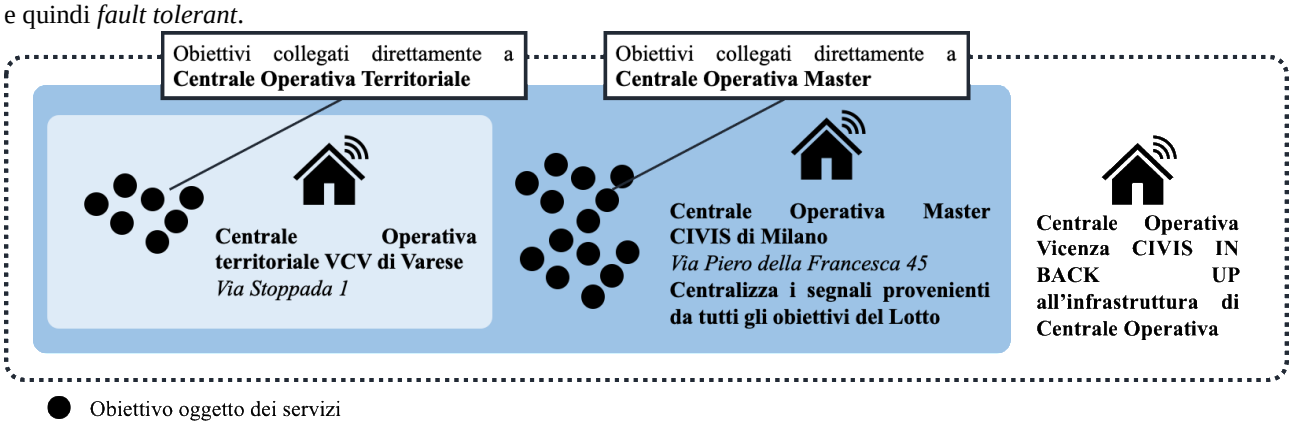


Figura 29 Struttura dell'infrastruttura di Centrale Operativa prevista per il Lotto, con evidenza delle Centrali Operative territoriali, delle Centrali Operative Master che concentrano tutti i flussi dati del Lotto, nonché delle Centrali Operative in back-up.

L'Infrastruttura di Centrale Operativa dell'Offerente è quindi ridondante grazie alla capacità di condividere i segnali bidirezionali scambiati. Ciò assicura la possibilità di poter disporre sempre di Back Up per le trasmissioni e per la gestione dei dati, assicurando la continuità operativa

Ridondanza degli apparati di ricezione delle Centrali Operative

Oltre alla ridondanza di Centrali Operative, **gli apparati di ricezione delle Centrali Operative sono tutti ridondati,** così da ottenere la massima affidabilità nella gestione dei flussi di dati. Ciò consente di gestire flussi di dati multipli e multi-canale in assoluta sicurezza.

E' presente inoltre un sistema di acquisizione e centralizzazione automatica dei dati provenienti dal campo, che permette di creare una partizione dei dati provenienti dalle periferiche remote. Questo sistema di gestione permette di gestire i dati provenienti dagli impianti oggetto della convenzione in maniera molto più efficace rispetto ai sistemi tradizionali, con maggiore velocità nella gestione dei dati trasmessi dalle periferiche remote, la possibilità del controllo statistico delle fasce orarie di accensione e spegnimento degli impianti e l'estrapolazione, anche mensile, di tutte le segnalazioni d'allarme pervenute (es. falsi allarmi, mancanza rete elettrica, segnalazioni di aggressione, allarmi tecnologici in genere).

Adozione dell'approccio "back-up caldo"

I flussi di dati bidirezionali scambiati fra Centrale Operativa e campo sono registrati su calcolatori duali in "backup caldo". Il backup a caldo o (backup dinamico) è applicato ai dati che rimangono disponibili per gli utenti mentre l'aggiornamento è in corso. Questo metodo evita i tempi di inattività degli utenti e la perdita di produttività e comunque la possibilità di accedere sempre in tempo reale alle elaborazioni e/o ai segnali pervenuti e registrati.

Ciò assicura l'affidabilità dei dati ma anche la reattività della struttura di ricezione nell'acquisizione dei dati trasmessi e nella possibilità di utilizzo contestuale, in supporto all'attività operativa.

Piattaforma per la gestione dei flussi di dati Civis Supervisor Platform (CSP)

L'infrastruttura di Centrale Operativa è gestita dalla piattaforma CSP, una "web application" ingegnerizzata dalla divisione IT di Civis per la ricezione e gestione di tutte le segnalazioni tecnologiche e di Sicurezza provenienti dal "campo". Essa **centralizza i protocolli di svariate tecnologie abilitanti su di un'unica piattaforma di gestione, a sua volta integrabile all'interno di ulteriori piattaforme, quali CSC.** L'architettura modulare ed espandibile di CSP e l'interfaccia web-based sono il valore aggiunto di un vero e proprio **Centro Operativo multi-vettoriale e polifunzionale** con la caratteristiche di garantire la più assoluta protezione dei dati e la massima tutela della privacy contro possibili intrusioni non autorizzate sia fisiche che informatiche. La piattaforma CSP dispone delle seguenti funzionalità

- Tracciatura di tutte le attività effettuate dagli operatori;
- Gestione di agende, programmate da CSP, per accensione/spegnimento o monitoraggio degli impianti con periodi standard, ferie, festivi, eccezioni;
- Statistiche interne sull'andamento di tutte le segnalazioni;
- Gestione integrata di tutte le comunicazioni da a e verso Clienti, registrando le conversazioni;
- Archiviazione tutte le segnalazioni ricevute compresi file audio, immagini, video;
- Invio di e-mail, su allarme, a due indirizzi differenti, programmabili indipendentemente, evento per evento.

Attraverso la piattaforma CSP, la Centrale operativa non riceve solo la segnalazione di allarme generico ma tutte le informazioni specifiche sullo stato dei sensori o delle apparecchiature che l'hanno generato, sulla cronologia e la dinamica degli eventi e sulla natura dell'emergenza. La Centrale Operativa è in grado di

visualizzare puntualmente quale apparato tecnologico ha generato l'allarme con evidenza sulla mappa del sito in gestione.

Grazie a questo processo automatizzato la Centrale Operativa è in grado di discriminare gli allarmi generati da intrusioni reali rispetto ad eventuali falsi allarmi, e integrare le tecnologie quali la geolocalizzazione delle pattuglie, necessarie per una pronta risoluzione dell'evento. Ogni segnalazione è accompagnata dalle seguenti informazioni consultabili in maniera immediata dall'operatore:

- I dati principali del sito da cui proviene la segnalazione di allarme;
- La tipologia degli impianti installati;
- La tipologia di connessione con i sistemi di sicurezza installati;
- L'elenco delle segnalazioni in ricezione;
- Visualizzazione degli eventi su mappe grafiche CSP consente anche di geo-referenziare tutte le periferiche collegate e di poter precaricare una planimetria legata all'utenza in modo da poter fare interagire gli allarmi direttamente sulla stessa;
- Procedure operative stabilite con il Cliente;
- Il controllo sulle fasce orarie di attività aziendale o di permanenza dell'utenza privata, aiutando l'operatore a discriminare eventuali dimenticanze o tentativi di accesso per coercizione del proprietario fuori dagli orari di apertura.

La centrale Operativa Civis dispone del **sistema SMART [→ cfr. par. C.1.d.2.4]**, ossia di una centralizzazione video integrata nella piattaforma CSP che permette all'operatore di poter effettuare una valutazione più rapida, efficace e risolutiva di una condizione di emergenza, anche in assenza di parte dei segnali per eventuale avaria o manomissione.

L'Operatore, ricevuta una segnalazione di allarme da un sito, potrà verificare in tempo reale le immagini riprese dal sistema di telecamere eventualmente presenti. Tale attività consentirà di verificare lo stato attuale della proprietà e visualizzare ogni possibile intruso all'interno dell'area inquadrata.

La possibilità di accedere anche alle informazioni registrate nei minuti precedenti fornisce all'operatore uno strumento inconfutabile per discriminare l'evento di intrusione da un tentativo eseguito solo per mettere alla prova il sistema di allarme. In entrambi i casi la Centrale Operativa di Civis può fornire importanti informazioni specifiche alle Forze dell'Ordine operanti sul territorio per un intervento tempestivo o per un'attività investigativa efficace e risolutiva e soprattutto per l'efficace gestione delle emergenze.

In particolare il sistema del cliente dialoga con il Centro di Controllo che consente, anche in multi-connessione, la visualizzazione su allarme o su richiesta dell'Operatore delle immagini in modalità Live e Play con ricerca cronologica dagli archivi periferici, la gestione di mappe grafiche, la ronda automatica e semiautomatica, l'export delle immagini e con il modulo software Setup, la tele-configurazione. In caso di allarme, sia da ingressi digitali che da activity detector e da diagnostica, il DVR può connettersi al Centro di supervisione gestendo fino a 3 indirizzi IP in modalità contemporanea o in *fallback*.

Tecnologia per l'attivazione della rosa di utenti interessati

La piattaforma CSP (Civis Supervisor Platform) include anche un approccio particolarmente importante ai fini di assicurare la pronta reattività ad eventi che possono interessare gli impianti e le trasmissioni. CSP Può infatti interfacciarsi con la rete telefonica nazionale e contattare, contemporaneamente, attraverso SMS o altri canali a disposizione, più utenti collegati alle segnalazioni degli impianti. CSP può distinguere fra:

- Segnali di malfunzionamento, per cui sono attivate, previo accordo dell'operatore di Centrale Operativa, chiamate al personale reperibile della struttura organizzativa per risolvere l'inconveniente / evento di anomalia – guasto;
- Segnali di allarme, per cui l'operatore può attivare in automatico, ad esempio, la pattuglia più vicina all'impianto che denunzia un segnale di allarme per eseguire la verifica sul posto.

Detto sistema garantisce l'esclusione di eventuali errori umani permettendo inoltre la gestione automatica con più utenti contemporaneamente. Tutto ciò comporta un alto grado di affidabilità del servizio offerto in quanto, gli operatori preposti, restano a disposizione degli utenti per assistere quelle situazioni che devono essere gestite direttamente ed esclusivamente dall'uomo.

C.3. Turnazione e sostituzione del personale

Nel presente paragrafo sono descritte le modalità operative adottate dall'Offerente per la gestione del personale. Esse seguono le linee guida:

- **Continuità**, in termini quantitativi e qualitativi, delle competenze del personale per la corretta esecuzione dei servizi;
- **Stabilità** del gruppo di lavoro, così da assicurare familiarità relativamente agli obiettivi vigilati e avere la perfetta conoscenza delle peculiarità, caratteristiche e necessità per mitigare il livello di rischio.

C.3.a Logica territoriale dei nuclei operativi

Ciascun gruppo di lavoro dedicato ai Servizi sul Territorio o sugli Obiettivi è organizzato su base territoriale:

- **Per quanto riguarda i servizi sul territorio** (vigilanza ispettiva, Pronto Intervento) l'Offerente suddivide il territorio del Lotto in aree di competenza, le cosiddette aree operative; all'interno di ciascuna aree, come accennato nella parte sezione organizzativa, opera un nucleo operativo dimensionato per la corretta erogazione dei servizi previsti. Le aree territoriali contigue possono supportarsi in caso di picchi di lavoro – di carico o di imprevisti.

- **Per quanto riguarda i servizi tecnici,** questi ultimi sono suddivisi per provincia di competenza, e assicurano in ogni momento la necessaria copertura di competenze nel caso fossero necessarie attività di manutenzione ordinaria, correttiva o straordinaria sugli impianti installati dall'Offerente (impianti e apparati di remotizzazione dei segnali e dei flussi video, altri impianti innovativi per offrire servizi di teleallarme e televigilanza evoluti quali NOD, sistema SMART illustrati nel paragrafo C.1, etc.)
- **Per quanto riguarda i servizi sugli obiettivi**, sono previsti nuclei operativi che, a seconda della saturazione e delle fasce orarie, possono essere dedicati esclusivamente ad un singolo complesso (sedi complesse, quali sedi di provincia, sedi di particolare sensibilità perché hanno in custodia informazioni sensibili o valori etc.) oppure ad una area territoriale di competenza, al cui interno possono operare per coprire i differenti servizi;

L'organizzazione territoriale permette di creare una struttura di risorse effettivamente aderente alle necessità di sicurezza dei singoli obiettivi sulle aree territoriali del Lotto.

Ciò consente inoltre di avere la necessaria flessibilità operativa, data la non omogenea distribuzione di obiettivi sul territorio. Al progredire della Convenzione, è sufficiente saturare ed aggiungere risorse all'interno delle aree interessate dagli ODF approvati.

C.3.b Strutturazione in gruppi di lavoro "estesi" OSCURATO

C.3.c Modalità di affiancamento in itinere

Per mantenere costante nel tempo la competenza e la conoscenza degli obiettivi da parte del gruppo di lavoro esteso, il progetto prevede **modalità di affiancamento in itinere**, *durante la rotazione progressiva del gruppo di lavoro esteso,* quando ritenuto necessario.

Al momento della rotazione periodica del gruppo di lavoro, quando ritenuto necessario (es. cambiamento delle prescrizioni di sicurezza, variazioni nelle modalità di erogazione dei servizi etc.) il sostituto affiancherà il personale titolare presso il presidio per un periodo, **a costo zero per l'Amministrazione Contraente.** E' pertanto previsto un **affiancamento** non solo a inizio dell'appalto o post inserimento di neo-assunti nel ruolo, come visto in precedenza, ma **anche in occasione delle rotazioni periodiche in caso di necessità.** I tempi di affiancamento saranno tipicamente pari ad un turno lavorativo. In caso di inserimento di una GPG neo-assunta o comunque di avvicendamento, l'Offerente ha definito specifiche soluzioni per garantire la continuità del gruppo di lavoro, delle competenze e della familiarizzazione acquisita, e quindi per garantire la **continuità del livello di servizio.**

C.3.d Modalità operative di avvicendamento (turnover) per sostituzione

Il progetto include specifiche *modalità gestione dell'avvicendamento e formazione* dei neo assunti.

In caso di avvicendamento del personale, l'Offerente ha previsto **specifiche soluzioni organizzative** per limitare l'impatto dell'eventuale turnover del personale, sempre utilizzando la **"camera di compensazione" degli addetti di sostituzione in rotazione progressiva a disposizione.** La modalità di gestione è illustrata nello schema concettuale di Figura 30**.** Con questo approccio organizzativo è possibile garantire una **rotazione minima** del personale sulle strutture e quindi una **altissima efficienza di esecuzione delle attività** (le risorse hanno una profonda conoscenza dei luoghi, delle particolarità e dei vincoli operativi eventuali), rispettando in pieno le richieste della documentazione di gara. L'Offerente si è anche impegnato nell'inserimento di soluzioni e modalità che consentano di mitigare il turnover, assicurando la stabilità del gruppo di lavoro per l'esecuzione dei servizi.

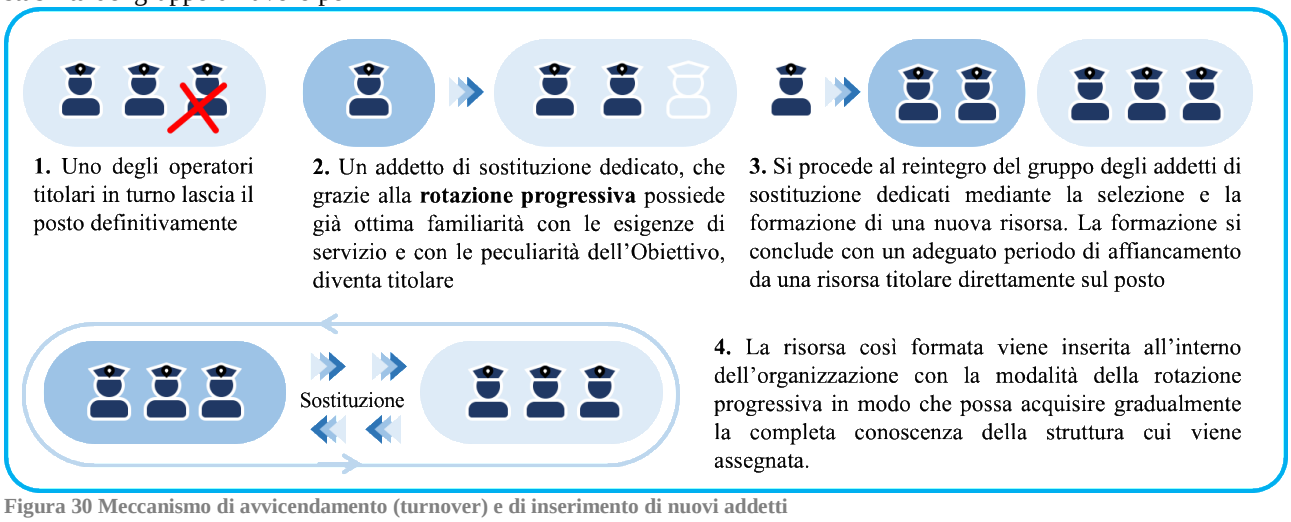


Figura 30 Meccanismo di avvicendamento (turnover) e di inserimento di nuovi addetti

C.3.e Modalità operative di prevenzione del turnover

Il progetto include specifiche *modalità di prevenzione del turnover a*l fine di garantire la stabilità del personale impiegato e la fidelizzazione al contesto di esecuzione.

- **Costruzione di un gruppo di lavoro stabile.** Il nuovo personale eventualmente impiegato sarà inoltre selezionato in base alla vicinanza della propria residenza alle aree ed ai siti oggetto del servizio. Ciò infatti, dall'esperienza dell'Offerente, permette di ridurre sensibilmente la tendenza del personale al cambiamento del posto di lavoro.

Modalità di gestione dei servizi con enfasi sulle necessità dei lavoratori (pianificazione dei turni). La disponibilità di risorse di sostituzione aggiuntive e la rotazione periodica degli addetti permettono di gestire le turnazioni del personale in maniera attenta alle esigenze di ciascuna persona, nei limiti consentiti dagli standard di servizio e di sicurezza dei siti vigilati. È possibile, ad esempio, modificare rapidamente i turni di una persona che ne abbia necessità, oppure variare le risorse che devono effettuare i turni notturni, e così via. Inoltre, al fine di creare una squadra di lavoro stabile dedicata al servizio, le turnazioni sono costanti, ossia l'operatore è assegnato ad un obiettivo o a un insieme limitato di obiettivi, sui quali la programmazione può ruotare nel medio periodo.

- **Programmazione dei turni con estensione della fascia oraria non superiore alle 8 ore.** Per assicurare condizioni lavorative agevoli, ma anche per garantire la costante attenzione e le migliori condizioni psico – fisiche del personale preposto a delicati compiti di vigilanza ispettiva, l'Offerente prevede ove possibile turni della lunghezza massima di 8 ore, con la possibilità di segmentare tale fascia oraria a seconda di specifiche esigenze del personale.
- **Monitoraggio della soddisfazione del personale.** Per poter cogliere "segnali deboli" che possono preannunciare problematiche nella gestione del personale, il progetto di servizio prevede un **controllo, con frequenza semestrale**, del livello di soddisfazione all'interno della organizzazione di commessa. Il controllo, effettuato sotto forma di **questionario totalmente anonimo**, ha lo scopo di individuare **elementi sistematici di instabilità, elementi di disagio o insoddisfazione** all'interno dell'organizzazione che possono portare a conflitti e quindi suggerisce le azioni per poter appianare tali elementi.

C.3.f Modalità operative di gestione delle sostituzioni pianificate e delle assenze non previste

La gestione delle assenze, sia prevedibili sia non prevedibili, è stata oggetto di un'approfondita analisi da parte dell'Offerente, al fine di garantire la copertura continua dei servizi e assicurare che il sevizio sia svolto senza soluzione di continuità.

C.3.f.1 Modalità per le sostituzioni pianificate / pianificabili

C.3.f.1.1Dimensionamento per le sostituzioni pianificabili

Per garantire la massima robustezza a fronte di assenze ordinarie e straordinarie prevedibili (malattia, infortunio, gravidanza, puerperio, condizioni meteorologiche dichiarate dai bollettini, eventi sociopolitici preannunciati, etc.) l'Offerente ha ricavato dall'analisi statistica sulle proprie commesse (intero territorio nazionale), il tasso "fisiologico" di sostituzione, che si attesta intorno al 16 - 18% circa. Nella pianificazione della dislocazione del personale presso le postazioni dell'Amministrazione Contraente, si mantiene una percentuale pari al 20% dei lavoratori (denominati sostituti), compatibilmente con i requisiti dei CCNL di categoria sottoscritti, al fine di poter coprire tutti i turni di riposo settimanali previsti. L'ufficio competente emette con cadenza quindicinale i turni del proprio personale dove sono riportati gli orari di servizio giornalieri, i giorni dei riposi spettanti e la postazione assegnata in doppia copia e sottoscritta dal lavoratore, provvede a fornire i mattinali di tutto il personale al Capo Servizio per la corretta gestione dei turni comprese eventuali variazioni per (malattia ferie etc.) e per ogni altro tipo d'impedimento. Il Capo Servizio inoltre comunicherà agli Uffici Competenti tutte le anomalie riscontrate e le emergenze verificatesi giornalmente al fine di garantire la continuità dei servizi resi.

> Come ulteriore parametro di sicurezza, l'Offerente prevede di dimensionare la rosa delle risorse di sostituzione, sia dedicate sia condivise, in ragione quindi di una **percentuale pari circa al 25% del personale direttamente impiegato nel servizio**.

Il dimensionamento, effettuato generalmente mediante personale condiviso, permette di sopportare indisponibilità, anche multiple, del personale.

C.3.f.1.2Dimensionamento per le sostituzioni pianificabili

> L'Offerente ha definito un sistema di gestione delle assenze programmate / programmabili all'interno del Sistema Informativo Gestionale.

Per assicurare la continua copertura dei turni, l'Offerente ha predisposto specifiche soluzioni per **assenze programmate / programmabili** del personale, quali la gestione, nel modulo di Programmazione, del **Piano di formazione e sostituzione integrato con il piano ferie e assenze.** Tale piano, compilato con alcuni mesi di anticipo, permette di anticipare i fabbisogni di personale in quantità e qualità (competenze) e quindi di garantire la continuità dei servizi.

In particolare, la programmazione delle ferie spettanti ai lavoratori, come stabilito dai CCNL di categoria sottoscritti e precisamente su due periodi estivo e invernale. Le **ferie estive** vengono erogate di norma dal 15 giugno al 15 settembre di ogni anno, suddivise per ogni dipendente in giorni 15 di calendario. L'ufficio del personale emette il piano ferie entro 20 marzo di ogni anno e dopo averlo trasmesso a tutto il personale provvede alla sostituzione; dopo aver stilato il programma delle ferie estive, provvede a comunicare alla propria direzione il numero dei dipendenti da sostituire con cadenza quindicinale e necessari per la copertura delle postazioni. La direzione provvede in caso di necessità, dopo aver selezionato e formato, all'assunzione di personale a tempo determinato per un periodo non inferiore a mesi 4. Mentre la gestione delle **ferie invernali** che vanno dal 1° ottobre al 30 maggio di ogni anno per un massimo di 7 giorni di calendario saranno garantite attraverso il personale addetto alle sostituzioni dei riposi settimanali e se necessario attraverso nuove assunzioni a tempo determinato.

C.3.f.2 Modalità per le sostituzioni non pianificate / non pianificabili

C.3.f.2.1 Modalità di anticipazione delle assenze pre-turno **OSCURATO**

C.3.f.2.2 Modalità di attivazione progressiva delle risorse per la copertura delle indisponibilità non previste

L'Offerente ha messo a punto una ***procedura di attivazione progressiva*** delle risorse per la copertura delle eventuali indisponibilità non segnalate "dell'ultimo momento".

Grazie all'applicazione **Civis.TEAM** è possibile anticipare l'informazione sulla indisponibilità e garantire sempre la presenza di personale addestrato e competenze per l'erogazione dei servizi. Questo anche grazie alla specifica procedura di attivazione delle risorse per gestire le indisponibilità.

Se si verifica, nonostante gli strumenti di prevenzione, l'indisponibilità di personale per l'effettuazione dei servizi di vigilanza, ad esempio la mancata timbratura di una GPG che tuttavia aveva confermato la propria presenza, l'Offerente ha definito la seguente procedura, che prevede l'attivazione progressiva di vari elementi organizzativi e che permette di effettuare la sostituzione, anche non preventivamente comunicata, di una GPG in soli 30 minuti [→ cfr. Figura 47].

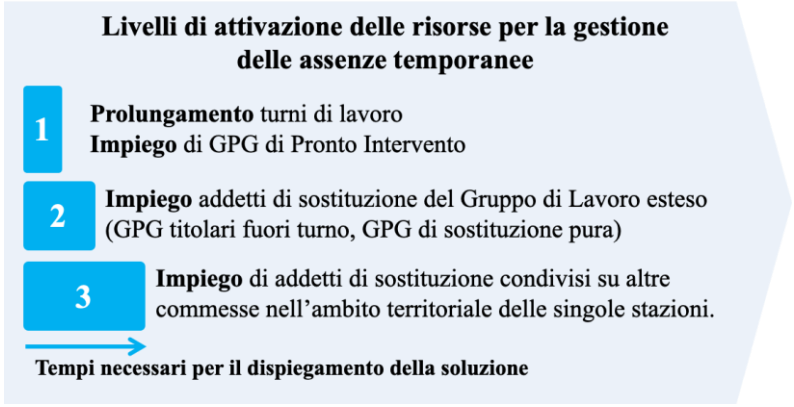


Figura 31 Schema concettuale con i livelli di attivazione delle risorse per la gestione delle indisponibilità non previste

Soluzioni LIVELLO 1. Le soluzioni di prima linea (soluzioni tampone per minimizzare gli effetti dell'indisponibilità e garantire la continuità del servizio) sono:

[1] il prolungamento del turno dell'addetto a copertura completa dell'intero servizio, se disponibile. Con questo accorgimento è possibile assorbire eventuali ritardi ovvero assenze di personale e garantire la continuità del servizio mentre la Centrale Operativa attiva le risorse di sostituzione dedicate all'obiettivo ovvero all'area territoriale:

[2] l'immediata attivazione del personale di sostituzione ove non fosse presente il turno precedente;

[3] l'attivazione, in caso di necessità, di GPG di pronto intervento grazie al meccanismo di copertura degli obiettivi *durante gli orari di cambio turno*, in modo da garantire la continuità / presenza di personale durante il dispiegamento delle altre soluzioni organizzative per minimizzare l'impatto.

L'Offerente, grazie alla copertura territoriale di autopattuglie che coprono il territorio del Lotto entro gli in torni territoriali di ubicazione degli obiettivi, interviene con una pattuglia di pronto intervento che prende in consegna il servizio ed effettua il servizio di vigilanza, fissa o ispettiva. Grazie a questa misura, nel periodo subito prima e a ridosso dei cambi turno i coordinatori di ciascuna stazione sono sicuri che *vi è sempre una pattuglia in appoggio per risolvere eventuali problematiche di personale in ritardo o mancante.*

Soluzioni LIVELLO 2. A valle delle soluzioni tampone, o in assenza di turni precedenti, l'Offerente può attivare quindi le soluzioni di seconda linea, quale **l'attivazione** degli addetti di sostituzione. Per ciascun sito e per ciascuna fascia oraria è definita una **rosa di addetti di sostituzione in reperibilità**, che possono raggiungere il sito in brevissimo tempo anche grazie alla **estesa rete di mezzi dell'Offerente presente sul territorio del Lotto**.

Focus: Rosa di addetti di sostituzione in reperibilità:

Soluzioni LIVELLO 3. In caso di ulteriore necessità (assenze estese, particolari situazioni operative non preventivabili a priori) è prevista **l'attivazione** immediata delle ulteriori risorse GPG condivise sul territorio, che consentono la copertura di assenze anche di notevole entità. La situazione delle coperture dei turni e le eventuali assenze sono disponibili in tempo reale per consultazione anche ai Referenti dell'Amministrazione Contraente, attraverso la piattaforma CSC.

Attualmente, il numero di personale condiviso sul territorio del Lotto, in pronta attivazione dietro richiesta, è il seguente:

Risorse condivise sul Lotto di pronta attivazione	GPG	Pattuglie diurne	Pattuglie notturne
Totale Lotto 01	**319**	**12**	**37**

La procedura illustrata permette di **minimizzare l'impatto delle assenze non programmate del personale**. La presenza di una procedura informatizzata **mette inoltre a disposizione dell'Amministrazione i dati relativi**, offrendo così un importante strumento di monitoraggio del livello di servizio (gestione delle indisponibilità e tempistiche di sostituzione).

C.4. Procedura di verifica dei livelli dei servizi ed azioni volte a migliorarli

C.4.a Modello procedurale dell'autocontrollo

L'Offerente ha ulteriormente migliorato le proprie **procedure di autocontrollo** dei sevizi in Convenzione. Esse si basano:

- **Su un ciclo di miglioramento continuo**, che permette di evidenziare co costanza eventuali scostamenti rispetto ai livelli di servizio condivisi e attesi. Il ciclo permette di identificare, sulla base degli scostamenti, qualità e quantità delle azioni correttive eventuali;

- **Su un continuo ritorno informativo**, effettuato direttamente dalle GPG, dal personale di coordinamento operativo, da figure organizzative deputate al controllo (Auditor e Servizio Ispettorato GPG).

L'autocontrollo definito dall'Offerente si basa su **due tipologie di verifica, integrabili fra loro all'interno della reportistica periodica:**

- **Verifiche automatiche.** Sono svolte mediante l'elaborazione dei dati registrati all'interno della piattaforma CSC. La piattaforma integra i dati provenienti dalla Centrale Operativa (sistemi di geolocalizzazione, dati dagli impianti di teleallarme e televigilanza), gestiti dalla **piattaforma CSP**, con i dati provenienti dai sistemi di tracciatura delle presenze e dei sistemi di certificazione elettronica delle attività di ronda ispettiva, nonché dal sistema di workflow documentale (schede di consuntivazione, rapporti di servizio etc.);
- **Verifiche ispettive.** Le verifiche ispettive sono svolte da personale preposto (personale operativo, di coordinamento ovvero *Auditor* interni dell'Offerente) i cui risultati sono conservati all'interno di **check List di controllo**. Queste sono *completamente integrate* con il Sistema informativo e sono gestite e compilabili *direttamente sul campo ed in tempo reale*, grazie ai tablet / smartphone del personale operativo e di controllo.

SLA	METODO DI CALCOLO	LEGENDA
Rispetto dell'orario di inizio turno (OI), misura il rispetto degli orari di turnazione	$OI = \frac{N_{i\_rit}}{N_{tot}}$	▪ N_{i_rit}: n° turni iniziati con ritardo ▪ N_t: n° totale dei turni previsti
Rispetto dell'orario di fine turno (OF), misura il rispetto degli orari di turnazione	$OF = \frac{N_{f\_rit}}{N_{tot}}$	▪ N_{f_rit}: n° turni finiti con anticipo ▪ N_t: n° totale dei turni previsti
Tempo di sostituzione medio (TSM), misura la tempestività di sostituzione in caso di assenza della GPG	$TSM = \frac{\sum T_s}{NS}$	▪ $\sum T_s$: sommatoria dei tempi di sostituzione ▪ NS: n° totale delle sostituzioni
Rispetto dei passaggi di ronda (PR), misura la corretta esecuzione del servizio di ronda	$PR = \frac{P_{ne}}{P_t}$	▪ P_{ne}: n° passaggi non eseguiti ▪ P_t: n° totale passaggi da eseguire
Indice di funzionamento degli impianti tecnologici (FI), misura l'efficienza dei componenti impiantistici manutenuti	$FI = \frac{H_g}{H_t}$	▪ H_g: ore di guasto degli impianti ▪ H_t: ore totali di funzionamento
Indice di Tempestività (IT), misura la capacità di eseguire l'intervento tempestivamente	$IT = 1 - \frac{S_r}{S_t}$	▪ S_r: n° interventi non eseguiti nei tempi stabiliti ▪ S_t: n° totale richieste
Efficacia di Intervento (EI), misura la qualità dell'intervento eseguito	$EI = 1 - \frac{I_{NC}}{I_C}$	▪ I_{NC}: numero interventi ritenuti non conformi ▪ I_C: numero interventi controllati
Tempo di risposta Call Center (TR), misura il tempo di risposta del Call Center	$TR = \frac{R_r}{R_t}$	▪ R_r: n° risposte non avvenute entro i tempi stabiliti ▪ R_t: n° totale chiamate
Indice di Affidabilità del Servizio (IAS), controlla la capacità operativa dei tecnici e l'efficienza del servizio erogato	$IAS = 1 - \frac{RS}{I_T}$	▪ RS: numero di reclami/solleciti ricevuti ▪ I_T: numero di interventi fatti
Indice di Riscontro Positivo della Valutazione del Servizio (IRPVS), misura la soddisfazione dell'utenza nei confronti del servizio offerto	$IRVPS = \frac{Q_{ep}}{Q_f}$	▪ Q_{ep}: numero di questionari che hanno dato esito positivo ▪ Q_f: numero totale di questionari fatti

Figura 32 Stralcio del cruscotto KPI definibile u Report On Line

Grazie al ritorno informativo garantito da numerosi strumenti a disposizione, **è possibile definire specifici indicatori o KPI con i rispettivi valori di soglia.** In base a questi ultimi, si valutano i differenziali fra livelli di servizio / prestazioni obiettivo ed effettivi, individuando anche quantità e qualità delle azioni correttive per mantenere il singolo contratto attuativo "in rotta" rispetto alle attese. L'avanzatissimo sistema di reportistica **Report On Line di CSC** permette di elaborare KPI pre-definiti e di inserire indicatori personalizzati, coerentemente con le necessità dell'Amministrazione.

C.4.a.1 Organizzazione del modello di controllo

L'Offerente ha previsto specifiche competenze per la gestione del ciclo di miglioramento continuo, sotto ogni punto di vista. Data la particolare importanza delle tematiche ambientali e della protezione dei dati personali, sono previste figure organizzative specifiche quali la Funzione *Gestione Ambientale* e *Compliance Normativa e Protezione Dati Personali*.

Qualità Aziendale e Sicurezza. Implementa e gestisce il processo di ottenimento e rinnovo delle certificazioni del Sistema di Gestione. Presiede la configurazione del sistema di monitoraggio e controllo sul livello di servizio erogato nonché sull'obsolescenza della strumentazione utilizzata nell'ambito dei servizi. Include anche la figura del RSPP. Ha fra l'altro la responsabilità della scrittura delle disposizioni di servizio che debbono essere rispettate a livello di coordinamento e a livello operativo e, in questo, si interfaccia con i Referenti dell'Amministrazione.

Servizio Ispettorato. La Funzione è composta da GPG che controllano la conformità al Regolamento di Servizio obbligatorio e alle disposizioni di servizio, per tutti i servizi oggetto della Convenzione.

Auditing Interno e Miglioramento Continuo. Queste figure, interne all'Offerente ma appartenenti a linee gerarchiche indipendenti, effettuano le verifiche relative a processo e risultato, alle misure di tutela ambientale, alla sicurezza sul lavoro, alla tutela dei dati personali, nonché le attività di recepimento della Customer Satisfaction, in maniera tale da garantire la costanza ed il miglioramento continuo del livello di sevizio erogato. Effettuano la reportistica su tutti i Servizi erogati ed evidenziano eventuali anomalie nell'erogazione. Definiscono inoltre le azioni correttive per la risoluzione delle non conformità. Monitorano nel tempo l'efficacia delle azioni correttive già implementate.

Gestione Ambientale. Cura la verifica delle soluzioni e procedure di gestione ambientale, previste dalla Norma UNI 14001. Supporta l'Auditing Interno e Miglioramento Continuo. Promuove l'integrazione di specifiche soluzioni per la mitigazione dell'impatto ambientale all'interno del RTI (es. progetto Green Patrol, cfr. par. D.3).

Compliance Normativa e Protezione Dati Personali. Presiede le verifiche relative alla protezione dei dati personali e delle informazioni sensibili con il supporto dell'Auditing Interno.

Personale e Formazione. Data l'importanza della formazione per ottenere risorse professionali e competenti, il sistema di ritorno informativo comprende anche la verifica del processo formativo, inteso sia come rispetto dei programmi di formazione di ciascuna persona, sia l'efficacia dell'azione formativa (verifica di apprendimento e di assimilazione della formazione erogata). La Funzione Personale e Formazione effettua periodicamente le verifiche a caldo e a freddo per individuare eventuali differenziali fra competenze obiettivo e competenze effettive del personale.

C.4.a.2 Strumenti per le procedure di autocontrollo

L'obiettivo dell'Offerente è quello di offrire uno strumento per la rilevazione della qualità del servizio che abbracci tutte le dimensioni del servizio, compresa la percezione e la formazione degli operatori (aspetti questi solitamente trascurati ma invece essenziali per la piena conformità del servizio e soddisfazione del Committente). Sono pertanto previsti *specifici strumenti* all'interno delle procedure di autocontrollo, che permettono una precisa e puntuale rilevazione dei livelli di servizio erogato. **Essi sono tutti integrati nella piattaforma informativa CSC.**

C.4.a.3 Piattaforma CSC e funzionalità specifiche per l'autocontrollo OSCURATO

C.4.a.4 Check List per le visite ispettive

Le check list per le visite ispettive di processo e di risultato, anche dette griglie di riscontro, sono utilizzate per le verifiche ispettive e sono gestite elettronicamente dall'applicazione **CIVIS.AUDIT**, come detto. Con le check list il personale preposto ai controlli registra *real time* i risultati delle verifiche sulla piattaforma CSC, che sono così immediatamente disponibili alle elaborazioni.

Le check list sono registrate in maniera trasparente all'interno del Sistema Informativo e sono accessibili ai Referenti dell'Amministrazione Contraente per eventuali elaborazioni indipendenti.

Le check list saranno utilizzate anche per valutare i risultai delle simulazioni periodiche, soprattutto per "mettere alla prova" il dispositivo di intervento in caso di emergenza (risposta entro i tempi richiesti / dichiarati, rispetto delle procedure di emergenza etc.)

Le check list sono utilizzati anche per i *Mistery Audit*, **Audit in incognito** sempre realizzati dalla Funzione Audit Interno e Miglioramento Continuo, che hanno la finalità di verificare il rispetto delle procedure e delle disposizioni di servizio da parte degli operatori presso gli obiettivi, durante i turni di lavoro.

C.4.a.5 Check List per le visite ispettive

Check list sulla formazione. Attraverso CIVIS.AUDIT è possibile anche condividere i dati relativi alla conformità del processo di formazione delle competenze attraverso i seguenti strumenti:

- Check list della conformità delle attività formative rispetto ai programmi formativi;
- Check list delle verifiche "a caldo", subito a valle della formazione erogata
- Check list delle verifiche a freddo, a distanza temporale dall'erogazione, per valutare l'effettiva applicazione sul campo di quanto appreso.

C.4.a.6 Questionari di soddisfazione

Ulteriori strumenti del sistema di controllo sono i questionari di verifica della soddisfazione dei Referenti dell'Amministrazione Contraente e del Soggetto Aggregatore, parte del sistema tracciabile di Customer Satisfaction e rilasciati all'interno delle apposite sezioni della piattaforma **Civis Security Cloud**.

I questionari attribuiscono un punteggio a differenti aspetti riguardanti la percezione del servizio da parte del soggetto Referente (differenziati per Referente dell'Amministrazione e per Referenti del Soggetto Aggregatore), quali cortesia e professionalità del personale, perfezione del livello di servizio erogato sul campo etc.

L'elaborazione dei questionari permette di determinare il livello di percezione del servizio da parte dei Referenti e degli utenti.

C.4.a.7 Dettaglio delle procedure del processo di miglioramento continuo

Di seguito è illustrata la tabella relativa alle procedure di verifica del sistema di controllo. Sono in evidenza modalità di controllo, strumenti utilizzati, responsabili del controllo e frequenza definita.

Tipologia di controllo	Portale / App CSC	Sistema di tracciatura	Raccolta Reclami	Check List	Check List formazione	Questionari Soddisfazione	Personale Operativo	Coordinatori / Responsabili	GPG Ispettorato	Auditor	Compliance	Personale e Formazione
Autocontrollo quotidiano. Comprende i controlli di processo effettuati giornalmente dal personale operativo e di coordinamento. Verificano il costante allineamento alle consegne di servizio, alle procedure convenute, al Regolamenti di Servizio.												

Tipologia di controllo	Portale / App CSC	Sistema di tracciatura	Raccolta Reclami	Check List	Check List formazione	Questionari Soddisfazione	Personale Operativo	Coordinatori / Responsabili	GPG Ispettorato	Auditor	Compliance	Personale e Formazione
Verifica consegne di servizio (decoro, comportamento etc.)	●		●	●			G	G				
Conformità nella compilazione di registri di servizio (registro consegne, registro degli eventi, etc.)	●						G	G				
Conformità delle procedure e delle dotazioni di sicurezza	●						G	G				
Certificazione delle presenze e delle attività (sistema di tracciatura con etichette NFC)		●					G	G				
Controllo a sistema del corretto funzionamento degli impianti tecnologici (segnali) e relativa reportistica	●						G					
Controlli di processo. Verifica della conformità delle procedure seguite dal personale ai regolamenti di servizio, alle prescrizioni di servizio e di sicurezza. ("le procedure sono conformi alle prescrizioni?"). I controlli sono focalizzati sulla verifica del rispetto del Regolamento di Servizio e delle disposizioni di servizio.												
Conformità al Regolamento di Servizio e codice di comportamento			●	●		●			ME			
Corretta applicazione delle metodologie operative		●		●	●				ME			
Conformità delle dotazioni del personale				●	●				ME			
Conformità delle procedure adottate alle prescrizioni D.M. 269/2010 per i singoli servizi attivati	●	●		●	●				ME		TR	
Conformità al Piano di Gestione Ambientale				●						TR		
Conformità alle prescrizioni della normativa sulla sicurezza sul lavoro (D.L.gs 81/08 e s.m.i.)				●						ST		
Conformità alle alla tutela dei dati personali GDPR				●							TR	
Controlli di risultato. Sono focalizzati ad esempio sul rispetto delle fasce orarie e dei turni programmati, del tempo di intervento, del numero e frequenza delle visite ispettive, sul rispetto delle turnazioni, sul livello di capacità operativa e gestionale dei sistemi, sulla disponibilità del Portale CSC, sulla conformità di collegamento e disponibilità dei sistemi di sicurezza.												
Conformità del registro consegne (elettronico) e dei turni	●								ME			
Esecuzione e puntualità delle attività programmate	●	●								CO		
Presenza del personale nelle fasce orarie e nei turni previsti	●	●								CO		
Esecuzione delle ronde		●								CO		
Funzionalità degli impianti tecnologici e/o loro gestione	●									ME	TR	
Tempi d'intervento (pronto intervento)	●	●								ME		
Controllo di Customer Satisfaction e Percezione. I Controlli di Customer Satisfaction sono mirati a evidenziare il livello di soddisfazione dei Referenti dell'Amministrazione Contraente e del Soggetto Aggregatore. I **controlli di percezione** servizio offerto sono basati su questionari, raccolta reclami e Mistery Audit. Sono finalizzati a individuare, al di là del rispetto delle consegne di servizio, la percezione del servizio e l'aderenza di questa ai parametri oggettivi misurati.												
Raccolta ed elaborazione reclami	●		●							TR		
Verifica di soddisfazione Referenti Amm.ni Contraenti			●			●				TR		
Verifica di soddisfazione Referenti Soggetto Aggregatore			●			●				SE		
Mistery Audit				●						AN		

Tipologia di controllo	Portale / App CSC	Sistema di tracciatura	Raccolta Reclami	Check List	Check List formazione	Questionari Soddisfazione	Personale Operativo	Coordinatori / Responsabili	GPG Ispettorato	Auditor	Compliance	Personale e Formazione
Controllo della Formazione. Sono effettuati dal personale di Audit e Miglioramento Continuo in collaborazione con la Funzione Personale e Formazione. Hanno lo scopo di verificare il formale rispetto dei programmi formativi del personale (possesso delle certificazioni, presenza ed effettuazione dei corsi assegnati, etc.). Tale verifica permette di considerare il primo elemento della verifica delle competenze, ossia l'erogazione della formazione. Il secondo elemento, ossia l'assimilazione dei contenuti, è verificata attraverso verifiche a caldo (subito a valle della formazione erogata), a freddo (a distanza temporale dalla formazione erogata) e dalla valutazione delle non conformità di processo e di risultato associabili e ascrivibili a ciascuna persona. Questo strumento permette quindi di individuare le azioni formative e correttive per riallineare le competenze del persone.												
Controllo progressione del percorso formativo	●				●							CN
Controllo a **caldo**					●							CN
Controllo a **freddo**					●							QU
Audit di simulazione operativa. Sono effettuati per valutare periodicamente l'efficacia di implementazione delle procedure, in particolare per quanto concerne la gestione dei siti sensibili (sedi di Enti con presenza di grosse somme di denaro, banche dati e informazioni ad alta sensibilità). Tali audit verificano la comunicazione in situazione di emergenza, la tempestività del Pronto Intervento, la correttezza e completezza della documentazione inviata all'Amministrazione e relativa agli eventi accaduti.												
Esecuzione audit simulazione operativa (siti ad elevata sensibilità	●	●	●	●		●				SE		

CO: continua. ST: settimanale. ME: mensile. TR: trimestrale. QU: quadrimestrale. SE: semestrale. AN: annuale. CN: contestuale a formazione.

C.4.a.8 Modalità di analisi dei controlli effettuati e di gestione delle criticità

Tutti gli strumenti di raccolta informazioni sono **integrati all'interno della piattaforma CSC, ed alimentano la base dati da cui le potenti funzionalità di analisi ed elaborazione dati – Report On Line - consentono di confrontare i livelli di servizio ottenuti con i livelli di servizio di automonitoraggio proposti.**

Tutti gli strumenti sono accessibili attraverso dispositivi portatili di campo (smartphone in dotazione al personale). Grazie alla elaborazione dei dati integrati all'interno del Sistema Informativo, l'Offerente ha strutturato un **cruscotto degli indicatori di servizio**, che permette un'analisi anche temporale dell'evoluzione degli indicatori del livello di servizio in maniera personalizzata per ciascuna Amministrazione Contraente.

Mensilmente è messo a disposizione, all'interno della sezione dedicata, il documento "Report sulla verifica dei servizi", suddiviso secondo i servizi prima citati. Le sezioni sono strutturate:

- in una prima parte di **sintesi delle risultanze**, in cui sono presentati i valori dei KPI, il loro trend storico, la eventuale disaggregazione per obiettivo o per ambito territoriale, a seconda delle esigenze della Amministrazione Contraente;
- in una sezione contenente le **informazioni di dettaglio**, ossia:
  - Il **registro degli eventi**, per singolo obiettivo, con l'evidenza delle ispezioni effettuate.;
  - I **file log** con le registrazioni di dettaglio di tutti i dati di tracciatura delle attività, per ciascun servizio. Tali dati, forniti in maniera trasparente, consentono all'Amministrazione di condurre ulteriori analisi se necessario o a richiedere nuove viste / query sui dati di gestione dei servizi;
  - Tutte le **schede di audit** compilate durante le visite ispettive, strutturate ed ordinate per obiettivo e per visita ispettiva;
- In una sezione contenente le **azioni correttive** ed i **conseguenti piani di rientro** proposti per risolvere le singole non conformità.

Comitato di Gestione ODF

I risultati delle analisi sui controlli effettuati sono condivise con l'Amministrazione Contraente attraverso il **Comitato di Gestione ODF**. Esso **[→ cfr. par. A.1.b.2.2]** riunisce con **periodicità trimestrale** le figure di riferimento dell'Amministrazione Contraente e dell'Offerente. Il Comitato è uno strumento utile per **condividere in maniera trasparente** eventuali "casi di successo" nell'ambito del contratto ed **eventuali situazioni con criticità sistemiche**. Nella seguente tabella sono illustrate le figure che partecipano stabilmente alle riunioni periodiche del Comitato.

Soggetto	Componenti del Comitato di Miglioramento Continuo
Offerente	Supervisore (facoltativo), Gestori del Servizio, Funzione Miglioramento Continuo.
Amministrazione	Supervisori, REC, Referenti dell'Amministrazione per la Security.

L'elemento progettuale permette la condivisione e soprattutto un ciclo di miglioramento esteso a tutte le Figure organizzative interagenti nell'ambito dell'ODF. In particolare consente il monitoraggio e la condivisione della documentazione e delle risultanze dei piani di rientro delle criticità riscontrate.

Modalità di analisi e di definizione delle azioni correttive

Il verificarsi di valori negativi degli indici dei livelli di servizio costituisce tuttavia un "segnale di guasto" nel sistema delle procedure e dei risultati ottenuti dall'Offerente.

Ecco perché l'approccio progettato per l'appalto consiste in:

- **Ricerca della causa scatenante il "guasto",** ossia il valore negativo dello specifico indice oppure l'andamento discendente nel tempo (trend negativo) dello stesso;
- **Implementazione delle MISURE DI GESTIONE,** ossia delle azioni specifiche per far sì che gli indici di servizio ritornino ai valori positivi di riferimento;
- **Implementazione delle MISURE DI PREVENZIONE,** ossia delle azioni specifiche per far sì che le cause alla base del peggioramento degli indicatori di prestazione / controlli e verifiche non si ripetano.

Lo scopo dell'Offerente è quello di selezionare le cause da aggredire prioritariamente, che portano i risultati negativi e quindi potenziali penali e disservizi all'Amministrazione Contraente:

Risoluzione immediata della Non Conformità (NC) rilevata	Analisi di sistematicità della NC rilevata	Analisi periodica per il monitoraggio di efficacia delle azioni correttive, la prevenzione delle NC e il miglioramento continuo
• Rilevata la NC, essa viene presa in carico e viene fatta ripetere l'attività, curando che le operazioni siano effettuate secondo le istruzioni operative e secondo il Regolamento di Servizio. In tal modo si elimina la possibilità che la non conformità sia sistematica, cioè dovuta a procedure o protocolli non adeguati; • Viene fatta ripetere la verifica del risultato; • È valutata la criticità o la ripetitività della NC; • Nel caso la NC sia riscontrata nuovamente, si procede con la definizione di una azione correttiva; • È effettuata l'azione correttiva; • È verificata l'efficacia dell'azione correttiva attraverso una nuova verifica. • La NC e le relative azioni correttive sono inserite nella base dati statistica del Sistema Informativo, per l'analisi nel tempo e per individuare eventuali periodicità o sistematicità	Le NC rilevate, anche in termini di scostamenti dai valori ottimali degli indicatori, sono analizzate da Gestore del Servizio e Audit e Miglioramento Continuo. Sono individuati i fattori che comportano la deviazione dai risultati attesi e sono quindi valutate le potenziali soluzioni a disposizione: • Correzione delle condizioni operative • Modifiche alle procedure e alle metodologie operative • Interventi di formazione autocorrettivi • Ripetizione dell'addestramento operativo • Altre opzioni di soluzione Le NC insieme alle azioni correttive sono inserite nella statistica periodica al fine di monitorare la risoluzione delle stesse, ovvero la necessità di una riprogettazione di parti del servizio, anche in sede di Comitati di Gestione ODF	In occasione dei Comitati di Gestione ODF, sono presentati ed analizzati i dati estratti dal Sistema Informativo al fine di ripristinare la qualità prevista attraverso la riprogettazione delle parti di servizio che non soddisfano gli standard richiesti. In particolare i passaggi che caratterizzano il processo di riprogettazione del servizio sono i seguenti: • Analisi delle cause e delle non conformità e dei punti critici che hanno generato il calo delle performance non in linea con il risultato del quadro qualitativo richiesto; • Modifica delle procedure o delle metodologie operative in accordo con l'analisi di rischio aggiornata e con le esigenze della Amministrazione Contraente; • Individuazione delle ulteriori soluzioni organizzative, gestionali, formative; • Applicazione provvisoria delle soluzioni individuate; • Monitoraggio di efficacia delle soluzioni di riprogettazione individuate: se il risultato ottenuto è coerente con le attese, approvazione delle soluzioni. In caso contrario, si ripercorre il processo di analisi per il miglioramento continuo.

Figura 33 Processo di gestione delle non conformità rilevate (controlli e verifiche con esito negativo)

C.4.b Sistema tracciabile di Customer Satisfaction sui servizi svolti

L'Offerente ha definito un sistema di Customer Satisfaction migliorativo rispetto alle esigenze espresse dalla documentazione di gara. Esso infatti:

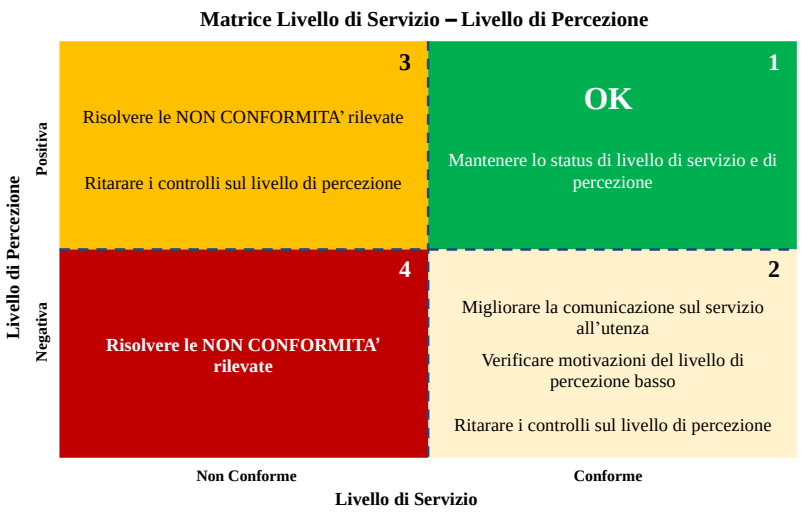
- Estende il novero dei soggetti di cui si misura la percezione del servizio, poiché considera anche gli utenti degli obiettivi;
- Definisce specifiche modalità di monitoraggio, fruibilità e gradimento che permettono una rilevazione continua della percezione del servizio, mediante le nuove tecnologie.

C.4.b.1 Metodologia di analisi della percezione del servizio

Il sistema di Customer Satisfaction è integrato nel più generale **sistema di autocontrollo** oggettivo prima descritto. Ciò permette di comprendere non solo come il servizio sia percepito, ma anche in che rapporto stanno servizio erogato e servizio percepito.

L'Offerente utilizza una *matrice di valutazione* che integra i due aspetti, in base alle risultanze del **ciclo di ritorno informativo**. La **matrice** definisce l'approccio da adottare per mantenere costante l'allineamento del livello di servizio erogato con gli obiettivi, e mantenere l'allineamento fra livello effettivamente erogato e livello di servizio percepito. Per tutti i soggetti, il sistema di controllo abbina due tipologie di rilevazione:

- **Rilevazione a caldo**, contestuale o subito a valle dell'esecuzione del servizio. E' utile per rilevare le *percezioni immediate* dell'utente riguardo il servizio;
- **Rilevazione a freddo**, effettuata periodicamente, che restituiscono in forma aggregata su un determinato periodo la percezione dell'utente sul servizio.



Le informazioni di ritorno sono utilizzate per monitorare la Customer Satisfaction e per predisporre le **necessarie e dovute azioni di miglioramento e di allineamento.**

Il sistema di monitoraggio è totalmente integrato all'interno della piattaforma informativa, grazie al modulo di gestione dei controlli, il quale comprende anche la programmazione, la registrazione delle verifiche e l'elaborazione degli indicatori di Soddisfazione. La piattaforma informativa, con gli strumenti di rilevazione della percezione del servizio ad essa connessi permette di gestire i controlli di soddisfazione, sia a caldo (contestuali all'erogazione del servizio) sia a freddo (rilevazioni periodiche della soddisfazione afferenti i servizi erogati).

C.4.b.2 Organizzazione per il sistema di Customer Satisfaction

Il Sistema di Customer Satisfaction è presieduto organizzativamente dalle seguenti figure, ordinate in base alla costanza e continuità delle azioni di recepimento della percezione:

- **Struttura di Centrale Operativa / Call Center**, le cui risorse sono deputate al monitoraggio continuo delle segnalazioni e dei reclami. Gli addetti di Call Center interni (raggiungibili con apposito numero verde pubblicizzato all'interno delle strutture) costituiscono un affidabile "termometro" dello stato di percezione del servizio e degli eventuali elementi che possono influire sulla soddisfazione degli utenti, compresi i Referenti dell'Amministrazione;
- **Audit e Miglioramento Continuo.** Hanno il compito di programmare, effettuare e rendicontare le verifiche periodiche di soddisfazione, effettuate sia attraverso l'elaborazione dei dati provenienti dai questionari online;
- **Gestori del Servizio**, che periodicamente effettuano riunioni di recepimento della soddisfazione del Referente dell'Amministrazione, nell'ambito delle quali è riempito un questionario strutturato di soddisfazione. Questo approccio permette di approfondire tutti gli eventuali elementi di disagio, di insoddisfazione o di percezione negativa del Referente e di apporre i correttivi;
- **Supervisore della Convenzione,** che periodicamente effettua riunioni di recepimento della soddisfazione dei Referenti del Soggetto Aggregatore, nell'ambito delle quali è sottoposto e discusso un questionario strutturato di soddisfazione. In particolare saranno previsti momenti di monitoraggio della soddisfazione a metà e alla fine del periodo di convenzionamento, e a metà della vita dei Contratti attuativi e alla conclusione dei contratti, in maniera tale da tracciare l'andamento della soddisfazione e rilevare i principali elementi che possono aver influito, in bene o in male, sulla soddisfazione del Soggetto Aggregatore.

C.4.c Strumenti e contenuti dei controlli del Sistema di Customer Satisfaction OSCURATO

C.5. Percorsi formativi e/o di aggiornamento che l'Offerente intende implementare per la corretta erogazione dei servizi

C.5.a Piano Formativo e ampliamento delle competenze del personale impiegato

Il percorso formativo e di aggiornamento illustrato è stato definito con l'obiettivo di estendere le competenze del personale impiegato. Il percorso è articolato in moduli, attivabili a seconda del differenziale fra competenze effettive e competenze obiettivo di ciascuna persona in relazione al ruolo ricoperto.

La formazione, sia di base sia specialistica, sarà erogata all'intero gruppo di lavoro esteso, quindi sia ai titolari sia al personale di sostituzione. In questo modo sarà possibile rispondere automaticamente alla richiesta di Capitolato Tecnico, che prevede la sostituzione di un operatore entro 7 giorni.

La sostituzione sarà *quasi immediata*, con semplice cambiamento dello status dell'operatore da "sostituto" a "titolare".

Il percorso formativo del personale impiegato nel servizio si articolerà su 3 livelli:

- **Livello 01:** formazione *minima di legge* per lo svolgimento della professione di GPG, necessariamente già acquisito da parte di tutto il personale di servizio e non sarà ulteriormente considerato.
- **Livello 02:** formazione *specialistica di base* stabilita dal Capitolato Tecnico, che sarà erogato al personale in funzione del gap di competenza rispetto ai moduli previsti;
- **Livello 03:** formazione *specialistica aggiuntiva* offerta dall'Offerente, al fine di far aderire le competenze del personale alle proposte organizzative, procedurali, tecnologiche contenute nella presente Offerta Tecnica. Tali competenze, già possedute da gran parte del personale dell'Offerente, saranno oggetto di un piano di formazione dedicato per tutti i lavoratori eventualmente riassorbiti.

La formazione di livello 03 si propone l'ampliamento delle competenze del personale, sia nell'ambito della prestazione specialistica sia in differenti ambiti dei servizi in Convenzione:

- **Competenze operative specifiche dei servizi.** Tali competenze permettono agli addetti di personalizzare i servizi attivati presso gli obiettivi, in base alle esigenze e peculiarità dell'Amministrazione.
- **Competenze di sicurezza (safety),** comprendente la competenze per l'effettuazione di manovre salvavita e il corretto utilizzo del defibrillatore;
- **Competenze relative al corretto trattamento dei dati.** Questa tematica è oggi particolarmente sentita e necessita di competenze e accortezze specifiche, che devono essere possedute dal personale di vigilanza;
- **Competenze comunicative**, in maniera tale che le GPG possano prevenire e gestire efficacemente le situazioni di conflitto;
- **Competenze di gestione ambientale.** Include competenze per la corretta gestione delle tematiche ambientali e per l'utilizzo delle dotazioni di servizio mitigandone il più possibile l'impatto (es. utilizzo degli automezzi);
- **Competenze per il servizio digitalizzato 4.0.** Tali competenze permettono agli addetti l'utilizzo efficace delle soluzioni tecnologiche e informatiche messe a disposizione della Convenzione, nell'ottica di "servizio digitalizzato" Security 4.0.

Nella seguente tabella sono schematizzati i rapporti fra i moduli definiti dall'Offerente per ciascun singolo ambito, insieme con il numero di ore previste e la figura organizzativa a cui la formazione è destinata. *Nota: **[PEF]**: Piantonamento fisso; **[VIR]**: Vigilanza ispettiva / ronda; **[VII]**: vigilanza ispettiva con modalità innovative (SAPR / unità cinofila); **[TEL]**: operatori di teleallarme / televigilanza; **[TEC]**: addetti tecnici.*

Competenze	Modulo Formativo	Ore	PIF	VIR	VII	TEL
Competenze operative specifiche per i servizi	Gestione delle emergenze, del panico e assistenza a persone disabili	10	●	●	●	
Competenze operative specifiche per i servizi	Corso di gestione di ambienti e ingressi con presenza di pubblico.	6	●			
Competenze operative specifiche per i servizi	Modulo di familiarizzazione con il contesto operativo	3	●	●	●	
Competenze operative specifiche per i servizi	Modulo specifico per la vigilanza fissa e ispettiva / di ronda	4	●	●	●	
Competenze operative specifiche per i servizi	Modulo specifico per la vigilanza fissa	4	●			
Competenze operative specifiche per i servizi	Modulo specifico per la vigilanza ispettiva / di ronda	4		●	●	
Competenze di sicurezza (Safety)	Corso FUllD (BLSD + PBLSD): rianimazione cardiopolmonare e defibrillatore	6	●	●		
Competenze relative al corretto trattamento dei dati	Corso di tutela dei dati sensibili	4	●	●	●	●
Competenze comunicative	Corso di comunicazione efficace e mediazione verso aggressività e violenza	8	●			
Competenze di gestione ambientale	Corso di guida sicura ed ecologica	4		●	●	
Competenze per servizio digitalizzato Security 4.0	Gestione digitale del servizio: Security 4.0	6	●	●	●	●
Competenze per servizio digitalizzato Security 4.0	Sistemi innovativi per teleallarme e televigilanza	4	●			●

Per tutti i moduli che non presuppongono l'utilizzo di apparecchiature o automezzi l'Offerente ha già organizzato modalità di didattica ad elevata sicurezza, che garantiranno – ove necessario – il distanziamento sociale fra i discenti.

Di seguito sono illustrati in dettaglio i corsi del Livello 3, che rappresentano la formazione specialistica richiesta dal Capitolato Tecnico. Per ciascun corso sono evidenziati gli obiettivi formativi, le tematiche affrontate, la durata e modalità di erogazione, il sistema di valutazione e la frequenza di aggiornamento.

Competenze operative per l'erogazione dei servizi

Modulo Formativo	Gestione delle emergenze, del panico e assistenza a persone disabili
Obiettivi formativi	Il corso ha l'obiettivo di ampliare le competenze del personale coinvolto nella gestione delle emergenze, in maniera tale che sappia sempre "cosa fare, quando e come farlo" per garantire salute e incolumità durante le situazioni di emergenza. Particolare attenzione è rivolta all'assistenza delle persone con disabilità.

Tematiche affrontate	**Gestione delle emergenze e del panico (5 ore).** Situazioni di panico: meccanismi di diffusione. Le problematiche delle situazioni di panico. Leadership in situazioni di emergenza e panico. Aspetti psicologici e sociali della folla: comunicare in modo efficace. Cosa fare e cosa non fare. **Assistenza a persone disabili (2 ore).** Assistenza e procedure di evacuazione di persone con disabilità. Tecniche per il trasporto di persone disabili in emergenza (persone con disabilità della vista, con disabilità dell'udito e disabilità motorie. **Gestione dell'emergenza in caso di esplosivi di circostanza (3 ore).** Riconoscere oggetti sospetti e sapere come comportarsi e come isolare la zona in attesa dell'arrivo degli organi preposti ad effettuare i relativi controlli.	
Durata e modalità di erogazione	**10 ore**	Lezioni frontali / online e prove pratiche con simulazioni di situazioni di emergenza, panico, presenza di persone disabili.
Docenza	Docente esperto della Croce Rossa Italiana, formatore qualificato, esperto in psicologia e traumatologia. Docente esperto nel riconoscimento e disattivazione di esplosivi e manufatti di circostanza, formatore qualificato	
Sistema di valutazione	Prova di profitto con superamento di test obbligatorio a domande chiuse. Attestato di certificazione.	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	
Modulo Formativo	Gestione di ambienti e ingressi con presenza di pubblico.	
Obiettivi formativi	Il corso ha l'obiettivo di ampliare le competenze del personale coinvolto nella gestione degli ingressi e degli ambienti degli obiettivi che fossero sottoposti a importanti flussi di pubblico. Il corso permette di acquisire le tecniche di comunicazione, organizzazione e prevenzione sia di security sia di health & safety a livello degli ingressi. Essi sono fra i principali elementi degli obiettivi oggetto di potenziali minacce elementi a maggiore rischio degli obiettivi.	
Tematiche affrontate	**Gestione dei flussi di persone in ingresso e uscita dagli obiettivi (4 ore).** Il corso verte sulle seguenti tematiche, focalizzate sulla gestione dei flussi di traffico all'ingresso degli obiettivi: **(a)** Scanning capacità di riconoscere persone o eventi destabilizzanti e pericolosi; **(b)** *Problem solving*: Tecniche di screening e profiling psicologico; **(c)** Il linguaggio del corpo: le espressioni del volto; **(d)** Motivazioni e profili di molestatori; **(e)** Screening e tipizzazione del profilo psicologico; **(f)** Gestione della folla; **(g)** Lo scambio verbale corretto. **Gestione dei flussi dei visitatori in regime di distanziamento sociale (2 ore).** Il corso, come misura restrittiva per l'emergenza sanitaria Covid-19, contiene le indicazioni di buona pratica per l'utilizzo del Kit salute, oltre ai protocolli da osservare per rispettare le norme e indicazioni anti-contagio all'interno degli ambienti chiusi.	
Durata e modalità di erogazione	**6 ore**	Lezioni frontali / online e prove pratiche con simulazioni tipiche per nella gestione della folla e del distanziamento.
Docenza	Docente esperto della Croce Rossa Italiana, formatore qualificato, esperto in psicologia e traumatologia. Docente esperto nella comunicazione efficace e nella scienza di gestione della folla.	
Sistema di valutazione	Prova di profitto con superamento di test obbligatorio a domande chiuse. Attestato di certificazione.	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	
Modulo Formativo	Familiarizzazione con il contesto operativo	
Obiettivi formativi	Il modulo ha l'obiettivo di formare la competenza di contesto dell'operatore, definendo con precisione organizzazione della Convenzione, organizzazione per l'erogazione dei servizi, contesto procedurale e	
Tematiche affrontate	**Organizzazione dell'Offerente** nel contesto del Contratto e degli obiettivi. Figure di coordinamento e di interfaccia, organigramma generale di commessa, organizzazione per singolo sito. Modalità e procedure di sostituzione per la copertura dei singoli obiettivi in base alle loro peculiarità. **Dotazioni aggiuntive per l'esecuzione dei servizi**. Descrizione delle dotazioni aggiuntive per l'esecuzione di tutti i servizi, per dare all'operatore una vista dell'insieme di risorse a disposizione del gruppo di lavoro. Procedure di utilizzo corretto delle dotazioni **Procedure di verifica dei livelli dei servizi.** Definisce i razionali in base ai quali gli operatori sono giudicati e valutati. Chiarisce gli aspetti del servizio su cui fare attenzione per erogare un sevizio conforme alle aspettative. Conoscenza degli impianti tecnologici degli obiettivi dell'Amministrazione	
Durata e modalità di erogazione	**3 ore**	Lezioni frontali / online.

Docenza	Docente interno / Gestore del Servizio, con il supporto di Audit e Miglioramento Continuo. Tecnici dei produttori delle apparecchiature e delle dotazioni.	
Sistema di valutazione	Prova di profitto con superamento di test. Attestato di partecipazione.	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	
Modulo Formativo	Modulo specifico per la vigilanza fissa e ispettiva	
Obiettivi formativi	Il modulo consente di formare operatori con la formazione personalizzata per la corretta erogazione dei sevizi presso gli obiettivi della singola Amministrazione.	
Tematiche affrontate	Catena di comando del servizio. Compiti affidati alle GPG. Norme e disposizioni di servizio specifiche per le GPG, procedure operative di servizio. Manuali di procedure di Amministrazione / obiettivo. Modalità di segnalazione eventi e di riporto all'infrastruttura di Centrale Operativa / Control Room	
Durata e modalità di erogazione	**4 ore**	Lezioni frontali / online.
Docenza	Docente interno / Gestore del Servizio	
Sistema di valutazione	Prova di profitto con superamento di test. Attestato di partecipazione.	
Aggiornamento	2 anni o all'ingresso o aggiornamento autocorrettivo.	
Modulo Formativo	Modulo specifico per la vigilanza fissa	
Obiettivi formativi	Il modulo consente di formare operatori con la formazione personalizzata per la corretta erogazione dei sevizi di piantonamento fisso.	
Tematiche affrontate	Consegne al personale e regole di dettaglio per singolo obiettivo: turni, obblighi di riservatezza, procedure operative di dettaglio per gli obiettivi dell'Amministrazione. Coordinamento con i servizi di portierato eventualmente presenti. Rilevazione delle presenze del personale con le dotazioni assegnate. Modalità di controllo con apparati radiogeni (ove previsti). modalità e procedure di reazione e di documentazione degli eventi. Modalità e procedure per i servizi di catena di custodia.	
Durata e modalità di erogazione	**4 ore**	Lezioni frontali / online.
Docenza	Docente interno / Gestore del Servizio	
Sistema di valutazione	Prova di profitto con superamento di test. Attestato di partecipazione.	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	
Modulo Formativo	Modulo specifico per la vigilanza ispettiva / ronda	
Obiettivi formativi	Il modulo consente di formare operatori con la formazione personalizzata per la corretta erogazione dei sevizi di piantonamento fisso.	
Tematiche affrontate	Vigilanza ispettiva e pronto intervento. Procedure e tempistiche di intervento. Strumentazione e dotazione per la vigilanza ispettiva ed il pronto intervento. Modalità di esecuzione delle ronde ispettive con le dotazioni tecnologiche assegnate. Rilevazione dei passaggi di vigilanza ispettiva. Vigilanza SAPR: modalità operative di esecuzione, procedure per il supporto operativo all'unità di ronda SAPR. Vigilanza con unità cinofila: strutture e occasioni in cui si utilizza l'unità cinofila. Modalità di supporto all'unità cinofila per la massima efficacia operativa.	
Durata e modalità di erogazione	**4 ore**	Lezioni frontali / online.
Docenza	Docente interno / Gestore del Servizio	
Sistema di valutazione	Prova di profitto con superamento di test. Attestato di partecipazione.	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	

Competenze di sicurezza (Safety)

Modulo Formativo	Corso FUllD (BLSD + PBLSD): rianimazione cardiopolmonare e defibrillatore	
Obiettivi formativi	Il modulo consente l'apprendimento da parte del partecipante dell'esecuzione, efficace e sempre aggiornata, delle manovre di rianimazione cardiopolmonare e dell'utilizzo in maniera appropriata del defibrillatore semiautomatico, sia in età adulta che pediatrica.	
Tematiche affrontate	Il corso ha i seguenti contenuti: **(a)** rianimazione cardiopolmonare e utilizzo del DAE; **(b)** algoritmo universale BLSD (Basic Life Support – Defibrillation); **(c)** cenni di rianimazione cardiopolmonare in età pediatrica PBLSD (Pediatric Basic Life Support – Defibrillation)	
Durata e modalità di erogazione	**6 ore**	Lezioni frontali / online ed esercitazioni pratiche con attuazione di manovre salvavita (liberazione vie aeree, ventilazione, compressioni toraciche, defibrillazione)
Docenza	Docente interno / Gestore del Servizio	
Sistema di valutazione	Prova di profitto con superamento di test. Attestato di partecipazione.	

Aggiornamento	2 anni o aggiornamento autocorrettivo.

Competenze per il corretto trattamento dei dati

Modulo Formativo	Corso di tutela dei dati sensibili	
Obiettivi formativi	Il corso approfondisce i concetti della tutela e protezione dei dati personali / sensibili dell'Amministrazione durante l'erogazione dei servizi.	
Tematiche affrontate	Il nuovo Codice di Protezione dei Dati (GDPR: General Data Protection Regulation). Il ruolo dell'operatore di sicurezza e il corretto utilizzo dei dati. Informazioni considerate sensibili. Gestione dei dati sensibili su qualunque supporto e nella effettuazione dei servizi. Cosa fare e cosa non fare. Come utilizzare le dotazioni nel rispetto della riservatezza (es. utilizzo delle body cam). Sistemi di tracciatura delle apparecchiature (GPS, sistema NFC etc.) e tutela dei dati personali	
Durata e modalità di erogazione	**4 ore**	Lezioni frontali / online e studio di casi aziendali
Docenza	Docente esperto di tutela della privacy e formatore qualificato	
Sistema di valutazione	Prova di profitto con superamento di test obbligatorio a domande chiuse.	
Aggiornamento	1 anno o aggiornamento autocorrettivo.	

Competenze comunicative

Modulo Formativo	Corso di comunicazione efficace e mediazione verso aggressività e violenza	
Obiettivi formativi	Il corso è pensato per trasferire agli operatori le competenze necessarie a prevenire episodi critici, di aggressività e conflitto. Nel caso si verifichi un conflitto, il corso fornisce gli strumenti per gestire la situazione e	
Tematiche affrontate	Il corso è articolato in **2 moduli**: • **Prevenzione situazionale degli episodi critici (4 ore).** Comunicazione verbale e non verbale. La negoziazione e il riconoscimento di situazioni di conflitto potenziale. Tecniche per disinnescare il conflitto; • **Capacità di gestione efficace degli episodi critici (4 ore).** Significato e ruolo delle emozioni. Tecniche di negoziazione con soggetti aggressivi. Condotte utili e condotte a rischio durante le situazioni di conflitto. Simulazione comportamentale.	
Durata e modalità di erogazione	**8 ore**	Lezioni frontali / online e studio di casi. Simulazione comportamentale, simulazione e osservazione di casi concreti.
Docenza	Docente esperto di psicologia, psichiatria, criminologia	
Sistema di valutazione	Prova di profitto con superamento di test. Attestato di certificazione	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	

Competenze di gestione ambientale

Modulo Formativo	Corso di Guida Sicura ed Ecologica	
Obiettivi formativi	Il corso approfondisce i concetti teorici e pratici della guida sicura ed ecologica, per l'apprendimento delle tecniche di guida ed utilizzo dei mezzi che favoriscono l'utilizzo ecologico degli automezzi di servizio.	
Tematiche affrontate	Progetto Green Patrol e nuove tecnologie di alimentazione degli automezzi. Automezzi elettrici ed ibridi. Tecniche per l'acquisizione di una condotta di guida meno dispendiosa energeticamente: tecniche di guida, di accelerazione e frenata, modalità di guida urbana ed extra-urbana. Tecniche di guida sicura (perdita di aderenza, guida con ostacoli, guida su fondi sdrucciolevoli). Razionali di guida ecologica e pianificazione dei tragitti.	
Durata e modalità di erogazione	**4 ore**	Lezioni frontali con prove pratiche, simulazioni con automezzi aziendali su piazzale attrezzato
Docenza	Docenti esperti di sicurezza stradale	
Sistema di valutazione	Prova di profitto con superamento di test obbligatorio a domande chiuse. Prova pratica e attestato di certificazione	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	

Competenze per il servizio digitalizzato Security 4.0

Modulo Formativo	Gestione digitale del servizio: Security 4.0
Obiettivi formativi	Il corso ha l'obiettivo di estendere le competenze del personale per metterlo in grado di comprendere ed utilizzare con efficacia gli strumenti innovativi messi a disposizione, sia informatici sia tecnologici.
Tematiche affrontate	**Piattaforma CSC e relative applicazioni.** Caratteristiche, modalità di accesso e di utilizzo per l'erogazione dei servizi. Catena di comando e piattaforma informativa per la condivisione dei dati di servizio. Modalità di tracciatura e consuntivazione dei servizi con

	la piattaforma e i dispositivi di campo. Integrazione delle procedure operative all'interno dell'architettura informativa.	
Durata e modalità di erogazione	**6 ore**	Lezioni frontali / on line di supporto e prove pratiche per acquisire padronanza con le procedure informatizzate.
Docenza	Docente interno della divisione Infrastruttura Tecnologica del Gruppo CIVIS	
Sistema di valutazione	Prova di profitto con superamento di test e prove pratiche. Attestato di partecipazione.	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	
Modulo Formativo	Sistemi innovativi per teleallarme e televigilanza	
Obiettivi formativi	Il modulo ha l'obiettivo di estendere le competenze del personale relativamente agli strumenti a disposizione per la vigilanza remota degli obiettivi, alcuni dei quali brevetti CIVIS.	
Tematiche affrontate	Consistenze impiantistiche degli obiettivi dell'Amministrazione. Sistemi innovativi di sorveglianza remota integrata. Tecnologie per la ridondanza dei segnali e dei flussi video a disposizione. Sistema di teleallarme e videosorveglianza integrata SMART. Sistema di videosorveglianza attiva NOD (Neural Object Detection). Modalità operative di vigilanza (modalità reattiva, proattiva, tecniche di riconoscimento e individuazione di falsi allarmi, procedure di gestione delle situazioni di emergenza).	
Durata e modalità di erogazione	**4 ore**	Lezioni frontali / online e prove pratiche / simulazioni, osservazione di casi di utilizzo combinato di teleallarme, televigilanza, personale di vigilanza.
Docenza	Docente interno della divisione Infrastruttura Tecnologica del Gruppo CIVIS	
Sistema di valutazione	Prova di profitto con superamento di test e prove pratiche. Attestato di partecipazione.	
Aggiornamento	2 anni o aggiornamento autocorrettivo.	

C.5.b Ore di formazione minime garantite

Per quanto riguarda la durata dei singoli corsi è possibile fare riferimento al prospetto riepilogativo che segue, all'interno del quale ai corsi specialistici di base è stata assegnata la durata ordinaria in ore prevista per lo specifico percorso formativo, mentre ai corsi specialistici aggiuntivi è stata riportata la durata da proposta nell'ambito del percorso formativo strutturato precedentemente descritto.

Si sottolinea che a ciascun addetto saranno erogate ore di formazione in relazione alle effettive necessità formative, discendenti dalla valutazione del gap fra competenze effettive e competenze obiettivo. Di conseguenza il totale del monte ore di formazione deve intendersi come un monte ore massimo, erogato ad addetti neoassunti.

Percorso formativo - Moduli formativi previsti	Ore
Formazione di base *(cfr. Capitolato Tecnico) Livello 02*	
Sicurezza e salute sui luoghi di lavoro (D.Lgs. 81/08 e s.m.i.)	12
Addetti antincendio	12
Addetti al Primo Soccorso Sanitario (Pronto Soccorso)	12
Circolazione stradale, tutela e conservazione del suolo pubblico	8
Psicologia comportamentale	6
Antiterrorismo	6
Prevenzione della criminalità mafiosa	6
Corso di formazione in analisi della Scena del Crimine	6
Totale Formazione di base	**68**
Formazione specialistica proposta dall'Offerente Livello 03	
Modulo di familiarizzazione con il contesto operativo	3
Modulo specifico per la vigilanza fissa e ispettiva / di ronda	4
Modulo specifico per la vigilanza fissa	4
Modulo specifico per la vigilanza ispettiva / di ronda	4
Gestione delle emergenze, del panico e assistenza a persone disabili	10
Gestione di ambienti e ingressi con presenza di pubblico	6
Corso FUllD (BLSD + PBLSD): rianimazione cardiopolmonare e defibrillatore	6
Corso di tutela dei dati sensibili	4
Corso di comunicazione efficace e mediazione verso aggressività e violenza	8
Corso di guida sicura ed ecologica	4
Gestione digitale del servizio: Security 4.0	6
Sistemi innovativi per teleallarme e televigilanza	4
Totale Formazione specialistica Livello 03	**63**

L'Offerente ha predisposto un efficace Piano Formativo per **garantire una idonea preparazione di tutto l'organico in ogni istante della vita della commessa**. Il Piano è concepito con un **assetto modulare**: si concretizza nella strutturazione

di numerosi corsi formativi che, oltreché essere necessariamente erogati all'avviamento del singolo contratto , offrono il prezioso vantaggio di poter essere attivati in ogni momento in funzione delle **specifiche esigenze** di ciascuna risorsa.

C.5.c Ciclo di miglioramento continuo per la formazione

L'Offerente ha infatti sviluppato un sistema di formazione basato sul ciclo di feed-back (**ritorno informativo).** Il sistema adotta un **ciclo di feed-back in continuo** che individua le necessità formative attraverso la continua **valutazione del differenziale delle competenze** (competenze obiettivo vs. effettive di ciascuna persona). Sulla base di quantità e qualità del differenziale il metodo definisce efficacemente i percorsi formativi delle persone. Il **ciclo di ritorno informativo** è reso possibile dalla **tracciatura dell'intero processo formativo e delle verifiche all'interno della piattaforma Civis Security Cloud (CSC) messa a disposizione dall'Offerente.** Il programma formativo è inoltre articolato in **moduli**, attivabili a seconda del fabbisogno formativo manifestato da ciascuna persona, così da permettere percorsi formativi **fortemente strutturati, in grado di assicurare il raggiungimento di competenze omogenee fra i discenti,** ma **flessibili** e **personalizzati** in base alle esigenze di ciascuna singola persona. Ciò permette di adattare la formazione e l'apprendimento alle esigenze di ciascuna GPG in relazione al proprio ruolo.

Di seguito è illustrato in particolare il **processo di valutazione continua delle competenze**, sulla cui base è definito il percorso formativo personalizzato per ciascun dipendente.

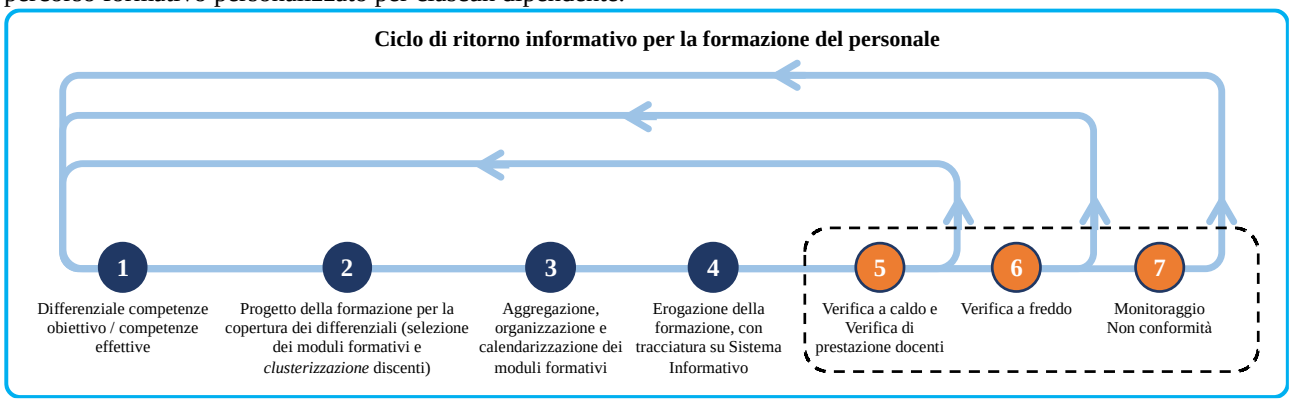


Figura 34 Ciclo di ritorno informativo per la formazione del personale

Il processo è interamente presidiato dalla **Funzione Personale e Formazione, con il supporto dei Gestori del Servizio e delle Funzioni Audit e Miglioramento Continuo / Personale e Formazione.** La valutazione del differenziale delle competenze permette di raggruppare le persone in base alle necessità formative e di costruire periodicamente delle **"classi", basate su differenziali omogenei.** La Funzione Personale Formazione può con questi dati a disposizione costruire un percorso di apprendimento e di addestramento focalizzato sulle effettive necessità delle persone, con la selezione delle corrette modalità di erogazione e delle figure docenti più adeguate per rendere la formazione più efficace possibile.

C.5.d Metodologie didattiche e strumenti utilizzati nell'erogazione dei corsi

L'Offerente ha previsto di procedere all'erogazione di ciascun corso mediante una fra le metodologie didattiche descritte nel seguente schema illustrativo:

Lezioni frontali in aula, che possono prevedere la discussione di casi ed essere supportate da materiale didattico (slide, presentazioni, audiovisivi etc.). **Le lezioni frontali conterranno anche contenere specifici moduli di "mirroring"**, moduli formativi tesi ad aumentare le capacità di comunicazione non verbale del personale

Formazione e-learning Disponibile direttamente su dispositivi di ciascun addettc (smartphone etc.) questa modalità sarà utilizzata soprattutto per l'erogazione della formazione di aggiornamento

Addestramento operativo / palestra formativa. Metodologia specifica per l'assimilazione di comportamenti, procedure operative etc.

Figura 35 Metodologie didattiche e strumenti utilizzati nell'erogazione dei moduli formativi

C.5.e Modalità di verifica della formazione erogata OSCURATO

C.5.f Tracciabilità della formazione

Tutte le informazioni relative ai corsi erogati al personale (argomento, durata, data, luogo di erogazione, docente) e tutti i riscontri di apprendimento sono contenuti all'interno della piattaforma informativa CSC, alla quale i Referenti dell'Amministrazione hanno completo accesso. La piattaforma permetterà di accedere ai **Dossier della Formazione, aggregati o per singolo addetto**, per dare modo all'Amministrazione di verificare direttamente, se del caso, la situazione formativa del personale impiegato dall'Offerente presso i siti dell'ODF e rimanere sempre allineata a riguardo:

- schede del personale con percorso formativo e risultati delle verifiche;
- calendario dei moduli formativi da erogare nel periodo;
- registro della formazione erogata.

Le sezioni supportano la valutazione dei differenziali formativi nel tempo permettendo di creare un circolo di ritorno informativo efficacissimo per la valutazione continua del livello di competenze di ciascuna singola risorsa, per l'omogeneizzazione dei gruppi di personale in base ai fabbisogni formativi e per la progettazione dei percorsi formativi di aggiornamento.

I dati contenuti in ciascuna sezione possono essere estratti, aggregati ed elaborati in funzione delle esigenze per ottenere **report riepilogativi** sul progetto formativo implementato dall'Offerente.

C.5.g Cronoprogramma della formazione

La prima fase del cronoprogramma di formazione sarà costituita dall'allineamento degli operatori al livello 02. Successivamente a questa fase, si procederà all'erogazione dei corsi facenti parte della formazione specialistica aggiuntiva in precedenza richiamati (Livello 03). L'intero percorso formativo sarà erogato entro le tempistiche massime prescritte dal Capitolato, pari a 30 giorni dall'attivazione della Convenzione:

Cronoprogramma del percorso formativo (W: week - settimana)	W1		W2		W3		W4	
Allineamento formazione specialistica di base Livello 02								
Gestione delle emergenze, del panico e assistenza a persone disabili								
Gestione di ambienti e ingressi con presenza di pubblico								
Corso FUllD (BLSD + PBLSD): rianimazione cardiopolmonare e defibrillatore								
Modulo di familiarizzazione con il contesto operativo								
Corso di comunicazione efficace e mediazione verso aggressività e violenza								
Corso di tutela dei dati sensibili								
Corso di guida sicura ed ecologica								
Gestione digitale del servizio: Security 4.0								
Sistemi innovativi per teleallarme e televigilanza								
Modulo specifico per la vigilanza fissa e ispettiva / di ronda								
Modulo specifico per la vigilanza fissa								
Modulo specifico per la vigilanza ispettiva / di ronda								

Come si vede, saranno erogati con priorità i moduli formativi relativi alla sicurezza e alla gestione delle emergenze, per poi erogare l'intero insieme dei moduli ai singoli cluster di discenti entro i 30 giorni prescritti.

D. Sicurezza, Ambiente e gestione delle emergenze

D.1. Procedure inerenti la gestione della sicurezza

Nelle seguenti tabelle è illustrato il possesso della certificazione in materia di sicurezza e salute dei lavoratori.

D.1.a Dichiarazione di possesso della certificazione OHSAS 18001 o aggiornamenti successivi

La Norma OHSAS 18001 è stata recentemente sostituita dalla UNI ISO 45001:2018. L'Offerente si è già allineato al nuovo iter di certificazione.

UNI ISO 45001:2018	CIVIS	VCV
Possesso della certificazione UNI ISO 45001:2018	**SI**	**SI**
Ente certificatore	Quaser certificazioni	Quaser certificazioni
Certificato n.	039	047
Data prima emissione	22/02/2013	16/12/2013
Data emissione corrente	21/02/2019	27/12/2019
Data di scadenza	21/02/2022	15/12/2022

D.1.b Dichiarazione di possesso della certificazione ISO 14001:2015

ISO 14001:2015	CIVIS	VCV
Possesso della certificazione UNI ISO 14001:2015	**SI**	**SI**
Ente certificatore	Quaser certificazioni	Quaser certificazioni
Certificato n.	A097	2182
Data prima emissione	19/07/2013	23/04/2020
Data emissione corrente	02/07/2019	23/04/2020
Data di scadenza	18/07/2022	23/04/2023

D.2. Gestione delle emergenze e di reperibilità

D.2.a Sistema di gestione del servizio di reperibilità

Rosa dei reperibili. L'Offerente ha progettato, anche sulla base della attuale Convenzione, un servizio di reperibilità che si basa su una rigorosa pianificazione dei turni integrata alla pianificazione delle attività operative. Il programma prevede, per singolo obiettivo e per fascia oraria, l'assegnazione in turno di reperibilità a personale GPG. Per ciascun obiettivo è selezionata una **rosa dei reperibili**, per ciascuna fascia oraria di servizio, con priorità di chiamata differenziata:

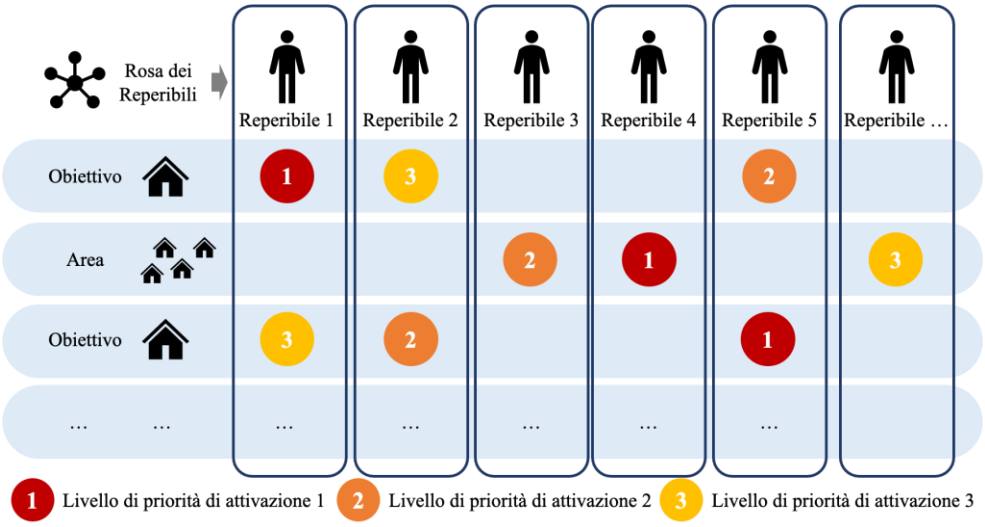


Figura 36 Schema concettuale di gestione della rosa dei reperibili relativamente a ciascun obiettivo (esempio servizio di piantonamento)

La programmazione è svolta considerando i seguenti vincoli:

- **Per le strutture con Piantonamento Fisso**, ad elevata sensibilità (es. Sedi della Provincia, altri Enti con depositi di valori o di informazioni sensibili, CED; etc.) il personale in turno di reperibilità è costituito da risorse **titolari fuori turno e da risorse di sostituzione dedicate alla struttura**. Ciò garantisce che le risorse intervengano entro tempistiche contenute. La scelta consente inoltre di avere a disposizione **personale già accreditato** presso le strutture, semplificando l'eventuale accesso ad aree ad accesso ristretto;
- Per le altre strutture e per i servizi al territorio (es. vigilanza ispettiva) i turni di reperibilità sono strutturati utilizzando le **risorse di sostituzione**, così da disporre delle dotazioni (automezzi, etc.) necessarie alla corretta effettuazione delle attività previste dal Capitolato.

La programmazione è svolta dai Gestori del Servizio, con il supporto dell'Ingegneria di Convenzione (Pianificazione e Programmazione). Per ciascun turno di reperibilità, il sistema di programmazione definisce unità progressive di operatori in reperibilità, da attivare a seconda delle esigenze e della contemporaneità delle richieste. In tal modo sia li Gestore del Servizio sia la Centrale Operativa hanno, grazie al Sistema Informativo, la chiara situazione delle risorse da attivare per ciascun obiettivo e per fascia oraria, minimizzando errori e indecisioni.

Al momento dell'attivazione del servizio di reperibilità, selezionando l'obiettivo in base alla fascia oraria il Gestore del Servizio ha immediatamente a disposizione i dati relativi alle risorse da attivare.

D.2.b Sistema di gestione delle emergenze

Il progetto di servizio prevede:

- **Soluzioni di prevenzione delle emergenze**, che **minimizzano la probabilità** di accadimento di situazioni di emergenza;
- **Soluzioni di gestione delle emergenze**, finalizzate a **mitigare** il più possibile gli impatti delle situazioni di emergenza su attività istituzionale e sicurezza di cose e persone.

D.2.b.1 Soluzioni di prevenzione delle emergenze

D.2.b.1.1 Aggiornamento costante dello stato di rischio per la prevenzione delle situazioni critiche

Durante la fase di convenzionamento, la Funzione **Security Manager** supporta la valutazione del **livello di rischio** (Risk Assessment) a cui sono sottoposti gli **obiettivi** vigilati. L'analisi **[→ cfr. par. B.2.b.1]** definisce gli **indicatori di rischio** per ciascuna **tipologia** di **minaccia**, e sono definiti all'interno di un **cruscotto di analisi e supporto alle decisioni**, condivisibile all'interno al Sistema Informativo. Il cruscotto è accessibile attraverso il **Portale Civis Security Cloud (CSC)** e condivisibile con i Referenti delle Amministrazioni Contraenti. Esso è uno **strumento fortemente dinamico**, sottoposto ad un **aggiornamento almeno annuale** (semestrale nel caso di obiettivi di particolare sensibilità, quali sedi centrali di Amministrazioni che gestisco informazioni sensibili ovvero valori). Il percorso di aggiornamento, svolto dalla **Funzione Security Manager** dell'Offerente, integra le informazioni di **intelligence** (es. circolari e comunicazioni dalle Questure o dalle Forze dell'Ordine), **l'analisi delle vulnerabilità** delle contromisure rispetto alle minacce all'obiettivo, il **contesto operativo** dell'obiettivo e le **risultanze dell'analisi di "sentiment" popolare**, in particolare sui Social Media. **[→ cfr. par. D.2.b.1.2].** L'approccio di analisi permette sostanzialmente di ridurre significativamente l'impreparazione a eventuali situazioni di emergenza, tipica di un approccio statico, in cui l'organizzazione può unicamente **"reagire".**

L'approccio di **analisi** e di **aggiornamento** dello stato di rischio **consente** invece alla struttura organizzativa **di prepararsi all'emergenza.**

Ad esempio, in considerazione di **innalzati livelli di allerta** relativamente a particolari situazioni di emergenza, l'Offerente può **pre-allertare** personale di **reperibilità e pronto intervento o personale di sostituzione**, in maniera tale da **diminuire i tempi di risposta**.

Le valutazioni sullo stato di rischio possono, grazie al cruscotto, essere condivise molto rapidamente e in maniera chiara con i **Referenti Security** delle Amministrazioni Contraenti, permettendo la preparazione

all'eventuale emergenza (es. servizi straordinari o intensificazione delle ronde, o copertura ulteriore di definiti obiettivi o fasce orarie).

Nella figura a lato è illustrato uno stralcio delle tavole di analisi del rischio, già utilizzate per il Risk Assessment iniziale in sede di PDI [→ cfr. par. B.2.b.1]. L'aggiornamento dello stato di rischio è svolto in coerenza con la normativa **UNI ISO 30001:2010** "Gestione del Rischio: principi e linee guida" ed alla sua guida applicativa, la UNI ISO 31010 "Risk Management – Guida alle tecniche di valutazione del rischio". Particolare importanza assume, al fine di una corretta valutazione dello stato delle minacce, la disponibilità all'interno del Sistema Informativo di strumenti avanzati di analisi, quali quello di analisi statistica dei Social Media, illustrato di seguito.

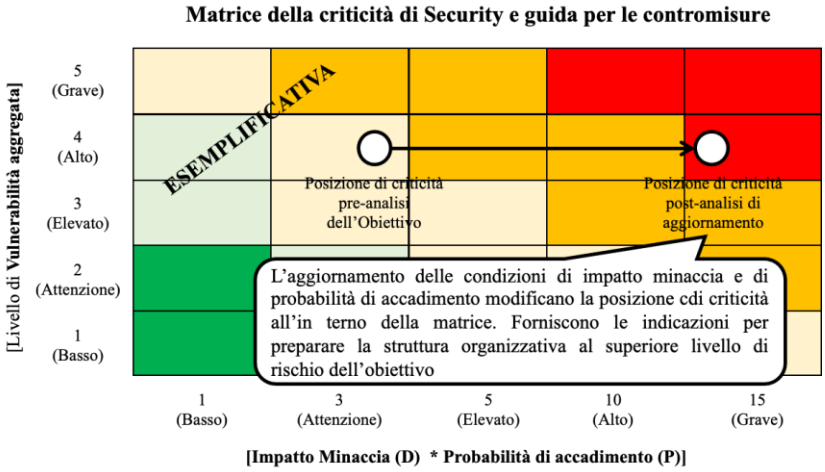


Figura 37 Matrice del rischio di Security in supporto all'aggiornamento dello stato di criticità

D.2.b.1.2 Analisi dei Social Media per la prevenzione di eventuali situazioni critiche

La Centrale Operativa di Lotto del Concorrente sarà dotata anche di **software specializzato nell'analisi del Social Media Sentiment.** Questo software è correntemente utilizzato da Ministero della Difesa, Finmeccanica, Poste Italiane. Dato il grandissimo utilizzo dei social, anche per l'organizzazione di eventi potenzialmente critici (picchetti, flash mob, manifestazioni, blocchi etc.) o vere e proprie azioni delittuose (es. occupazione abusiva di immobili) a danno della Pubblica Amministrazione, il software, nel pieno rispetto delle prescrizioni sulla materia specifica di protezione della privacy, effettua il monitoraggio dei principali canali sociali (es. Facebook, Snapchat, Twitter, Linkedin, Instagram etc.). Gli algoritmi del software permettono di effettuare: **(a)** La **ricerca di parole chiave** relative a potenziali iniziative, attraverso un avanzato algoritmo di **analisi semantica; (b) l'analisi statistica dell'interesse degli utenti** (es. organizzazione di una manifestazione non autorizzata presso uno specifico obiettivo).

Questa soluzione mete a disposizione un ulteriore efficace strumento per la prevenzione delle situazioni critiche e per adottare un **approccio predittivo** alla gestione delle situazioni critiche.

D.2.b.1.3 Integrazione ai Piani di emergenza di Amministrazioni e singoli obiettivi

L'Offerente prevede che il personale in servizio presso gli Obiettivi riceverà una formazione specifica, allo scopo di poter contribuire attivamente al coordinamento ed al supporto durante la gestione dell'emergenza e la conseguente eventuale evacuazione, anche sulla base dei piani di gestione delle emergenze specifici per il singolo obiettivo. Particolare enfasi è data al coordinamento con il personale dell'Amministrazione e di tutti gli altri attori dei piani di emergenza, per ciascun ODF, in maniera tale che sappiano con esattezza quali sono i loro compiti e responsabilità.

Il personale operativo e di coordinamento operativo può così portare un concreto contributo nella gestione di situazioni di emergenza in base alle specifiche esigenze e peculiarità dell'Amministrazione Contraente.

D.2.b.2 Soluzioni di gestione delle emergenze

Il progetto di servizio prevede un portafoglio completo di **soluzioni per mitigare gli impatti** delle situazioni critiche e delle emergenze, qualora si verificassero nonostante le soluzioni per prevenirle.

D.2.b.2.1 Modalità e soluzioni di segnalazione e coordinamento per le emergenze **OSCURATO**

D.2.b.2.2 Modalità di gestione delle pattuglie di Pronto Intervento sul territorio: **aree di reazione OSCURATO**

D.2.b.2.3 Modalità di intervento in caso di eventi critici

Modalità di attivazione dell'emergenza

Ove presente la Control Room, quest'ultima costituisce il perno della gestione della situazione di emergenza a livello locale, ovviamente con il supporto dell'intera infrastruttura di Centrale operativa. Il servizio è svolto da personale specializzato e adeguatamente formato alla gestione della Control Room locale, comandando e controllando tutti gli impianti di *Security* (anti-intrusione, videosorveglianza etc.) e di *Safety* (impianto antincendio, rilevazione fumi, antiallagamento etc.) eventualmente presenti presso l'obiettivo.

In caso di allarme o di situazioni anomale, l'operatore comunica con le altre GPG in servizio attraverso i dispositivi radio e, in caso di necessità, con la Centrale Operativa o le Forze dell'Ordine. L'operatore può attivare le **procedure di sicurezza nel rispetto del Manuale di Sicurezza Anticrimine e delle procedure condivise con l'Amministrazione Contraente,** e supportare il gruppo di lavoro grazie all'accesso ai segnali di allarme e soprattutto alle immagini

dell'evento criminoso in atto o verificatosi. Ulteriore ruolo di coordinamento è assunto nei confronti di conclamate situazioni di emergenza (incendio, allagamento, catastrofe naturale, incidenti, esplosioni, attentati): la Control Room opera in stretto contatto con il Responsabile del Piano d'emergenza dell'Amministrazione Contraente e richiede l'intervento dell'Autorità Giudiziaria, delle Forze di Polizia o dei Vigili del Fuoco, ove ritenuto opportuno e indispensabile. A seguito della segnalazione in Control Room / Centrale Operativa di una qualsiasi situazione di emergenza per una Guardia in servizio presso un punto protetto, la medesima Centrale attiva una procedura standard che prevede principalmente le seguenti azioni:

- Richiamata immediata della Guardia Particolare Giurata dalla quale è partito l'allarme per verificare la situazione, previo scambio di parola d'ordine di riconoscimento, per mirare meglio possibile l'intervento di supporto. La Guardia può rispondere sostanzialmente in tre modi diversi, a cui corrispondono tre situazioni e le relative diverse modalità di intervento:
  - Se la Guardia non risponde alla chiamata, la Centrale Operativa interpreta il fatto come una conferma di massima allerta, perché può significare che Essa è ferita, immobilizzata o sequestrata;
  - Se la Guardia risponde con una parola d'ordine anche di poco diversa da quella convenuta (segreta e personale per ogni Guardia e cambiata Al termine di tutte le azioni sopra ricordate, la Centrale Operativa redige sempre una verbalizzazione, che resta per le eventuali successive verifiche sia da parte degli Ispettori dell'Istituto sia di quelle dell'Ente, sia infine delle Forze dell'Ordine o della Magistratura.
  - Se la Guardia Giurata risponde con la parola d'ordine corretta e spiega, senza confondersi, la situazione, allora la Centrale Operativa può interpretare che si sia trattato di un allarme improprio oppure già gestito localmente.

Per quanto riguarda il Pronto Intervento in caso di allarme proveniente da Guardia Giurata dagli apprestamenti tecnologici di sicurezza, la struttura di Centrale Operativa attiva immediatamente la pattuglia afferente all'**area di reazione**, che effettua apposite azioni di pronto intervento armato ed ispezioni interne ed esterne. Tutte le modalità di richiesta saranno effettuate, come prescritto dal Capitolato Tecnico, secondo gli indirizzi operativi ed organizzativi delle singole Amministrazioni contraenti, che saranno appositamente definiti prima della stipula del contratto.

Grazie all'organizzazione delle pattuglie sul territorio, con l'approccio metodologico illustrato al punto D.2.b.2.2 della presente relazione, è possibile garantire la continua disponibilità di pattuglie di pronto intervento anche in caso di richieste contemporanee anche in zone differenti del Lotto. Nella seguente tabella è quindi presentata la *metodologia di attivazione del personale*, con elenco del personale attivato, per priorità di attivazione e sono presentate le caratteristiche del personale attivato, in funzione della severità ed estensione dell'emergenza:

N.	Tipologia di personale attivabile	Tempistica
1	Gestore del Servizio e coordinatore operativo afferenti l'obiettivo o gli obiettivi che denunziano la necessità di intervento.	Immediata
2	Personale di Piantonamento fisso / vigilanza ispettiva eventualmente presente o all'interno della area operativa in cui si verifica la richiesta, comprendendo anche il prolungamento dei turni per il personale in turno e il richiamo del personale fuori turno.	Immediata
3	Personale di Reperibilità e Pronto Intervento, attivato a supporto delle aree territoriali.	20 minuti
3	Personale di Reperibilità e Pronto Intervento territoriale, per tutti i tipi di obiettivo. Questo personale supporta anche il personale di Pronto Intervento dedicato, ove necessario.	20 minuti
4	Personale titolare fuori turno e personale di sostituzione in turno di attivabilità, dedicato al singolo obiettivo).	30 minuti
5	Personale condiviso sul territorio del Lotto e territori limitrofi.	60 minuti

L'approccio organizzativo dell'Offerente è costituito da **soluzioni modulari**, che possono essere attivate in relazione alla tipologia emergenza conclamata. Grazie all'attivazione progressiva e differenziata, in base alla situazione, delle differenti tipologie di personale, il modello di attivazione si adatta perfettamente a tutte le possibili situazioni che si possono verificare sul territorio del Lotto.

Attivabilità di tutti gli operatori e di tutti i mezzi sul territorio

In presenza di situazioni particolari, quali eventi naturali, situazioni di pericolo e di estrema emergenza, l'Offerente può attivare tutte le proprie risorse con un preavviso di 1 ora dalla richiesta. Di seguito è illustrata la **consistenza dell'organico attivabile**, in pronta disponibilità, condiviso anche su altre commesse, sul territorio del Lotto. Come si osserva, l'Offerente intende mettere a disposizione anche le risorse in pronta disponibilità ubicate sugli ambiti territoriali confinanti con il Lotto in oggetto e comunque afferenti al territorio della Lombardia.

Operatori e mezzi sul territorio del Lotto 01	Numero
GPG in pronta disponibilità	**319**
Automezzi in pronta disponibilità	**78**

Procedure operative per la gestione delle principali situazioni di emergenza

Procedura di gestione dell'evento incendio → Di seguito è illustrata la procedura di gestione di eventi incendio, fughe di gas e analoghi, che possono mettere a rischio la sicurezza e l'incolumità delle persone all'interno degli edifici.

[1]. Se l'evento incendio è di modesta entità, gli addetti fungono da veri e propri addetti antincendio e predispongono, grazie alla formazione e all'addestramento ricevuti, le prime misure per limitare e mitigare gli effetti dell'emergenza, utilizzando i mezzi portatili di estinzione in dotazione presso le strutture. La procedura prevede il disinserimento delle attrezzature elettriche e l'allontanamento di qualunque materiale combustibile / infiammabile che può essere interessato dall'evento. In ogni caso sono attivati i Vigili del Fuoco e le Forze dell'Ordine.

[2]. Nel caso di eventi di maggiore entità, che non sia possibile contrastare mediante i mezzi portatili a disposizione, la Control Room (interna o esterna a seconda dell'evolversi della situazione) aziona il segnale di evacuazione della struttura. I coordinatori per le emergenze dell'Amministrazione Contraente controllano l'evacuazione dell'edificio, con particolare attenzione per i disabili e le persone con difficoltà motorie, dirigendo il flusso di persone lungo le vie di fuga e verificando poi che ogni locale sia stato abbandonato. I coordinatori per le emergenze devono quindi sincerarsi dell'avvenuta evacuazione di tutti i colleghi alloggiati, con particolare attenzione a eventuali portatori di disabilità.

[3]. Contestualmente alla fase 2, durante l'evacuazione, la Control Room / Centrale Operativa contatta i Vigili del Fuoco e attiva delle pattuglie di Pronto Intervento dell'Istituto Offerente, in maniera tale da supportare l'azione delle Forze dell'Ordine.

[4]. All'interno della zona di evacuazione, il personale procede al controllo delle persone presenti e riporta le segnalazioni dei visitatori su eventuali persone mancanti. Con questa azione il personale supporta (ove possibile)l'eventuale rilevazione di persone intrappolate all'interno degli edifici e passa l'informazione alle Autorità Preposte (VV.FF. o Forze dell'Ordine).

La Centrale Operativa dell'Offerente si mantiene sempre in contatto con l'operatore sul posto e lo dirige nell'esecuzione di tutte le misure di contenimento dell'incendio, se l'incendio è di modesta entità, ovvero provvede a contattare gli Enti Esterni qualora l'evento lo renda necessario, supportando la gestione dell'emergenza.

Procedura di gestione di presenza di soggetti indesiderati o malintenzionati → Data la delicatezza delle attività svolte all'interno dei siti, è possibile che si verifichi la presenza di individui facinorosi o turbolenti. In tal caso la procedura è mirata alla gestione del conflitto grazie alla formazione ricevuta ed alla contestuale **richiesta di supporto alla propria Centrale Operativa, alle eventuali GPG presenti sul sito nel territorio oggetto di gara**.

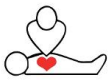
Qualora, al concretizzarsi della circostanza delineata in apertura, l'operatore di reception fosse impossibilitato al contatto mediante lo smartphone in dotazione, potrà avvalersi del **dispositivo antipanico** / uomo a terra in dotazione. Premendo il pulsante di emergenza presente sull'apparato, l'operatore invia un segnale di emergenza che viene ricevuto dalla Centrale Operativa, la quale attiva le procedure di gestione concordate.

Procedure di evacuazione → Nel caso di evacuazione, la procedura prevede che il personale, oltre a mettersi a disposizione del Responsabile delle Emergenze, effettui presso le persone all'interno dell'area di evacuazione la verifica relativa a persona ancora all'interno delle strutture. Questa informazione è utile per verificare il completamento delle operazioni di evacuazione.

Procedure in caso di altri eventi → Per la gestione di tutti gli altri eventi, la piattaforma procedurale è la medesima. La Reception rimane il perno su cui si articola l'intero processo di verifica e gestione dell'emergenza, una volta conclamata. In base al tipo di emergenza possono essere attivate risorse differenti:

Allagamenti. Sono attivate le squadre di manutenzione interna della Sede, che predispongono le azioni per limitare i danni derivanti dall'allagamento

Eventi naturali disastrosi. In caso di eventi quali quali terremoti, il personale attiva i coordinatori per le emergenze dei singoli siti oltre alle Autorità preposte (FF.OO., VV.FF., etc.) e partecipa attivamente al Piano di Emergenza ed Evacuazione



Malori o emergenza sanitaria. L'operatore provvede ad allertare il 118, la Centrale Operativa e, nel caso, a coordinare il primo soccorso. Il personale è inoltre abilitato all'utilizzo del defibrillatore semiautomatico di cui l'Offerente intende dotare i siti.

Figura 38 Procedure in caso di altri eventi

D.3. Automezzi a ridotto impatto ambientale

Con riguardo all'organizzazione di supporto ed in particolare alle pattuglie di Pronto Intervento e alle pattuglie all'interno dell'**area di reazione**, l'Offerente ha già da tempo avviato il progetto **"Civis Green Patrol" (Civis Pattuglie Verdi)**, che prevede l'intero **aggiornamento del parco auto con autovetture ad elevata sostenibilità ambientale**, elettriche o ad alimentazione ibrida. Il progetto diminuirà l'impronta ambientale del servizio. Inoltre, date le sempre più stringenti regole di attraversamento delle aree metropolitane (zone a traffico limitato etc.) la dotazione tecnica di automobili a elevata compatibilità ambientale consente di transitare in tutte le aree,

ottimizzando le capacità operative. Nella seguente tabella sono illustrate le consistenze e le percentuali degli automezzi che saranno utilizzati dall'Offerente:

Automezzi a ridotto impatto ambientale – Lotto 01	SI	NO	Totale
Milano / Monza e della Brianza	43		43
Lecco / Como	9	7	16
Varese	17	2	19
Totale complessivo	**69**	**9**	**78**
% automezzi a ridotto ambientale sul totale	**88,5%**		

D.4. Divise delle GPG

Per la presente Convenzione l'Offerente **si impegna all'utilizzo esclusivo** di divise per il personale impiegato che abbiano le seguenti caratteristiche: **(a)** Certificazione Ecolabel o altra etichetta equivalente; **(b)** Certificazione OEKO-TEX® Standard 100 o "Confidence in textile". Al riguardo, sono illustrate le caratteristiche tecniche delle divise. In allegato sono inoltre illustrate le schede tecniche delle divise che l'Offerente intende utilizzare, con evidenza delle certificazioni ambientali delle stesse.

Capi delle divise utilizzate dall'Offerente e tipologie di tessuto di cui sono composte		OEKO-TEX® INSPIRING CONFIDENCE STeP	OEKO-TEX® CONFIDENCE IN TEXTILES STANDARD 100	EU Ecolabel
	Camicia US uomo MC cod. CAM mod. CAMI15 marca KIMAY. Camicia modello US manica corta con pettorina e porta placca, con 4 bottoni oro.	●		
	CAMICIA US UOMO ML cod.CAM mod.CAMI16 marca KIMAY. Camicia modello US manica lunga con pettorina e porta placca, con 4 bottoni oro.	●		
	GIUBBINO DS cod. GIU mod.VENTO02 marca KIMAY. Giubbino DS con interno staccabile trapuntato, con spalline, porta placca e tre tasche.		●	
	PANTALONE 6T UOMO DS 4 TASCHE cod. // mod.TAT07 marca KIMAY. Pantalone 6t modello DS con cintura regolabile e cordoncino elastico alle caviglie, con quattro tasche.		●	●
	Calzatura da lavoro EN ISO 20347:2012 classe I (calzature in cuoio e materiali simili) ANF005, marca KIMAY			

L'etichetta di certificazione Ecolabel ha numero identificativo N. IT/16/07