MANAGEMENT OF SECURITY IN CIVIL SOCIETY ORGANISATIONS

PRACTICAL GUIDE FOR LOCAL ORGANISATIONS

Alianza por la Solidaridad
Member of actionaid

EU Aid Volunteers
We Care, We Act

EU AID VOLUNTEERS INITIATIVE

“Empowerment of local capabilities for humanitarian aid in Latin America and the Caribbean - CB4AID”

Project No. 2017-3658/001-001

Financed by the European Union Education, Audiovisual and Culture Executive Agency (EACEA)

Coordination:
Silvia de Benito Ruiz de Azúa
Alianza por la Solidaridad

Text:
Rosa Baños Polglase
Laura Cartanya
Consultoría Mehit

Collaborators:
Blanca Mingo de Miguel
Alianza por la Solidaridad

Carmen Vicente Sánchez
Alianza por la Solidaridad

Version:
Alianza por la Solidaridad

Design and layout:
Miguel Alonso Oleaga / alonsoleaga.com

www.alianzaporlasolidaridad.org

MANAGEMENT OF SECURITY IN CIVIL SOCIETY ORGANISATIONS

PRACTICAL GUIDE FOR LOCAL ORGANISATIONS

Index

INTRODUCTION

The EU AID Volunteers programme is a response to a European need to raise awareness among citizens of such important values as participation and peace-building. This programme provides specific possibilities for citizens to demonstrate their solidarity, by taking part in projects covering risk management, protection of vulnerable people, training, etc. EU Aid Volunteers allows volunteers and organisations from various countries (sending organisations) to provide technical, logistical and training support for humanitarian action projects, contributing towards a strengthening of local capacities and the resilience of the populations affected by various types of humanitarian disasters and crises. At the same time the programme enables local organisations (hosting organisations) to be bolstered by specialist personnel at no additional cost.

Security is an essential component for the EU, and various measures have been established in order to guarantee it. Firstly, volunteers are never deployed in countries with emergency response operations in progress or which are in open conflict. Furthermore, the obligatory training programmes for volunteers organised by EU Aid Volunteers (online and on-site) ensure that the volunteers are well prepared before leaving for the field. Finally, both the hosting and sending organisations must have demonstrated, during their certification process, a satisfactory capacity in terms of security.

This document is a response to the latter requirement. It is a guide document with a complementary audiovisual tutorial which will allow the organisation to design its own security guide or plan, taking into account its specific context and priorities. The document includes some theoretical concepts, but in a limited way, as its purpose is imminently practical.

For that reason, this guide is structured in four main modules.

Module 1 will accompany the organisation in carrying out its security analysis, taking into account its main factors and components (socio-economic, gender, natural disasters, health risks, risks to human rights, road security and others). Module 1 will guide the organisation in carrying out its risk evaluation and the definition of its basic security strategies.

Then **module 2** will help to design the management procedures for the security, such as organigrams, chains of command, incident reporting, the establishment of security levels, briefing and debriefing procedures, etc.

Module 3 will show the organisation how to develop security protocols (SOPs - standard operational procedures) for dealing with some key security problems, such as attacks, robbery, health problems, cultural awareness, protection of installations, volunteer programmes and others.

Finally, **module 4** covers extreme situations in terms of security, such as hibernation, evacuation and medical evacuation.

We wish you all the luck in your route towards establishing a quality security guide or plan!

ABBREVIATIONS

UNHCR	United Nations High Commissioner for Refugees
IDB	Inter-American Development Bank
CDERA	Caribbean Disaster Emergency Response Agency
CEPREDENAC	Coordination Centre for the Prevention of Natural Disasters in Central America
HR	Human Rights
DG ECHO	Directorate-General for European Civil Protection and Humanitarian Aid Operations
E-MINE	UN Mine Action (online site)
EACEA	Education, Audiovisual and Culture Executive Agency
EHRDs	Environmental human rights defenders
MAG America	Mines Advisory Group America
UN	United Nations
N1M	Not one More
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
OAS	Organisation of American States
WHO	World Health Organisation
UN Women	United Nations Entity for Gender Equality and the Empowerment of Women
PFA	Psychological First Aid
PEP	Post-exposure Prophylaxis
UNDP	United Nations Development Programme
PTSD	Post Traumatic Stress Disorder
HR	Human Resources
SOPs	Standard Operational Procedures
EU	European Union
UN	United Nations
UNDSS	United Nations Department of Safety&Security
UNEP	United Nations Environment Programme
UNFPA	United Nations Population Fund
UNIDIR	United Nations Institute for Disarmament Research
UNISDR	United Nations Office for Disaster Risk Reduction
UNMAS	United Nations Mine Action Service
UNODA	United Nations Office for Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime

MODULE I

MÓDULE I

ANALYSIS

In order to design a security guide with the necessary protocols, it is essential to firstly draw up a descriptive and diagnostic analysis of the situation with regard to the levels of risk, evaluating the probability and impact so as to be able to define adequate security strategies.

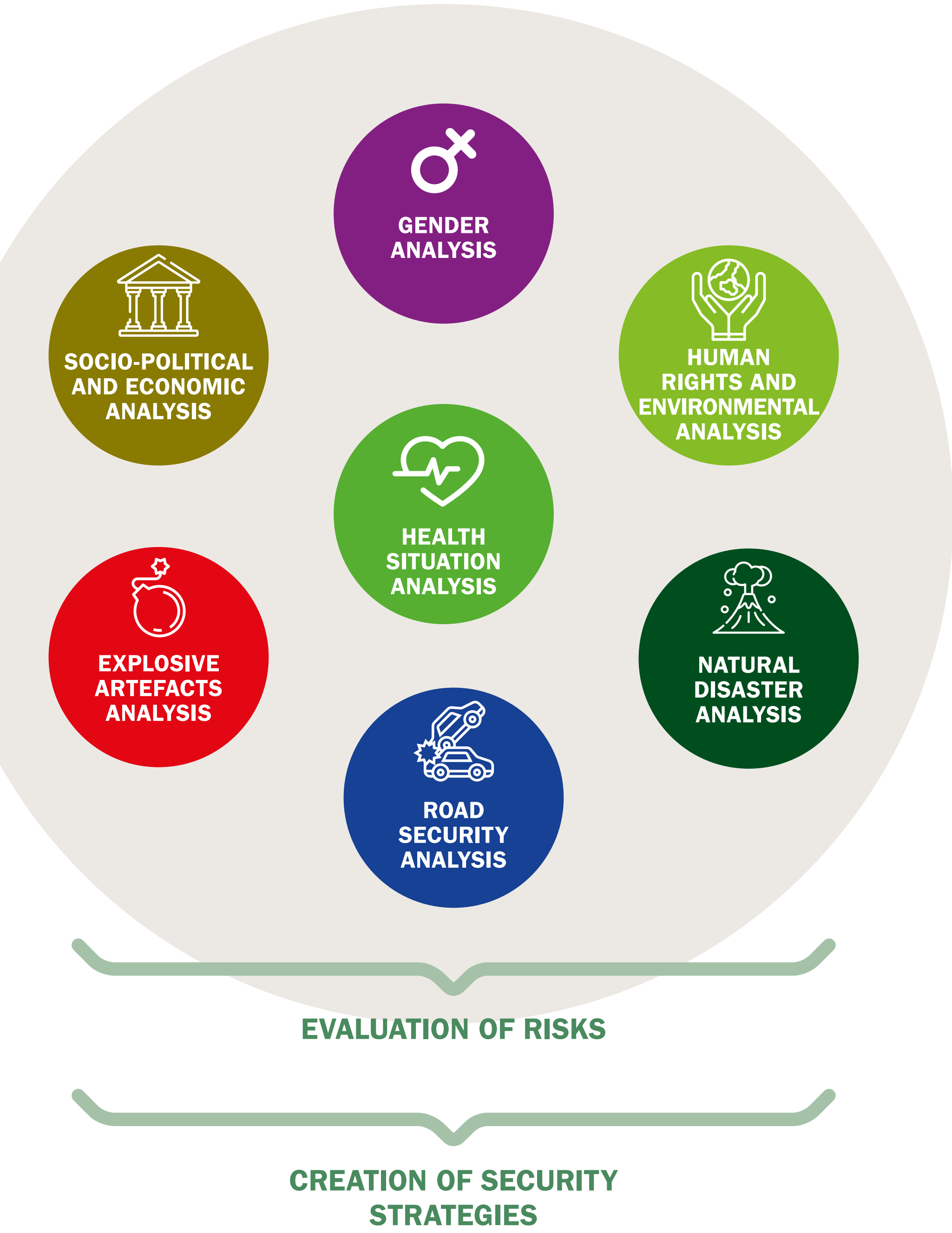
This analysis must be specific to each situation, each country, or even each zone.

This chapter will indicate the main aspects to be analysed, and how to go about it.

However, take into account that there may be other aspects of interest to be analyses in each specific context, apart from those indicated in this module.

In this module you will be guided in order to carry out an analysis of the situation regarding your organisation in terms of security, together with an evaluation of risks and the determination of security strategies.

Remember that the analysis must always be specific for each situation, and you may thus require other components apart from those suggested in this guide.



1 · A DEFINITION OF CONCEPTS

This section will allow you to understand the key concepts which are used to prepare a security plan. In your guide you can adopt the concepts as defined here, or adapt them using your own examples more in line with your country/zone.

REMEMBER

The initial analysis of the context, the diagnosis of threats, exposure to risk, and vulnerability to various events are the basis for defining adequate mitigating measures linked to the implementation of the programmes and the achievement of their objectives.

SECURITY IS THE DOUBLE COMFORT OF "BEING AND FEELING SAFE"

WE SHALL BEGIN WITH SOME
KEY CONCEPTS

RISK:

→ The way in which a threat impacts the personnel, assets, reputation or scheduling of the organisation. Examples of risk: flooding of the organisation, the collapse of buildings, infection from cholera or other illnesses, etc.

THREAT:

→ Any event which places at risk the security of personnel within the organisation or assets, within the context in which it is operating. Types of threat: violence, conflict, natural disasters, terrorism, health problems, political interference, crime and corruption, etc. Examples of threat: criminality, events of physical origin (floods, earthquakes, contaminated water); institutional neglect (lack of rules, organigrams, training, etc.).

VULNERABILITY:

→ It expresses both the exposure to risk and the extent of the response capability faced with such events. Examples of vulnerability; untrained personnel, location of office close to clayey land, deficient conditions in buildings, lack of emergency plans, etc.

IMPACT:

→ Seriousness of the consequences of a security incident.

SECURITY:

→ Security is an intrinsic human need. It is an emotional situation which allows us or prevents us from carrying out our private, social and working activities, within an atmosphere of normality and calm. Security is the combination of protection and resistance. It is the certainty of knowing that something has occurred, the possibility of immediately finding out what is happening, and the comfort of knowing that, in the event of an intrusion, immediate action can be activated. It implies the protection of the organisation's personnel, volunteers or resources against actions of violence, robbery or damage.

Security has two main components:

Individual responsibility: this is understood as all those actions performed by persons individually in order to assume their obligations and ensure minimum security standards.

Institutional Responsibility: these are measures, actions and procedures to manage risk for individuals/organisations faced with threats (Security Plan/ Guide).

1 · B.1

SOCIO-ECONOMIC AND POLITICAL ANALYSIS

This section will help you to be able to respond to the following type of question:

How does poverty in the country affect the climate of security?

What type of criminal behaviour is there in the project's intervention zones?

Are there tensions between different ethnic or religious groups?

Do armed groups control part of the territory? Do the pre and post election periods involve instability or conflict?

Are there differing cultural norms with respect to population or territory?

What is the degree of a polynomial?

What players are key in the socio-political panorama?

SOCIETY AND ECONOMY

- This describes the social structure of your country: demographic pyramid, population density, geographical distribution, economic resources and access to those resources. Difficulties or tensions regarding access to resources.
- It describes the phenomenon of poverty in your country, and the way it is distributed geographically and socially.
- It describes the ethnic and/or religious groups and their interactions.
- It described the cultural patterns and rules for the population and its differences in relation to social, ethnic or religious groups (including languages, etc.).

POLITICAL SYSTEM

- It describes the system of political organisation in the country, focusing on the full or partial control of the territory by the State, the full, partial or non-existent guarantee of civil liberties and social rights (including control over and access to information).
- It describes the main players on a political level, focusing on possible para-military groups, armed groups, terrorists, militias, etc.
- It describes possible political instability and/or chronic, acute or recurrent conflicts.

CRIMINALITY AND VIOLENCE

- It describes the most frequent types of criminality in the country by geographic area if relevant, and whether there are populations that are the priority target of criminality (potential targets).
- It describes the main players associated with criminality, including maras, gangs, etc.
- It analyses the level of violence associated with criminality.
- It describes the problem of the illegal drug trade in the country.

REMEMBER

The socio-political and economic characteristics vary from country to country, and inside countries.

The specific questions to take into account must always arise from the context.

APPROXIMATE LENGTH:
Two pages.

WHERE DO I OBTAIN THIS INFORMATION?

- Participative diagnosis and analysis within your working team.
- Government databases on a national/local level on poverty, society and criminality.
- Country reports and analyses by international bodies such as UNDP, OAS, IDB and others.
- Reports on criminality: OAS Inter-American Observatory on Security, Insight Crime, UNODC.

ANNEXES

Ensure you include as annexes:

- A map of the country.
- A detailed map of the intervention zones.
- A map of criminality zones.
- A map of conflict zones by country and zone, and national/local criteria.

1 · B.2 GENDER AND VULNERABLE POPULATIONS

This section will help you to be able to respond to the following type of question:

What risks are specifically faced by women?

What other groups are affected specifically?

REMEMBER

In general, the most serious violations of human rights suffered by women are caused by men in their environment. However, these abuses, despite their seriousness, tend to be under-represented in official statistics. The private space has scarcely been considered in analyses and under security policies.

APPROXIMATE LENGTH:
One page.

- It analyses violence against women: restrictions on mobility, obstacles to participation in social life, their dependence on protection from other people (generally men) and more subjective factors such as a lack of self-confidence and trust in others, isolation, the transmission of a sense of security to girls, and feelings of guilt and responsibility regarding incidents.
- It analyses risks, and the frequency and zones of attacks and sexual violence.
- It describes the discriminatory effects deriving from the assignation of roles and opportunities.
- It describes the needs, experiences and abuses suffered by women, due to the fact of being women, or which affect them disproportionately.
- It analyses the leadership and political participation by women in the working zones; including training and education. Inequality in access to health care and/or economic resources.
- It analyses other vulnerable groups, such as LGBTI, sex workers, etc.; risks they face (violence or others).

WHERE DO I OBTAIN THIS INFORMATION?

- Participative diagnosis and analysis within your working team, particularly with women's groups.
- Government databases on a national/local level on poverty, society and criminality.
- Country reports and analyses by international bodies such as UN Women, UNFPA, UNDP, OAS, IDB and others.

1 · B.3

HUMAN AND NATURAL ENVIRONMENTAL RIGHTS

What are the risks associated with the defence of human and environmental rights?

This section will allow you to be able to identify the existence or probability of suffering violent incidents due to the nature of the actions your organisation is carrying out.

This module is applicable above all in your organisation works with defenders of human and/or environmental rights.

REMEMBER

On average, in the world every week three defenders of human or environmental rights die violently. In 2018, 321 activists were murdered, according to Front line Defenders.

The persecution and attacks on activists are frequently aggravated by gender, in addition to the cascading effect on their families and communities, causing trepidation that may place at risk the continuation of actions in defence of rights.

APPROXIMATE LENGTH:
One page.

- It documents the attacks suffered (extortion, stigmatisation, disappearance, murder, etc.) by personnel and communities with a focus of gender when relevant, and included their consequences in families and communities.
- It analyses the structural causes of the attacks, with the aim of putting forward long-term measures which cover the causes, and proposing strategies to anticipate crises in time and be able to prevent, reduce or mitigate them.
- It identifies spaces for coordination between movements and organisations working on human and environmental rights, in order to be able to articulate their demands and unite their voices, It locates the ancestral bodies working it the zone.
- It evaluates the way to access any judicial or quasi-judicial mechanisms which exist.
- It identifies the zones of impact for the phenomena and their recurrence. It dentifies for each event how many times it has occurred, and if they are widespread phenomena or one-off events.

WHERE DO I OBTAIN THIS INFORMATION?

- Participative diagnosis and analysis within your working team and/or communities.
- Government databases on a national/local level on complaints.
- Data and analysis on your country by specialist international bodies, such as Universal Right Group, UNEP, EHRDs Universal Rights Group, Global Witness, N1M, UNHCR, Front line Defenders.

ANNEXES

Ensure you include as annexes:

- A detailed map including risks with respect to human and environmental rights in the intervention zones.

1 · B.4

HEALTH

This section will help you to be able to respond to the following type of question:

Which vaccines must the volunteer personnel have in order to enter the country?

What precautions must be taken with food and drinks?

Which diseases in the country present the potential for an epidemic?

What are the tasks to be carried out by personnel that imply a risk to their health?

How can the risk be prevented or minimised?

REMEMBER

Health is a state of complete physical, mental and social well-being, and not only the absence of illness. It is a basic human right, and its implementation requires the combined action between other sectors, in addition to health, such as social and economic sectors. Prevention is essential. All personnel must be informed regarding their own responsibilities in security matters, and particularly on the risks to health, in the knowledge that the organisation has analyses the risks and has prepared itself to minimise them and provide a response.

APPROXIMATE LENGTH:
Two pages.

RISKS TO HEALTH

- It analyses the type of risk to health that personnel may be exposed to (attacks, diseases, violence, accidents, hygiene, environmental, chemical, etc.). Do not forget the risks to mental health and in particular the possibility of stress that may be faced by personnel (PTSD). It defines the responsibility and frequency of check-ups and the updating of the diagnosis.
- It identifies work/occupational risks associated with the specific tasks carried out by personnel, and identifies ways to minimise them (protective equipment and others).
- It particularly analyses the risk of epidemics in the zones where the organisation works, and health during journeys (see section 1.b.6).

PREVENTION

- It contains information on the vaccinations and medicines necessary for the prevention of diseases which exist in the country (on a national or local level) (do not forget malaria, yellow fever, rabies, dengue, zika virus, and others, depending on the country).
- It defines the training necessary for personnel (first aid, psychological first aid,self-protection and resilience, etc.). If applicable, it identifies resource personnel/committees (health and safety committees).

WHERE DO I OBTAIN THIS INFORMATION?

- Participative diagnosis and analysis within your working team.
- Analysis of the health situation by the WHO office on a national and regional level.

ANNEXES

Ensure you include as annexes:

- A vaccination card covering those recommended/obligatory in the country.
- A geographical map of diseases with a potential for epidemics.
- A list of hospitals and health centres with the capacity to respond to emergencies to visit if necessary (contacts, location) (do not forget an analysis of the surgical capacities, and also include on the list quality trusted dentists).

1 · B.5

NATURAL DISASTERS

This section will help you to be able to indicate the existence or possibility of natural phenomena which imply a risk to the security of individuals, and the characteristics of the zones susceptible to being the site for a catastrophic event.

The analysis of natural risks serves as a basis for the elaboration of containment plans faced with disasters.

REMEMBER

The number of natural disasters which occur throughout the world has increased.

Some of these natural phenomena are predictable and there are models for forecasting. However, others cannot be predicted, and their affects are increasingly more devastating.

It is of prime importance to analyse how they may affect your country nationally and locally.

APPROXIMATE LENGTH:
One page.

- It identifies the natural phenomena that have affected the country at some moment, such as unstable land, flooding, rivers bursting their banks, volcanoes, earthquakes, hurricanes, tsunami, seaquakes, or any other phenomenon that could affect your area.
- It analyses the intensity in relation to the previously described phenomena, together with the impact zones and the probability of future occurrence, including factors contributing to the dynamic of the phenomena, such as the over-exploitation of land, the probability of fires, inappropriate construction, etc.
- Draw up a map of the risk zones: a delimitation which is as precise as possible for natural phenomena, including all the affected or potentially affected zones.
- Evaluation of vulnerability. The affect on human life, housing, goods, infrastructures, agricultural land. The capability to respond and recover, factors which impact vulnerability: social (political, institutional, organisational, educational, ideological, cultural), economical, physical, environmental in the impact zones.

WHERE DO I OBTAIN THIS INFORMATION?

- Participative diagnosis and analysis within your working team.
- Government databases on a national/local level on natural phenomena.
- Data and analysis by specialist international bodies such as ECHO, CDERA, CEPREDENAC, UNISDR, UNDP and OCHA.

ANNEXES

Ensure you include as annexes:

- Detailed map of risks in intervention zones.

1 · B.6

This section will help you to identify the risks associated with journeys made by road or by air:

What routes are the safest in order to access the projects in the field?

What should I take into account before setting out on a journey?

Is it better for the vehicle to be identified or not?

The analysis will serve to identify safe routes and possible evacuation routes.

REMEMBER

A large number of incidents, such as robberies, attacks, kidnappings and accidents are suffered by humanitarian personnel during journeys (or are related to them) by road, tracks or paths, whether from the airport to the office or accommodation, from the office to the residence, or during journeys to the projects in the field and/or to meetings.

Among expatriate workers and collaborators, road accidents are one of the main factors in morbidity/ mortality.

APPROXIMATE LENGTH:
One page.

ROAD SECURITY

- It identifies the type and frequency of incidents (robberies, attacks, kidnapping, road accidents, etc.) which have affected the various roads/minor roads and rural tracks normally used in personal and work journeys.
- In the case of new working zones it identifies the risks associated with access routes, and seeks alternative ways in the case of problems or incidents.
- It locates safe points on the routes used where you can stop to rest, refuel and/or eat, and safety points and maintenance garages which have protected or guarded parking areas.
- It analyses the risks and advantages of driving in vehicles marked with the badge of the organisation when travelling, and states what policy the organisation will follow.
- It identifies the most suitable type of vehicle to drive in the work zones and/ or the city.
- It contains a map of the risk zones: delimitation of events on the map as precisely as possible.
- It identifies a list of taxi companies and vehicle renting adapted to your needs, which can be entrusted to make journeys that cannot be made by the organisation's own vehicles. Check that they meet security requirements; check the vehicles.
- For journeys by air, it locates companies that are certified by the International Air Transport Association (IATA).
- If applicable in your country/zone, identify water transport companies that implement safe water transport practice, and have basic security equipment on the boats.

WHERE DO I OBTAIN THIS INFORMATION?

- Participative diagnosis and analysis within your working team.
- Government databases on a national/local level on road and security incidents.
- Ratings in security matters given to air carriers.
- Coordination meetings with other bodies/organisations.

ANNEXES

Ensure you include as annexes:

- A detailed map of roads/tracks/paths/ways with events identified, including secondary roads and ways.

1 · B.7

UNEXPLODED EXPLOSIVE DEVICES, MINES, WAR REMNANTS

This section will serve to be able to indicate the existence or the possibility of coming across unexploded explosive devices, mines or war remnants in your working area.

The risk analysis serves as the basis for establishing adequate security protocols for prevention and response.

REMEMBER

Only suitably trained specialists must seek and handle land mines, unexploded devices or war remnants, due to the high degree of danger.

APPROXIMATE LENGTH:

One page.

- It identifies whether there are officially or unofficially identified zones (boundary tape, wooden poles, painted rocks, etc.) indicating the possible presence of unexploded devices or mines.
- It locates indications of conflict or military activity (damaged civil or military vehicles).
- It analyses the behaviour of the population in the zone, and identifies the zones which are not used by the local population. Empty streets or those with little traffic could be good indicators.
- It identifies whether there are abandoned houses or villages.
- It locates bodies and/or organisations that work with this matter, and could report on zones, any risky behaviour to avoid, community strategies for avoiding them, and the response in the event of explosion, etc.
- It has a map of the risk zones: delimitation of risk zones on the map as precisely as possible.

IMPORTANT: DO NOT TAKE RISKS AND DO NOT APPROACH POTENTIAL RISK ZONES

WHERE DO I OBTAIN THIS INFORMATION?

- Participative diagnosis and analysis within your working team and population.
- Government databases on a national/local level on devices. Information from inhabitants of suspect zones.
- Data and analysis by specialist international bodies such as UNMAS, MAG AMERICA, E-MINE, EU, UNODA, UNIDIR.

ANNEXES

Ensure you include as annexes:

- Detailed map of risks in intervention zones.
- Contacts in organisations which are experts in the matter.

1 · C

EVALUATION OF RISKS

Once the context has been analysed, and the threats and vulnerabilities have been identified, it is necessary to evaluate the risk. Remember that:

T*V=R

This chapter will help you to classify risks, from the most serious to those that have a lower impact, taking into consideration factors such as the personnel affected, the degree of probability and the impact.

It is neither possible nor effective to establish security measures to counter each of the possible threats.

It is important to balance the need to work in a zone with the need to reduce exposure to risks.

THREAT * VULNERABILITY = RISK

A · IDENTIFICATION OF THREATS AND VULNERABILITIES

- It analyses the main threats and dangers diagnosed during the design and implementation of its projects in the country, and in the regions where it works.
- It analyses the threats to security that affect other countries/zones close by, and which may impact on your own.
- It identifies the level of vulnerability when facing the threats, and who could be affected to a greater extent.

It classifies the probability that an event occurs as:

- **Very probable:** daily.
- **Probable:** once per week.
- **Moderately probable:** every year.
- **Improbable:** every two or three years.
- **Highly improbable:** every four years or more.

It classifies the impact of the event as:

- **Critical:** death or serious injury, the cancellation of activities or large losses.
- **Serious:** serious injuries, serious disturbance to the organisation or significant loss of goods.
- **Moderate:** injuries that do not threaten life or create high stress levels, delays to activities or some losses.
- **Minor:** some minor injuries, limited delays or possible minor damage or losses.
- **Insignificant:** no injuries, minor disturbance to activities.

B · CLASSIFICATION OF RISKS

The combination of probability of occurrence with the impact caused in the event of it taking place. It classifies the risk matrix in accordance with the following scale:

- **Very high risk:** immediate action. If the risk can be mitigated by contingency plans, then it must be ensured that these work.
- **High risk:** priority action - elaboration and verification of contingency plans.
- **Medium risk:** greater awareness-raising and specific procedures.
- **Low risk:** greater awareness and management via routine procedures.
- **Very low risk:** management via routine procedures.

REMEMBER

To reduce or mitigate risk is one of the main aims of the security plan.

Each organisation must define the threshold of "acceptable risk".

This will depend on the capacity of the organisation to manage risk and its ability to work in environments with moderate or high risk.

APPROXIMATE LENGTH:
Two pages.

C. RISK MITIGATION MEASURES

With the threats identified and classified, the implementation of mitigation measures in order to reduce exposure to risk is recommended.

Preventive measures to reduce the probability that an event occurs (with the aim that the incident does not occur).

→ Example: carrying out vehicle maintenance.

Reactive measures to reduce the impact when an incident occurs (with the aim of reducing negative effects, assuming there were any).

→ Example: ensure use of the safety belt.

Take into account that if the probability is high and only reactive measures are implemented, the effect of the actions will be limited.

The mitigation measures will be covered specifically in module III of this guide: the elaboration of protocols to mitigate threats (SOPs).

D. RISK MATRIX

It includes the following data on:

→ **Risk classification table:**

It specifies the Impact and Probability of events, and is colour-coded according to the level of risk.

Take into account that it is the organisation that defines the level of risk based on its thresholds.

→ **Risk matrix:**

Type of Threat; Location; Players implicated in the risk Indicators; Vulnerability; Probability; Impact;the measures to take for each threat identified on the risk matrix.

ANNEXES

Ensure you include as annexes:

→ The risk matrix **(see example on the following page)** and risk classification table.

RISK CLASSIFICATION

		IMPACT				
		INSIGNIFICANT	**MINOR**	**MODERATE**	**SERIOUS**	**CRITICAL**
PROBABILITY	**Very probable**	**Theft without violence**				**Earthquake**
	Probable				**Traffic accident**	
	Moderately probable				**Attack on the field office**	
	Improbable					**Volcanic eruption**
	Highly improbable					**Kidnap**

RISK MATRIX

THREAT	LOCATION	THREATENED PLAYERS or AGENTS	WHO IS AT RISK? VULNERABILITIES	IMPACT	INDICATORS
It identifies all threats and develops a table for each of them	**It specifies where the threat is located as precisely as possible**	**Who or what may pose the threat**	**What type of personnel is at greatest risk** **Characteristics of the identified personnel**	**Loss of life, loss of assets, risk to reputation, etc.**	**How to measure the threat**
Flooding	North zone of the country	Climate change	Staff/population	Temporary or permanent physical injury Death, damage to office or goods Temporary suspension of activities	Declaration of state of emergency by authorities
Attack on the road	West area of the swamps	Armed groups/ delinquents or maras	Staff/population	Temporary or permanent physical injury Death Kidnap Sexual violence	Reported incidents

1 · D

CREATION OF SECURITY STRATEGIES

With the context and risks analysed, what are the next steps? What strategies can be followed to reduce risks?

This chapter describes the main strategies adopted prior to the deployment of the security plans, and are more of an "organisational culture" nature than of protocol.

ACCEPTANCE

A relationship of trust based on the acceptance of your presence, your working procedures, and the purpose of your activities.

→ **In order to build acceptance, you will need:**

- Mapping of the players.
- The identification of allies and the establishment of constructive relations with them.
- The involvement of all members of the organisations, consultations with the community and the adaptation of programmes to real needs.
- The dissemination of coherence regarding its identity, work and working plans (internal and external).
- To analyse the local situation and understand aspects that may impede its acceptance.

Take into account that acceptance takes time; is the most difficult element to achieve, and at the same time the easiest to lose.

→ Example: if it is a religious organisation, clearly communicate how this affects or does not affect its work.

→ Example: explain from where its funds come and what are its planned priorities (mission and vision).

PROTECTION

The aim of protection is to reduce the risk (not the threat) through a reduction in the vulnerability of the organisation.

→ Protection measures are established in relation to an analysis of physical threats and vulnerability factors for the organisation.

→ Measures will be adopted to reduce the vulnerabilities that have been identified.

→ All measures must be applied to all personnel equally, and be clearly described.

Take into account that, if the adopted measures are disproportionate with respect to the risks, this may have a negative impact on the image of the organisation.

→ Example: protective measures at installations (fences, alarms, guards, etc.) Try to avoid the creation of a bunker.

→ Example: protective measures to guarantee security during journeys (radios, telephones, policies of regular contact, etc.).

REMEMBER

It is important that your organisation reflects on the security strategies it normally uses (whether consciously or not), and understands their advantages and drawbacks, and how to operationalise them.

Do not forget that the responsibility for the security of the organisation falls on the putting into practice of its protocols and strategies, both at an organisational and individual level.

APPROXIMATE LENGTH:
Two pages.

DETERRENCE

Measures which directly affect whoever is making the threat, and serve to counteract threats and armed actions with legal, political or economic sanctions.

→ **The coordination of players between your organisation and other organisations and sources of support is essential for security. Take into account:**

- The limits before which it may threaten the withdrawal of its services, or withdraw them in an effective way.
- The need for armed personnel as security guards during journeys.

Take into account that these measures may place your acceptance at risk.

→ Example: the use of armed personnel during journeys usually has consequences for working with the communities.

→ Example: if a withdrawal or suspension of activities is possible, anticipate the consequences for the beneficiary populations and for personnel, and mitigate damage (the payment of salaries, remote monitoring, etc.).

COORDINATION

In countries where there are forums and coordination groups for security matters.

→ **The coordination of players between your organisation and other organisations and sources of support is essential for security. Take into account:**

- Existing forums on security at which you want your organisation to be present, and who will be responsible for representing your organisation.
- The identification of additional sources of reliable information (online forums, sms/email alerts).
- The location of local contacts with UNDSS and other national and international organisations.
- An evaluation of the reliability and quality of information from those sources.
- Include contacts in an annex in your guide: civil authorities, specialist organisations, etc.

MODULE II

MODULE II

SECURITY PLANNING AND MANAGEMENT

Organisations must include their analysis and conclusions regarding security (module 1) within their institutional policies and organisation.

Thus, now that you have analysed the security situation in your country/ zone in relation to your organisation, in this module you will see what is required for the management of security in your organisation on an institutional level:

How is security implemented and managed on an institutional level?

What general organisational structures and procedures are required or need to be adopted by the organisation?

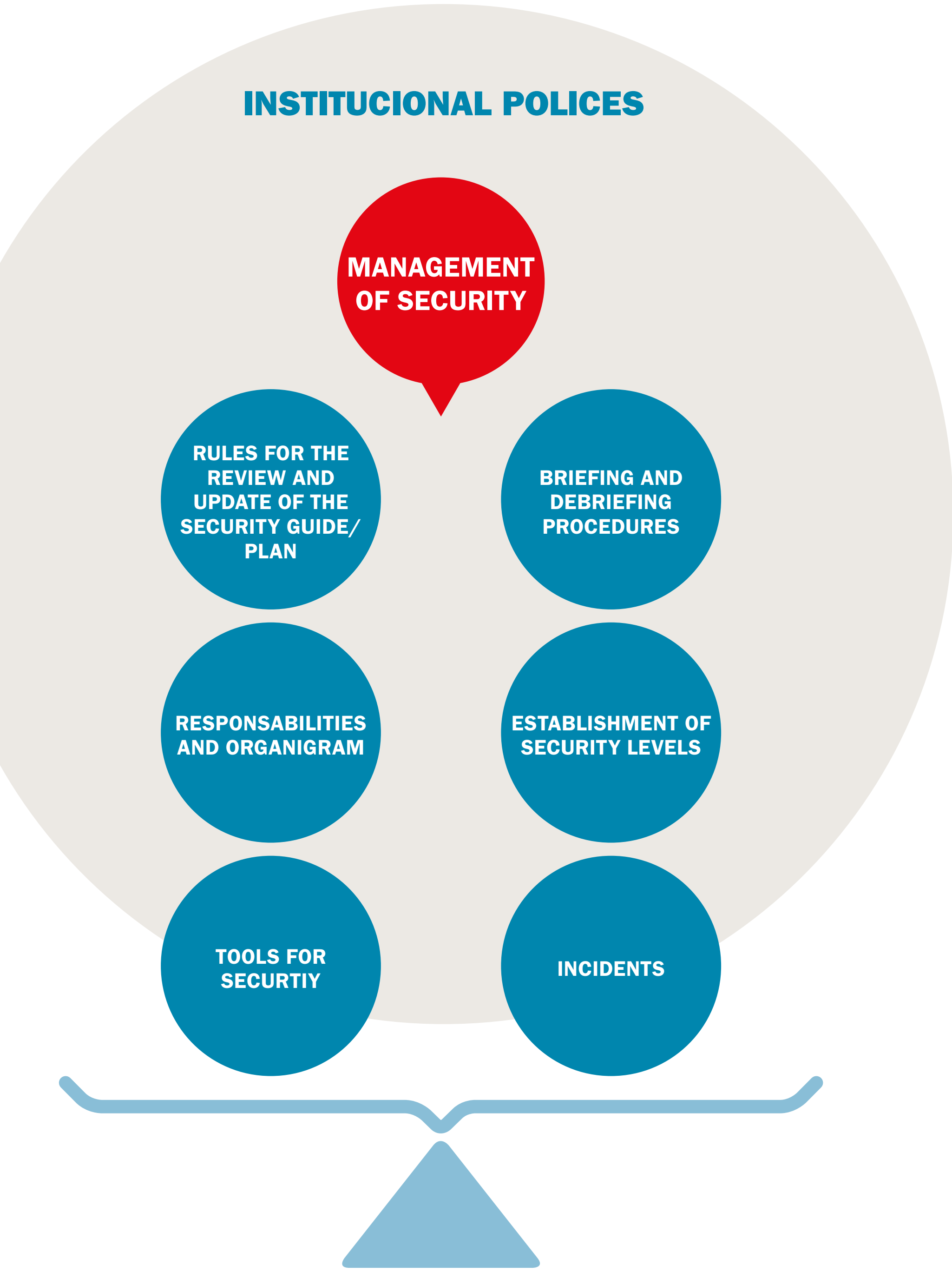
REMEMBER

Good organisational management of security is an essential element for the successful functioning of all the operational procedures you design.

The definition of this management is thus a prior step to the definition of operational plans against specific identified threats and risks.

In this module you will be guided in order to be able to plan and manage security in your organisation.

Remember that the management of security must be adapted to your context, and you must thus adapt your organigram and information flow based on the size and characteristics of your organisation.



2 · A

RESPONSIBILITY AND ORGANIGRAM

Each worker has responsibility for their own security, that of colleagues, and to an extent that of the organisation.

An organigram describes who is who in an organisation in relation to their responsibilities and tasks established in a chain of command which is more or less vertical, depending on each organisation.

Normally a security organigram follows the general organigram for the organisation and respects positions of command (although they may not coincide exactly), but specific positions for security are probably necessary.

LEVELS OF RESPONSIBILITY

When creating your guide, take into account:

INDIVIDUAL RESPONSIBILITY

- All personnel in the organisation must be responsible for their own security and apply common sense. They must support the security of their colleagues and counterparts, and report to their coordinators regarding any unsuitable or unsafe behaviour or incidents which have occurred. There must be a code of conduct and the security organigram (see the following point) must set clear reporting lines.

MANAGERIAL RESPONSIBILITY

- Each coordinator has responsibility for the security of the personnel they manage.

ORGANISATIONAL RESPONSIBILITY

- The organisation must establish policies, procedures and standards that ensure the highest level of security possible. Any existing and potential risks to personnel and programmes must be monitored, and measures must be proposed to mitigate those risks. It is essential to anticipate the necessary training, security evaluations and support for personnel.

ORGANIGRAM

Your organisation needs an organigram for the management of security. This organigram must include:

- The levels people have in the management of security: a good definition of responsibilities, tasks and the chain of command, processes and spaces for decision-making and approval.
- A definition of committees or working groups if applicable (security committee).
- It is important that the chain of command is clear to all members of the organisation. A description of the measures to share and, if there are changes, to update it.

It is recommended that the chain of command considers gender equality, ethnic and social groups, etc.

- Communication is essential when dealing with security. It is important that in this section your organisation defines a "call tree" for dealing with incidents (who calls/contacts who), and that instructions are expected and codes and messages will be used if necessary.
- A list must be created with all the telephone numbers that personnel use, and it must establish what to do if someone does not answer, and how often to check and update the lists.

Do not leave anyone off this call tree. Pay particular attention to national and international volunteers.

REMEMBER

A poor or unclear security organigram may generate a lack of clarity regarding where the responsibilities rest when faced with critical incidents, which could lead to difficulties with the response and have consequences of varying degrees of seriousness.

APPROXIMATE LENGTH:
Two pages.

Take into account that international personnel in the organisation (volunteers or others), on arrival in the country, are usually obliged to register at the embassies or consulates of their respective countries, and must also follow the security policies established by those institutions.

2 · B RULES FOR THE REVIEW AND UPDATE OF THE SECURITY GUIDE/PLAN

Why is the security guide important for all personnel?

Who is responsible for preparing and updating the plan and informing personnel?

When was the document written?

The updating of the security Policy will be carried out periodically in accordance with the needs of the context.

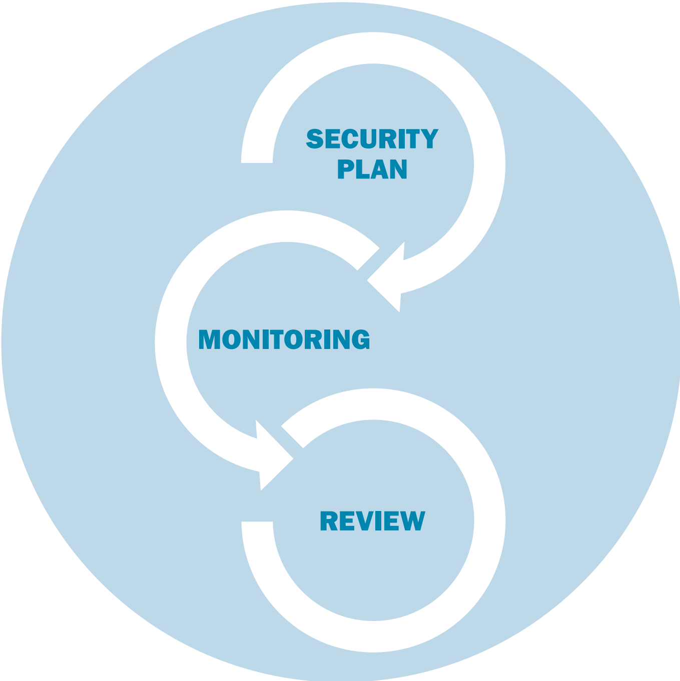
The updating of the security Policy will be carried out periodically in accordance with the needs of the context and through a participative process including local partners and personnel.

REMEMBER

Security plans must be practical and available to all personnel.

It is critical that the plans are reviewed continuously, reflecting any change to the security situation, which will help prevent and/or mitigate security incidents.

APPROXIMATE LENGTH:
One page.



MONITORING

The management of security requires the constant monitoring and analysis of both security incidents and the adoption of the analysis carried out in the previous module (see module 1), taking into account that contexts change and tend to evolve, even if this evolution is sometimes imperceptible. As a consequence, under this point your guide must foresee:

- How to draw up an incident map.
- How and who will analyse the incidents occurring and their degree of impact.
- The establishment of key criteria/incidents for the update of the security plan.

REVIEW

The updating of the security plans and distribution among personnel must be a frequent routine in order to ensure that the plans remain relevant and effective. This means:

- The periodical review of security rules in order to verify that they meet minimum standards and are effective (as a minimum every three months, and whenever necessary).
- The establishing of mechanisms for carrying out detailed research, taking into account the decisions and actions that were taken with respect to a serious incident. Anticipating the carrying out of reviews of the security procedures
- Anticipating a review of the security plan for the organisation if necessary, based on information received from the field.
- Anticipating the review of its security plan in the event of serious incidents affecting other organisations.
- The establishment of a system to keep all members informed.

2 · C

BRIEFING AND DEBRIEFING PROCEDURES

How are the security plans socialised? What are the key moments for the sharing/recording of information and instructions?

The arrival of volunteers, their sending to the field? Who are responsible for carrying it out?

Security plans must be simple, easy to use, and provide information in a format that personnel can use in their daily work.

The rules must be distributed and put into practice as soon as possible.

REMEMBER

It must be ensured that all personnel can access the policy and procedures quickly, and that they must be able to be implemented reliably, and that everyone understands their role, their responsibilities, and those of others.

APPROXIMATE LENGTH:
One page.

BRIEFING

- The establishment of meetings (briefing) to share information regarding security in working zones/places, together with procedures and responsibilities in accordance with the type of personnel, according to need and in accordance with key moments (such as the incorporation of the organisation, land journeys, etc.).
- The provision of a paper copy of the security guide to each person in the organisation, and written assurance of reception, reading and compliance. The creation of a specific paper format to sign for acceptance.
- Ensuring that all members of the organisation, including volunteers, are aware of and understand to organisation's code of conduct, and are aware of their responsibilities on an individual level.
- The provision of specific instructions on incident management mechanisms, including critical incidents.
- The establishment of mechanisms so that personnel are regularly updated on security risks, trips and health, together with evacuation procedures for the country or region.
- The establishment of meetings prior to deployment in areas of high risk, and the establishment of the need to carry our prior security training (in which cases and who will be responsible for this).
- Ensuring the availability of the appropriate first aid teams in key locations (office, cars, etc.).
- A definition of regular rest periods for personnel in high risk or stressful situations
- For international personnel, a check that they are registered with their embassies, and follow the trip advice established by their countries of origin.

DEBRIEFING

- It designs safe spaces and specific procedures in which the members of the organisation can provide information on the security situation following each journey and/or security incidents which have occurred.
- It establishes the necessary protocols and procedures which ensure that, in the case of an incident having taken place, personnel receive adequate medical and psychological attention.

2 · D

ESTABLISHMENT OF SECURITY LEVELS

The general security situation changes and moves through different levels.

Each level will require actions and limitations.

All workers must be aware of the current level or phase in which they are operating.

The person responsible for security will decide which events in the environment indicate a change in the security situation, and thus a change of level.

REMEMBER

The security levels or phases are practical, above all for comparing one location or country with another. However, this system does not always reflect small changes which could have a large impact and require a greater degree of warning.

APPROXIMATE LENGTH:
One page.

SECURITY LEVELS

It establishes indicators which define its levels of security.

→ Example: delinquency, kidnap, disturbances in the street, the assassination of leaders, robbery of NGOs, etc.

It defines levels according to established indicators.

→ Example: level zero (normal situation) to level four (deteriorated situation).

It indicates organisational responses (mitigating and response measures) for each level.

→ Example: on level two movements in the field will be monitored every three hours via radio or telephone checks.

It establishes individual actions to be carried out by personnel in the organisation.

→ Example: on level two journeys will not be made alone after 8 in the evening in specific zones (or in any zone).

Take into account that the security levels do not have to be uniform throughout your country. Establish zones and map the various security levels (refer to the prior analysis –module 1–)

→ Example: the zone where the office is located may be in a safe zone for which the security level is zero, while the zone where activities are carried out may be close to a militarised zone with a high degree of tension, and a security level of three.

Ensure you include in this chapter your security level matrix (see example below).

LEVEL	Indicators	Organizational response	Individual action
0	Levels of delinquency are normal. Unrestricted movement of personnel at all times. Programme activities continue as normal.	Communication with leaders/ authorities regarding activities. Brifing/debrifing on security matters. SOPs for journeys and trips by personnel, communications, access to facilities, etc.	Monitoring of security situation and recording of incidents.
1	Social disruption and/or high levels of localised delinquency. Restrictions on movement of personnel in specific places. Programme activites continue as normal.	Notification of all personnel regarding new security situation. Ensure all journeys be personnel to affected zones are monitored. Check security measures and procedures.	All personnel must avoid travelling alone to areas of conflict.
2	Social disruption and/or high levels of delinquency throughout the country. Assassinations of leaders/ prominent politicians. Activities suspended at some times	Notify all personnel regarding new security situation. Ensure all field trips are authorised and follow communication protocols. Check and update evacuation relocation plans. Prepare provisions.	Ensure that residences/offices have adequate provisions (water, food, first aid kits, etc.) and working communication equipment.
3	A lot of civil disturbance and general violence. Armed incidents and confrontation between specific groups or terrorist activities. Restrictions on movement of personnel. Some activities suspended. Threats to NGOs and civil society organisations. Relocation of personnel.	Relocate/evacuate non-essential personnel (and dependents) and ban visitors. Ensure that personnel receive updated information on the security situation (daily). Journeys must be duly authorised by those responsible for security.	Personnel should return to base and/or designated safe area and await instructions. Personnel must have a bag with essential articles ready for the event of possible immediate evacuation (limit on number of kilos to be transported.
4	Military action or armed conflict near the offices and/or residences. Restrictions on the movement of all personnel. All activities suspended. Evacuation of personnel. Offices closed.	Suspend all programme activities and close the office. Begin evacuation/relocation plan. International personnel must be ready for immediate evacuation. National personnel returned to their places of origin or safe place	Ningún movimiento excepto para la evacuación y/o reubicación.

2 · E

TOOLS IN THE MANAGEMENT OF SECURITY: COMMUNICATION

What mechanisms are useful for security?

What communication systems can we use?

What is their reliability?

Communication systems are crucial for the success of the response, as they ensure a good flow of information. Without them, managing security could become impossible.

Frequently, during an emergency or crisis, the first things to be cut are communication systems, and it is thus essential to foresee this and have alternative lines of communication and backup systems.

REMEMBER

Reliable communication systems are essential for the management of security, and must be replaced in the event of loss or damage. That must be taken into account when drawing up budgets for the organisation.

Furthermore, take into account that the use of communication systems may be seen as suspicious by local authorities and military groups.

APPROXIMATE LENGTH:
One page.

MOBILE TELEPHONES

- The use of mobile telephones is very common, although reception in some countries is limited to main cities and municipalities. In the majority of disaster situations the telephone networks are among the first systems to be disrupted. Check whether all the telephone companies offer the same reception in the country, and if necessary use more than one company for signal reception. Define your organisational policies regarding telephone costs.

SATELLITE SYSTEMS

- They provide effective, portable communication links in remote places, although they depend on the direct visibility of satellites, and thus communication must take place in open spaces. Satellite communication is very costly, particularly for data transfer. In some areas at the request of the government a satellite signal is not available for reasons of security.

COMMUNICATION BY RADIO

- The most used radio communication systems on the ground are those of very high frequency (VHF), ultra high frequency (UHF) and high frequency (HF). The VHF/UHF systems are very cheap and are used for communication over a short distance. The communication depends on the height of the aerial and the topography of the land. HF is used for long distances, is usually more expensive, and requires advanced technical knowledge in order to install the system correctly.
  - Radio communication is never confidential; take into account that messages transmitted using this system may be misinterpreted by other people, and that may possibly put your security at risk. Establish protocols for radio calls, which messages can be given and how.

The choice of a communication system should take into account various aspects. Among these are:

- **What is the security strategy in your organisation?**
  If your organisation has a low profile, the fitting of radios and high frequency aerials to vehicles may lead to your organisation being perceived in a different way, placing your security at risk.
- **Operational requirements:** types of programmes, number of personnel, areas covered by the project, etc.
- **Surrounding terrain** (mountainous, flat or urban).
- **Exchange** (voice, data, or both).
- **The need for an autonomous system or one integrated with other associations.**
- **Local regulations and customs.**
- **Licensing system.**
- **The funds the organisation has available.**

ANNEXES

Ensure you include as annexes:

- Protocols of use and maintenance for communication systems (radio, telephone, etc.)
- Communication protocols for radio, telephone, scrambled codes, etc.

2 · F INCIDENTS

Is what to do in the event of an incident related to security clearly established?

Do the personnel in the organisation know who to contact, and when and how to do it?

Knowledge and analysis of security incidents which occur in the workplace is essential for the protection of your personnel.

The records of incidents must summarise and map the key information which affects personnel.

This is essential for monitoring patterns and trends, and enables a deeper analysis of the security situation.

Define what type of incidents are considered as such in your organisation and ensure that the team understand what is or what could be an incident, what is not an incident, the need to define them and the responsibility to report them. If in doubt about whether or not something is an incident, always recommend that your personnel consider it as such and report it.

Your guide will have to take into account that an incident is:

- Any event that affects the physical or emotional welfare of personnel and/or causes damage to the organisation's property and/or affects the activities within its programmes.
- An event that affects the security of another organisation, individual or group.
- Any "suspicious activity": threat, warning, advice received or monitoring of the personnel in the organisation or community.
- Those events that, without having consequences, could have had them if procedures had not been followed, or because there was some "good luck".

Incidents are classified according to magnitude:

- **Minor incident:** any event that does not result in an interruption to operations but caused minor damage or loss of assets.
- **Critical incident:** any event that results in a temporary/limited interruption to operations, and localised damage to assets.
- **Crisis:** any event that results in the interruption to operations/services and significant damage to goods. It requires intervention from outside the country.

Establish reporting lines and formats, taking into account that there must be, in general terms:

An immediate report of the incident:

- This is normally done verbally, generally by telephone. Concise, factual information must be provided regarding what happened, the personnel affected and damage.

Incident updates:

- During the reporting of an incident the nature of the subsequent communication to report on changes to the situation or to provide additional details is established.

Formal report of the incident:

- This is done in writing and sent to the person responsible for managing incidents (according to the established organigram). It must include:
  - **The type of incident** (robbery, armed robbery, theft, accident in transit, etc.).
  - **Place** (where the incident occurred).
  - **Day, date and time.**
  - **Description of the incident** (who was involved, who or what caused the incident, the impact on those affected, and details of any material loss, etc.).
  - **Decisions and actions taken.**

REMEMBER

The perception of what is a security incident depends on the person and the place in which it occurs.

Ensure that all incidents are reported, however insignificant they appear, as they could help to seen the need/advisability of a change to the security procedures.

APPROXIMATE LENGTH:
Two pages.

- **Who was informed about the incident** (local authorities, agencies, other players, etc.).
- **Need for assistance from other bodies** (EU, UN, police, etc.).
- **Recommendations for the future to improve the security of personnel.**

Recording of incident and mapping:

→ Set up a record of incidents which have been reported, indicating the date, type of incident (robbery, attack, etc.) and consequences.

The creation and use of a standard form for reporting incidents and facilitating monitoring is recommended.

The organigram must clearly indicate who security incidents should be reported to.

IMPORTANT: EU Aid Volunteers Critical Incident Management establishes that the organisation must carry out an evaluation and report by email to the head of the EACEA project in the case of a minor incident, and by telephone in the case of a critical or serious incident. If your organisation collaborates with this programme, ensure that contact details are included on your organigram.

If despite the security procedures and measures the organisation has suffered an incident, it is important to analyse the situation as deeply as possible. Create the procedures and formats necessary to ask about:

The objective of the incident:

→ Types of questions that must be put when analysing the objective: Was the incident planned? Was your organisation the target, or are all organisations? If you have evidence that it was planned against your organisation, the analysis must focus on the motives: Were the motives financial, social, religious, political? What could have led to the actions by the perpetrators? Could your organisation or any of your personnel provoked the incident through any action, declaration or behaviour?

Trends:

→ Do the events happen repeatedly? Over time? Places? Affected personnel?

Effectiveness of security measures:

→ Were measures considered to prevent this incident? Were the measures in place effective? Were the measures misunderstood or incorrectly implemented by personnel? What could be improved?

IMPORTANT: pay attention to and take into account any incidents reported by other related organisations and/or from the same sector, which could constitute a threat or affect the management of security.

The analysis of incidents happening to your organisation and other organisations will help you to decide whether or not to maintain your level of security and/or change procedures and protocols.

MODULE III

MODULE III

PREVENTION, MITIGATION AND RESPONSE: THE DEVELOPMENT OF SOPs

Once you have analysed your context in security terms, evaluated the risks and drawn up your first security strategies (module I); and you have designed your internal procedures for the management of security in your organisation (module II), it is time to proceed with the designing of specific protocols in accordance with the context and risks that you have identified.

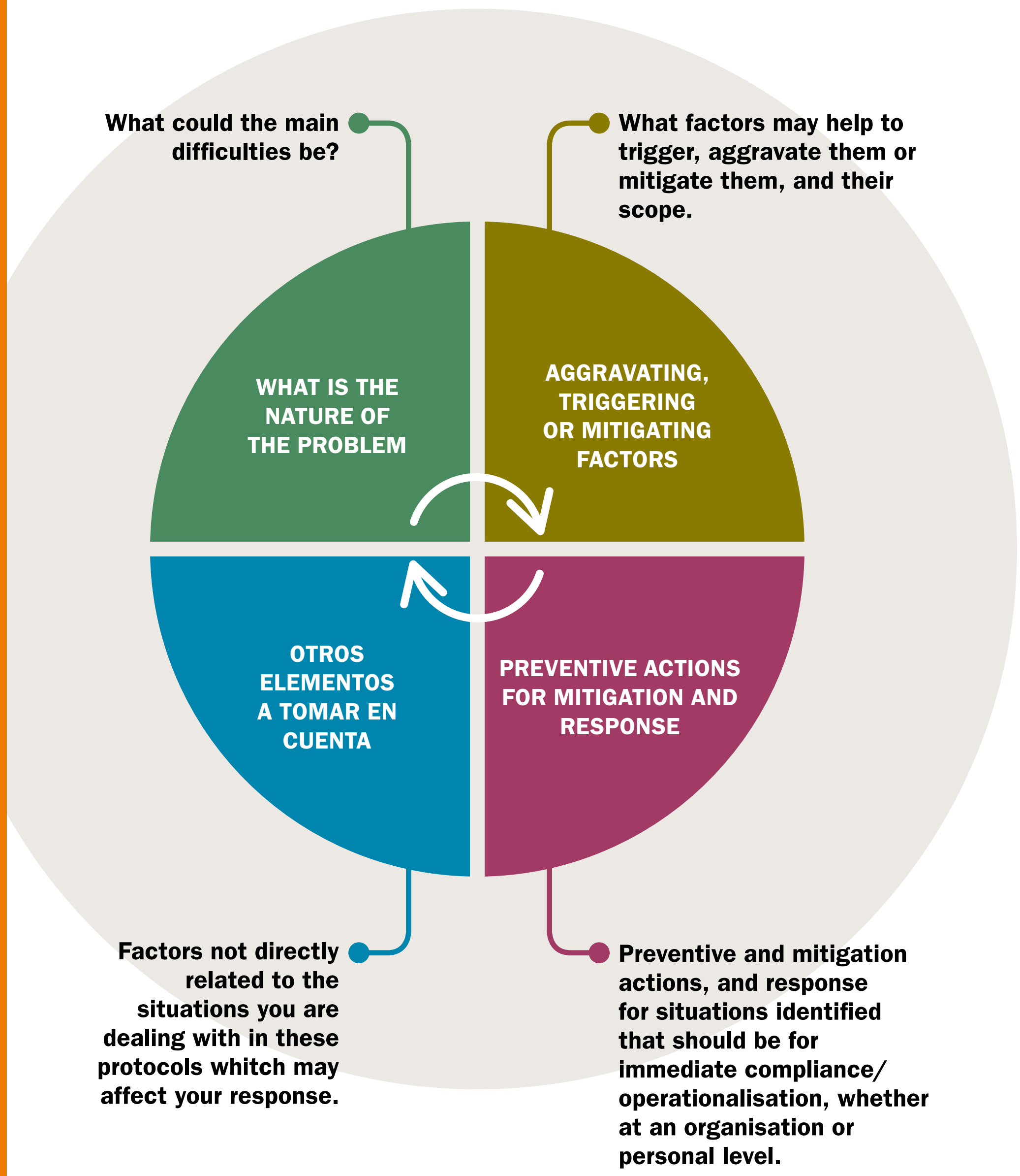
REMEMBER

Los procedimientos operativos de seguridad (también llamados SOPs: procedimientos operacionales estándar por sus sigles en inglés) tienen que ser claros, concisos y contener una estructura más o menos estándar.

There is not a single way to develop specific protocols for the prevention, mitigation and response to the identified risks.

This guide will provide you with a possible model to follow, although you may adapt it according to your specific needs and context, providing you do not leave out any of the main elements to take into account.

When developing specific protocols for specific issues or problems (SOPs: standard operational procedures), various key areas must be considered:



3·1 CULTURAL AWARENESS

Cultural differences are the wealth of peoples, but if they are not shared and work is not done in a suitable way, they may lead to misunderstandings which sometimes may be used politically.

REMEMBER
Culture is a defining aspect of society and individuals.

All actions designed with respect to this topic must take the form of recommendations and not impositions, and must arise through a consensual process involving discussion and acceptance.

APPROXIMATE LENGTH:
One page.

This section is particularly aimed at international personnel who are workers or volunteers in your organisation, as they do not probably have first-hand knowledge of the cultural codes and practices which exist. However, it may also be useful for national personnel who have moved to zones with different cultural codes and practices.

The description of the social context from module 1 will serve as support/reference.

DEFINITION OF THE PROBLEM	Define the main difficulties that may exist in terms of knowledge and cultural awareness regarding the peculiarities of your context (country/zone, etc.). → Example: cultural codes with respect to clothing, which may be radically different to the countries of origin of international volunteers; the role of religion in the zone/country; respect for the elderly, etc.
ASSOCIATED FACTORS	Analyse the factors associated with your context, for example: → Partial or complete lack of knowledge of the local language by international volunteers or personnel, etc. → Cultural codes associated with gender.
OTHER ELEMENTS TO CONSIDER	Identify whether there are other elements to consider, for example: → Local prejudice against specific groups. → Foreign nationalities. → Traditional structures. → Political instrumentalisation of cultural differences.
PREVENTIVE ACTIONS, MITIGATION AND RESPONSE	Identify and define actions to take to prevent, mitigate and/or respond. For example: → Share written information on cultural codes and practice on the country of your organisation in order to inform your international personnel (and also about the origin country of international personnel for national personnel); socialise this information. → Establish a process of cultural mentoring or coaching for international personnel with the support of local personnel. → Regarding national personnel boost the cultural wealth of your organisation by promoting spaces to share cultural codes between personnel from different zones/ethnicities, etc. → Share the basic rules for communication and acceptable levels of familiarity between colleagues and the community.

3 · 2 HEALTH

To which hospital should your international voluntary personnel go in the case of serious illness?

How should we respond to the main health risks that have been detected?

Who is responsible for checking the first aid kit in your organisations, where should it be located, and what should it contain?

The protocols defined by your organisation regarding health must respond to the previously defined health risk situation (module 1).

REMEMBER

The protocols require specific, well-defined actions with respect to instructions, those responsible, etc.

That is essential for any protocol, and particularly in the case of health.

APPROXIMATE LENGTH:
One page.

In the specific case of health, you have already defined the main risks to health in module 1, together with basic preventive intervention. That will facilitate the task of this module.

DEFINITION OF THE PROBLEM	Starting with the situation that you defined in module 1, you must now prioritise the main situations to which you wish to respond through the health protocols to be developed. Focus on those situations with a greater probability and impact. → Example: where to go and how to respond in the event of needing urgent surgery; how to avoid food poisoning; a response to epidemics; health during journeys.
ASSOCIATED FACTORS	Situations or factors that may have an influence on the defined health problem/s, for example: → Natural disasters. → Traffic accidents. → Rainy season (an aggravating factor for some epidemics and attenuating for others). → Personnel with chronic illnesses and the need for regular medication.
OTHER ELEMENTS TO CONSIDER	Of a varied nature, according to the case, for example: → Accessibility to health services. → The possibility to carry out medical evacuations. → The availability of quality medicines of all types in the country/zone. → First aid kits/PEP kits.
PREVENTIVE ACTIONS, MITIGATION AND RESPONSE	Identify and define actions to take to prevent, mitigate and/or respond. For example: → Establish written recommendations for travelling on the consumption of food and drink. Be careful with water. → Define the components of the first aid kit(s) necessary for your organisation and where they should be located (offices, cars, field offices, etc.). Name a person responsible for checking and refilling them. → Establish clear instructions prior to the deployment of new personnel (basically volunteers and non-local personnel – less used to the health risks in the zone –): necessary medical reports, check-ups, certificates, health and illness insurance to contract and procedures to do that, written recommendations on medicines and first aid kit which each individual must have, etc. → Establish a list of hospitals/health centres of preference according to the problem. → Define action protocols in the event of accidents and/or illness of personnel, where to refer the person to and/or the evacuation process.

3 · 3 SECURITY IN FACILITIES

What is the best location for an office?

What risks are there in the zone where you have the office?

Is a new office, residence or store being considered?

How will the installation of an office be perceived by the population?

What is the level of threat?

What measures of deterrence can be taken to improve security?

What strategies can be adopted to improve acceptance?

REMEMBER

In the use of the infrastructure by your organisation you must consider not only operational criteria (location, space and price) but also security and potential risks to persons and/or goods.

Urban or rural zones have different social behaviours. Ensure you create understanding with your neighbours.

APPROXIMATE LENGTH: One page.

All organisations need to use infrastructures for the location of offices, residences, stores, etc. The effective management of these infrastructures will allow the organisation to work in a safe protected environment, and thus operate in a more effective manner.

DEFINITION OF THE PROBLEM

Through the analysis of the context carried out in module 1, you can identify the risks and threats that your organisation and personnel may have to confront. Determine for what situations the organisation is going to take measures of protection or deterrence.

- Example: you know that the probability of attacks on houses in high and decide to take protective measures in the house by improving the perimeter and changing gates and doors.

ASSOCIATED FACTORS

Situations or factors that may have an influence on the defined problem/s, for example:

- Levels of crime in the area where the facilities are located.
- The type of incidents that have occurred and whether other organisations in the area have been victims.
- The title of the owner of the property.
- Location close to potential targets, such as government buildings or military and/or religious buildings.
- Accessibility to the property.
- Natural dangers which may affect the facilities.
- Nearby protective factors: the presence of security forces, embassies, etc.

OTHER ELEMENTS TO CONSIDER

Regarding the security of facilities you should take into account that your facilities and the perimeter of the property may be controlled by you. However, the area around your perimeter may affect you and will not be under your control. You will have to consider acceptance strategies to reduce the risk associated with the perimeter (see section 1.d).

PREVENTIVE ACTIONS, MITIGATION AND RESPONSE

Identify and define actions to take to prevent, mitigate and/or respond. For example:

- Ensure the external and internal perimeter (E.g. well defined barriers, safe walls or railings. Safe exterior windows and doors, and illuminated access points).
- Access control for facilities, with established procedures (identification documents, key control, controls over entry and exit, accompaniment of visitors.
- Guards and other measures of deterrence, the installation of alarms).
- Precaution against fire. Extinguishers, established, visible procedures shared with personnel.

3 · 4 TRAVELLING, JOURNEYS, TRAFFIC ACCIDENTS

Has your organisation had many security incidents related to journeys?

The greatest risks to personnel are linked to routine journeys, traffic accidents, attacks, shootings, kidnap, unexploded devices, etc.

REMEMBER

Procedures for journeys and travelling are essential in order to minimise security risks.

APPROXIMATE LENGTH: Two pages.

The preparation and organisation of journeys is an essential aspect for minimising security incidents. Check the record of incidents, risk diagnosis and security reports for zones you are travelling to (modules 1 and 2).

DEFINITION OF THE PROBLEM	In module 1 you analysed your context and defined places and zones of potential risk for your organisation, whether due to the existence of delinquents, armed groups, mines or roads in poor condition. Taking into account where personnel are most vulnerable during a journey, establish procedures for actions associated with those situations.
ASSOCIATED FACTORS	→ **Human:** driving under the influence of alcohol or drugs, overtaking in prohibited areas, speeding. → **Mechanical:** breakdowns to vehicles, poor response. → **Environmental:** rain. fog, poor lighting, the state of the roads, incorrect or non-existent signals
OTHER ELEMENTS TO CONSIDER	→ What elements can provide us with physical protection during and following an accident? (safety belts, air bags, etc.). → Vehicle maintenance. Servicing of mechanical elements on the vehicle (who, frequency, written monitoring). → Type of vehicles used for journeys.
PREVENTIVE ACTIONS, MITIGATION AND RESPONSE	Identify and define actions to take to prevent, mitigate and/or respond. For example: **JOURNEY PLAN** ■ Establish routes for journeys: Know the area where the journey is being made, define alternative routes. Avoid routes through zones of high criminality. ■ Avoid travelling alone. ■ Define communication procedures to monitor the location of vehicles. Moments of contact, and the drawing up of emergency information/ contact numbers (module 2). Ensure that all personnel know how to use the communication equipment. ■ Define procedures for parking vehicles day and night. ■ Check and prepare vehicles prior to setting off with spares (tyre, provisions, etc.) and first aid kit. ■ Documentation: Ensure you have the documentation for the car, driver and passengers. **CONTINGENCY PLANS** ■ For any problem, road accident, attack, etc. define what to do, where to go, who to contact. **POLICIES FOR VEHICLE USE** ■ Timetables. ■ Persons who are eligible to drive. ■ Policy on the non-use of arms. ■ Policy regarding unauthorised passengers: police, soldiers and/or armed militia.

3 · 5 ATTACKS/ROBBERY

Have you been the victim of a robbery or attack at any time in your life?

Where did it take place? Is it common in the place where you live or work?

Gender is a key factor is the area of personal security, and leads to the risk being seen differently within the same environment.

Specifically, female workers face a higher risk than male workers of rape and/or sexual attack, and also from other types of violence and aggression.

REMEMBER
Armed robbery by individuals or gangs are more frequent than the threat from armed conflict.

APPROXIMATE LENGTH:
One page.

The basic personal security measures must not be forgotten, as they are the best way to avoid the threats and risks faced in your place of residence or work.

DEFINITION OF THE PROBLEM	If your organisation has identified delinquency in module 1 as one of the possible threats, whether to personnel or to the organisation's property, it is probable that there should be a protocol for this matter. Remember that it must always be adapted to your analysis of the context.
ASSOCIATED FACTORS	There are multiple factors which may be associated with this problem and should be considered. Among them here are some examples: → Unemployment and socio-economic marginalisation. → Family disintegration, school absenteeism and the age structure of the population. → The consumption of drugs. → Self-protection committees, the presence of civil authorities.
OTHER ELEMENTS TO CONSIDER	It is important to evaluate whether the criminality follows seasonal patterns, if it is linked to political or social demonstrations, if there are moments of upsurge, etc. It is also important to understand the results of the incidents.
PREVENTIVE ACTIONS, MITIGATION AND RESPONSE	Identify and define actions to take to prevent, mitigate and/or respond. For example: **PREVENTIVE** ■ Establishing self-protection protocols (such as not walking alone at certain times, etc.) ■ Limiting the amount of cash, valuable articles and assets kept in offices and residences. ■ Avoiding habitual routines regarding banks or ATMs. Attempting to vary the payment times for salaries, to avoid predictability. ■ Improving the security measures for facilities. **MITIGATION WHEN FACING AN ATTACK** ■ Train personnel in the main keys when facing aggression, such as: the importance of meeting their demands. No material object is worth your life. Do not make sudden movements. Your hands should be visible and you should tell armed attackers what you are going to do before you do it, etc. The importance of not using languages that the attackers do not understand. Do not use a language that the attackers do not understand. ■ Remember the importance of reporting incidents (module 2). **RESPONSE** ■ Incorporated in health protocols (physical and psychological). ■ PEP kits (available and reachable).

3 · 6 SURVIVAL IN A HOSTILE ENVIRONMENT

Corruption, authoritarian or ineffective governments, high levels of poverty and an large number of arms in circulation are factors that in part explain the spiral of insecurity that leads to phenomena such as maras, drug trafficking and social revolts.

Criminal organisations have a large presence in cities and rural zones, and their members display a high degree of territoriality.

REMEMBER

These problems tend to be linked to dimensions which go way beyond those of your organisation. Basically, you should adopt a perspective of prevention and mitigation.

It is probable that professionals are required to address the matter.

APPROXIMATE LENGTH:
Two pages.

There are security situations for which the dynamics or violence and insecurity are as dangerous as any armed conflict. Workers may suffer situations involving bribery and extortion, and retention/kidnap.

DEFINITION OF THE PROBLEM	If in your environment there is a problem of violence associated with maras, drug trafficking and/or social revolts, it is probable that you need to establish prevention measures in order to work in this hostile environment, including specific protocols.
ASSOCIATED FACTORS	Possible associated factors: → Government anti-mara or anti drug trafficking policies may be a factor that unleashes greater violence between groups. → Pre/post election periods. → Economic crises, high inflation.
OTHER ELEMENTS TO CONSIDER	Identify whether there are other elements to consider. For example: → Your organisation may be a target due to disputes or frustration related to the activities within the programmes or the process of distribution for goods or services (common in organisations with activities involving distribution direct to populations).
PREVENTIVE ACTIONS, MITIGATION AND RESPONSE	Identify and define actions to take in order to fundamentally prevent and mitigate, and to a lesser extent in this case, to respond. For example: **PREVENTION. Instruct your personnel through** ■ The establishment of clear, constant messages on your activities, so that there is no doubt regarding the impartiality of your organisation, and no one believes that the activities go against their interests. ■ Do not identify with groups opposing those dominant in the area where you are working; maintain an attitude of neutrality. ■ Use protection and self-protection measures, such as avoiding dark. lonely places, check whether you are being followed, carry an identification card. ■ Use social media in a suitable way (Facebook, Instagram, etc.) ■ Identify areas to avoid in the case of social revolt (government buildings, etc.) and areas of protection. **MITIGATION** ■ Train personnel on how to respond to extortion and/or threats. **RESPONSE** ■ Your organisation may decide to have procedures prepared in the event of potential kidnap (code, key question, etc.), (requires professionals).

3 · 7

DEFENDERS OF HUMAN AND ENVIRONMENTAL RIGHTS

Human rights and the protection of the environment are interconnected.

In order to fully enjoy human rights a clean, sustainable environment is necessary.

Among other things, defenders of human rights make efforts to protect and promote human rights in relation to the environment.

States should establish a safe, favourable setting so that defenders of human rights can work free from threats, harassment, intimidation or violence.

REMEMBER

Although individual protection is necessary, collective protection should be a priority.

APPROXIMATE LENGTH: **One page.**

The defenders of human and environmental rights are among the individuals most exposed to risks, which are particularly serious for indigenous peoples and traditional communities which depend on the natural environment for subsistence and culture.

DEFINITION OF THE PROBLEM

If you have defined in module 1 that in your setting/organisation there are threats and risks (normally violence, attacks, extortion, kidnap, including death) faced by defenders of human and environmental rights and your organisation works with them, then you should develop protocols in that respect.

ASSOCIATED FACTORS

There are multiple factors which may be associated with this problem and should be considered. Among them here are some examples:

- Questions of gender.
- People trafficking.
- State terrorism.
- Extractive projects (such as mining and logging, hydro-electric projects, road infrastructures, agricultural expansion).
- Possible protective elements; organisations which defend human rights, regional partnerships, the United Nations.

OTHER ELEMENTS TO CONSIDER

It is important to identify the attacks in order to understand their structural origins. You will also have to consider the existing risk prevention measures on an individual, family or community level, and their consequences on a community level.

You must also consider previously established protocols, given that they will already provide procedures that may serve for these situations.

PREVENTIVE ACTIONS, MITIGATION AND RESPONSE

Work with defenders of human rights requires coordination and articulation between specialist movements and organisations, in order to acquire more power against external players that may be hostile.

It is important to design and coordinate possible actions for the prevention, mitigation and response to those organisations in a coordinated manner with specialist bodies.

3·8 STRESS MANAGEMENT

How can the security situation affect the stress of personnel?

How can stress affect the security response expected from personnel?

How can its effects be minimised, possible avoided, detected and responded to?

REMEMBER

Stress is a state of physical and emotional tension caused by situations to which we are subjected, demanded or challenged, which exceed or appear to exceed our capacity to respond.

In small doses it is positive for survival, because it allows us to be alert, but over prolonged periods it can be damaging for the health, and result in psychological disorders.

APPROXIMATE LENGTH:
One page.

There is no health without mental health. It is a principle globally accepted and covered by the WHO Action Plan. However, there are many aspects to resolve, such as the neglect of services and attention to mental health, or the violation of human rights and discrimination against persons with mental disorders and psycho-social disabilities.

DEFINITION OF THE PROBLEM

This section may already be integrated within the health protocol (chapter 3.2), but your organisation may decide to have a specific protocol to provide it with greater visibility and importance, given that lamentably it is an issue that tends to be neglected.

ASSOCIATED FACTORS

There are multiple factors which may be associated with this problem and should be considered. Among them here are some examples:

- Factors increasing stress linked to possible overwork, the security situation and/or individual factors.
- Tensions regarding HR within your organisation.
- Factors or interventions which may reduce stress (dispelling doubts, informal sessions, group activities, etc.).

OTHER ELEMENTS TO CONSIDER

Stress is not a factor to which people respond in the same way, nor is it caused in the same situations. It will be important to maintain a certain degree of flexibility regarding individual responses.

PREVENTIVE ACTIONS, MITIGATION AND RESPONSE

Identify and define actions to take to prevent, detect and mitigate, and if necessary respond. For example:

PREVENTION, DETECTION AND MITIGATION

- Training on Psychological First Aid (PFA).
- Anticipate key personnel for PFA if possible within your organisation (or external).
- Work closely with the area of human resources.
- Identify possible moments for increases in stress (arrival in the organisation, a worsening of the security situation, internal tensions, etc.).

RESPONSE

- Collaboration protocols with specialists.
- Policy level facilities for human resources.

3 · 9 INTERNATIONAL VOLUNTEERS

The EU Aid Volunteers programme allows volunteers and organisations from various countries (sending organisations) to send volunteers to provide technical, logistical and/ or training support for humanitarian action projects, contributing towards strengthening local capacities and the resilience of populations affected by various types of disasters and humanitarian crises.

At the same time, the programme makes it possible for small local organisations (hosting organisations) to be bolstered by specialist personnel at no additional cost.

REMEMBER
The EU Aid Volunteers programme is governed by DG ECHO and EACEA regulations.

APPROXIMATE LENGTH:
One page.

This section is particularly important if your organisation works within the EU Aid Volunteers programme, either as a hosting or sending organisation. It is also of particular relevance if it is in the process of qualification/certification for one of the two categories, given that the programme demands, among other things, compliance with some standards in terms of security.

DEFINITION OF THE PROBLEM	If you have responded in the affirmative to the previous point, your aim is that this security guide reflects as a minimum the full requirements demanded within the EU Aid Volunteers programme. This can also serve for all types of volunteers who may come via programmes other that the EU programme, or individually.
ASSOCIATED FACTORS	If you have drawn up a good security guide up to this point, in reality international volunteers (and also national volunteers) should find, along with other personnel, their place in the remaining instructions and analysis in the guide. In any case, there are certain specifics that must be considered. Some examples of associated factors: → The place of origin of international volunteers. → Previous experience of the international volunteers. → If you are a hosting organisation, the capacity of the sending organisation with which you are collaborating.
OTHER ELEMENTS TO CONSIDER	Check the legal and regulatory documents from the EU Aid Volunteers programme, essentially implementing regulation (1244/2014 of 20th November, 2014): Article 28, and the European Parliament and Council regulations establishing the programme (375/2014 of 3/4/2014) and establishing its standards(1398/2014 of 24/10/2014), together with security instructions established by DG ECHO. Be mindful of updates and modifications to these regulations.
PREVENTIVE ACTIONS, MITIGATION AND RESPONSE	As previously established, be careful to ensure, for example, that: → The procedures foreseen by your organisation comply with the requirements of the programme and can be adapted if necessary. → Your organisation (if a hosting organisation) will work together with the sending organisation in order to meet all the requirements of the programme. → There is good coordination between the hosting and sending organisations, particularly in the process of sharing information with volunteers, briefing/debriefing, and procedures are written and are signed by the volunteers, after they have been understood. → Foresee a response to the need for early termination of the volunteer period for various possible reasons, including a possible worsening of security conditions.

MODULE IV

MODULE IV

EMERGENCY RESPONSES

In previous chapters you have analysed the context in which you live and work, identifying risks and threats, and establishing procedures to minimise risks and provide responses. However, there are situations which can lead to a deterioration of the security situation to levels which are unacceptable for your organisation, and which force you to take measures of extreme urgency. It does not happen frequently, but sometimes occurs, and the organisation should be prepared. In this chapter we will look at the basic emergency responses which should be described in your security plan/guide.

REMEMBER

Although responses to crises are never the same, having procedures for emergency measures when facing specific crises will help you to make the right decisions.

APPROXIMATE LENGTH: One page.

Firstly, the organisation must establish its acceptable or unacceptable security levels (based, among other factors, on the levels of tolerance to risk) and at what time each defined type of response will be used. Bear in mind that there may be different measures for national and international personnel, and for workers and volunteers.

The diagram below presents a common scale of responses to emergencies, which range from the suspension of activities to evacuation. Your organisation should establish what type of situation would lead to each type of response.

4 · 1 HIBERNATION - RELOCATION - EVACUATION

Organisations often work in zones in which natural disasters may occur, or which are affected by armed conflict or other violent situations.

If the situation becomes highly insecure, what measures are the organisation going to take?

How will evolution of the situation be monitored in order to decide how long the measures are going to be in place, or when the security level is going to change? Who is going to take those decisions?

When drawing up your security plan/guide you must define the emergency plans you consider necessary to identify, and jointly agree with personnel the "triggering factors" for activating the various emergency plans.

Remember that your organigram (Module II) should include who is/are responsible for taking decisions and the management of crises. Anticipate remaining in contact with other organisations and embassies. Coordination is essential.

SUSPENSION OF ACTIVITIES	In order to avoid emerging threats or to see how the security situation is evolving following an incident, your organisation may decide to temporarily suspend activities. The suspension time will depend on how security is evolving. → Establish criteria to define when to carry out a suspension of activities. E. g. if the forecast for rain may reach historic levels, which generally as a consequence lead to the flooding of roads, it is probable that your organisation will decide to suspend activities in the zone. Bear in mind that the suspension of activities may have consequences regarding acceptance, in they are not understood or accepted by the beneficiaries. Ensure that the suspension of activities is adequately communicated.
RELOCATION	If the organisation has identified that it may be the target of an attack and/or risk, it may be appropriate to change the offices and/or activities within the same country from an unsafe zone to a safe one. → Identify possible locations (other NGO offices, guest houses, etc.) where your personnel and/or offices can be relocated. These locations must have safe access, and possible evacuation routes. → Ensure that there are emergency stocks (food, water, first aid) and adequate communication systems. Everything must be stored in accessible places. → Establish transport mechanisms and pick-up points.
HIBERNATION	If relocation or evacuation of personnel is very dangerous, whether due to access roads being cut (or there is the risk of attacks) or for other reasons, the organisation may establish that personnel hibernate in one or more locations within the organisation. Hibernation is also usually a step prior to evacuation, while the details and logistics of evacuation are finalised. → Identify which of your offices or residences may serve as a refuge for your personnel during this stage. E.g. the building with greatest resistance to earthquakes. → Ensure there are emergency stocks, fuel, adequate communication equipment and established communication procedures. Define these details in your guide. → Establish transport mechanisms and pick-up points, if necessary.

REMEMBER

The security situation must be constantly evaluated in order to be able to react rapidly to any change of context.

Crisis situations should be foreseen sufficiently in advance. Improvisation implies a great deal of risk.

APPROXIMATE LENGTH:
Two pages.

<table>
<tr><td>EVACUATION</td><td>If the security level has deteriorated greatly, the organisation may decide to carry out the physical removal of personnel (normally international personnel) to another country, and the closure of offices in the area.
→ Bear in mind that national personnel are sometimes working in zones they are not from. Ensure that personnel and their families are in safe zones.
→ Pay personnel their salaries in cash prior to evacuation.
→ Establish channels of communication with communities, so that they can help to determine when it is safe to return.
→ Plan the means of transport and bear in mind any requirements if crossing another country (visas, etc.) and how to cross the border (via air, land, sea). All this must be planned in advance.</td></tr>
<tr><td>PHASES</td><td>Independently of the emergency response that your organisation decides to apply when faced with specific security situations and risks, you must take into account that normally three periods of time are defined in these processes:
→ Alert phase: In which all involved parties are notified that a response is to be activated and that it is necessary to be ready.
→ Activation phase: The emergency plan is activated.
→ Recovery phase: The moment when the organisation will once again carry out operations in a secure manner is defined.
The responsibility for the management of crises during each phase must be clearly stipulated on the organigram and communicated to all personnel.</td></tr>
</table>

4 · 2 MEDICAL EVACUATION

Risks to health, both physical and mental, have already been analysed in module I, and associated procedures in module III. In this module your organisation will have to establish how and when a medical evacuation should take place.

What level of services are available? Are there pharmaceuticals available and, fundamentally, safe blood transfusion and adequate surgical capabilities?

What type of medical facilities are there? Can they respond to any high risk situations, such as heart attacks, kidney failure, etc.?

REMEMBER

Medical emergency plans seem easy, but in the case of an incident stress and logistic failures may impair the outcome.

APPROXIMATE LENGTH:
One page.

Your organisation must anticipate an emergency response such as medical evacuation, and define for what category of personnel the procedures are applicable, who is responsible for contracting the associated insurance, how it works and in which cases and in what way will it be decided if it is necessary or not, and what is the role of your organisation in that respect.

You should consider possible problems with respect to insurance and specific questions regarding gender that may arise.

Near in mind that medical information is confidential.

Some examples of important points to consider, depending on the context:

- Define on your organigram (module II) who is responsible for the management of a medical crisis, and medical monitoring. Remember that medical evacuation may be limited to international personnel and covered by donors, their own medical insurance or the insurance of the sending organisation or volunteer programme, etc. The cases may vary but your organisation should be up to date, and analyse and clearly define your role.
- Analyse the details of insurance cover (who is covered, what is covered, what is the response and its limitations, where might there be shortcomings, what information is required and when, contact details).
- Analyse medical assistance and the response capabilities in your country and/or area (module I), essentially in terms of surgical capacities, transfusion safety, and specialist personnel. Visit hospitals that have been identified and decide which are the referral hospitals.
- If air evacuation is necessary it is necessary to establish a prior relationship with the services offering this and ensure they understand any existing requirements.
- Ensure that medical information for personnel is available if necessary, in the event of an emergency, and is in accordance with the recommendations of professionals with respect to the information to be included and how it is handled.
- Establish communication mechanisms in order to carry out the evacuation.

Alianza por la Solidaridad | Member of actionaid

EU Aid Volunteers
We Care, We Act

We World

actionaid
Αλλάζουμε ζωές, αλλάζουμε τον κόσμο

actionaid
REALIZZA IL CAMBIAMENTO

MINISTERE DE L'INTERIEUR
DIRECTION DE LA PROTECTION CIVILE

FANM DESIDE

ASPRODE
ASESORÍA A PROGRAMAS
Y PROYECTOS DE DESARROLLO

ADES

ASOCIACION SALVADOREÑA DE AYUDA HUMANITARIA
PRO VIDA
LABORATORIO INTEGRAL DE CALIDAD DE AGUA
"PROF. FRANK A. ESCHER"

Asociación para el Desarrollo Integral de la Mujer

ASOM
Asociación de Mujeres Afrodescedientes del Norte del Cauca

RELIGIOSAS ADORATRICES