



cesvi



POLICY SICUREZZA

Maggio 2024

INDICE DEI CONTENUTI

INTRODUZIONE	4
LA NOSTRA MISSIONE	4
RISORSE UMANE	4
PERCHÉ UNA POLICY SICUREZZA?	4
APPLICAZIONE E AMBITO DI APPLICAZIONE DELLA POLICY	6
APPLICAZIONE.....	6
AMBITO DI APPLICAZIONE	6
PRINCIPI DI BASE	6
DEFINIZIONE DI SICUREZZA	6
PRIMATO DELLA VITA	7
LIVELLO DI RISCHIO E DIRITTO DI RECESSO.....	7
ECCEZIONI.....	7
STRATEGIE ADEGUATE E ANALISI DEI RISCHI	8
STRATEGIE A DISPOSIZIONE DELLE ONG	8
<i>Accettazione (o consenso)</i>	8
<i>Protezione</i>	9
<i>Deterrenza</i>	9
<i>Strategia consigliata</i>	9
PROCESSO DI ANALISI DEL RISCHIO: COMPONENTI DI BASE.....	10
QUADRO GIURIDICO	11
DECRETO LEGISLATIVO 81/2008	11
RESPONSABILITÀ, SOGGETTI E STRUMENTI UTILIZZATI NELLA GESTIONE DELLA SICUREZZA	11
RESPONSABILITÀ E PARTI INTERESSATE	11
<i>Responsabile salute e sicurezza (H&S Manager)</i>	12
<i>Medico competente</i>	12
<i>Security Advisor</i>	12
<i>Altre parti coinvolte</i>	12
<i>Country security manager</i>	13
<i>Focal point per la sicurezza a livello nazionale e sul campo</i>	13
<i>Team di gestione delle crisi</i>	14
STRUMENTI E SISTEMI ORGANIZZATIVI PER LA GESTIONE DELLA SICUREZZA	15
<i>Documento di valutazione dei rischi</i>	15
<i>Guida generica alla sicurezza ECHO 2004 e Manuale di sicurezza CESVI</i>	15
<i>Analisi del rischio: Country Traffic Light</i>	16
<i>Analisi dei rischi: il profilo della ONG nel Paese</i>	16
<i>Analisi del rischio: rischio accettabile</i>	17
<i>Piano di sicurezza del Paese</i>	17
<i>Relazione annuale e bilancio annuale sulla sicurezza</i>	17
<i>Formazione</i>	18
<i>Analisi di incidenti e inconvenienti</i>	18
<i>Assicurazione</i>	19
ATTORI E SITUAZIONI SPECIFICHE	20
COINVOLGIMENTO DEL PERSONALE LOCALE.....	20
SALUTE	20
<i>Principi generali</i>	20
<i>Malaria</i>	20
<i>Gestione dello stress e dei traumi</i>	20
<i>La gravidanza</i>	21
USO DI SISTEMI E STRUMENTI DI DISSUAZIONE	21
<i>Armi</i>	21

<i>Guardie armate</i>	21
<i>Utilizzo di società di sicurezza private</i>	22
GESTIONE DELLE SITUAZIONI CRITICHE.....	22
<i>Attacchi, arresti</i>	22
<i>Rapimento e sequestro</i>	22
<i>Evacuazione</i>	23
ASPETTI AMMINISTRATIVI E DATI SENSIBILI.....	24
<i>Trasferimento e gestione del denaro</i>	24
<i>Protezione dei documenti e delle informazioni</i>	25
COMUNICAZIONI.....	25
<i>Principi, mezzi e metodi</i>	25
<i>Debriefing e consegna</i>	26
TRASPORTO.....	26
<i>Utilizzo di auto e veicoli a motore</i>	26
<i>Voli</i>	27
SELEZIONE DEI SITI E DEI LOCALI.....	27
FOTOGRAFIA E RAPPORTI CON I MEDIA.....	28
COORDINAMENTO.....	28
<i>Gestione congiunta della sicurezza</i>	28
<i>GISF</i>	28
<i>INSO</i>	29
<i>Alleanza2015</i>	29
<i>Unità di Crisi del Ministero degli Affari Esteri</i>	29
<i>Agenzie delle Nazioni Unite</i>	30
<i>Relazioni civili e militari</i>	30
<i>Rapporti con le autorità locali</i>	31
VISITATORI, FAMILIARI, ACCOMPAGNATORI.....	32
FINANZIAMENTO DELLE MISURE DI SICUREZZA.....	32
PANNOCCHIA.....	32
MONITORAGGIO E REVISIONE DELLA POLICY.....	33
ALLEGATI.....	34
PARTE SPECIALE DEL MODELLO ORGANIZZATIVO RELATIVA ALLA SALUTE E ALLA SICUREZZA SUL LUOGO DI LAVORO.....	34
<i>Modulo per la segnalazione di incidenti/incidenti</i>	34
<i>Allarme precoce</i>	36
<i>Contenuti del piano di sicurezza nazionale</i>	36
<i>Contenuti del rapporto annuale sulla sicurezza</i>	37
APPENDICE.....	38
APPENDICE 1 - GESTIONE DELLA SICUREZZA.....	38
<i>Policy di CESVI</i>	38
<i>Diversi modelli di gestione della sicurezza</i>	38
APPENDICE 2 - DESCRIZIONE DEL LAVORO.....	39
<i>JD del Security Advisor</i>	39
<i>JD del Regional/Area Manager</i>	39
<i>JD dell'Head of mission</i>	40
<i>JD del Country security manager</i>	40
<i>Punto focale di sicurezza sul campo JD</i>	41

Versione	Data	Approvato da:
Versione 3	Maggio 2024	Consiglio di amministrazione di CESVI
Versione 2	Dicembre 2017	Consiglio di amministrazione di CESVI
Versione 1	Aprile 2009	Consiglio di amministrazione di CESVI

INTRODUZIONE

La nostra missione

Missione

CESVI ETS¹ opera in tutto il mondo per sostenere le popolazioni più vulnerabili nella promozione dei diritti umani e nella realizzazione delle loro ambizioni, per uno sviluppo sostenibile.

All'insegna degli ideali di giustizia sociale e di rispetto dei diritti umani, CESVI persegue il benessere delle popolazioni vulnerabili in condizione di povertà o colpite da guerre, calamità naturali e disastri ambientali. Ciò avviene, anche a livello internazionale, attraverso opere di aiuto umanitario, sia nel contesto dell'emergenza che dello sviluppo, a sostegno delle categorie più deboli - bambini, donne, anziani ed emarginati sociali -, supportandole nel raggiungimento dei loro obiettivi con l'obiettivo di promuovere l'autosufficienza in un futuro sostenibile.

Visione

CESVI ritiene che il riconoscimento dei diritti umani contribuisca al benessere di tutti gli abitanti del pianeta, una casa comune da salvaguardare.

Le attività di cooperazione e aiuto umanitario sono svolte da persone per le persone. Le risorse umane, ben addestrate e capaci di operare in situazioni inospitali e pericolose, sono ciò in cui le ONG sono realmente specializzate.

Risorse umane

L'efficacia e il successo delle iniziative di sviluppo e di aiuto umanitario dipendono soprattutto dal contributo di tutto il personale. Il lavoro di un'organizzazione che opera in situazioni di emergenza e di sviluppo pone una grande pressione sul suo personale. La Policy delle risorse umane di CESVI riconosce quindi la propria responsabilità nel garantire il benessere fisico e psico-sociale del personale, prima, durante e dopo il lavoro con CESVI.²

Perché una Policy sicurezza?

Negli ultimi decenni il contesto in cui opera la Cooperazione è cambiato in modo significativo. Abbiamo assistito a un progressivo e drammatico aumento della violenza contro coloro che lavorano nel settore umanitario e contro i loro programmi. Le organizzazioni umanitarie e il loro personale sono state vittime dirette di attacchi politici e criminali, dovuti al deterioramento del tessuto sociale ed economico generale, in modo più evidente nei Paesi in cui operano.

Questa situazione di rischio crescente ha portato alla necessità di definire progressivamente approcci strategici alla gestione della sicurezza, di innalzare il livello di professionalità e di coordinare le attività.

¹ La denominazione legale della Fondazione è CESVI Fondazione - ETS o CESVI ETS ai sensi del Decreto Legislativo D.Lgs. 117/17, di seguito indicata anche come "CESVI".

² Policy risorse umane di CESVI ETS, 2024.

strumenti delle agenzie, e quindi di rivedere e aggiornare le relative linee guida, per consentire a **CESVI** di agire con **umanità, neutralità, indipendenza e imparzialità**.³

La presente Policy è il principale strumento di attuazione della responsabilità di garantire la sicurezza e la protezione del proprio personale attraverso iniziative adeguate (Duty of Care), nei termini dei principi guida della **CHS Alliance** (ex *People in Aid Code of Good Practice in management and support of aid personnel*) sottoscritti nel 2015.

Il livello di adempimento degli standard di sicurezza richiesti ai datori di lavoro per l'incolumità dei propri lavoratori (Duty of Care) è sostanzialmente aumentato, rendendo obsoleti e superati i criteri un tempo considerati adeguati; si tratta dell'obbligo legale e morale di salvaguardare i dipendenti e coloro che agiscono per conto dell'organizzazione da qualsiasi rischio ragionevolmente prevedibile.

L'**obbligo di diligenza** è la garanzia che in un determinato contesto il datore di lavoro metta in pratica **misure adeguate a prevenire e reagire a qualsiasi possibile incidente**, misure di cui il personale è informato e che è in grado di attuare adeguatamente.

A tal fine, CESVI si impegna a utilizzare metodologie e strumenti in grado di far emergere tutti i rischi prevedibili connessi a un determinato ruolo o attività, a stabilire adeguate misure di mitigazione e protezione, a sviluppare piani di emergenza, a garantire al personale un'adeguata informazione, a sensibilizzare il personale e infine a fornire un adeguato supporto per l'assistenza al personale nel caso in cui sia vittima di un incidente.

Sebbene il dovere di diligenza riguardi in egual misura contesti ad alto e basso rischio, ci si aspetta che le organizzazioni si assumano una maggiore responsabilità nei confronti del personale che lavora in situazioni o aree considerate a rischio più elevato.

Poiché non tutti i rischi possono essere esclusi, la distribuzione dell'**Avviso di Sicurezza** assicura che il dipendente sia debitamente informato e accetti consapevolmente i possibili rischi residui nel contesto lavorativo nonostante le precauzioni adottate. Tuttavia, questo documento non rappresenta un'esenzione dalla responsabilità dell'organizzazione.

³ I quattro principi cardine dell'aiuto umanitario secondo il Codice di Condotta della Croce Rossa Internazionale sottoscritto da CESVI nel 2002 e le successive policy e codici dell'organizzazione.

APPLICAZIONE E AMBITO DI APPLICAZIONE DELLA POLICY

Applicazione

La presente Policy sicurezza riguarda **tutto il personale di CESVI**: personale della sede centrale, espatriato, locale, a tempo pieno, part-time e occasionale, consulenti in missione a breve o lungo termine, familiari debitamente autorizzati ad accompagnare o visitare il personale durante le missioni, visitatori autorizzati, volontari, stagisti e qualsiasi altra persona che collabora formalmente e direttamente con la ONG. Sono esclusi dalla copertura: il personale di altre ONG, il personale di agenzie e governi, i dirigenti e i dipendenti di aziende, anche se coinvolti in qualche modo nei programmi di CESVI (questi soggetti sono considerati parti interessate esterne).⁴

L'adesione alla Policy sicurezza è **obbligatoria** e contestuale all'avvio di qualsiasi forma di collaborazione con CESVI. La Policy è vincolante per tutti i destinatari. Qualsiasi violazione della Policy sicurezza e delle linee guida sarà considerata una violazione disciplinare e trattata secondo il *Codice di Condotta*, la *Policy del Personale* e il *Codice Etico* di CESVI.

Ambito di applicazione

La presente Policy si applica alle **persone, ai beni, alle risorse, ai documenti** (compresi quelli amministrativi) appartenenti o a disposizione di CESVI all'estero, in tutti i suoi programmi e in qualsiasi circostanza.

La legge italiana, TU 81/2008, che garantisce la sicurezza e l'incolumità del personale sul luogo di lavoro in Italia, è considerata da questa Policy solo se applicabile alle attività all'estero. La presente Policy non riguarda i rapporti con i donatori, le comunicazioni, né la tutela e la promozione della reputazione e dell'immagine pubblica della ONG.

PRINCIPI DI BASE

Definizione di sicurezza

La gestione della sicurezza deve essere sempre pienamente integrata nei progetti, contribuendo così a garantire il **raggiungimento degli obiettivi delle iniziative sul campo**, siano esse di emergenza o di sviluppo. Ciò significa che il massimo livello di sicurezza e di protezione del personale deve sempre coincidere con il rispetto degli obblighi assunti nei confronti dei beneficiari e delle altre parti interessate (donatori, fornitori di servizi, ecc.).

La gestione della sicurezza deve essere sviluppata in modo da fornire opzioni flessibili adatte alle condizioni e ai rischi delle varie situazioni.

La protezione e la sicurezza si ottengono, a seguito di una valutazione dei rischi esistenti in un determinato contesto, quando sono soddisfatte le seguenti condizioni:

- Il personale è protetto e può operare in sicurezza;
- proprietà e risorse (attrezzature, risorse finanziarie, locali, documentali) sono tutte protette al massimo livello possibile.

⁴ Tuttavia, qualsiasi comportamento o decisione di parti interessate esterne che metta a rischio il personale, i beni o le risorse di CESVI deve essere debitamente affrontato dal personale di CESVI, in modo da ridurre al minimo i rischi sia per loro stessi che per CESVI.

L'attuazione delle misure di sicurezza contenute nella presente Policy e nei documenti correlati non indebolisce il raggiungimento degli obiettivi della cooperazione allo sviluppo e dell'aiuto umanitario, né mette a rischio l'efficacia e l'efficienza dei programmi e dei progetti, ma anzi ne rende più fattibile il raggiungimento e ne aumenta la qualità.

Primato della vita

Le decisioni e le azioni riguardanti la sicurezza, la protezione e la salute del personale hanno la precedenza su qualsiasi attività volta a preservare beni, attrezzature, risorse finanziarie, documenti o infrastrutture.

Livello di rischio e diritto di recesso

Il personale viene sempre informato in anticipo del livello di rischio di una determinata missione e ha il diritto di ritirarsi in qualsiasi momento. Nell'interesse della sicurezza e dopo averne discusso con il proprio Line Manager⁵, qualsiasi membro del personale, indipendentemente dalle sue funzioni o dal parere del **Security Advisor di CESVI** o del suo Line Manager, può decidere di ritirarsi da un'area o interrompere un'attività. **CESVI** farà tutto il possibile per facilitare il ritiro e non addebiterà al membro del personale in questione alcun costo sostenuto nella fase di ritiro.

Il personale che non si sente in grado di affrontare il livello di rischio di una determinata attività o posizione può chiedere al proprio Line Manager di essere assegnato ad altre attività o posizioni. Nei termini del contratto, CESVI farà tutto ciò che è in suo potere per soddisfare tale richiesta.

Eccezioni

Ogni eccezione o deroga a quanto specificato nella Policy sicurezza può essere autorizzata dal Direttore Generale solo per iscritto al Security Advisor, all'Organismo di Vigilanza sul personale espatriato e alle parti interessate. Nel caso in cui il Direttore Generale non sia raggiungibile, questa responsabilità sarà assunta dal Presidente, che potrà consultare il Consiglio di Amministrazione, la cui decisione sarà presa a maggioranza.

⁵ Il Line Manager è la persona, indicata nel documento che formalizza il rapporto del lavoratore con CESVI (contratto di lavoro, accordo di volontariato, ecc.) o nella Job description, a cui il lavoratore deve riferire durante le operazioni.

STRATEGIE E ANALISI DEL RISCHIO APPROPRIATE

Strategie a disposizione delle ONG

L'analisi teorica e l'esperienza maturata negli ultimi anni nel coordinamento della sicurezza hanno portato all'identificazione di tre principali approcci gestionali: **Accettazione** (o consenso), **Protezione** e **Deterrenza**.

Accettazione (o consenso)

L'**accettazione** (o consenso) mira a **ridurre o eliminare il pericolo** di operare in un determinato contesto, **migliorando l'apprezzamento dell'agenzia** e del lavoro che svolge.

L'**accettazione** è unanimemente considerata da tutte le ONG come l'approccio che meglio si adatta agli obiettivi delle organizzazioni umanitarie e di cooperazione. Così come una buona operazione di sviluppo o di emergenza non può essere portata a termine senza la creazione di un consenso con le parti interessate (a partire dai beneficiari dei progetti, dai gruppi sociali comunque interessati e dalle autorità locali), non è pensabile che si possano mantenere alti livelli di protezione e sicurezza senza contare sull'immagine positiva che le ONG riescono a guadagnarsi nei luoghi in cui operano.

L'**accettazione** non è qualcosa che avviene da sola, ma fa parte di una **strategia complessa**, il cui successo dipende da:

- l'utilizzo di un modello che aggiunge valore ai processi condivisi, aumentando la partecipazione, la trasparenza, la sostenibilità e la gestione di feedback e reclami;
- la reputazione della ONG e la sua credibilità come attore dello sviluppo e dell'aiuto umanitario;
- la qualità del personale selezionato;
- la reputazione e l'affidabilità dei partner e degli attori locali che collaborano con la ONG;
- la qualità e la pertinenza dei programmi realizzati;
- la capacità della ONG di comunicare ciò che fa in tutti i modi: rapporti, visibilità, media, amministrazione, gestione delle risorse umane, ecc.

È necessario tenere in considerazione anche l'atteggiamento della popolazione locale nei confronti delle organizzazioni internazionali, a cui le ONG vengono spesso paragonate.

Un'organizzazione che ha raggiunto il massimo grado di accettazione possibile nell'area in cui opera è generalmente un'organizzazione protetta, al riparo dalla maggior parte dei rischi, che conta su numerosi fattori di protezione offerti dalla comunità in cui la ONG opera.

Tuttavia, questo spesso non è sufficiente a garantire la massima sicurezza, laddove esistono rischi che richiedono soluzioni diverse: un'area con un'alta frequenza di calamità naturali, ad esempio, o la presenza di gruppi criminali indifferenti al ruolo della ONG.

Protezione

La protezione è il secondo approccio più diffuso adottato dalla maggior parte delle ONG. Un approccio di protezione utilizza dispositivi e procedure di difesa per **ridurre la vulnerabilità** alla minaccia al personale, ai beni, alle attrezzature, ai documenti e alle infrastrutture, ma non è in grado di ridurre la minaccia stessa.

Questo approccio può essere seguito in due modi: rafforzando l'obiettivo o modificando il livello di visibilità (una maggiore o minore visibilità può essere strategicamente più o meno adeguata a seconda del contesto).

Un esempio di questo tipo di approccio sono le misure adottate dalle ONG per proteggere i locali, come le sbarre alle finestre, l'illuminazione notturna, ecc. o quelle relative ai trasporti e alle comunicazioni, come veicoli moderni e sicuri o sistemi di comunicazione affidabili. Anche la formazione e le regole di comportamento del personale locale e straniero devono essere considerate misure di protezione.

Deterrenza

In diversi Paesi la neutralità delle ONG non è riconosciuta. Sempre più spesso sono vittime di aggressioni, rapimenti o attacchi da parte di vari tipi di gruppi criminali o terroristici, tanto che questo tipo di violenza rappresenta il principale fattore di rischio per il personale umanitario.

In questo contesto, è quindi necessario aggiungere alle misure di gestione del rischio **la deterrenza**, attraverso il **contenimento della minaccia** o la **contrapposizione con una contro-minaccia**. Le strategie di dissuasione comprendono il ricorso a guardie armate e bodyguard, la minaccia di abbandonare l'area interrompendo i programmi e l'assistenza, il ricorso a società private di gestione della sicurezza, ecc.

La deterrenza è quindi una contro-minaccia espressa in termini giuridici, economici, politici o militari. Il suo scopo non è tanto quello di agire sui rischi in generale e implicitamente o esplicitamente sulla vulnerabilità, quanto quello di utilizzare apertamente una contro-minaccia per fermare o rallentare la minaccia originale.

Strategia consigliata

Alla luce della loro missione e dei principi e valori di cui sono portatrici, le ONG tendono a preferire il **consenso come approccio strategico più appropriato**. Tuttavia, anche se è la base della strategia di sicurezza, non può essere efficace contro tutte le minacce. In luoghi dove la criminalità, il banditismo e il terrorismo sono diffusi, dove le fazioni in guerra perseguono obiettivi nazionali o globali e dove gli obiettivi delle agenzie di aiuto non sono riconosciuti, l'approccio del consenso da solo non può essere sufficiente.

D'altra parte, anche la protezione e la dissuasione non sono esenti da problemi. Adottando l'approccio di protezione, l'agenzia si identifica come un potenziale bersaglio, rischiando di generare una mentalità paranoica da "bunker", che può pregiudicare i rapporti con gli altri, compresi quelli delle comunità assistite; il ricorso all'approccio di dissuasione, che implica l'uso di scorte o guardie armate, può essere in contrasto con la rivendicazione dei principi di non violenza e indipendenza dell'organizzazione, fino al rischio di apparire aggressivo.

Una strategia di sicurezza richiede quindi una **combinazione flessibile ed equilibrata di vari approcci ai problemi**, che può essere efficace solo se sviluppata in base alle caratteristiche dell'ambiente in cui verrà utilizzata, e solo se l'organizzazione ha la capacità e le competenze per gestirla adeguatamente, mantenendola aggiornata e adattandola alla luce dell'evoluzione del contesto e dei relativi rischi.

In nessun caso è possibile, sia con una singola strategia che con una combinazione, ridurre il rischio a zero.

Infine, occorre tenere presente che, indipendentemente dall'approccio o dal mix di approcci che si decide di adottare, ci sarà un costo e un obbligo costante da parte dell'organizzazione nell'allocazione delle risorse, anche quelle non necessariamente legate al settore della sicurezza (programmi, operazioni, risorse umane, ecc.).

Processo di analisi del rischio: componenti di base

L'analisi del rischio consiste nello **stabilire il livello di vulnerabilità** di una persona, di un'organizzazione, dei suoi beni e dei suoi programmi a uno specifico pericolo innato nel contesto della messa in pratica dell'attività o del progetto.

Questo esercizio permette non solo di sviluppare una serie di misure in grado di mitigare i rischi, ma anche di valutarli rispetto all'aiuto che il progetto porterà ai beneficiari. La gestione responsabile - di se stessi e degli altri - implica l'impegno a non mettere inutilmente in pericolo persone o beni, cioè a non esporli a rischi sproporzionati rispetto all'impatto dell'aiuto che si intende portare ai beneficiari.

L'analisi dei rischi deve essere trattata come un documento vivo, e come tale deve essere sottoposta a **revisioni e aggiornamenti periodici**, in base a cambiamenti significativi del contesto operativo, e comunque in occasione dell'inizio, della fine o dell'ampliamento dell'attività in questione, o in occasione di eventi particolari (come campagne elettorali, minacce di instabilità sociale o economica, previsione di particolari condizioni climatiche, ecc.)

Da un altro punto di vista, il rischio può essere definito e misurato calcolando oggettivamente la probabilità che una determinata minaccia si verifichi e il potenziale impatto sulle persone direttamente coinvolte (danni fisici, morali o psicologici) o sull'organizzazione nel suo complesso (attività programmate, danni economici o all'immagine o alla reputazione, ecc.)

L'analisi dei rischi deve portare all'attuazione di una **serie di misure di mitigazione**, secondo l'approccio scelto dalla ONG. Queste misure possono avere lo scopo di ridurre le debolezze della ONG, aumentare i suoi punti di forza, modificare le sue attività e/o cambiare la sua area operativa, ecc.

Nessuna misura di sicurezza può in genere coprire tutti i rischi. La soluzione migliore è una combinazione di più azioni, che in genere includono le seguenti:

- **ritiro:** nessuna azione ulteriore
- **controllo:** utilizzo di misure preventive o di mitigazione del rischio
- **distanziamento:** allontanamento temporaneo del bersaglio minacciato
- **trasferimento:** il rischio viene trasferito ad altri attori (compagnie di assicurazione, subappaltatori, partner).

Quest'ultima opzione dovrebbe essere considerata con estrema attenzione, poiché la responsabilità morale di valutare le conseguenze del rischio trasferito rimarrebbe a CESVI. La decisione di condurre una missione tramite controllo remoto o gestione a distanza è sempre presa al livello più alto, in CESVI dal Direttore Generale, e implica il trasferimento del rischio a partner o operatori locali.

QUADRO GIURIDICO

Decreto legislativo 81/2008

CESVI è conforme al decreto legislativo TU 81/2008⁶ e successive modifiche, che stabilisce per tutti gli enti di diritto italiano specifiche misure per la sicurezza e la protezione del personale.

La sede centrale di CESVI ha quindi elaborato un Documento di valutazione dei rischi.

CESVI ha nominato il Responsabile Salute e Sicurezza (H&S Manager). Sono stati inoltre nominati il Rappresentante dei Lavoratori per la Sicurezza e gli addetti al primo soccorso e alla prevenzione degli incendi, come previsto dal TU 81/2008. È stato inoltre nominato un medico competente. I corsi di qualificazione necessari per poter svolgere queste funzioni sono organizzati come previsto dalla legge. Tali corsi vengono ripetuti a intervalli regolari, come previsto dalla legge.

Nella sede centrale il GM è direttamente responsabile dell'applicazione delle misure di sicurezza con l'ausilio di un suo delegato, nel caso specifico l'Head of Finance & Accounting, che ha ricevuto il mandato il 1 agosto 2016.

Il Consiglio di Amministrazione ha deciso che il Responsabile H&S debba avvalersi, per tutto ciò che riguarda l'attività istituzionale all'estero, di un **Security Advisor**, nominato con specifico mandato, per un lavoro di consulenza e monitoraggio. Tali attività, oltre a essere prevalenti, sono anche le più esposte a vari tipi di rischio.

RESPONSABILITÀ, SOGGETTI E STRUMENTI UTILIZZATI NELLA GESTIONE DELLA SICUREZZA

Responsabilità e parti interessate

CESVI ritiene che la **distribuzione delle responsabilità**, la **comunicazione tra il personale** e la **verifica dell'applicazione delle misure adottate** siano fattori chiave per gestire al meglio la sicurezza e la protezione. Tutti i membri del personale sono quindi chiamati a riconoscere le proprie responsabilità personali in materia di sicurezza e a dare il proprio contributo in queste tre aree.

Tutto il personale deve essere costantemente attento alle questioni relative alla sicurezza e alla protezione. L'esistenza di servizi specifici e di soggetti responsabili non esonera nessun membro del personale da:

- comprendere e implementare le misure di sicurezza;
- essere attenti ai rischi e alla sicurezza del proprio team;
- essere responsabili della propria sicurezza e di quella dei propri sottoposti;
- comportarsi positivamente come membro di CESVI, promuovendo il Codice di condotta del personale di CESVI;
- partecipare alla creazione di una "cultura della sicurezza";

⁶ *Testo unico sulla salute e sicurezza sul lavoro*, secondo la legge italiana.

- segnalare qualsiasi azione o violazione della Policy sicurezza e dei relativi documenti al proprio Line Manager (si veda anche il paragrafo *Strumenti organizzativi per la gestione della sicurezza*);
- utilizzando il proprio giudizio⁷, laddove le misure di sicurezza sono deboli o inapplicabili.

Responsabile Salute e Sicurezza (H&S Manager)

Il Responsabile della Salute e Sicurezza è la figura prevista dalla legge italiana per occuparsi dei problemi di sicurezza delle aziende (comprese le organizzazioni non profit). Questa figura ha quattro compiti: individuare i pericoli ed eliminare i rischi conseguenti, supervisionare la redazione del Documento di Valutazione dei Rischi, formare il personale e promuovere la salute dei lavoratori.

In CESVI, la figura del Datore di Lavoro è assunta dal Direttore Generale, che dal 1 agosto 2016 ha delegato il ruolo di H&S Manager all'Head of Finance & Accounting che, per le attività all'estero, si avvale del Security Advisor.

Medico competente

Il **medico competente** è la figura prevista dalla legge italiana per la vigilanza sulle problematiche sanitarie del personale.

Security Advisor

Tutte le misure di sicurezza devono essere applicate all'estero da tutto il personale di CESVI, che opera in stretta collaborazione con il **Security Advisor**, delegato dal Datore di Lavoro in data 19 giugno 2017, ai sensi dell'art. 16 del D.Lgs. 81/08.

Il Security Advisor riporta al GM e ha il compito **di consigliare e supportare il personale espatriato**; questa figura monitora l'efficacia delle misure di sicurezza adottate dall'ONG nei vari Paesi in cui opera e fornisce al GM la sua valutazione.

Il *Security Advisor* elabora anche **raccomandazioni generali o specifiche**. Tali raccomandazioni, una volta autorizzate dal GM, vengono comunicate al personale interessato. Le raccomandazioni sono tratte dall'analisi di situazioni, incidenti avvenuti o da informazioni condivise con le reti di sicurezza, con le quali il Security Advisor è costantemente in contatto. Man mano che vengono emanate, le raccomandazioni diventano parte integrante della presente Policy sicurezza. Se necessario, il Security Advisor può essere inviato all'estero e assumere il ruolo di Security Manager su base temporanea o permanente.

La descrizione delle mansioni del Security Advisor è specificata nell'Appendice.

Altre parti coinvolte

Le misure di sicurezza - in Italia e sul campo - sono applicate secondo la struttura operativa di CESVI.

Pertanto, presso la sede centrale, il Direttore Generale è direttamente responsabile dell'applicazione delle misure di sicurezza, con il supporto del suo delegato⁸. All'estero, le misure di sicurezza vengono applicate seguendo la gerarchia della struttura operativa, a partire dal Direttore Generale

⁷ Può essere utile ricordare la sintesi proposta da Medici con l'Africa CUAMM, per capire cosa si intende per giudizio: 1. osservare ed essere attenti e prudenti; 2. fare attenzione alle proprie impressioni; 3. cambiare spesso abitudini (percorsi e orari); 4. essere rispettosi ma non sottomessi; 5. mantenere la calma; 6. non mettere mai a rischio la propria vita per difendere le risorse materiali.

⁸ Il 1° aprile 2016 il responsabile del settore finanziario e contabile ha ricevuto il mandato.

all' Head of International Programmes, al Regional/Area Manager insieme all'Head of mission del Paese, fino ai Focal Points per la sicurezza presenti in ogni Paese (o area all'interno del Paese).

Nei Paesi ad alto rischio è prevista anche una figura specifica, il **Country Security Manager** (CSM). Laddove non sia possibile o necessario assumere un CSM dedicato, il ruolo sarà assegnato a un team di personale che, coordinato da un team leader, fungerà da punto focale della struttura di sicurezza. La composizione e le specifiche procedure di lavoro del team saranno definite a livello di singolo Paese, seguendo le linee guida generiche e con il supporto del Security Advisor.

Per essere in grado di svolgere questo ruolo, il personale dovrà dimostrare disponibilità e attitudine, oltre a ricevere un sostegno, una formazione e un riconoscimento sufficienti da parte dell'organizzazione per semplificare l'aggiunta di questo compito alle sue normali attività. Il personale responsabile della sicurezza deve avere le proprie funzioni chiaramente formulate nei mandati individuali e nei parametri di valutazione e performance.

Il Security Advisor svolge un ruolo di stimolo, indirizzo e controllo nei confronti della struttura operativa.

Country security manager

È il responsabile della gestione e della supervisione delle misure di sicurezza nei **Paesi a maggior rischio**: effettua analisi dei rischi, fa circolare le informazioni e forma il personale in loco.

Questo ruolo non può essere generalmente compatibile con quello dell'Head of mission (salvo circostanze particolari e previa approvazione del GM) poiché, tra gli altri fattori, la responsabilità del controllo, del supporto, della consulenza, della formazione e della rappresentanza in materia di sicurezza deve essere tenuta separata da altri ruoli di gestione o di rappresentanza. Può essere affidata a personale espatriato o locale con compiti di natura preferibilmente logistica. Il Country Security Manager risponde all'Head of mission e si consulta e chiede consiglio al Security Advisor (per il JD si veda l'appendice).

Focal points per la sicurezza a livello nazionale e sul campo

In ogni Paese viene istituita una **Country Security Team (CST)**, composta dai Focal points di sicurezza nazionali e coordinata da un Capo squadra.

Il CST collabora allo sviluppo e alla revisione della Policy sicurezza, alla determinazione dei requisiti minimi di sicurezza e alla revisione delle procedure di sicurezza dell'organizzazione; il team supporta inoltre i responsabili della messa in pratica e del controllo di gestione del rischio di sicurezza per quanto riguarda i parametri e le attrezzature a disposizione nel Paese; infine, assicura che i piani per la gestione delle crisi siano elaborati, messi in pratica e testati periodicamente.

I *Security Focal Point* (SFP) che compongono il CST devono essere selezionati in modo da formare un gruppo eterogeneo, che comprenda personale nazionale e internazionale, e un gruppo equilibrato.

numero di uomini e donne, in modo da essere rappresentativi di tutte le realtà lavorative della missione.

Ogni SFP, nel contesto specifico della struttura di sicurezza del Paese, collabora con la missione per **promuovere la sicurezza del personale** e garantire la conoscenza e il rispetto della Policy sicurezza e delle procedure in vigore.

L'SFP è responsabile della **raccolta e della diffusione di informazioni affidabili** relative **alla sicurezza**, che possono contribuire all'aggiornamento dell'analisi del contesto; l'SFP tiene inoltre informati i colleghi, contribuendo così alla creazione di una cultura della sicurezza.

Team di gestione delle crisi

In caso di gravi situazioni di crisi, incidenti o minaccia di gravi minacce, CESVI attiva un **Crisis Management Team (CMT)**.

La squadra, presieduta dal GM, rimane attiva per tutta la durata della crisi e si riunisce in modo informale e con qualsiasi mezzo (anche elettronico). È composta da:

Squadra di gestione delle crisi (CMT):

- General Manager
- Head of International/National Programmes Department
- Security Advisor
- Head of Fundraising & Communication Department
- Head of Finance & Accounting Department
- Head of Human Resources
- Legal & Compliance Manager
- Area/Regional Manager
-

La CMT può decidere di coinvolgere qualsiasi altra persona che possa contribuire alla gestione e alla soluzione della crisi (ad esempio il Presidente, il Head of mission, il Country Security Manager o qualsiasi altro membro del personale CESVI nel Paese interessato dalla crisi).

Di seguito sono riportati alcuni esempi di crisi a cui l'équipe risponde:

- morte, incidente grave o malattia di un membro del personale;
- rapporti con i parenti più prossimi del personale vittima di un incidente grave;
- disastro o altro evento che impedisca al coordinamento o agli uffici locali del Paese di funzionare regolarmente;
- interruzione delle comunicazioni con una delle basi estere o grave malfunzionamento informatico della sede centrale;
- rapimento;
- richieste di risarcimento danni derivanti da incidenti.

Il Team si occupa anche di qualsiasi altro evento che il GM ritenga necessario trattare, compresi quelli proposti da altri membri del Team.

Il GM riferisce al Consiglio di amministrazione sulle attività del Team e sottopone all'approvazione del Consiglio di amministrazione tutte le questioni relative a quest'ultimo.

Il GM può autorizzare la creazione di una Squadra di Crisi in loco per gestire eventuali situazioni contingenti, chiamando il personale più adatto a gestire la crisi nel Paese in questione.

Strumenti e sistemi organizzativi per la gestione della sicurezza

Per la gestione della sicurezza e della protezione sono disponibili i seguenti **strumenti e sistemi organizzativi o prerequisiti**:

- questa Policy, illustrando le linee guida di base e la distribuzione delle responsabilità;
- un Documento di Valutazione dei Rischi (solo per HQ) come da TU 81/2008;
- un Manuale generale sulla sicurezza del personale all'estero: ECHO, Guida generica alla sicurezza, 2004;
- il manuale *Gestione operativa della sicurezza in ambienti violenti* della Rete di pratiche umanitarie (HPN);
- materiali di formazione
- un documento di definizione sintetica dei rischi specifici di un paese (il suo "semaforo") e definizioni del profilo da utilizzare in ciascun Paese;
- Piani di sicurezza nazionali per tutti i paesi
- Rapporto annuale sulla sicurezza;
- bilancio generale per le misure di sicurezza e la formazione;
- piano di allenamento;
- raccolta e analisi dei dati relativi a incidenti e inconvenienti del personale;
- forme di assicurazione del personale e di copertura sanitaria adatte a ciascun Paese;
- il rispetto di quanto previsto dal Modello Organizzativo definito nel D.Lgs. 231/01;
- compiti di segnalazione all'Organismo di Vigilanza ai sensi del D.Lgs. 231/01.

Documento di valutazione del rischio

Previsto dal TU 81/2008. Riguarda l'analisi dei rischi relativi alla sede. Questo documento è obbligatorio per la legge italiana. Viene aggiornato dal H&S Manager.

Guida generica alla sicurezza ECHO 2004 e Manuale di sicurezza CESVI

Questi due documenti, essendo il primo più generale e completo mentre il secondo più semplice e immediato, sono i **principali riferimenti operativi** per quanto riguarda la gestione delle misure di sicurezza generiche per tutto il personale. In particolare, nei due documenti il personale che si sente impreparato in situazioni impreviste può trovare utili check list che consigliano le migliori azioni da intraprendere.

Il Manuale di sicurezza di CESVI è uno strumento semplice per la gestione di situazioni non specifiche legate alla sicurezza. Viene utilizzato da CESVI come manuale di riferimento quando non sono obbligatori strumenti più appropriati (come il piano di sicurezza nazionale). Ha il grande vantaggio di essere disponibile in inglese e francese e di essere di facile consultazione.

Analisi del rischio: Country Traffic Light

L'analisi dei rischi è il processo che sta alla base della Policy sicurezza di CESVI. Il suo obiettivo è quello di ridurre la vulnerabilità prima che si verifichino minacce concrete, affrontando per primi i rischi più probabili, senza mai trascurare quelli meno probabili, soprattutto se possono avere un grande impatto.

Come già detto, mantenere vivo questo processo, dirigerlo, trarne suggerimenti e conclusioni, fa parte del mandato del Security Advisor.

Uno degli strumenti di analisi del rischio di CESVI è il **Country Traffic Light**. Si tratta di una tabella in cui cinque diversi colori (verde, giallo, arancione, rosso e grigio)⁹ indicano i diversi livelli di rischio dei Paesi in cui opera CESVI.

Il Country Traffic Light è composto da sette Categorie, ulteriormente suddivise in Sottocategorie più specifiche, per la Sicurezza (intesa come libertà da rischi o danni derivanti da violenza o altri atti intenzionali) e per la Protezione (intesa come comfort e libertà da minacce non intenzionali, fenomeni naturali, malattie ecc.)

Gli indicatori che compongono il **Country Traffic Light** sono rivelatori di una condizione specifica; gli indicatori devono essere analizzati nel loro insieme, e in relazione al contesto specifico del Paese, come guida per formulare un giudizio sul livello di minaccia o di rischio; tuttavia, non tutti gli indicatori sono necessariamente applicabili in contesti diversi e richiedono l'interpretazione del personale di sicurezza.

Ad ogni livello/colore corrispondono una o più posture, condizioni preliminari, procedure e catene di comando diverse (R.A.C.I.).

Analisi dei rischi: il profilo della ONG nel Paese

Non è possibile redigere un Piano di Sicurezza Nazionale senza stabilire in anticipo, all'inizio della missione o il prima possibile, sia gli **obiettivi del progetto e i limiti** entro i quali si collocano le risorse e le attività che la ONG intende sviluppare, sia il **tipo di visibilità** della ONG nel dato Paese.¹⁰

La scelta del tipo di Profilo Paese (ad alto o basso input di progetto; ad alta o bassa visibilità) viene decisa dall'Head of Programmes Department and the Regional/Area Manager, poiché influenza l'intera struttura delle misure di sicurezza adottate nel Paese dalle fondamentali. La decisione viene presa insieme al Security Advisor e al Direttore generale e può essere rivista se necessario. Ogni revisione comporta l'aggiornamento del piano di sicurezza per includere il nuovo profilo. La scelta del profilo del Paese implica la definizione del livello di rischio accettabile in quel Paese.

⁹ Il colore rosso indica la presenza di diversi rischi di alto livello nel Paese. Per affrontarli, quindi, deve essere in vigore uno specifico Piano di sicurezza nazionale, con raccomandazioni dettagliate sulla sicurezza e sulla gestione delle emergenze nel Paese. Indica inoltre che è stato scelto un membro del personale per ricoprire il ruolo di Country Security Manager. Il personale non deve essere accompagnato da familiari durante le missioni in questi Paesi ad alto rischio (nessuna stazione di servizio per i familiari). Il giallo indica che il Paese è sotto osservazione speciale per la valutazione di nuovi rischi. È necessario introdurre un piano di sicurezza specifico o riportare l'indicatore al livello più basso il prima possibile. Il verde indica che il Paese è considerato una destinazione a basso rischio.

¹⁰ Un conto è operare in un Paese in cui le attività delle ONG godono di un ampio consenso e i programmi sono realizzati con una ricchezza di risorse che implica un alto profilo in termini di visibilità e di apporto progettuale (personale numeroso, risorse economiche significative, rapporti espliciti e diffusi con le comunità e le autorità interessate, ecc. Altra cosa è quando si deve mantenere un profilo basso, con poca o nessuna visibilità, e l'apporto progettuale è limitato (rapporti solo con i gruppi interessati e più vicini, risorse economiche limitate, personale ridotto allo stretto indispensabile, ecc.)

Analisi del rischio: rischio accettabile

Nelle situazioni più critiche, il processo descritto brevemente sopra mira anche alla definizione di un **rischio accettabile**, cioè una **soglia** oltre la quale sarebbe meglio introdurre azioni di mitigazione del rischio o ritirarsi:

- le conseguenze dell'attuazione del programma sarebbero così gravi da giustificare l'accettazione di un tale rischio?
- sono state esplorate tutte le alternative possibili per raggiungere gli obiettivi dei programmi?
- sono stati compiuti tutti gli sforzi in termini di risorse umane e finanziarie per ridurre il rischio a un livello medio?
- quale strategia è stata utilizzata per evitare che i rischi non eliminabili crescano ulteriormente?
- quali sarebbero le conseguenze della mancata attuazione del programma o della sua interruzione?

La verifica del livello di rischio accettabile è di competenza del Security Advisor. Quando in un Paese, considerando i programmi attuati, i rischi valutati sono superiori alla soglia di accettabilità, il Regional/Area Manager il Responsabile del Dipartimento Programmi vengono informati dal Security Advisor.

Solo i più alti livelli di responsabilità di CESVI - Presidente, Direttore Generale e Consiglio di Amministrazione - possono innalzare congiuntamente la soglia di rischio accettabile presente in un Paese, in questo sollecitati dal Capo Dipartimento Programmi, dal Security Advisor.

Piano di sicurezza del Paese

Il **Piano di Sicurezza Nazionale** è un documento essenziale per la gestione quotidiana della sicurezza nei Paesi ad alto rischio. Nessun Piano Paese è uguale a un altro, perché ognuno deve corrispondere alle condizioni specifiche in cui CESVI opera nel Paese in questione. **I rischi più probabili**, o eventualmente quelli di maggiore impatto, vengono identificati per il Piano analizzando il contesto in cui operano le ONG nel Paese, o quello di un'area specifica. Vengono inoltre descritte le misure preventive per la gestione dei rischi o le reazioni alle minacce che potrebbero verificarsi.

L' Head of mission è responsabile della redazione e dell'aggiornamento del Piano di sicurezza nazionale, mentre il Responsabile della sicurezza nazionale e/o il Punto focale di sicurezza nazionale ne sono responsabili, con il supporto del Security Advisor. Il Piano di sicurezza deve essere aggiornato almeno una volta all'anno, e comunque ogni qualvolta si verificano cambiamenti che rendano inefficace l'edizione.

Il processo di elaborazione del Piano di Sicurezza Nazionale deve essere condiviso, includendo il personale di programmazione e operativo a tutti i livelli (manageriale e sul campo), nazionale e internazionale, con un adeguato equilibrio di genere, al fine di rispettare - nell'analisi dei rischi e nella proposta di soluzioni - i punti di vista di tutto il personale interessato.

CESVI fornisce le linee guida per lo sviluppo e la stesura del Piano.

Relazione annuale e bilancio annuale sulla sicurezza

Il **Rapporto Annuale sulla Sicurezza** viene redatto annualmente dal Security Advisor e riassume, per il Direttore Generale, il Consiglio di Amministrazione e l'Organismo di Vigilanza

tutto ciò che è accaduto durante l'anno in merito alla sicurezza della ONG. È accompagnato da un bilancio finale.¹¹

Il Security Advisor elabora annualmente una pianificazione sintetica accompagnata da un bilancio di previsione volto a coprire i costi generali della sicurezza sostenuti dalla sede della ONG.

Formazione

L'applicazione delle misure di sicurezza deve essere sostenuta da un **processo basato sulla partecipazione e sull'attenzione**, rafforzato da sessioni di formazione. CESVI si impegna a redigere un piano di formazione sulla sicurezza. Il Security Advisor è incaricato di redigere e rivedere questo piano, che specifica nel dettaglio tempi, contenuti e destinatari della formazione, modalità di erogazione e caratteristiche dei formatori.

Deve includere e gestire:

- formazione di base prima della partenza per tutto il personale espatriato (indipendentemente dal tipo di impiego e dalla responsabilità);
- formazione specifica per il personale che assume il ruolo di Country Security Manager in loco;
- la possibilità e i criteri che consentono al personale di partecipare a formazioni generali o specifiche organizzate da soggetti ufficiali, con o senza il contributo di CESVI ai costi;
- formazione specifica per tutto il personale, compreso quello locale, nei Paesi in cui è in vigore un Piano di sicurezza nazionale (Paesi ad alto rischio).

Il Piano, rivisto ogni volta che è necessario, è un documento interno e comprende anche:

- informazioni sui contenuti, i tempi e i formatori del corso di base prima della partenza, del corso per manager della sicurezza del Paese, del corso per il personale assegnato ai Paesi ad alto rischio;
- un elenco dei soggetti che offrono formazione specifica e informazioni sulla possibilità di usufruirne;
- informazioni sui corsi svolti in loco: contenuti, metodi, formatori.

La partecipazione di familiari, giornalisti, personale di altre ONG o altre persone interessate ai corsi di formazione tenuti da CESVI è soggetta all'approvazione del Security Advisor. CESVI sostiene i costi della formazione che offre.¹²

Tutte le persone formate sono tenute a contribuire all'applicazione delle misure di sicurezza di CESVI, nei limiti delle loro capacità e responsabilità.

Analisi di incidenti e inconvenienti

L'analisi degli incidenti e degli inconvenienti che si verificano più frequentemente nel personale della ONG è utile per migliorare la formazione e la promozione di misure di protezione e sicurezza sempre più adeguate a fronteggiare i rischi a cui la ONG è soggetta. Il compito del Security Advisor è quello di tenere aggiornato il **database** degli incidenti e degli **inconvenienti** della ONG e prevede anche la redazione di un capitolo specifico nel rapporto annuale. Gli operatori devono comunicare, entro 48 ore, direttamente o tramite il proprio Line Manager, gli eventi (a prescindere dal tipo di incidente) che si sono verificati.

¹¹ Un esempio del contenuto del rapporto annuale sulla sicurezza è riportato negli allegati.

¹² Viaggio, alloggio, materiale didattico e pedagogico.

causa: salute, incidente o violenza) che hanno in qualche modo influito sulla sicurezza dell'organizzazione. Se ritenute importanti, queste informazioni dovrebbero essere estese a fatti riguardanti altre ONG con cui CESVI ha rapporti nella stessa area operativa. Per il modulo di segnalazione degli incidenti si rimanda agli allegati della presente Policy.

La formazione comprende la segnalazione e l'analisi degli incidenti.

La relazione deve essere trasmessa all'Organismo di Vigilanza annualmente, tranne nei casi di infortuni sul lavoro gravi con prognosi superiore a 40 giorni, nel qual caso la comunicazione è immediata.

Assicurazione

Tutto il personale espatriato che opera per CESVI (indipendentemente dal tipo di impiego o dalle responsabilità) ha una **copertura assicurativa** contro malattie, infortuni, responsabilità civile, morte, **evacuazione medica urgente e rimpatrio per motivi di salute, che copre anche i casi di guerra.**¹³

Nel caso in cui il personale abbia una propria polizza assicurativa, CESVI valuterà in ogni caso se estendere la propria copertura assicurativa standard. In caso contrario, gli operatori dovranno rinunciare esplicitamente al diritto alla polizza assicurativa offerta da CESVI. I premi assicurativi stipulati da CESVI sono a carico di CESVI.

Il personale deve sempre fornire i nomi delle persone da contattare in caso di emergenza (parenti prossimi).

La copertura assicurativa per tutto il personale assunto nel Paese è definita a livello locale, in base alle leggi e alle pratiche locali. La Policy delle risorse umane di CESVI stabilisce inoltre che tutto il personale di CESVI deve avere un'assicurazione contro gli infortuni e la pensione, laddove non sia prevista dalle leggi locali sul lavoro. Tutti i progetti devono prevedere un budget adeguato.

Il personale locale che opera in aree diverse da quelle di provenienza (vedi "Evacuazioni") è incluso nella categoria del personale pagato da CESVI in caso di evacuazione medica, attraverso una speciale copertura assicurativa o accordi ad hoc con società specializzate in evacuazioni mediche urgenti.

In caso di dubbio, ogni dipendente può chiedere chiarimenti sulla copertura assicurativa al team delle risorse umane o al proprio manager di linea.

¹³ Le coperture assicurative scelte da CESVI sono tra le migliori disponibili. Tuttavia, presentano anche alcune eccezioni: i singoli membri del personale sono responsabili della verifica dei contenuti e dei massimali delle polizze assicurative che li riguardano.

ATTORI E SITUAZIONI SPECIFICHE

Coinvolgimento del personale locale

Definire, applicare e verificare le misure di sicurezza non è mai un processo semplice o limitato: interessa tutto il personale e tutti gli aspetti di ogni missione di CESVI. CESVI crede nelle sessioni di formazione per rendere tutto il personale consapevole delle proprie responsabilità (vedi Policy del Personale): maggiore è la collaborazione, maggiore è la sicurezza. Il coinvolgimento del personale locale sarà sempre richiesto, sia in fase di individuazione degli strumenti di sicurezza, sia in fase di formazione e applicazione, fino alle fasi di controllo.

Salute

Principi generali

Le condizioni operative espongono il personale a **rischi per la salute**. CESVI ha pertanto elaborato un sistema dettagliato per la corretta gestione della tutela della salute. Esso comprende quanto segue:

- esami del sangue (indicati dal medico competente);
- un elenco delle vaccinazioni raccomandate per ogni area operativa;
- visita medica effettuata dal medico competente per stabilire l'idoneità al Paese di destinazione;
- controllo da parte del medico della validità delle vaccinazioni;
- assicurazione;
- metodi di gestione dello stress e dei traumi (supporto psicologico);
- programmazione dei periodi di riposo (specificati nei contratti di lavoro) e R&R¹⁴ in missioni particolarmente stressanti;
- l'assicurazione sociale e sanitaria per il personale locale in base alle normative locali sul lavoro.

Gli strumenti di sicurezza o i sistemi organizzativi (Piano di protezione, Piano di sicurezza, ecc.) di ciascun Paese devono dedicare adeguata attenzione alle misure di prevenzione sanitaria, diagnosi e cura attivabili per il personale nei contesti locali (come ad esempio la stipula di polizze assicurative o di convenzioni con cliniche locali).

Malaria

Trattandosi di una delle malattie tropicali più pericolose, CESVI è particolarmente attento a informare il personale designato a lavorare nei Paesi considerati a più alto rischio.

Gestione dello stress e dei traumi

Al personale vengono offerti due metodi ordinari per affrontare le **situazioni di stress** legate alle attività di cooperazione allo sviluppo e agli aiuti umanitari.

Il manager di linea dell'operatore è la prima persona incaricata di gestire i segnali di stress o di trauma. Il personale espatriato può inoltre sempre accedere a uno psicologo esperto tramite il team HR della sede centrale, che si occuperà delle domande del personale con discrezione.

¹⁴ R&R: riposo e recupero. Le modalità di applicazione specifiche vengono decise caso per caso (si veda anche la Policy sulle risorse umane).

Gli episodi gravi di natura traumatica devono essere sempre comunicati al Direttore Generale, al Security Advisor o al Responsabile della Direzione Risorse Umane. Il Security Advisor verifica e indaga le condizioni operative per individuare le cause di stress e prevenirle.

Una sezione specifica del Documento di valutazione dei rischi è dedicata allo stress lavoro-correlato.

Gravidanza

Lavorare in progetti umanitari e di cooperazione allo sviluppo in **gravidanza** non ha alcun effetto sui risultati raggiunti, ma è spesso sconsigliato a causa dei rischi ambientali e delle relative misure proposte per combatterli, come nel caso delle vaccinazioni, che a volte possono essere incompatibili con la gravidanza.

La gravidanza implica un'assunzione di responsabilità più ampia e profonda da parte del personale, affinché le misure di sicurezza e protezione che lo riguardano siano gestite nel migliore dei modi:

- trattamento preventivo per il viaggiatore internazionale: viaggio, stress, vaccinazioni, farmaci;
- valutazione dei rischi specifici dell'area di destinazione;
- valutazione dei compiti.

CESVI informa il personale in gravidanza dei rischi generali che corre, offrendo al contempo il massimo supporto possibile.

Uso di sistemi e strumenti di deterrenza

Armi

Portare armi (armi da fuoco, coltelli, esplosivi) mette a rischio la **posizione di neutralità e imparzialità** che CESVI cerca di mantenere in tutti i contesti.

La presenza di armi costituisce un rischio per la sicurezza del personale e di coloro che operano con loro (destinatari del programma).

Pertanto, il personale di CESVI non è autorizzato a portare armi.

Nessuna persona armata può avere accesso a veicoli o locali - anche se affittati - che ricadono sotto la responsabilità di CESVI. CESVI farà tutto il possibile per vietare l'uso di qualsiasi tipo di arma in tutti gli ambienti in cui opera l'ONG.

Guardie armate

Poiché CESVI segue un approccio alla sicurezza non basato sulla deterrenza, evita di utilizzare **guardie armate o scorte** per svolgere le sue attività.

Tuttavia, in alcune circostanze l'uso di guardie armate può essere richiesto dai governi dei Paesi in cui CESVI opera come condizione preliminare per autorizzare le operazioni della ONG, oppure può essere necessario per consegnare aiuti umanitari urgenti in situazioni apertamente minacciose.

In queste situazioni, e in tutti i casi in cui se ne presenti la necessità, solo il Direttore Generale, in collaborazione con il Security Advisor e con adeguate informazioni da parte del Regional/Area Manager interessato, può acconsentire a una **deroga**, basata su una specifica analisi dei rischi, per consentire l'uso di guardie o scorte armate.

L'autorizzazione è sempre legata a una situazione specifica e non può essere generalizzata per includere altre situazioni simili. In nessun caso tali guardie o scorte possono essere assunte direttamente da CESVI. Devono far parte di organismi militari, di polizia o di sicurezza riconosciuti dal Paese che ospita la ONG.

Utilizzo di società di sicurezza private

Il ricorso ad **agenzie di sicurezza private** per la sorveglianza è consentito a condizione che soddisfino i requisiti e le misure di sicurezza indicati nel paragrafo precedente, sia conforme alla legge del Paese ospitante e non violi le policy e i codici a cui l'organizzazione aderisce. Le agenzie private contrattate devono aderire e applicare il Codice di condotta internazionale dell'Associazione dei fornitori di sicurezza privata (ICoCA).

Gestione delle situazioni critiche

Attacchi, arresti

La **prevenzione delle aggressioni** (come rapine, intimidazioni, aggressioni sessuali, ecc.) è una componente essenziale della formazione e dei Piani di protezione e di emergenza sanitaria di tutti i Paesi in cui CESVI opera.

A tal fine, ogni Piano deve prevedere un'analisi dei rischi e dei comportamenti che possono prevenirli: evitare certe zone in certe ore del giorno, evitare certi luoghi, evitare percorsi abituali, ecc. In caso di aggressioni a un membro del personale, le persone informate dei fatti, o la persona con il più alto livello di responsabilità nel Paese, devono inviare una **relazione dettagliata** al Security Advisor, evidenziando le misure da adottare per prevenire eventi simili in futuro.

In caso di arresto di un membro del personale espatriato, CESVI informerà le autorità consolari e deciderà le azioni da intraprendere **per facilitarne il rilascio nel più breve tempo possibile**. Se necessario, verrà contattato un avvocato per assistere il caso. CESVI valuterà anche se esistono le condizioni per informare la Croce Rossa Internazionale. Azioni simili vengono messe in atto nel caso di personale locale.

Rapimento e sequestro di persona

Il rapimento e la rapina sono due delle **minacce più gravi** che il personale delle ONG deve affrontare.

La formazione di base del personale CESVI in partenza per i Paesi in cui questo rischio è diffuso comprende una sezione specifica su come affrontare o prevenire questo evento. Il Country Security Manager è responsabile dell'attuazione di una sessione di formazione in loco per tutto il personale locale.

Se un membro del personale di CESVI viene rapito, la sede centrale di CESVI deve essere informata il prima possibile.

Il Direttore Generale attiverà il Team di gestione della crisi CESVI per organizzare quanto segue:

- contatti con i membri della famiglia;
- contatti con le autorità competenti (se necessario, anche con l'Unità di Crisi del Ministero degli Affari Esteri italiano);
- se necessario, la scelta di un mediatore;
- contatti con i media;
- scelta della migliore strategia per interagire eventualmente con i rapitori, anche quando non è stata fatta una richiesta specifica di riscatto.

Evacuazione

Ogni piano di sicurezza deve includere informazioni specifiche sulla **corretta gestione di un'evacuazione** e delle sue fasi preliminari, tenendo conto delle condizioni specifiche del Paese.

A corredo del Piano, dovranno essere predisposti i seguenti elenchi:

- un elenco del personale espatriato;
- un elenco del personale locale che vive e opera nell'area in cui è stato assunto;
- un elenco del personale locale che opera in un'area diversa da quella in cui è stato assunto o da cui proviene.

Il piano di evacuazione deve includere metodi di attuazione specifici per ogni categoria di personale menzionata.

CESVI è responsabile dell'evacuazione **del personale espatriato**, che seguirà le indicazioni contenute nel Piano di Sicurezza dell'area in questione o altre modalità definite da CESVI.

CESVI è responsabile dell'evacuazione in aree più sicure del proprio personale nazionale (locale) che opera lontano dall'area di provenienza.

CESVI non è responsabile dell'evacuazione del personale di CESVI che proviene dall'area in cui opera. Tuttavia, se sono evidenti rischi specifici per la sicurezza di questo personale, CESVI farà tutto il possibile per facilitare la loro evacuazione in aree protette, utilizzando le risorse del Paese colpito.

Tutte le categorie di personale sopra citate saranno informate sulle procedure da seguire in caso di evacuazione a seconda della categoria di appartenenza durante le sessioni di formazione sulla sicurezza in loco.

Il personale deve fare riferimento al Security Advisor per qualsiasi altra informazione.

In tutti i casi **le procedure di evacuazione** devono identificare almeno quanto segue:

- beni, attrezzature, documenti e personale da evacuare in caso di **pre-evacuazione**¹⁵ (personale non indispensabile e beni e risorse difficili da evacuare in caso di rapido deterioramento della situazione);
- personale da lasciare in loco, specificando con quali risorse e responsabilità;
- l'importo dello stipendio da versare in anticipo al personale locale (numero di mesi);
- metodi di sospensione del programma.

¹⁵ La pre-evacuazione avviene quando la situazione in un Paese si sta deteriorando ma c'è ancora tempo sufficiente per evacuare i beni e il personale non indispensabili.

Come indicato all'inizio di questa Policy, nessun operatore, sia esso locale o espatriato, può subire pressioni per continuare a lavorare per CESVI.

La decisione di interrompere temporaneamente le attività in un'area (**ibernazione**) - lasciando il personale sul posto, a causa dei pericoli che si corrono nel rimuoverlo - o di procedere a un'**evacuazione completa o parziale del personale**), è decisa dal Direttore generale in consultazione con il Capo del Dipartimento Programmi, su richiesta del Security Advisor del Area Manager/area.

Allo stesso modo vengono prese decisioni relative al **ritiro** da un Paese o alla **ripresa delle attività** in un Paese che è stato parzialmente o completamente evacuato.

In quest'ultimo caso, è necessario procedere quanto prima a una revisione delle misure di sicurezza nell'area prima della completa ripresa delle attività.

Nel prendere le suddette decisioni, CESVI agisce esclusivamente **nell'interesse del proprio personale e dei propri programmi**, ma valuta anche le informazioni e le indicazioni provenienti da numerosi soggetti (come le Nazioni Unite, le Ambasciate europee, le Autorità locali e i partner, l'Unità di Crisi del Ministero degli Affari Esteri italiano, altre ONG e altre organizzazioni internazionali, ecc.) Anche in questo caso, in caso di "ordini" di evacuazione emessi dalle autorità locali, CESVI agisce nell'interesse del proprio personale e dei propri programmi.

L' Regional/Area Manager è responsabile delle decisioni che riguardano i livelli di attenzione e di allarme che possono precedere un'evacuazione, ma si raccomanda sempre di consultare il Security Advisor.

Salvo i casi in cui l'improvviso verificarsi degli eventi sia accompagnato da un blackout delle comunicazioni (casi in cui decide il responsabile di CESVI con la massima responsabilità in loco), il personale sul campo deve sempre seguire esclusivamente le indicazioni concordate, come da linee guida sopra citate.

Il principio applicabile è che CESVI, essendo responsabile della sicurezza del suo personale, della protezione delle sue risorse e del successo dei suoi progetti, decide in ultima istanza sulle scelte di natura strategica (come quelle relative all'evacuazione o meno del personale, fatto salvo il diritto di recesso di cui gode ciascun operatore).

Aspetti amministrativi e dati sensibili

Trasferimento e gestione del denaro

La movimentazione e il maneggio di denaro devono avvenire secondo quanto descritto nel Modello Organizzativo in ottemperanza al D.Lgs. 231/01.

La gestione del denaro è un'attività rilevante in termini di sicurezza.

In tutti i Paesi esistono ormai servizi bancari affidabili che gestiscono i trasferimenti di denaro senza movimenti di contante. Tuttavia, se esigenze imprescindibili del progetto rendono necessari movimenti di denaro contante, è necessario ricorrere a **servizi specializzati** (società specializzate in trasferimenti di denaro, in grado di compensare eventuali perdite di denaro con una garanzia formale), evitando così di utilizzare il personale CESVI o semplici civili.

Nell'ambito della gestione quotidiana delle attività amministrative dell'ufficio CESVI, non è consentito tenere somme superiori a quelle necessarie per far fronte a emergenze o evacuazioni. In nessun caso possono essere conservati importi in contanti superiori a 10.000 euro¹⁶ in qualsiasi valuta presso una singola base CESVI.

Due membri del personale devono essere coinvolti nelle procedure di ricezione, conteggio e protezione del contante.

Qualora ragioni programmatiche rendano necessario lavorare con somme di denaro o procedure di gestione che non corrispondono a quelle previste da questa Policy e dal Manuale amministrativo, il Regional/Area Manager deve chiedere una deroga, fornendo una **Valutazione dei rischi**.

Protezione dei documenti e delle informazioni

La documentazione deve essere riservata e gestita in modo accurato e ordinato per prevenire azioni criminali.

L'**uso corretto delle informazioni e la loro corretta circolazione** è una parte importante di qualsiasi misura di sicurezza. Tutte le informazioni sono per definizione importanti in termini di sicurezza e vengono quindi fatte circolare solo tra il personale a cui sono destinate. Tutti i membri del personale sono responsabili delle informazioni che ricevono e inoltrano. È necessario evitare qualsiasi circolazione non necessaria, sia interna che esterna all'ONG. Le informazioni riguardanti i progetti, la sicurezza, l'amministrazione, il personale, il contesto, le proprietà, le risorse e i siti sono sempre riservate e devono essere trattate con prudenza per evitarne la circolazione impropria.

CESVI non utilizza abitualmente crittografia o cifratura nelle sue modalità di comunicazione. Tutti gli operatori devono prestare la massima attenzione nell'**utilizzare in modo appropriato i vari mezzi di comunicazione** (radio, e-mail, Skype, ecc.), evitando di mettere a rischio la propria sicurezza, quella dei colleghi o quella di altre parti eventualmente interessate.¹⁷

Comunicazioni

Principi, mezzi e metodi

Senza compromettere la protezione dei documenti e la riservatezza delle informazioni, una **buona comunicazione** con i colleghi e con tutte le principali parti interessate è **indispensabile per mantenere un elevato standard di sicurezza** nella ONG. Tutti i membri del personale sono tenuti a contribuire personalmente.

La concorrenza malsana tra i membri dello stesso team e tra le ONG è un fattore che mina notevolmente la capacità di rispondere ai rischi.

Al fine di prevenire situazioni problematiche, CESVI promuove **soluzioni trasparenti dei conflitti interni** (si veda la Policy sulle Risorse Umane) e intende collaborare con altre ONG e attori dell'aiuto umanitario per mantenere relazioni del più alto standard possibile.

¹⁶ Questa deve essere considerata una cifra massima, che comprende tutte le risorse necessarie per un'evacuazione improvvisa. Occorre fare il possibile per ridurre la quantità di contanti negli uffici.

¹⁷ Ulteriori indicazioni si trovano nei documenti e negli strumenti di riferimento di CESVI sulla protezione dei dati.

L'innalzamento della qualità complessiva del sistema di relazioni tra gli attori dell'aiuto umanitario può contribuire in modo significativo al mantenimento della sicurezza.

L'impiego e il corretto utilizzo dei moderni strumenti di comunicazione (radio, telefoni, ecc.) è di grande utilità per la gestione delle misure di sicurezza. CESVI si impegna a perseguire il più alto standard possibile in tutti i suoi progetti per garantire gli strumenti di gestione della sicurezza più efficienti attraverso strumenti e sistemi di comunicazione adeguati.

Debriefing e consegna

Il contributo di tutto il personale alla corretta applicazione e al miglioramento delle procedure di sicurezza è essenziale per l'applicazione della presente Policy. La partecipazione del personale a questo processo di scambio e apprendimento è garantita dai seguenti metodi minimi:

Il Security Advisor richiederà e raccoglierà valutazioni e suggerimenti da tutto il personale, sia individualmente che collettivamente, durante le missioni di monitoraggio condotte sul campo.

Trasporto

Utilizzo di auto e veicoli a motore

I problemi derivanti dagli spostamenti in autoveicoli sono estremamente importanti in termini di protezione del personale.

Purtroppo gli incidenti sono frequenti. Le seguenti raccomandazioni mirano a prevenirli o a ridurre le conseguenze.

Non è consentito l'utilizzo di autovetture o veicoli a motore che non abbiano superato una regolare prova su strada in conformità alle leggi del Paese di riferimento. Tutti i veicoli devono essere regolarmente assicurati secondo le norme del Paese di riferimento. I premi assicurativi devono essere adeguati a garantire la copertura dei costi derivanti da gravi danni a terzi.

In nessun caso considerazioni economiche possono impedire la sostituzione di veicoli a motore usurati e inefficienti con altri più efficienti e moderni.

Nei Paesi a più alto rischio¹⁸, CESVI consente l'**utilizzo di auto e veicoli a motore** esclusivamente ad autisti locali opportunamente selezionati e preparati. La verifica della corretta applicazione del codice della strada da parte degli autisti è un dovere per tutto il personale, in particolare per il Head of mission, che deve risolvere il contratto degli inadempienti in caso di ripetuti atti di negligenza, secondo le procedure specificate negli stessi contratti.

Il Piano di sicurezza del Paese o la SOP di sicurezza del Paese, se presenti, indicano espressamente i limiti applicati al personale nell'utilizzo di auto e veicoli a motore.¹⁹

I motocicli possono essere guidati solo se si indossa il casco di sicurezza.

L'uso delle cinture di sicurezza è obbligatorio su tutti i veicoli che ne sono dotati, a meno che, in situazioni particolari, ciò non aumenti la visibilità del personale e lo esponga a maggiori rischi.

In tutti i Paesi il comportamento corretto alla guida e altri problemi relativi alla guida di veicoli a motore (ad esempio, come comportarsi in caso di incidenti stradali) sono trattati in un programma specifico e regolare.

¹⁸ Indicato nel "Country Traffic Light" con il colore rosso.

¹⁹ Ulteriori indicazioni sono contenute nella *SOP CESVI per la gestione della flotta* (2024).

sessione di formazione organizzata sotto la responsabilità dell'Head of mission o, se previsto, dal Country security manager.

Anche nel caso di incidenti causati dal personale di CESVI, con una valida copertura di responsabilità civile, va valutata la possibilità di mitigare le conseguenze del danno aiutando immediatamente (anche finanziariamente) le vittime e i loro familiari.

Voli

CESVI non consente al proprio personale di utilizzare aerei appartenenti a compagnie che figurano nell'elenco delle compagnie aeree vietate dall'UE (**lista nera dell'UE**).

Le autorità dell'aviazione civile degli Stati membri dell'UE sono qualificate per ispezionare gli aerei delle compagnie che volano da/per gli aeroporti dell'UE; data la natura casuale di tali controlli, non è possibile esaminare tutti gli aerei che atterrano in tutti gli aeroporti dell'UE. Pertanto, se una compagnia non è inclusa nella lista nera dell'UE, ciò non significa che soddisfi automaticamente le misure di sicurezza attualmente in vigore.

Tuttavia, il fatto che una certa azienda compaia nell'elenco "fa suonare un campanello d'allarme" a CESVI.

Poiché i controlli al di fuori dell'Europa possono essere talvolta superficiali o inesistenti, **l'affidabilità della compagnia aerea prescelta** deve essere sempre verificata caso per caso e la scelta migliore deve essere fatta sulla base di una serie di informazioni utili alla decisione, da parte di tutti gli attori in contatto con CESVI. Tutti i piani di protezione o di sicurezza devono contenere le raccomandazioni esistenti in materia.

Il ricorso a società senza scopo di lucro non costituisce garanzia di un servizio più sicuro. Anche l'affidabilità di queste società deve essere scrupolosamente valutata, utilizzando l'esperienza pratica e le informazioni disponibili nell'area operativa di riferimento.

Il Security Advisor è a disposizione per consigliare il personale sulla scelta più adatta.

Le norme aeroportuali e doganali relative alla sicurezza dei voli e al trasporto delle merci devono essere scrupolosamente rispettate.²⁰

Selezione dei siti e dei locali

La scelta del sito per l'apertura di un ufficio o di una base operativa ha conseguenze importanti per la sicurezza complessiva di una missione. Il personale incaricato della selezione deve quindi seguire le **istruzioni contenute nella SOP CESVI Facility Management**.

Il Security Advisor è a disposizione del personale per effettuare la scelta migliore tenendo conto di tutti i fattori: il contesto politico e sociale, lo scopo ufficiale della sede, le relazioni con le parti interessate, la disponibilità di servizi, l'accessibilità, i fattori di protezione intrinseci, il budget disponibile, ecc.

²⁰ Per esempio: non trasportare pacchi senza conoscerne il contenuto, preparare personalmente il proprio bagaglio, ecc.

Fotografia e rapporti con i media

Il personale di CESVI dovrebbe considerare la fotografia come un'**operazione da pianificare in anticipo** come qualsiasi altra attività e/o rapporto con i media, poiché è un complemento indispensabile a qualsiasi resoconto del lavoro con i colleghi, i donatori e il pubblico in generale.

Questa attività deve essere svolta nel rispetto della normativa sulla **tutela della privacy**. Per illustrare le corrette modalità di svolgimento CESVI ha predisposto **particolari documenti sull'utilizzo delle immagini**.²¹

Il personale non deve mai dimenticare che nelle comunicazioni con i media entrano in gioco importanti fattori di sicurezza, per cui è necessario seguire attentamente i contenuti dei documenti sopra citati.

CESVI incoraggia le visite di giornalisti e fotografi ai suoi progetti, considerandole importanti nell'ambito della sua più ampia responsabilità di **rendicontazione** nei confronti dei donatori e del pubblico in generale. Tuttavia, durante la fase di pianificazione delle missioni, i responsabili devono consultarsi con il Regional/Area Manager e con il Security Advisor, se necessario, per verificare che la sicurezza del personale e del programma CESVI non ne risenta.

Il personale di CESVI che supervisiona le missioni fotogiornalistiche in loco deve cercare di evitare situazioni che ostacolino il personale e i progetti di CESVI.

Inoltre, il personale non deve mettere a rischio se stesso o i progetti fotografando o filmando luoghi in cui tali attività sono generalmente vietate, come aeroporti, edifici pubblici, riunioni politiche, religiose e sociali, installazioni militari, ecc.

Coordinamento

Gestione congiunta della sicurezza

Il coordinamento con altre organizzazioni è essenziale per il corretto apprendimento, la gestione e lo sviluppo delle misure di sicurezza. CESVI incoraggia il proprio personale a partecipare a queste reti.

CESVI favorisce anche le attività di reti o servizi promossi autonomamente dalle ONG.

CESVI utilizza generalmente diverse reti, per la gestione quotidiana della sicurezza o per l'apprendimento e lo scambio di informazioni generali. Tutti i piani di sicurezza nazionali devono indicare chiaramente le reti di sicurezza locali esistenti e il tipo di relazioni che intrattengono con CESVI. Devono inoltre prevedere misure di emergenza nel caso in cui la rete cessi di funzionare per qualsiasi motivo.

GISF

CESVI Security Advisor è membro del **GISF**, il **Global Interagency Security Forum**, composto dal personale di sicurezza delle agenzie umanitarie europee che operano a livello internazionale. Lo scopo del GISF è quello di facilitare la collaborazione e lo scambio di informazioni.

²¹ Si vedano i seguenti documenti di CESVI: Policy di tutela dei minori (2024), Linee guida sulla protezione dei dati (2024).

informazioni, sviluppare ricerche e analisi interne, fornire suggerimenti accurati ed empirici, ecc. Il GISF è un meccanismo di collaborazione e non un fornitore di servizi.

INSO

CESVI raccomanda, nei Paesi in cui è presente, la registrazione e l'utilizzo dei servizi di **INSO (International NGO Security Organization)**, un'organizzazione britannica senza scopo di lucro, che opera per la sicurezza delle agenzie umanitarie in situazioni ad alto rischio. L'INSO fornisce una serie di servizi gratuiti alle agenzie che si registrano, tra cui il networking con altre organizzazioni, il monitoraggio e l'informazione in tempo reale su incidenti e crisi in corso, rapporti analitici periodici, dati statistici sulla sicurezza e la loro mappatura, aiuto nella gestione delle crisi, formazione e orientamento del personale.

L'utilizzo dei servizi INSO richiede una registrazione gratuita in loco, che può essere facilitata dalla sede centrale di CESVI.

Alliance 2015

Dal 2000, i membri della **rete Alliance2015** hanno acquisito una notevole esperienza lavorando insieme in situazioni di emergenza e di sviluppo. Questo ha creato forti legami tra i partner non solo a livello di programma, ma anche nello sviluppo di nuovi metodi di lavoro (monitoraggio reciproco, formazione, supporto, advocacy, ecc.) che hanno portato all'utilizzo di approcci e strumenti operativi condivisi e armonizzati.

All'interno di Alliance2015 esiste un **gruppo di lavoro composto dai responsabili della sicurezza** a livello globale, che collabora allo scambio di informazioni e si riunisce periodicamente con agende condivise.

Sebbene ad oggi non esista un protocollo comune ufficiale per la gestione della sicurezza, CESVI raccomanda, laddove possibile nel Paese, la collaborazione con altri partner del consorzio per aumentare la quantità e la qualità delle informazioni sulla sicurezza e il loro scambio, la consapevolezza dei rischi esistenti e la circolazione e promozione delle buone pratiche e delle lezioni apprese.

Unità di crisi del Ministero degli Affari Esteri italiano

L'**Unità di Crisi** del Ministero degli Affari Esteri è l'organo ministeriale che assiste i cittadini italiani all'estero. In diversi Paesi esistono servizi analoghi che si occupano di crisi o emergenze all'estero. Questi servizi sono principalmente interconnessi tra loro e sono in contatto con quelli delle Ambasciate.

Una delle attività dell'Unità di Crisi è il monitoraggio della presenza degli italiani nel mondo attraverso il sito web: www.dovesiamonelmundo.it.

Tutto il personale espatriato di CESVI è registrato sul sito dal team HR. L'Unità di crisi è responsabile della gestione del sito.

In situazioni di emergenza, CESVI può contattare l'Unità di crisi per proteggere il proprio personale.

Tuttavia, CESVI valuta in modo indipendente le indicazioni fornite dall'Unità di Crisi del Ministero degli Affari Esteri italiano, dalla rete delle Ambasciate e da altri servizi analoghi di altri Paesi, e non è tenuto a farle seguire al proprio personale.

Il Security Advisor, che tiene informato il Direttore generale, è la persona incaricata di interagire con l'Unità di crisi. In situazioni gravi, il Team di gestione delle crisi di CESVI può interagire con l'Unità di crisi.

Agenzie delle Nazioni Unite

CESVI collabora con le **agenzie delle Nazioni Unite** nell'attuazione di programmi di aiuto umanitario o di cooperazione allo sviluppo.

La valutazione della posizione delle Nazioni Unite e delle misure di sicurezza di fronte a rischi o minacce persistenti in un determinato contesto è di grande importanza. Tale valutazione viene effettuata a livello nazionale dal Country security manager, dall' Head of mission e, a livello globale, dal Security Advisor. CESVI è consapevole che l'interazione con tali agenzie è spesso di fondamentale importanza per una proficua e continua analisi dei rischi dei contesti in cui opera. CESVI sottolinea che, non avendo tali Agenzie alcuna responsabilità specifica nei confronti del personale delle ONG (talvolta anche per i progetti cofinanziati con risorse ONU), è responsabilità primaria di CESVI garantire la sicurezza del proprio personale.

Relazioni civili e militari

Sempre più spesso le ONG si trovano a operare in **situazioni in cui le forze armate sono attive**, legittimate o meno, da uno Stato riconosciuto dalle Nazioni Unite. Vi sono poi situazioni in cui le forze armate sono coinvolte in operazioni di mantenimento o rafforzamento della pace, con o senza un mandato esplicito delle Nazioni Unite.

La questione delle relazioni civili e militari nel contesto degli aiuti umanitari è quindi complessa e in continua evoluzione.

Attraverso le reti a cui aderisce (ad esempio VOICE.²²), CESVI segue con attenzione e partecipazione lo sviluppo di riflessioni sulle relazioni civili militari e sul coordinamento, il dialogo e la convivenza tra forze militari e ONG.

CESVI ha appreso come il **coordinamento civile-militare** sia utile per il successo delle azioni di aiuto umanitario in diverse occasioni. Ciò si è verificato, ad esempio, quando le forze militari avevano un mandato chiaro, quando c'era un'ampia accettazione dello stesso da parte della popolazione del Paese in cui si svolgevano le operazioni, quando le forze militari rispettavano il ruolo e lo "spazio umanitario" in cui operavano le ONG.

In queste occasioni, può essere utile il supporto logistico (trasporti, voli aerei, comunicazioni) che le forze militari sono in grado di offrire.

Ogni situazione è diversa dalle altre; pertanto, prima di avviare qualsiasi forma di collaborazione, è necessario prestare attenzione ai rischi che il personale di CESVI, i destinatari del programma e le persone che vi partecipano possono correre.

²² www.ngovoice.org.

altre ONG e al rischio di compromettere la neutralità, l'indipendenza e l'autonomia di CESVI. posizione imparziale.

L'analisi tiene conto dell'atteggiamento della "comunità umanitaria" (ONG, Agenzie delle Nazioni Unite, Croce Rossa Internazionale) nell'area.

Per questo motivo, CESVI invita il suo personale ad assumere un **atteggiamento cooperativo e positivo** nei confronti delle possibili sinergie che potrebbero nascere in ogni particolare contesto con le forze armate legittimate dalle Nazioni Unite, ma a non sottovalutarne le conseguenze.

Fatta salva l'autonomia del personale sul campo nel valutare le situazioni, il Security Advisor deve essere consultato per avere indicazioni in anticipo su qualsiasi situazione che richieda lo svolgimento di relazioni non occasionali con le forze militari.

Tutti questi accordi formali richiedono l'autorizzazione del Direttore generale.

Rapporti con le autorità locali

Il personale, i visitatori e chiunque si rechi in locali o attività sotto la responsabilità di CESVI deve rispettare le leggi locali in materia di commercio, esportazione e importazione di merci e denaro, accesso a determinate aree, edifici, visti, permessi di accesso, residenza e transito, leggi sul lavoro, codici della strada ecc. Qualsiasi situazione poco chiara deve essere discussa con il Line Manager.²³

Oltre ad essere un principio generale della missione di CESVI, il **rispetto delle leggi e degli usi locali** è di grande importanza per sviluppare il consenso alle operazioni della ONG, nonché per il successo dei programmi e, in ultima analisi, anche per la sicurezza del personale, di qualsiasi nazionalità.

CESVI verificherà quindi come **ottenere la regolare registrazione della ONG nel Paese in cui opererà**, se possibile, prima dell'inizio della missione e la completerà il prima possibile.

Tutto il personale sarà dotato di **visti e permessi di lavoro** in conformità con gli obiettivi delle missioni affidate.²⁴

Le leggi sul lavoro e sugli affari in vigore nei vari Paesi, applicabili anche alle ONG, saranno oggetto di un'analisi approfondita da parte del personale incaricato della Gestione Paese, in modo che le operazioni della ONG siano gestite in conformità alle leggi locali.

Oltre ai requisiti formali che possono esistere, le informazioni relative alle attività della ONG saranno comunicate alle autorità locali competenti attraverso relazioni, incontri, ecc. in modo informale e saranno finalizzate a ottenere l'approvazione delle operazioni svolte, al fine di rafforzare il sostegno delle autorità per i programmi futuri. Tutto ciò ha importanti conseguenze in termini di sicurezza e protezione del personale e dei programmi della ONG. In caso di problemi con le autorità locali, il Crisis Management Team deve essere informato.

²³ Questo elenco è solo un esempio e non è assolutamente esaustivo.

²⁴ Il Regional/Area Manager è responsabile delle registrazioni, dei visti, dei permessi di lavoro, ecc.

Visitatori, familiari, accompagnatori

Tutti i visitatori dei progetti CESVI sono invitati a prendere visione delle misure di sicurezza contenute nella presente Policy, anche quando non esiste un contratto formale tra il visitatore e CESVI.

Tutti gli uffici all'estero hanno un avviso all'ingresso che ricorda che "La corretta osservanza delle regole che CESVI ha adottato per la sicurezza del suo personale e dei suoi visitatori è una garanzia di protezione per tutti". Chiunque necessiti di ulteriori informazioni sulla Policy sicurezza di CESVI in vigore presso questa base deve fare riferimento al [Nome del Country Security Manager o dell'Head of mission], Data e firma dell'Head of mission".

I membri del personale di CESVI che accompagnano o organizzano la missione dei visitatori sono tenuti a informarli delle misure di sicurezza esistenti. I membri del personale di CESVI sono tenuti a informare i propri familiari o conoscenti in visita del contenuto della Policy sicurezza di CESVI e degli altri documenti correlati. Gli accompagnatori devono inoltre prevenire, affrontare e risolvere qualsiasi forma di comportamento dei visitatori che possa in qualche modo mettere in pericolo CESVI e il suo personale.

FINANZIAMENTO DELLE MISURE DI SICUREZZA

L'attuazione di un quadro efficace di gestione del rischio ai fini della sicurezza richiede un impegno adeguato di **risorse umane e finanziarie**, che devono essere destinate all'assegnazione di posizioni di sicurezza, all'acquisto di materiali e attrezzature e alla formazione del personale.

La maggior parte dei donatori riconosce che garantire la sicurezza del personale è essenziale per il corretto completamento di un programma e di conseguenza è sempre più disposta a finanziare i relativi costi.

È responsabilità del Regional/Area Manager assicurarsi che le proposte di progetto includano sempre i **costi relativi alla gestione della sicurezza**, in base al livello di rischio nei Paesi interessati. CESVI contribuisce con le proprie risorse ai costi relativi alla formazione e alla posizione del Security Advisor.

Il Security Advisor supporta il personale nell'accesso alle risorse dei donatori per coprire i costi della sicurezza ed è a disposizione del personale durante la preparazione della sezione del bilancio del progetto relativa ai costi della sicurezza.

BENCHMARK

CESVI cerca di offrire al proprio personale il miglior sistema possibile di misure e procedure di gestione della sicurezza. Nel corso degli anni si è assistito a uno **sviluppo molto positivo delle pratiche di gestione della sicurezza** tra le ONG. Questo processo è ancora in corso e la positiva competizione tra le ONG continua ad aumentare la qualità dei servizi offerti.

CESVI ritiene che questo processo contribuisca alla **credibilità** e all'**affidabilità** complessiva delle ONG.

CESVI intende contribuire a questo processo condividendo le proprie procedure e misure di sicurezza con le ONG disposte a fare altrettanto, con l'obiettivo di lavorare insieme per aumentare la qualità del lavoro svolto dalle ONG.

MONITORAGGIO E REVISIONE DELLA POLICY

Il monitoraggio dell'effettiva diffusione della presente Policy è affidato al Security Advisor, che si impegna a verificarne il grado di diffusione.

Il Security Advisor può utilizzare metodi di consultazione partecipativa per verificare come vengono applicate tutte o alcune parti della Policy. I risultati saranno riportati nel Rapporto annuale sulla sicurezza.

ALLEGATI

Parte speciale del Modello Organizzativo relativa alla salute e alla sicurezza sul luogo di lavoro

Modulo per la segnalazione di incidenti

La raccolta dei dati relativi agli incidenti è un'attività importante per individuare eventuali lacune e per monitorare l'applicazione delle procedure di sicurezza sul campo. Questa procedura è inoltre obbligatoria in caso di incidenti che causano traumi al personale.

Di seguito viene proposto un modello di modulo per la raccolta dei dati.

Il modulo di segnalazione dell'incidente deve essere compilato con i seguenti casi:

- Devono essere inclusi tutti gli eventi, anche le semplici minacce non seguite o gli eventi che hanno causato danni a oggetti, persone, beni o risorse. Devono essere incluse anche le azioni violente e le malattie gravi. Devono quindi essere inclusi anche i furti tentati e non realizzati.
- Non si deve fare distinzione tra eventi che coinvolgono il personale locale o quello espatriato: tutto il personale è ugualmente importante per CESVI.
- Anche eventi che coinvolgono altre ONG, soprattutto quelle che hanno un rapporto formalizzato con CESVI: partner, ONG di Alliance2015, ecc.
- Sospensioni della normale prosecuzione dei programmi causate da incidenti o dalla minaccia di incidenti.
- Incidenti occorsi ai principali attori (ad es. ONU, Cooperative Nazionali di Sviluppo, ecc.) nella stessa area in cui opera il personale CESVI.

Nota bene: la legge italiana impone la denuncia di qualsiasi infortunio occorso al personale con contratto registrato in Italia. Deve essere comunicato alla sede INAIL entro 48 ore dall'evento che ha causato la sospensione del lavoro per almeno tre giorni. La mancata denuncia costituisce una grave infrazione contrattuale.

Gli incidenti vengono segnalati al Security Advisor e alle Risorse umane della sede centrale.²⁵

²⁵ Per i contratti registrati in Italia, viene informato anche l'Amministratore del personale.

RAPPORTO SULL'INCIDENTE	
Nome e posizione della persona che effettua il rapporto	
Data del rapporto	
Paese	
Tipo di incidente	
Data e ora dell'incidente	
Luogo esatto dell'incidente	
Personale e altre persone coinvolte	
Descrizione dell'incidente	
Reazione esterna (comunità locale, autorità, leader religiosi), stampa...)	
Misure adottate	
Totale stimato costo dell'incidente	
Giorni persi: N°	
Azioni future suggerite	
Note e commenti	
Allegati	

Allarme preventivo

Il Security Advisor, o in alternativa l'Head of Programmes Department, è la persona incaricata di ricevere eventuali avvisi tempestivi. I loro contatti vengono normalmente forniti a tutto il personale prima dell'inizio di una missione e sono inclusi negli elenchi di contatti a disposizione del personale sul campo.

Gli altri canali devono essere attivati localmente:

- il Country Security Manager, se esistente
- l' Head of mission
- Ambasciate interessate
- il Regional/Area Manager
- il sistema di evacuazione medica, quando necessario
- l'Unità di Crisi del Ministero degli Affari Esteri italiano (in situazioni di imminente pericolo di vita)
- ogni altro contatto definito come tale in caso di emergenza (es. Autorità locali, Polizia locale, ecc.) incluso nel Piano di Protezione della Salute e di Emergenza e nel Piano di Sicurezza.

Contenuti del piano di sicurezza nazionale

Un Piano di sicurezza nazionale deve sempre contenere un approfondimento dei seguenti aspetti, ma non deve mai superare le venti pagine (esclusi gli allegati):

- Titolo: le aree in questione
- Profilo della ONG nel Paese: obiettivi, progetti, controparti, visibilità, personale e responsabilità, ecc.
- Cosa fare prima di arrivare nel Paese.
- Cosa fare appena arrivati nel Paese.
- Localizzazione e descrizione delle aree operative: uffici, alloggi del personale, strade, ecc.
- Regole generali di comportamento: abbigliamento, leggi e usanze locali, equipaggiamento personale, precauzioni sanitarie, luoghi da visitare o da evitare, coprifuoco, comportamento in situazioni critiche (ad es. intimidazioni, aggressioni, ecc.), visitatori, ecc.
- Norme relative alla guida di veicoli a motore e ai trasporti (voli, blocchi stradali, viaggi notturni, ecc. e relative agli incidenti).
- Qualsiasi informazione generale sulla presenza di mine o bombe inesplose.
- Regole di gestione delle comunicazioni
- Regole per le visite sul campo.
- Coordinamento con altri attori sul campo.
- Mezzi e metodi di comunicazione: radio, sistemi di allarme rapido, ecc.
- Problemi di salute, emergenza ed evacuazione medica.

Questioni amministrative:

- Gestione quotidiana della sicurezza: guardie, R&R, ecc.
- Note e raccomandazioni relative alle aree operative speciali.
- Piani di evacuazione per ogni base operativa.
- Cosa fare in caso di chiusura di una missione.
- Qualsiasi altra informazione utile.

Allegati:

- Descrizione del contesto nazionale e dei principali rischi esistenti;
- Elenco dei contatti (personale, ONG, enti pubblici, polizia, organizzazioni internazionali, ecc;)
- Elenco dei centri sanitari;
- Mappe
- Acronimi

Contenuti del rapporto annuale sulla sicurezza

Include quanto segue:

- Attività del Security Advisor(Raccomandazioni, Missioni, Valutazioni, Networking, ecc.);
- La gestione della sicurezza delle ONG: problemi che emergono;
- Semaforo di sicurezza;
- Incidenti e valutazione;
- Formazione;
- Bozza dei piani di sicurezza;
- Attività volte a preservare lo "spazio umanitario";
- Idee di lavoro future;
- Bilancio finale e previsioni.

APPENDICE

Appendice 1 - Gestione della sicurezza

Policy di CESVI

L'applicazione delle misure di sicurezza, in Italia e sul campo, segue le linee gestionali della struttura operativa di CESVI.

Nella sede centrale il Direttore generale è direttamente responsabile dell'applicazione delle misure di sicurezza. All'estero, l'applicazione delle misure di sicurezza segue la linea operativa che va dal Direttore Generale al Responsabile dei Programmi Internazionali, al Regional/Area Manager e, infine, all' Head of mission (HoM).

Nei Paesi a maggior rischio è **prevista la** figura specifica del Country Security Manager (o Officer) ²⁶. Il Security Advisor ricopre una posizione, rispetto alla struttura **operativa**, di formazione, incoraggiamento, orientamento e verifica.

Diversi modelli di gestione della sicurezza

1. **Modello della linea operativa (Mainstreaming):** La responsabilità della gestione della sicurezza segue quella della **linea operativa**, che comprende il personale amministrativo, delle risorse umane e della programmazione.

Vantaggi	Svantaggi
<ul style="list-style-type: none"> • Conoscenza e comprensione del programma; • Possibilità di includere e ottimizzare la sicurezza in tutte le attività di pianificazione (finanza, logistica, risorse umane); • Ideale per il consenso delle comunità (come strategia di mitigazione); • Più razionale nella definizione dei budget di sicurezza; • Minore rischio di conflitti interni a livello decisionale; 	<ul style="list-style-type: none"> • Richiede tempo (a seconda del contesto nazionale); • È più difficile trovare personale con una doppia formazione professionale; • Minore capacità di gestione delle crisi; • Richiede una cultura della sicurezza radicata nella ONG; • Facoltativo se la funzione deve essere ad personam o a Termini di Riferimento

2. **Il modello dello specialista della sicurezza (Pure Security Officer)**: Questo modello è generalmente utilizzato nei Paesi ad alto rischio o nelle aree di intervento; prevede uno o più specialisti della sicurezza assegnati alla sede centrale e agli uffici di coordinamento e sul campo della missione; la loro autorità è subordinata a quella dell'Head of mission.

Vantaggi	Svantaggi
<ul style="list-style-type: none"> • Competenza tecnica superiore; • Maggiore capacità di gestione delle crisi; • Più facile da inserire nell'organigramma; • Completamente dedicato alla sicurezza; • Contribuisce ad aumentare la cultura della sicurezza; 	<ul style="list-style-type: none"> • Costoso; • Difficoltà di assunzione; • Percezione della sicurezza come settore separato; • Più burocrazia; • Meno conoscenza e comprensione del programma del programma; • Tendenza a privilegiare la protezione/deterrenza piuttosto che il consenso; • Maggiore rischio di controversie decisionali interne (HoM);

²⁶ Il ruolo di Country Security Manager non è, di solito, compatibile con quello di Head of mission (se non per brevi periodi), al fine di tenere distinte le responsabilità di controllo, supporto, consulenza, formazione e rappresentanza in materia di sicurezza da altri compiti di gestione o rappresentanza.

3. **Modello del Security Advisor(misto):** la responsabilità della sicurezza è assegnata alla direzione operativa con il supporto di un consulente interno o esterno senza autorità manageriale diretta.

Vantaggi	Svantaggi
<ul style="list-style-type: none"> • Economico, facile e veloce da aggiungere a un'organizzazione preesistente; • Buona capacità tecnica; • Buona capacità di gestione delle crisi; • Completamente dedicato alla sicurezza; • Efficace per le ONG con scarsa cultura della sicurezza; • Contribuisce ad aumentare la cultura della sicurezza; 	<ul style="list-style-type: none"> • Nessuna operazione sul campo

Appendice 2 - Descrizione del lavoro (compiti di sicurezza)

JD del Security Advisor

Il Security Advisor di CESVI è responsabile della sicurezza del personale all'estero. Il **Security Advisor**:

- informa, supporta, dirige e trae conclusioni dal processo di analisi del rischio;
- sviluppa, promuove e monitora l'applicazione delle misure incluse nella Policy e nei documenti correlati (Piani di sicurezza nazionali, SOP, ecc.);
- consiglia qualsiasi altro funzionario (Presidente, H&S Manager/GM, Head of Programmes, Regional/Area Manager, Head of Mission, Country Security Manager, staff) su questioni riguardanti i rischi, la protezione e la sicurezza del personale all'estero;
- supervisiona e attua il piano di formazione sulla sicurezza e, ove possibile, promuove la formazione del personale ed è direttamente responsabile di quella del Country Security Manager;
- offre consulenza a tutti i membri del personale su questioni relative alla sicurezza;
- verifica che le misure di sicurezza corrispondano a quelle della presente Policy;
- suggerisce modifiche alla presente Policy e alle misure di sicurezza;
- aggiorna e analizza la banca dati sugli incidenti;
- redige il Rapporto annuale sulla sicurezza.

Il Security Advisor dispone di un budget annuale per le attività di cui sopra.

JD del Regional/Area Manager

Nello svolgimento delle sue mansioni il **Regional/Area Manager**:

- è responsabile dell'applicazione di tutte le misure di sicurezza (elaborate dal Security Manager del Paese specifico e riviste dal Security Advisor della sede centrale) per i Paesi a cui è assegnato;
- si assicura di volta in volta che le misure di sicurezza in quei Paesi (piano S&S, Country Traffic Light, rapporto mensile, rapporto sugli incidenti, ecc.) siano aggiornate sia per rispettare scadenze fisse sia in casi eccezionali in base al contesto del Paese;
- è responsabile della scelta del modello organizzativo per la gestione della sicurezza per i propri Paesi (Sicurezza pura, Mainstreaming, Mista)
- è responsabile della definizione dell'organizzazione del personale di sicurezza nel Paese, da cui dipenderanno le comunicazioni e le relazioni gerarchiche e funzionali tra il personale con ruoli di sicurezza in sede e sul campo;
- è responsabile della valutazione periodica delle competenze, dell'impegno e dei risultati raggiunti dal personale con ruoli di sicurezza;
- è responsabile di garantire l'assegnazione annuale dei fondi per la sicurezza;
- è responsabile di comunicare al Security Advisor del quartier generale qualsiasi modifica dell'organigramma del personale con ruoli di sicurezza;
- supporta il team di gestione della crisi nei seguenti compiti:
 - o fornire assistenza diretta agli uffici all'estero;
 - o assistere il CMT nei primi contatti con le autorità competenti;
 - o fornire informazioni contestuali;
 - o comunicare con il team di gestione degli incidenti locale.

JD dell'Head of mission

Il JD è lo stesso del Regional/Area Manager, ma viene svolto a livello di Paese in coordinamento con il Regional/Area Manager e il Security Advisor.

JD del Country security manager

La funzione CSM può essere assegnata come ruolo singolo a una persona dedicata, o come compito aggiuntivo a una persona con un'altra responsabilità principale, o distribuita tra varie persone con altre mansioni principali.

Nello svolgimento del suo ruolo il **Country Security Manager** è responsabile di:

i. Sicurezza generale

- ha la responsabilità della sicurezza del personale locale e internazionale, dei beni, delle risorse e dei documenti di CESVI nel Paese, attraverso l'applicazione delle istruzioni e il rispetto dei principi contenuti nella Policy sicurezza, nel Piano di sicurezza nazionale e negli altri documenti di riferimento relativi alla sicurezza;
- promuovere la conoscenza da parte del personale del Manuale di sicurezza di ECHO e dei documenti interni di CESVI relativi alla sicurezza (Policy sicurezza, procedure e strumenti) e quelli relativi all'analisi del contesto e dei rischi residui in termini di Due Diligence e circolari sulla sicurezza;
- promuovere l'applicazione e l'aggiornamento della normativa vigente, con particolare attenzione alla movimentazione del personale, alla protezione dei siti di lavoro, alle vie di comunicazione e di evacuazione, compresi tutti gli aspetti burocratici connessi (rilascio di visti, voli, ecc.);
- ha la responsabilità di rivedere la documentazione di sicurezza, adattandone i contenuti allo specifico contesto locale;
- garantisce la stesura di rapporti e l'elaborazione di informazioni su questioni di sicurezza indirizzate al Project Manager e all'Head of mission per la stesura dei conti dovuti a terzi (finanziatori, sede centrale, Contatto, enti governativi del Paese ospitante, ecc;)
- monitora le informazioni quotidiane e periodiche contenute nei bollettini di sicurezza e nei mass media, al fine di identificare i fatti principali e le tendenze emergenti per un'adeguata distribuzione e comunicazione ai destinatari appropriati
- rende ufficiali e archivia le decisioni e le modifiche fondamentali in materia di sicurezza;
- osserva, sulla base di un'analisi continua del contesto nel Paese/Area di intervento, l'esistenza di possibili minacce imminenti o di tendenze emergenti in materia di sicurezza, e fornisce consulenza e sostegno per mitigare le possibili conseguenze.

ii. Formazione

- forma il personale espatriato e nazionale sulle questioni di sicurezza e ne assicura l'aggiornamento periodico con incontri individuali o di gruppo;
- è responsabile di tenere un briefing introduttivo sulla sicurezza per il personale della sede centrale in missione, per i dipendenti e i collaboratori dei progetti, per i consulenti in missione di breve o lunga durata, per le famiglie del personale debitamente autorizzato ad accompagnare o visitare la missione, per i visitatori autorizzati, per i volontari sul campo, per gli stagisti e per ogni altra persona che abbia una partnership formalizzata e diretta con l'ONG;
- individua e facilita la formazione del personale, nei limiti delle risorse disponibili, attraverso la formazione esterna.

iii. Attività logistiche

- verifica e assicura che, per quanto riguarda la sicurezza, la logistica dei progetti in corso sia conforme alle normative vigenti nel Paese, alle regole stabilite dai finanziatori e alle procedure organizzative (Policy, Piano di sicurezza nazionale, ecc.);
- effettua missioni, nel Paese o nell'Area, per verificare che le attività di sicurezza previste siano messe in pratica, nonché quelle necessarie per il supporto di missioni esplorative o di emergenza;
- assicura un'organizzazione efficiente dell'ufficio e un'archiviazione ordinata (sia cartacea che informatica) della documentazione di sicurezza;
- garantisce che i mezzi di sicurezza, le attrezzature e gli apparati logistici per la sicurezza, in linea con gli obiettivi finali, siano inventariati e funzionanti;
- assicura il corretto utilizzo e la manutenzione di tutti gli apparati di sicurezza in dotazione e garantisce la formazione necessaria per un utilizzo sicuro e corretto da parte del personale.

iv. Identificazione di nuove proposte

- contribuisce a redigere, per gli aspetti di sua competenza, i paragrafi relativi alla sicurezza e all'analisi dei conflitti nelle nuove proposte di progetto;
- garantisce il necessario supporto in materia di sicurezza alle missioni per gli studi di fattibilità nel Paese e nell'area di sua competenza.

v. Amministrativo e legale

- collabora con l'amministratore per la corretta e tempestiva attribuzione delle spese di sicurezza di sua competenza;
- assicura una particolare cura nella conservazione e nel trattamento delle informazioni riservate di cui viene in possesso per il ruolo che ricopre;
- garantisce la gestione amministrativa della linea di bilancio per la sicurezza di sua competenza e di eventuali problemi connessi, tenendo informato il Head of mission;
- collabora al reclutamento del personale locale, seguendo i criteri del regolamento interno, verificando
- solo per gli aspetti di sicurezza - l'idoneità morale e professionale a svolgere il lavoro e la definizione dei compiti specifici;
- per il personale con contratto di diritto italiano (expat) opera in coordinamento con il Head of mission e l'amministratore delle Risorse Umane del Quartier Generale, per quanto riguarda le comunicazioni nei loro confronti, compresa la notifica tempestiva delle informazioni per la circolare sulla sicurezza.
- garantisce la raccolta e la conservazione di tutta la documentazione necessaria per le informazioni al personale, a fini legali e di revisione.

vi. Attività di visibilità e comunicazione

- per motivi di sicurezza e nel rispetto del profilo di sicurezza vigente nel Paese, supervisiona l'uso del logo e del materiale di visibilità di CESVI, seguendo le linee guida sulla visibilità e la comunicazione;
- partecipa, per gli aspetti di sicurezza, all'organizzazione delle missioni di comunicazione e raccolta fondi delle unità interne e di quelle di giornalisti, fotografi e addetti stampa di altre organizzazioni.

vii. Piano di gestione delle crisi

Completa il team di gestione degli incidenti a livello nazionale nel rispetto delle linee guida specifiche; le responsabilità dell' Head of mission riguarderanno in particolare:

- gestione delle crisi a livello locale;
- gestione della sicurezza di tutto il personale;
- gestione delle evacuazioni e dei trasferimenti necessari;
- coordinamento di comunicazione canali di comunicazione con le famiglie dei dipendenti nazionali e internazionali;
- mantenimento di contatti regolari con la CMT
- aggiornare la CMT sulla situazione sul campo, con informazioni accurate;
- creazione e aggiornamento di un registro di tutti gli aspetti della crisi;
- ruolo di coordinamento con:
 - *autorità nazionali in merito alla risoluzione dell'incidente*
 - *altre organizzazioni del Paese, come richiesto;*
 - *gli uffici locali e le ambasciate dei principali donatori*
- gestione, in accordo con il CMT, delle comunicazioni con i mass media garantendo la continuità operativa in caso di crisi prolungate.

JD del Field Security Focal Point

- è responsabile dell'applicazione delle istruzioni della Policy sicurezza, del Piano di Sicurezza Nazionale e degli altri documenti relativi alla sicurezza, limitatamente a un ufficio o a una specifica area di competenza (area di competenza);
- garantisce il coordinamento del personale dell'ufficio o della base assegnata per quanto riguarda il rispetto delle norme di sicurezza;
- è responsabile dell'inserimento, della formazione ecc. del personale che lavora nell'ufficio o nella base a lui assegnati;

- nell'ambito della propria area di competenza, è responsabile della raccolta e della trasmissione tempestiva di informazioni, da fonti primarie e secondarie, al fine di mantenere aggiornato l'intero contesto di sicurezza;
- è responsabile di informare tempestivamente il Security Manager e il Head of mission (o altra figura indicata nell'albero delle comunicazioni) in caso di pericoli imminenti che potrebbero richiedere la sospensione temporanea delle attività sul campo.