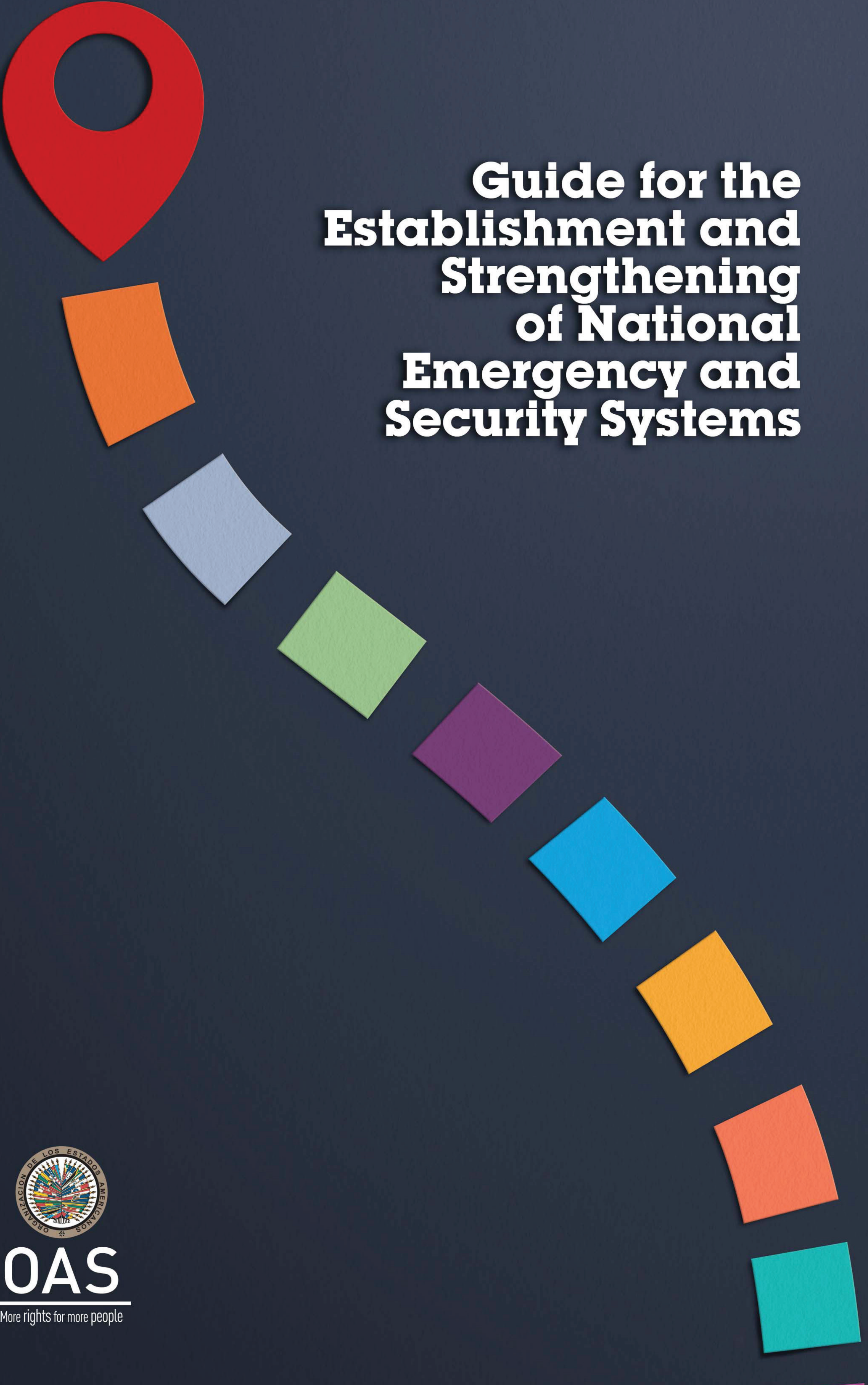
Guide for the Establishment and Strengthening of National Emergency and Security Systems



OAS
More rights for more people

About the OAS

The Organization of American States (OAS) is the main political forum in the region, bringing all the independent nations of the Western Hemisphere together to jointly promote democracy, strengthen human rights, promote peace, security, and cooperation, and advance in achieving common interests. Since its origins, the OAS has had the main objective of preventing conflicts and providing political stability, social inclusion, and prosperity in the region through dialogue and collective actions such as cooperation and mediation.

ISBN 978-0-8270-7243-5

OAS Cataloging-in-Publication Data

Organization of American States. Secretariat for Multidimensional Security. Department of Public Security.
Guide for the Establishment and Strengthening of National Emergency and Security Systems in the Member States of the Organization of American States (OAS) / [Prepared by the Department of Public Security of the Secretariat for Multidimensional Security of the Organization of American States].
v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.K/XLIX GTS/SES/doc.4/21)
ISBN 978-0-8270-7243-5
1. National security. 2. Internal security. 3. Public safety. 4. Emergency communication systems. I. Title. II. Subsidiary Technical Group on Emergency and Security Systems. III. Series.
OEA/Ser.K/XLIX GTS/SES/doc.4/21

Dedication

With respect and admiration for all personnel and first responders in the emergency and security systems of OAS member states who, in a professional, technical, and fully committed way, **respond to emergencies and various dangerous situations in addition to the traditional and emerging threats that arise in their every day work.** To all those who, despite risks, continue to give their best to safeguard and protect the lives of people who need assistance, **24 hours a day, 365 days a year.**

Acknowledgments

The drafting of this guide was possible due to the collaboration, contributions, effort, and dedication of a group of staff members from emergency and security systems and related agencies in the region. They all came together within the framework of the Subsidiary Technical Group on Emergency and Security Systems (STG-ESS) to develop this guide.

All those who participated in this process did so without knowing each other, working remotely, and within the context of one of the most severe pandemics humanity has ever faced. Despite all the above, they assumed the task of writing this guide selflessly and with a high level of commitment. Therefore, in gratitude, those involved in the drafting of the chapters of this guide are acknowledged below.

Thanks to their effort and hard work, the Subsidiary Technical Group on Emergency and Security Systems has fulfilled one of the recommendations issued during the Seventh Meeting of Ministers Responsible for Public Security in the Americas. Collaboratively, collectively and in a concerted manner, the STG-ESS has produced a regional public good that will be useful for all the member states of the Organization of American States (OAS).

Below are the agencies, countries, and names of the extraordinary people who participated in preparing, reviewing, and validating this guide. To all of them, we extend a special recognition for the work done.

9-1-1 Emergency System of Costa Rica (SE9-1-1 CRI)

Elena Amuy Jiménez,
Director

Johnny Hidalgo,
Operational Logistics Coordinator

Luis Fernando Alfaro Ubico,
Legal Counselor

Carolina Jiménez Rodríguez,
Planning Coordinator

Guiselle Mejía Chavarría[1]

911 National Emergency and Security Response System of the Dominican Republic

Brigadier General Vicente Mota Medina, ERD,
Executive Director

Lieutenant Colonel Pedro Ventura Chang, FARD,
Head of Plant Security

Lourdes Florentino,
Planning and Development Director

Teresa Garcés, Head of the Management Quality Department

Agustín Jiménez, Head of the Institutional Development Department

Luis Ferrand,
Operations Director

Tammy Ramírez,
Head of the Emergency Reception Department

Misael Ventura, Head of the Emergency Dispatch Department

Alfredo Arredondo,
Technology Director[2]

Luis Reyes,
Head of System Development and Implementation Department[2]

Mabely Díaz,
Director of Data Processing, Analysis, and Management of Information[2]

[1] At the time of publication of this guide, Guiselle Mejía Chavarría is no longer part of the 9-1-1 Emergency System of Costa Rica. However, during the time she was the agency's Director, she contributed with her support, leadership, and experience in the production of this document.

[2] At the time of publication of this guide, Alfredo Arredondo, Luis Reyes, and Mabely Díaz are no longer occupying these positions. However, during their tenure, they helped to write the chapters undertaken by the 9-1-1 National Emergency and Security Response System of the Dominican Republic.

National Information Center of Mexico

David Pérez Esparza, Head

Hernán Salgado, Head of Office

Juan Salazar Dominguez, Area Director

Oscar Laguna Maqueda, Deputy Director of Area

Moisés Salas, Deputy Director of Area

Laura Álvarez Susano, Deputy Director of Area

Integrated Security Service ECU 911 of Ecuador

Juan Zapata, General Director of the ISS ECU 911 and Chairman of the STG-ESS

Marco Garnica, Doctrine Technical Deputy Director of the ISS ECU 911

Bolívar Tello,Operations Technical Deputy Director of the ISS ECU 911

Angélica Buñay, Operations Analyst of the ISS ECU 911

Gary Almeida, National Regulatory Director in Emergencies of the ISS ECU 911

Celia Gómez, National Regulatory Emergency Specialist of the ISS ECU 911

Elisa Bravo, Director of Processes and Quality Control of the ISS ECU 911

Wilfrido Muñoz, National Director of Social Communication of the ISS ECU 911

Cassandra Arciniegas, Interinstitutional Coordination Specialist of the ISS ECU 911

Rosana Malta, Health and Occupational Security Specialist of the ISS ECU 911

Sistema de Emergencias 9-1-1 de Paraguay

Liliana Díaz, General Director

Daniel Rojas, Strengthening Coordinator

Carlos Román, Technical Support

Nilse Molinas, Technical Support

The valuable support provided by EENA and NENA Mexico-Latin America, two of the most prestigious associations supporting, advising, and accompanying emergency and security systems should also be acknowledged for their contributions. Their participation in the external validation process provided a second quality control check, strengthening even further the technical rigor of this guide's contents.

Cristina Lumbreras, Technical Director

Leonardo Dorony, President

A word of appreciation is extended to Patricio Tudela for his professional excellence, thoroughness, and steadiness. As an external consultant, he followed the review, editing, and validation stages of this guide and even made substantial contributions to many of its chapters.

The planning and production of this guide (noting that the original version of this document was in Spanish), were the responsibility of Karen Bozicovich, Chief of the Public Security Information and Knowledge Section of the OAS Department of Public Security.

This document was prepared by the OAS Department of Public Security with contributions from the 9-1-1 Emergency System of Costa Rica (SE9-1-1 CRI), the 9-1-1 National Emergency and Security Response System of the Dominican Republic, the National Information Center of Mexico, the Integrated Security Service ECU 911 of Ecuador, and the 9-1-1 Emergency System of Paraguay. The general technical orientation of the document was the responsibility of the Integrated Security Service ECU 911 of Ecuador.

The guidelines, suggestions, and recommendations expressed in this document represent the views of each chapter's authors and do not necessarily reflect the official positions of the OAS member countries.

General editors (of the Spanish original document): Karen Bozicovich and Patricio Tudela
Design and layout: Giovanny Guzmán
English translation: CABI Interpreters and Translators

GUIDE FOR THE ESTABLISHMENT AND
STRENGTHENING OF NATIONAL

EMERGENCY AND SECURITY SYSTEMS

Table of Contents

Acronyms 14
Glosary 16
Prologue by the General Director of the ISS ECU 911, Juan Zapata Silva 25
Prologue by the OAS Secretary General, Luis Almagro 27
Presentation 29
Introduction 32

01 CREATION AND ESTABLISHMENT

Introduction 36
1.1 Institutional and political support 37
1.2 Legal foundations and regulatory framework 37
1.3 Institutional anchoring 38
1.4 Ideation 38
1.5 Structure 39
1.5.1 Primary actors (or articulated institutions) 39
1.5.2 Supporting actors (or related institutions) 40
1.5.3 Subsidiary actors 41
1.6 Levels of operation 41
1.7 Coordination and cooperation 42
1.8 Strategic targeting 42
1.9 Executive Director (or similar position) 43
1.10 Financing and sustainability 44

02 STRATEGIC PLANNING

Introduction 45
2.1 Strategic planning 46
2.2 Fundamental components of a strategic plan 46
2.3 Guiding principles 47
2.4 Definition of strategic axes 48
2.5 Definition of strategies 48
2.6 Action plans 49
2.7 System of Indicators and Targets 50
2.8 Budget 50
2.9 Some tools for strategic planning and its execution 51
2.9.1 Pre-planning: SWOT Analysis 51
2.9.2 During planning: Strategic Map 52
2.9.3 Post-planning: Balanced Scorecard (BSC) 54
2.10 Assumptions of the strategic plan 56
2.11 Critical success factors 58
2.12 Risk identification and analysis 59
2.13 Continuity plan for strategic planning 64
2.14 Foresight and adaptation 65

03 SYSTEM DESIGN

Introduction 66
3.1 Operational models 67
3.2 Structure and organization (institutional architecture) 70
3.3 Functional requirements 72
3.3.1 Technological infrastructure /architecture 72
3.3.2 Information architecture 74
3.3.2.1 Incident typology 76
3.3.2.2 Typology of access channels 77
3.3.2.3 Call typology 78
3.3.2.4. Typology of prioritization levels 79
3.3.2.5. Inappropriate calls 81
3.3.2.6. Recording incident information 82
3.3.2.7. Interoperable and relational databases 82
3.3.2.8. Data processing, analysis, and display 83
3.3.2.9. Generation and use of information 83
3.3.2.10. Reporting system 84
3.3.2.11. Document management system 85
3.3.2.12. Functional area of information management 86
3.3.3. Physical infrastructure and equipment 87

04 TOTAL QUALITY MANAGEMENT

Introduction 88
4.1. Quality management model 90
4.2. Standardization of processes and implementation of protocols 93
4.3. Establishing and measuring indicators 95
4.3.1. Activity indicators 96
4.3.2. Process indicators 97
4.3.3. Evaluation indicators 97
4.3.4. Management indicators 98
4.3.4.1. Human resources 98
4.3.4.2. Operations 98
4.3.4.3. Quality 98
4.3.4.4. Administration and finance 98

05 CALL AND INCIDENT MANAGEMENT

Introduction 99

5.1. Handling requests, calls, and reports 101

5.2. Risk classification and prioritization 103

5.3. General guidelines for drafting protocols 103

5.4. Transfer of information to dispatch services 108

5.5. Dispatch and monitoring of units 109

5.6. Capturing, displaying, and storing data 111

5.6.1 For the operation 111

5.6.2 For evaluation and continuous improvement 111

06 HUMAN TALENT MANAGEMENT

Introduction 113

6.1. Planning and management of human talent 114

6.1.1. Job analysis 115

6.1.2. Job descriptions 116

6.2. Functional area for the management of human talent 118

6.3. Recruitment and selection of human talent 119

6.4. Induction of human talent 121

6.5. Ongoing training to strengthen skills and capabilities 123

6.6. Performance evaluation 124

6.7. Loyalty and retention of human talent 126

6.8. Departure process 126

6.9. Occupational health and safety 127

6.10.Code of Ethics and Code of Conduct 128

07 INFORMATION MANAGEMENT

Introduction 130

7.1. Information assessment 131

7.1.1. Sources 131

7.1.2. Information flows 132

7.1.3. Information resources 132

7.1.4. Products and services 134

7.2. Information cycle 134

7.3. Information at the functional levels 135

7.4. Identifying information needs 136

7.5. Obtaining information 137

7.6. Organization and storage 137

7.7. Development of information products or services 139

7.8. Exchange, distribution, access, and use of information 140

7.8.1. Interoperability and exchange of information 141

7.8.2. Development and continuous improvement of operations 141

7.8.3. Pre-judicial and judicial bodies 142

7.8.4. Communication, transparency, and accountability 143

7.8.5. Public policy process 143

7.9. Information audits 144

Contenido

08 SECURITY MANAGEMENT

Introduction 145

8.1. Information security 146

8.1.1 Information security policies and standards 146

8.1.2. Treatment of physical and digital documentation 148

8.2 Security of technology infrastructure for information and communication 148

8.2.1. Regarding IT systems 149

8.2.2. Communications security 150

8.3. Physical security 151

8.4. Risks and vulnerabilities 153

8.4.1. Risk analysis 153

8.4.2. Continuity of Operations Plan (COOP) 154

8.4.3. Contingency and recovery plans 156

8.5. Personnel health and safety 157

8.5.1. Risk factors 158

8.6. Continuous improvement 161

09 COMMUNICATION MANAGEMENT

Introduction 162

9.1. Communication planning 164

9.2. Planning organizational communication 164

9.3. Planning operational communication 165

9.4. Communication plan 167

9.5. Communication management 171

9.5.1. Spokespersons 172

9.5.2. Networks 173

9.5.2.1. Web platform (external) 173

9.5.2.2. Intranet (internal) 174

9.5.3. Media 175

9.5.3.1. Traditional media 175

9.5.3.2. Social Media 175

9.5.4. Public and community relations 176

9.5.5. Prerecorded messages 178

9.6. Communication planning and management in large-scale emergencies 178

9.7. Communication challenges 180

10 TRANSPARENCY AND ACCOUNTABILITY

Introduction 182

10.1. Planning for transparency and accountability 184

10.2. Inquiries and requests for public information 185

10.3. Quantitative data, indicators, and open data 186

10.4. Reporting system 187

10.5. Government purchasing and contracting of goods and services 188

10.6. Internal/external audits 189

10.7. Communication plan 189

10.8. Additional mechanisms 190

Table and Figures Index

Table 1 Example of table for the definition of strategic objectives 48

Table 2 Example of table for the definition of strategies 49

Table 3 Example of a system of indicators and goals 50

Figure 4 SWOFT example 51

Figure 5 Example 1 of Strategic Map 52

Figure 6 Example 2 of Strategic Map 53

Figure 7 Advantages of the Balanced Scorecard 55

Table 8 Example of table to define and explain assumptions 57

Table 9 Example of table for the ientification and classification of risks 60

Table 10 Example of table for risk analysis 61

Table 11 Example of table for risk treatment 61

Table 12 Example of table for monitoring and reviewing risks 62

Table 13 Example 1 of risk matrix 63

Table 14 Example 2 of risk matrix 64

Figure 15 Six Main Activities 68

Figure 16 Model B 69

Figure 17 Model C 69

Figure 18 Some recommended attributes for information architecture 75

Table 19 Classification of appropriate calls 78

Table 20 Prioritization scheme 79

Figure 21 Service Quality Management 93

Table 22 Identifying information needs 136

Figure 23 Identifying information needs 137

Table 24 Development of services and/or products 140

Table 25 Example of a risk matrix 154

Table 26 Risks and recommendations when answering calls and monitoring cameras 159

Table 27 Risks and recommendations when responding to emergencies in the field 160

Table 28 Template for the development of a Communication Plan 169

Acronyms

ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials
APM	Association for Project Management
ATR	Action Taken Report
ATS	Automatic Transfer Switch
AL	Automatic Vehicle Location
BSC	Balanced Score Card
BIA	Business Impact and Analysis
CACH	Computer Aided Call Handling
CAD	Computer Aided Dispatch
COBIT	Control Objectives for Information Technologies
COOP	Continuity of Operations Plan
CTI	Computer Telephony Integration
DSS	Decision Support System
EENA	European Emergency Number Association
EFQM	European Foundation Quality Management
EIS	Executive Information System
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GIS	Geographic Information System
GPS	Global Positioning System
IAED	International Academies of Emergency Dispatch
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
KPI	Key Performance Indicator
MDC	Mobile data computers
MDT	Mobile data terminals
NENA	National Emergency Number Association
NFPA	National Fire Protection Association
NISO	National Information Standards Organization
NOC	Network Operation Center
OLAP	On-line analytical processing
PABX	Private Automatic Branch Exchange
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PRAM	Project Risk Analysis and Management
PRV	Primary Response Vehicle
PSAP	Public Safety Answering Point
SMS	Short Message Service
TIA	Telecommunications Industry Assocation
TTY	Teletypewriter
ITU	International Telecommunication Union
VMS	Video Management Software
VOIP	Voice Over Internet Protocol

Glossary

Alert

Notification, call, or signal regarding an incident that has occurred, or is about to occur, enters the emergency and security system through any of the established communication paths, channels, or means.

Appropriate call

A call associated with an emergency and, as such, merits attention and, when necessary, the mobilization of units and resources to the field and timely coordination with the articulated institutions (first responders).

Balanced Scorecard (BSC)

A management approach and methodology for strategic planning that translates the organization's strategy and vision into action. It converts objectives, goals, and activities into indicators to track and measure the organization's overall performance, which is divided into perspectives, including financial perspective, customer/user perspective, internal process perspective, and learning for growth perspective.

Baseline

It is the first step in monitoring and evaluation. It provides an account of the initial situation/state in which the system, or its component, finds itself before initiating an intervention, reform, or change. A series of variables and indicators are usually used to establish it.

Chain of custody

Set of sequential activities and procedures applied in protecting and securing physical and digital evidence, from the reception of the call or video surveillance record, the location at the crime scene or scene, down to its presentation to the judicial authority.

Computer Assisted Dispatch

A computerized system for receiving calls, dispatching necessary units and resources to the place where the emergency is taking place and according to the type of incident, providing periodic updates on the status of the emergency based on the actions being conducted in the field, and analyzing, in a comprehensive manner, the services provided. It is commonly known and referred to by the acronym CAD (computer-assisted dispatch).

Confidentiality

Qualification of information that restricts access, use, availability, and disclosure to unauthorized persons, agencies, or entities.

Contingency plan

A set of planned processes, steps, and actions activated in the event of a contingency that affects the operation of an emergency and security system to minimize downtime and maximize recovery time.

Continuity of operations plan (COOP)

An emergency plan that, based on risk analysis and identification, and identification of critical and essential processes for the operation of an emergency and safety system, establishes the processes, steps, and actions to undertake, and assigns responsibilities, to guarantee and recover the operation of the system in the event of any contingency.

Continuous improvement

A systematic process of collecting, analyzing, using, and documenting information to follow up on actions aimed at producing a product or providing a service to identify corrective or improvement measures to keep the system in line with the standards established in protocols or reference instruments.

Disaster recovery plan

A planned and tested recovery process covering the data, hardware, and software considered critical and essential for the operation of an emergency and security system to resume operations if it has been affected by a contingency.

Dispatcher

The person in charge of assigning units and resources for the timely handling of an emergency, contingency, or incident that has generated an alert to the emergency response service.

Dispatch of resources

This involves choosing and assigning the available and necessary units and resources in response to an emergency, contingency, or incident. It is usually performed through a technological system or platform (see definition of computer-assisted dispatch). Additionally, dispatch of units is used.

Emergency

An unforeseen event, contingency, or incident reported to the emergency and security system through the different established communication paths, channels, or means, which affects or endangers the life or integrity of people and/or property, and therefore requires an immediate and effective response. There are different emergencies, including civil/public security, physical and mental health, public health emergencies, disasters and accidents, national security, and programmed events.

Words such as event, contingency, or incident are also used to refer to an emergency.

Emergency alert

A message transmitted by the entities that provide and manage emergency services through any means, platform, or technology. This message can be transmitted massively at the national, subnational, or zonal level or to a group of people, depending on the emergency or situation.

First responders (Articulated institutions or First-ring institutions)

First responders (Articulated institutions or First-ring institutions)
State or private sector agencies/institutions responsible for conducting the essential functions of an emergency and security system, which directly serves and responds to different types of emergencies (traffic and mobility; civil/public security; physical and mental health care; public health emergencies; fire, accidents, and disaster management).

Functional areas

A way of grouping and organizing activities of a homogeneous and interrelated nature, corresponding to an emergency and security system structure. They can be classified into two types: main or mission functional areas and supporting functional areas. The former is critical for fulfilling the aim of an emergency and security system. The following could be considered among the main or mission functional areas: Operations Management, Process and Protocol Management, Quality Management, Information and Communication Technologies, Security Management, and Information and Analysis Management. The latter, including Human Resources, Administration and Finance, Legal, Communication, Strategic and Operational Planning, and Project Management, play a supportive role.

Geographic Information System

Software for entering, integrating, analyzing, sharing, displaying, retrieving, and storing geographically referenced or spatially referenced data and information. It is often an essential software tool for the location, response, and management of emergencies.

High availability

Protocol for the design of an emergency and security system that when implemented indicates that the technological infrastructure can be resistant to interruptions and failures of the electrical system and can continue to function and provide services to the population.

Inappropriate call

A non-emergency call may be a prank call, incorrect or unintentional dialing, non-emergency inquiries, misuse of the emergency service, or communication problems, which do not require the assistance or displacement of units or resources of the articulated response institutions.

Information

Information is one of the most critical assets of an emergency and security system that can be manifested in various forms: textual, numerical, graphic, tabular, cartographic, or narrative, and in any type of media: magnetic, paper, electronic, audiovisual, and others. The classification, protection, monitoring, and control of information can follow the guidelines established by international and national standards defined for such purposes.

Information cycle

A process that aims to use information at each of the three functional levels of an emergency and security system (strategic, tactical, and operational) to guide decision- making and meet established objectives. It comprises a series of stages, guided by regulations, standards, and procedures, and streamlined or facilitated using the software.

Information security

A set of preventive, proactive, and reactive measures applied to preserve the confidentiality, integrity, and availability of information.

Interoperability

A capability of information systems, and the procedures that support them, to share data, and exchange information without restrictions and/or limitations, under the management and control of interested parties.

Misuse of the service

Requests, calls, and reports received by the emergency and security system that are due to improper, malicious, or fraudulent use or that entail the obstruction and unnecessary use of the system's material and human resources.

Multidispatch worksheet

Electronic system tool that requires mandatory fields to be filled out by the operator on an electronic form that may be simultaneously transferred to two or more response institutions.

Operator

The person in charge of receiving requests, calls, or reports, asking questions, categorizing the information, assessing the situation, and directing requests, calls, or reports to the appropriate dispatch institutions, based on established guidelines and procedures.

Ordinary worksheet

Electronic system tool that requires mandatory fields to be filled out by the operator on an electronic form to be sent to the dispatcher of a specific articulated institution (or first responder).

Prerecorded messages

Short messages, voice, or text, to communicate and inform the population about ongoing emergencies or scheduled/programmed events. One of the main reasons for using these messages is to avoid congestion of the line and other channels to report an emergency.

Prioritization levels

A categorization based on the estimated risk of requests, calls, and reports received by the emergency and security system. It is based on the characteristics and complexity of the incident or contingency, resulting in the prioritization of the response.

Process map

Graphic representation of the emergency and security system processes that makes it possible to identify and focus the attention on the processes considered critical to the system's operation.

Processes

A set and sequence of steps and actions to be followed in providing a service, accomplishing a task, or performing an activity. There are two types of processes: critical processes and support processes. Critical processes are a series of steps and actions taking place in the primary or mission-oriented functional areas of an emergency and security system, without which it would not be able to assist or respond to reported emergencies. Support processes are also a series of steps and actions, but these are carried out in the secondary or support areas and support the system's administrative functions.

Programmed events (also scheduled events)

Events the occurrence of which is known in advance and that require early activation of emergency and security systems to inform and communicate with the population about the status and evolution of these events and to prevent and act promptly in the light of possible incidents that may arise from the event.

Protocols

Normative instruments that establish what should be done and how to proceed and act in different situations/contexts. They contain a series of rules, instructions, and procedures to be followed in providing a service, fulfilling a task, or performing an activity.

Quality management

Management and organizational culture approach intended to satisfy users' requirements and needs through continuous improvement of the services provided by an emergency and security system based on international and national standards defined for such purposes.

Report

Verbal or written communication that describe the characteristics and circumstances related to an emergency.

Response resources

These are the resources deployed to assist and respond to an emergency, consisting of people, vehicles, and tools.

Risk analysis

A study to identify and evaluate potential hazards and threats, and to understand the potential consequences, effects, impacts, or damages, whether focused on planning, a project, a process, a service, personnel, or a facility, to establish prevention, protection, and mitigation measures. One of the tools typically used for risk analysis is the risk matrix.

Risk

A circumstance or event that in the face of a vulnerability has the potential to cause danger, damage, or loss and to threaten the operation of an emergency and security system. It is conceived as a combination of the probability of occurrence of a circumstance or event and its impact. It is usually the subject of analysis, which tends to be presented in matrices, and both (the analysis and the risk matrix) are used for risk management.

Risk management

Processes established and managed comprehensively for the identification, analysis of vulnerabilities, probability and impact, and design of responses to present and future emerging risk factors that could threaten the implementation of the strategic plan, the operation of an emergency and security system, the provision of services, the lives and safety of personnel and facilities. It could be part of or contribute to the quality management of an emergency and security system.

Risk matrix

A tool that allows for visualizing the probability of occurrence of contingencies, events, or casualties and their possible impacts on the emergency and security system, the implementation of its strategic plan, its personnel, its operations (processes and services), and its facilities, as well as the response strategies, including prevention, mitigation, and response measures. The matrix also facilitates monitoring, control, and risk management. It is linked to the risk analysis process.

Service delivery agreement

Contract or decision between the parties that constitute an emergency and security system, which defines the services to be provided by each of the entities and the standards that must be met to provide these services.

Strategic map

A tool used to visualize and monitor the cause-effect relationship between the objectives set and the strategic axes, plans, and components established as a result of the planning process.

Subsidiary actors (Third-ring institutions)

State agencies/institutions and other public, private, and civil society actors that participate in a complementary manner and seek to create conditions and capacities for the operation of an emergency and security system. Some examples of subsidiary actors are international agencies, civil society organizations, the business sector, the academic sector, and the media sector.

Supervisor (or Coordinator)

Person in charge of monitoring and controlling the activities carried out by the operators and/or dispatchers of the emergency and security system and the quality of the service provided, based on the established protocols and standards.

Supporting actors (Liaison institutions or Second-ring institutions)

State or private sector agencies/institutions and civil society groups that act as support entities and are vital in critical situations or to ensure the continuity of essential services. These may be entities in charge of specific segments of the population or specialized in specific issues, such as those related to the elderly, people with disabilities, and gender violence, among other sectors or issues needing priority or specific assistance; and entities in charge of providing essential services, including drinking water, electricity, food provision, education, among others.

User

A person requesting assistance in the event of an emergency, incident, or contingency that has occurred, is occurring, or is about to occur and who makes use of the services provided by an emergency and security system.

Video operator

Person in charge of monitoring and viewing the cameras in his/her charge, detecting and categorizing possible incidents that require immediate response or assistance, and analyzing, evaluating, and directing resources to provide such response or assistance.

Vulnerabilities

Weakness or diminished capacity of an asset, system, process, or tool that may represent a risk and be exploited by one or more threats generating a potentially harmful effect.

Prologue by the General Director of the ISS ECU 911,

Juan Zapata Silva

The strengthening of international cooperation in public security discussed during the Seventh Meeting of Ministers Responsible for Public Security in the Americas (MISPA VII), held in Quito in October 2019, was an excellent opportunity to disseminate and propose alternatives on a common topic: preventing and fighting organized crime.

The MISPA process - promoted by the Organization of American States (OAS) and with the participation of high-level security authorities and experts both national and international - introduces essential topics such as comprehensive security management; crime, violence, and insecurity prevention; police management; and citizen and community participation sustained by international cooperation. In the Seventh Meeting, for the first time since the creation of this forum of Ministers Responsible for Public Security Matters in 2008, emergency assistance and response were addressed, promoted by Ecuador through the Integrated Security Service ECU 911 (ISS ECU 911).

As Chair of the Subsidiary Technical Group on Emergency and Security Systems, resulting from the recommendations issued by the MISPA VII, I believe that the guide developed within the Group, as presented in this publication, is timely. It seeks to strengthen international cooperation regarding integrated emergency and security systems. The guide systematizes a series of guidelines, mechanisms, and tools available to all OAS Member States as technical suggestions, based on the practice and experience of all those who participated in its production.

During these difficult times, resulting from the global health crisis caused by COVID-19 and its multiple impacts, wherein emergency and security systems have played a key role, we hope that this guide will serve as a valuable and actionable tool to guide the creation or strengthening processes for this type of service within the Organization's member states.

The publication of this guide is the product of international cooperation. In that regard, we value the support and commitment of countries such as Costa Rica, Dominican Republic, Mexico, and Paraguay. Each of the countries that supported this initiative has provided the experiences of their emergency and security services, allowing us to transcend time regarding security matters by means of designing a technical-practical instrument that aims to suggest actions and establish mechanisms geared toward rationalizing the resources and logistics available to emergency and security services, to optimize the assistance provided to the population.

Having this guide and the possibility to share it with the other OAS member states opens the opportunity to share experiences and knowledge for addressing common emergencies and threats. It also provides a space for standardizing good practices regarding responses and interventions to safeguard and protect people's lives and integrity.

Thus, the commitment we undertook is ratified. We trust that in the short term we will be able to execute agreements that allow for establishing a single emergency number 9-1-1, in each country of the hemisphere, with standardized procedures for emergency response and coordination in the region.

Essential actions have been undertaken but many additional initiatives remain to be pursued to consolidate a continent with high levels of citizen security, peaceful coexistence, and public order.

Prologue by the OAS Secretary General, **Luis Almagro**

In the region of the Americas, there are several operational models for emergency and security systems. There are also various levels of progress in the region's countries with respect to the integration of services and interoperability, territorial coverage, the standardization of operating procedures, information and communication technological infrastructure, and IT support, among other aspects. Moreover, not all countries have a single number for handling calls for service.

This asymmetry and wealth of experiences within the hemisphere open an exciting and necessary multilateral area for work at the inter-American level.

The foundational event that incorporated emergency and security systems on the hemispheric security agenda and within the Organization was the International Seminar on Mechanisms and Tools for Regional Emergency Services Cooperation, organized by ISS ECU 911 in April 2019. On that occasion, a series of consensus proposals were presented, including creating a Subsidiary Technical Group on Emergency and Security Systems (STG-ESS) and preparing a Guide for the Establishment and Strengthening of National Emergency Systems within the OAS member states. These were later considered and adopted by the Ministers Responsible for Public Security in the Americas as part of the recommendations document they approved in their Seventh Meeting, held in Quito, Ecuador, in October 2019.

Based on these recommendations and within the framework of the Subsidiary Technical Group on Emergency and Security Systems (STG-ESS), with the leadership of the ISS ECU 911 and the technical support offered by the OAS Department of Public Security, the primary conditions necessary to enable the drafting of this guide were met.

This guide is intended for all countries in the region, either to create integrated national emergency and security systems or to strengthen existing ones. It is precisely due to the existing asymmetries and differences between countries regarding emergency assistance and response services that this guide hopes to make a contribution by reducing some of these gaps and promoting the best possible integration among systems.

The development of this guide is a milestone that deserves to be celebrated for several reasons. Firstly, because it is the product of the collaboration and coordination of five institutions: the 911 Emergency System of Costa Rica, the 9-1-1 National Emergency and Security Response System of the Dominican Republic, the Integrated Information Service ECU 911 of Ecuador, Mexico's National Information Center, and the 911 Emergency System of Paraguay, each of which contributed, from the standpoint of their knowledge and experience, by drafting between one to four chapters. Secondly, this guide was developed in the context of the most unprecedented pandemic in the last 100 years of human history, placing operators, dispatchers, first responders and health personnel in a situation of permanent alert and service, to try to save as many lives as possible. Despite this challenge and its associated responsibilities, these five institutions managed to create this guide. Thirdly, it represents a concrete, valuable and practical contribution for the other countries and systems in the region.

It may be defined as a regional public good that has been made available to everyone who works in emergency assistance and response so they can establish, improve, or strengthen the services they provide to the population.

Similarly, the production of this guide reappraises and enhances the existing collective areas of work as part of the operational and technical structure of the OAS. It is from these multilateral forums, populated by people with a vocation for service, capacity, experience, and knowledge, that it is possible to develop valuable reference products, such as this guide, for the use and benefit of all member states.

With Ecuador's leadership through the ISS ECU 911 and the creation of this guide, the Subsidiary Technical Group on Emergency and Security Systems is off to a promising and productive start. The OAS General Secretariat hopes this document will be one of many products that will guide the region's countries in maximizing their emergency and security systems' capabilities for the sake of greater quality, excellence, and professionalism when providing these services, aiming to achieve a scenario of greater cooperation and integration.

Presentation

The Guide for the Establishment and Strengthening of National Emergency and Security Systems in the member states of the Organization of American States (OAS) originated as a proposal from the Integrated Security Service ECU 911 (ISS ECU 911) of Ecuador. The proposal was presented within the framework of the International Seminar on Mechanisms and Tools for Regional Emergency Services Cooperation, which took place in the city of Quito, Ecuador, on April 25 and 26, 2019. At the time, an index proposal with ten chapters was presented, which was submitted for consideration by the participating delegations.

The International Seminar resulted in a consensus proposals document, in which the Subsidiary Technical Group on Emergency and Security Systems (STG-ESS) was entrusted with developing the guide.

The consensus proposals document was transmitted to the preparatory process of the Seventh Meeting of Ministers for Public Security in the Americas through the Hemispheric Security Committee. Thus, the proposals were incorporated in the Quito Recommendations for Strengthening International Cooperation in the area of Public Security, Preventing and Fighting against Transnational Organized Crime, which were adopted on October 31st, 2019. The 19 recommendations adopted by the Ministers Responsible for Public Security in the Americas on that occasion included the planning of the STG-ESS work by the Department of Public Security (DPS), with particular emphasis on the objective of completing the Guide for the Establishment and Strengthening of National Emergency and Security Systems in the OAS member states.

Thus, once the STG-ESS was established under the chairmanship of the ISS ECU 911, an initial planning meeting was organized on March 3, 2020, during which it was agreed that the DPS would prepare a Work Plan. On March 13, the DPS presented a Work Plan for the STG-ESS with four activities, including the development of the guide. Based on this proposal a decision was made to work collectively and collaboratively on the guide, inviting other Emergency and Security Systems and related institutions to participate in the process, drafting one or more chapters.

However, the assessment by the World Health Organization (WHO) that COVID-19 could be characterized as a pandemic on March 11 meant delaying the start of the guide's drafting process and redirecting the efforts of the STG-ESS to provide some response, assistance, and support to the region's Emergency and Security Systems in the fight against the coronavirus.

Faced with this new scenario, the ISS ECU 911, as chair of the STG-ESS, and the Department of Public Security, in its capacity as Technical Secretariat, took the initiative to create a Virtual Community. That community was created within the framework of the Educational Portal of the Americas so that Emergency and Security Systems' officials of the region could share, exchange, and consult existing materials that could be useful in responding to the public health emergency caused by the coronavirus. The Virtual Community of Emergency and Security Systems (ESS-Community), in turn, was accompanied by a series of virtual discussions. In 2020, as part of that series, four virtual events were organized for Community members on issues related to the pandemic.

Development of the guide resumed in June 2020. Thus, on June 8, representatives from Costa Rica, Dominican Republic, Mexico, and Paraguay, linked to emergency assistance and response, were invited to participate in the drafting of the guide and asked to choose one or more chapters to develop. In this way, the guide's ten chapters were distributed among them.

On June 19, a coordination meeting between the ISS ECU 911 and the DPS/OAS was held. In that meeting, the allocation of the ten chapters among the five participating institutions was presented: 911 Emergency System of Costa Rica was responsible for Chapter 1; the 9-1-1 National Emergency and Security Response System of the Dominican Republic selected Chapters 2, 3, 8, and 10; the Integrated Security Service ECU 911 took on Chapters 5, 7, 8 and 9; Mexico's National Information Center decided to work on Chapters 4 and 8; and the 911 Emergency System of Paraguay dealt with Chapter 6.

At that meeting, the DPS made a series of proposals for consideration by the ISS ECU 911, including a seven-stage plan, covering the months from July 2020 to May 2021, and general guidelines to develop the guide, covering aspects such as the approach/perspective that could be adopted, the format, the writing style and how to save the drafts, among others. Additionally, a shared folder was created on Google Drive, giving access to all those involved in the production of the guide. All documents related to the guide's development were made available in that shared folder, including the general and planning guidelines and successive versions of the chapters.

Once the ISS ECU 911 endorsed the proposals made by the DPS/OAS, they were presented to the participating institutions at a planning meeting held on July 1, 2020. That meeting can be considered the starting point of the guide's collective and joint production process, thus activating its first stage. As part of the first stage, individual meetings were held with the five participating institutions. These meetings were held to review the index of the assigned chapter(s), reach agreements on the contents expected to be covered in each chapter, review general guidelines, and answer questions that the teams may have had regarding the guide and the production process.

The second stage of drafting the guide's chapters covered the period between August 2020 and January 2021. This stage included several back-and-forth communications between the institutions drafting the chapters and the reviewing and editing team in the Department of Public Security. The Information and Knowledge Section Chief and an external consultant with extensive and recognized experience and knowledge on the subject made up the DPS reviewing and editing team.

Once a first draft of the guide was obtained, an internal review process was organized with the participating institutions themselves (third stage). Having read the entire guide as an integrated product, each country team could share and submit their comments and suggestions on the first draft.

The third stage of revision was followed by a fourth stage of validation, which consisted of submitting the first draft of the guide to EENA and NENA Mexico-Latin America scrutiny. In addition to receiving their comments in writing, two working meetings were organized with two representatives of the organizations mentioned above to give virtual feedback to all the participating institutions. In this way, an opportunity was created for exchange and learning among all those involved.

After all the contributions resulting from the review and validation stages were incorporated, the second draft was produced. This second draft went through a brief editing stage (fifth stage) and was promptly channeled to the sixth stage of translation, layout, and design.

Once the tasks of the sixth stage were underway, the guide was presented to the OAS member states at the First Meeting of the Subsidiary Technical Group on Emergency and Security Systems, chaired by ISS ECU 911. The meeting took place virtually on May 6 and 7, 2021, through the KUDO Platform. The drafting teams of the 911 Emergency System of Costa Rica, the 9-1-1 National Emergency and Security Response System of the Dominican Republic, Mexico's National Information Center, and the 911 Emergency System of Paraguay also participated in the panel. The EENA and NENA Mexico-Latin America representatives and the external consultant who accompanied and provided technical support throughout the guide's entire production process were also present.

Having been well received by the member states and highlighting the fact that the guide was a jointly developed product, based on the coordination, participation, effort, and experience of the region's Emergency and Security Systems and related agencies, the final version of the guide was published in digital format.

This is the product presented below.

Introduction

Implementing strategies and concerted actions to promote and strengthen the capacities needed to provide quality emergency and security services and increase their effectiveness is a recent objective in the hemisphere. This objective arises in response to the population's growing demand for protection and response from the agencies responsible for providing assistance, both in frequent incidents and daily contingencies, and in situations of greater danger and complexity.

A necessary starting point is to recognize security as a public good. This is a unique challenge based on the urgent need to promote conditions, processes, and mechanisms to reduce the gaps between security and insecurity, protection and vulnerabilities, justice and the effective exercise of rights, and impunity and peoples' defenselessness, among other dimensions.

In times of crisis and profound transformation, the need to design and rely on systems to protect people and provide them with more effective services forces a shift in the paradigms used until now. It also creates a need to innovate in the design of public services, particularly concerning the interaction among authorities, institutional actors, and users or beneficiaries. This represents an opportunity to encourage and enhance cooperation among OAS member states.

This guide arises from the need to make a set of guidelines and recommendations available to the OAS member states based on the experiences and lessons learned in the hemisphere, whether to install or strengthen capacities in emergency prevention, preparedness, and response, incidents associated with public and citizen security, as well as situations of greater magnitude and complexity. All these situations require different types of coordination and collaboration among immediate response institutions and, in some cases, the additional support of specialized institutions.

The public and critical nature of the work explains the need to promote joint action by public authorities at different levels and in different contexts, confronting obstacles and improving emergency assistance and response conditions, including those related to security, which may be conceived as a vehicle for achieving a better quality of life. This requires the approval of laws, the allocation of resources, and the design and implementation of public policies and programs that support this type of service.

At the hemispheric level, support came from the Subsidiary Technical Group on Emergency and Security Systems (STG-ESS). It took shape in this Guide for the Establishment and Strengthening of National Emergency and Security Systems in the OAS member states. The guide presents systematized guidelines and recommendations, organized in ten chapters, answering a wide range of questions. This objective has been achieved in a short period of time and the results have been endorsed in this guide.

The topics in this guide are approached from a political-strategic perspective, to shed light on and guide decision-making regarding the design and operation of an emergency and security system. It is not a handbook that explains how to do things nor a single recipe with ingredients and steps to be followed in a rigid and unilinear manner. It is presented as a consultation and reference tool, with guidelines and general observations on components, areas, processes, and tasks that should be taken into consideration in the creation, strengthening, and sustainable operation of this type of service.

Regarding the creation and establishment of an emergency and security system as outlined in **Chapter I**, a shared confirmation is the relevance of a systemic, integrated, and joint responsibility approach on horizontal cooperation and coordination. The system's governance is a driver and, at the same time, the strategic axis of an adequate institutional and organic design.

Without a vision and strategic planning of public services like that presented in **Chapter II**, it will hardly be possible to provide timely and quality assistance when requested by people at risk. The configuration of an effective model during the design of an emergency and security system involves choosing between different operational alternatives, which vary in structure, mechanisms, integration levels, and areas of collaboration among articulated (first response) and related (complementary) institutions. These questions and decisions intrinsic to the design stage of an emergency and security system are introduced in **Chapter III.**

This means focusing on reducing one of the main weaknesses observed, namely -in some cases- the insularity of organisms, the asymmetries, and gaps in effective capacities, and strengthening those decisive factors that form the basis of information and communication interoperability. There is no doubt that this challenge goes beyond improving coordination; it also involves efforts to integrate existing subsystems, the planning of interoperable technological and information architectures, sufficient infrastructure and resources, coverage and units in the various territories, among other elements.

Comprehensive quality management in an emergency and security system as outlined in **Chapter IV** seeks continuous improvement to provide users with a professional and effective service in a sustained and uninterrupted manner. It involves process maps, measurement, monitoring, evaluation, review of quality standards, and the implementation of improvements required to make the service provided more efficient, effective, and satisfactory.

The development achieved in information and communication technologies makes it more likely that the OAS member states will have tools that make processes more efficient. However, among the operational areas, call management and incident response are essential functions that merit special attention with continuously updated and validated protocols, procedures, and standards. For this reason, **Chapter V** of this guide focuses on receiving, handling, and responding to requests, calls, and reports entering the system. In this area, collective intelligence, organizational engineering, and the exchange of experiences and lessons learned become indispensable.

As the experiences on state modernization show, management of human talent involves a critical effort to increase the main asset of any public organization. For this reason, in this guide, **Chapter VI** puts particular emphasis on lines of action to ensure the professional quality of staff, from recruitment and selection to induction and continuous training, to evaluation and departure. It also focuses on employees' well-being through a series of criteria focused on promoting occupational health and safety and creating a safe and healthy work environment.

Information management is considered a leading process for the system's strategic objectives and the preparation and guidance needed for service delivery. For this reason, in **Chapter VII**, information management is linked to the organizational strategy and the levels of operation of an emergency and security system. As information is one of the main assets of this type of system, the suggestion is to also have a cycle of processes to optimize a series of stages related to obtaining, organizing, storing, distributing, accessing, and using this resource to develop products that support decision-making in the various bodies and instances associated with interoperability flows in handling and responding to emergency requests, calls, and reports.

In a system that handles and responds to emergencies, security management must be approached from a multidimensional perspective, paying particular attention to both the conditions for the operation of an operational center and the continuity of services. For this reason, **Chapter VIII** not only suggests courses of action to protect information, communications and computer systems, and to ensure physical, infrastructure and personnel security, but also addresses the analysis and management of risk. To this end, the chapter presents guidelines for developing at least two essential tools: continuity of operations plans and disaster recovery plans.

A central element in emergency management as well as during high-intensity incidents or large-scale crises is communication management, both institutional and operational. To address these situations, **Chapter IX** outlines the minimum elements that need to be considered when preparing a communication plan. This plan serves as a roadmap for managing communications using different channels and tools, including spokespersons, networks, traditional and social media, engagement with the population and communities, and prerecorded messages. Toward the end of the chapter, some guidelines are also suggested to guide crisis communication planning and preparedness.

Finally, **Chapter X** focuses on the transparency and accountability of an emergency and security system as pillars for democratic governance, integrity, and the quality of the service being provided to the population. They are presented simultaneously as principles or values to be enshrined and strengthened, objectives to be achieved, and processes to be followed.

Transparency and accountability are not add-ons or afterthoughts but need to be envisioned as part of the strategic planning process and organizational communication. The chapter proposes a series of tools and mechanisms to proactively provide information on the system's operation, management, and results and to facilitate access to the information produced.

!

Note on the use of inclusive language -in the Spanish version-: The use of terms such as "operator", "dispatcher", "video operator", "supervisor" and other nouns and articles in masculine, does not respond to discriminatory stereotypes, they only seek to facilitate the reading of the document.

CHAPTER

01

CREATION AND ESTABLISHMENT

Introduction

This chapter presents the essential elements for the creation of an emergency and security system, including (a) political and institutional support at the highest level, (b) a legal instrument that defines its purposes, its position within the structure of the State, institutions that comprise it, responsibilities and functions, services it would provide, resources it would have, among other foundational elements, and (c) financing.

Additionally, the chapter presents different types of anchoring and institutional positions that emergency and security systems could have, which would affect their legal, administrative, financial, and operational autonomy.

At least three types of actors could be considered as part of the structure of an emergency and security system. The chapter emphasizes the need for coordination and cooperation among the actors, advocating for a systemic approach that allows the parties to collaborate to deliver high quality and socially valuable products and services. Another element referred to in the chapter is the three levels at which a system could function.

The governance of an emergency and security system could be completed with the creation of an Inter-institutional or Intersectoral Commission or Committee and the appointment of an Executive Director (or similar position). In line with the levels of operation of a system, the first would be more focused on the strategic direction while the second would be responsible for tactical and operational issues.

1.1 Institutional and political support

To create an emergency and security system, willingness, leadership, and political support at the highest level are essential, guided by a vision of what type of system is being created and how to create it. This would have to be expressed in political-technical consensus and inter-institutional agreements, including service delivery agreements (public/private).

It would also be important to have the involvement of all entities deemed necessary based on their direct and indirect role in emergency response and assistance. From the outset, this involvement should be intended to generate a common identity, a feeling of ownership, and the empowerment of those who are part of the system. Likewise, it would help lay the foundations for coordination and collaboration among the member institutions, among other benefits.

The decision of the member institutions to be part of this type of project would have to be based on a shared conviction, such as the need to provide the population with an integrated system of emergency services to protect and save lives.

1.2 Legal foundations and regulatory framework

The most frequent legal instruments with which emergency and security systems have been created in Latin America have been laws and executive decrees.

These instruments outline powers and responsibilities, functions, and roles, as well as supra- and inter-institutional units for the coordination of institutions, bodies, and any other national and subnational entity related to the products and services delivered by an emergency and security system.

The ideal legal instrument for creating an emergency and security system would be a law, due to the legislative and executive support that it would represent, in addition to the fact that it would be a higher-ranking provision.

Additionally, it might be necessary to establish agreements between the participating institutions that define, at a minimum, the guidelines for coordination, collaboration, co-production, and shared responsibility.

In any case, the legal instruments used to create an emergency and security system would have to explicitly specify the mandatory participation of the institutions involved in emergency response and assistance in each country.

1.3 Institutional anchoring

The position of the emergency and security system in the State's structure will depend on the degrees of federalism, regionalism, centralization, and concentration in the administration, and the fiscal budget.

The emergency and security system could be created as a body attached to a state entity, whether pre-existing or not. The system's legal, administrative, financial, and operational autonomy will depend on that state entity.

One possibility is for the system to remain under the responsibility of an Executive Branch entity, in the public security sector, at the highest level, such as a Ministry of the Presidency, the Interior, Government, or Security. Another possibility is for it to remain attached to an Executive Branch institution but with legal, administrative, and financial autonomy.

A third possibility is for the emergency and security system to be established under the protection of a decentralized public institution.

In any anchoring scheme, the normative instrument would have to fully establish the powers, responsibilities, attributions, and functions that would be assigned to the components of the system, as indicated in Section 1.2 of this chapter, taking into account the types and magnitudes of emergencies.

It is recommended that the system not be attached to a preexisting entity, so as to facilitate coordination and collaboration among the member institutions, as well as impartiality and uniformity in operational activities.

1.4 Ideation

Based on a strategic vision, the system could be conceived as a public policy or an instrument of that policy, a management model, or a network of cooperating entities for the delivery of emergency services. This service network would have to respond to the need to improve interoperability among its component parts through integration and added value. For this reason, the system's configuration would also require adopting a systemic approach to achieve efficiency, comprehensiveness, and quality of service.

The emergency and security system could be strategically constituted as an institution articulated and operating with other institutions, in a context of interoperability, to respond to incidents and emergencies that affect the population.

Its strategic objectives should be geared toward benefitting collective interests and achieving more significant impact and quality in the services provided to the population.

By nature, the entity that is eventually formed would need to work as an organic whole, regardless of the responsibilities and tasks assigned to each of its parts. All of them would have to act in an integrated manner, contributing with their skills and resources to achieve a common goal seeking not individual objectives for each institution but rather collective ones related to the provision of effective and quality emergency services.

1.5 Structure

The emergency and security system created would have to be reflected in a structure that represents an opportunity for seeking synergy among the member institutions at the national and subnational level.

The structure of an emergency and security system could be thought of based on three types of actors:

- Primary actors (or articulated institutions or first-ring institutions)
- Supporting actors (or related institutions or second-ring institutions)
- Subsidiary actors (or third-ring institutions)

1.5.1 Primary actors (or articulated institutions)

Primary responders would be responsible for carrying out essential functions in an emergency and security system. These essential functions would include the following:

- Receiving, processing, and answering emergency requests, calls, and reports, and coordinating responses, in emergency situations, with coverage throughout the country.
- Enabling and maintaining multiple means of communication between users and the emergency and security system, including mobile and land lines, text messaging (SMS), applications, help or panic buttons, and social media, among others.
- Serving as a Coordination, Command, Communication and Control Center for Emergency Response and managing the video surveillance monitoring centers.
- Preparing, updating, and validating joint action and assistance protocols.
- Developing and maintaining high availability technological and communications infrastructure for the coordinated provision of services.
- Serving as an operational entity for the national risk and disaster management system, when appropriate.
- Maintaining a background registration system for the traceability of cases and the analysis of procedures, management audits, and the measurement of the effectiveness of services as well as periodic accountability exercises.

According to the types and magnitude of the event(s), the first-ring institutions are the ones that would provide the essential response services. Among the different types of emergencies, the following are to be noted:

- Transit and mobility:
  First responder institutions would be in charge of answering emergencies related to vehicular traffic issues or traffic problems on the country's roads.

- Citizen/public security:
  First responder institutions would be in charge of answering emergencies related to preventing and mitigating crime, preserving security, and maintaining public order.

- Health (physical and mental) care:
  First responder institutions would be in charge of answering emergencies related to events that threaten people's lives and health.

- Fire and incident management:
  First responder institutions would be in charge of fire prevention, fighting, mitigation, control, investigation, and evaluation. They would also be responsible for rescuing trapped or lost people.

- Disaster risk prevention, preparedness, and response:
  First responder institutions would be in charge of preparing, mitigating and responding, coordinating, and managing emergencies caused by small, medium, and large-scale disasters, including earthquakes, floods, hurricanes, cyclones, pandemics, or others.

1.5.2 Supporting actors (or related institutions)

According to the types of emergencies and the requirements of specific groups in situations of vulnerability and/or critical risk, first responder institutions may also need to coordinate with other state agencies as well as civil society associations. These would act as support entities. Their participation is vital for the management of critical situations or for ensuring the continuity of essential services.

The spectrum of entities available to provide sectoral services could be broad or narrow, depending on the institutional engineering of each country, coordination needs, and the circumstances of each situation:

- Entities at a national, sub-national, regional, and local level in charge of directing and implementing plans and programs such as Ministries, Technical Secretariats, Departments, Directorates, Special Commissions, and municipalities, among others.

- Entities in charge of specific population segments, including children, women, the elderly, people with disabilities, and minorities, among others.

- Entities in charge of assisting tourists and foreign nationals such as those that provide multilingual assistance and guide people who visit and stay temporarily in the country and people with an immigration status different from citizens or residents.

- Entities in charge of providing essential services, including drinking water, electricity, food, education, and health, among others.

1.5.3 Subsidiary actors

There is a third type of actor that could be called subsidiary entities, which would seek to generate conditions and capacities for the operation of the system. International organizations, civil society organizations, the business sector, the academic sector, and the media sector, among others, are some examples of subsidiary entities with which agreements could be signed or specific supports could be negotiated to contribute to the improvement of emergency services.

1.6 Levels of operation

There would be at least three levels of operation that would need to provide continuous feedback to each other for the provision of emergency services:

- Strategic level:
  Where long-term objectives and interactions with other entities are determined and where decisions that affect the system, its organization, and its structure are proactively made, with a view to the future and the sustainability of services.

- Tactical level:
  Related to the development and execution of action plans for service areas and core activities; and the coordination, supervision, and (quantitative and qualitative) evaluation of operations and goals to be met. This level consists of a series of internal processes that provide support for the system's operation

- Operational level:
  Related to the execution of services, activities, and routine operations established in the action plans.

In some cases, the tactical and operational levels could be merged.

1.7 Coordination and cooperation

First responder entities (first ring), supporting entities (second ring), and subsidiary entities (third ring) would need to align themselves around shared purposes, objectives, and goals within the framework of strategic planning (see Chapter II of this guide).

The system's proper operation would also require coordination and cooperation among the component entities, to provide a quality service with public value.

Work among these entities, particularly regarding first responder entities, should be based on a dynamic of horizontal cooperation among peers, with communication channels and flows, and mechanisms to facilitate the exchange of resources, information, ideas, and personnel.

Each of the entities' specific regulations would have to be respected, assuming they all operate under the same or similar conditions. Additionally, all of them would have to respect and adhere to the emergency and security system's regulations. The latter could be considered complementary, contributing to creating a common identity and purpose, and generating a work environment based on collaboration to provide a public service.

Coordination and cooperation among the entities that make up a system could assume different modalities:

- Collaborative and thematic networks
- Horizontal peer collaboration
- Promotion of mechanisms for sharing information and knowledge (systematized experiences and good/promising practices)
- Collaboration in design and evaluation processes
- Creation of effective alternatives for the exchange of research findings or products
- Promotion of public-private partnerships, and agreements with universities and international organizations
- Periodic training sessions and specialization courses
- Cooperation in the development of human talent and career paths, among others

1.8 Strategic targeting

As part of the governance and operation of the emergency and security system, it would be advisable to include the establishment of an Inter-institutional or Inter-sectoral Commission or Committee as part of the legal instrument that establishes its creation.

Meeting periodically, and in special sessions whenever necessary, the Commission or Committee could have some of the following functions:

- To define and approve inter-institutional processes, policies, procedures, and protocols.

- To supervise compliance with the guidelines defined as necessary so that the emergency and security system and each member institution meet the objectives established by law.
- To establish parameters and ensure quality and efficiency in the handling of emergency requests, calls, or reports.
- To establish the service quality parameters (quantitative and qualitative) of the emergency and security system from the moment the assistance request, call, or report is received until the moment when the emergency incident ends.
- To create the commissions it deems necessary for its proper operation.

In some cases, this body could exist temporarily to lead and monitor the design and installation of an emergency and security system. In others, it could be established to supervise the emergency and security system once it is installed and in operation. In this second scenario, it would assume a more permanent character.

This Commission, depending on its position and legal status, could be made up of the heads of the entities that comprise the system and be chaired by the highest authority of the corresponding Ministry.

The powers and prerogatives of the Commission must be established by law, together with the supporting regulations that may accompany it.

1.9 Executive Director (or similar position)

The legal instrument that establishes the emergency and security system would have to define the selection process and the profile for an Executive Director's position, according to the existing hiring framework for public officials in each country.

The Executive Director is responsible for the operational-tactical execution of service delivery. Therefore, it is considered appropriate that the position profile would incorporate the skills, abilities, knowledge, and experiences necessary for the management of an emergency and security system.

The selection process could be carried out within the framework of a public tender. It would have to be aligned with:

- A technically defined skills profile in the field of security, risk, and disaster management.
- The professional experience necessary to lead a strategic, tactical, and operational process.
- The probity required of all civil servants.

1.10 Financing and sustainability

Financing would first have to consider resources for the creation and establishment of an emergency and security system, which could come from a loan or international cooperation agreement. Funds would then be required to guarantee the system's functions and the continuity of its operations. These funds could come from at least two sources: a national budget (annual or multi-year) and an additional specific tax.

Given that the system's financing relies on fiscal resources, it would be dependent on the application and execution of each country's Public Sector Budget Act (or similar instrument). The resources would be subject to a control, audit, or oversight process.

One of the guiding criteria regarding the financing of systems of this type is that they do not depend on a single source but rather rely on a combination of multiple sources.

In line with the above, an additional source of funding could come from selling the system's services, subject to the requirements and conditions established in the legislation stipulating its creation and operations.

CHAPTER

02 STRATEGIC PLANNING

Introduction

This chapter presents strategic planning as a tool and as a process. As a management tool, the minimum components are presented. As a process, its standardization and institutionalization are accomplished by defining protocols, procedures, and instruments. The latter are presented based on the three stages inherent to the planning process: pre-planning, planning, and post-planning.

If planning is conceived as a tool, what results from the planning process is a strategic plan. On this point, the chapter focuses on making explicit the assumptions under which the plan will be implemented, identifying the critical factors for success, and analyzing the risks that could hinder and even impede the achievement of the established objectives and goals.

Strategic planning is presented in this chapter as a different tool compared to traditional planning. The former focuses on addressing the most significant medium- and long-term challenges, incorporating predictive analysis, considering possible future scenarios, and adapting to internal and external changes that an emergency and security system might experience.

2.1 Strategic planning

The strategic plan could be considered a management tool that brings together a set of goals, objectives, and activities established by an organization, with a view to achieving them within a specified period of time. It could also be considered a product that results from the culmination of a planning process, commonly known as a project or plan. All functional areas, the highest decision-making levels, and key actors of an emergency and security system would have to be included in this process. Throughout the process, it is important to encourage strategic thinking as well as to gather information and valuable propositions for establishing the objectives.

This exercise could be carried out by the planning and strategic management department of the emergency and security system itself and/or with the support of an outside consulting firm with extensive and recognized experience with this type of exercise.

The planning process would be subject to the specific context of each emergency and security system. However, like any critical process, for its operation and sustainability, it would have to be properly standardized and defined by a series of procedures, steps, and tools that could be carried out continuously and systematically.

2.2 Fundamental components of a strategic plan

The essential components of a strategic plan should be the following:

Vision:
Long-term definition of what the entity intends to be. It is how the entity sees itself in the future. It is the reference that guides the system to achieve the desired objectives. It usually relies on emotions and serves as a motivating force.

Mission:
Describes the fundamental objective of the entity, establishing its purpose and actions to achieve the vision. A mission statement is a fundamental tool encouraging the team to achieve the objectives and goals by providing them with a clear sense of direction and strategic intent.

Values:
Beliefs, virtues, or qualities based on which the entity is governed. They reflect its standards, evoke its essence, and express its identity. The values of an emergency and security system should reflect and be consistent with its purpose. Some of the values that could inspire the actions of an emergency and security system are honesty, loyalty, solidarity, respect, collaboration, responsibility, transparency, confidentiality, and a vocation for public services. These values should be reflected in the

Code of Ethics and Code of Conduct intended for the entity's personnel (see Chapter VI of this guide).

- Objetives:
  Measurable results that the entity wants to achieve; they could be short-, medium-, and long-term, as well as intermediate and final.
- Strategies:
  Roadmap that combines plans and means to achieve the established objectives.

2.3 Guiding principles

The guiding principles could be considered essential benchmarks or indications that govern the performance of an emergency and security system and must be consistent with its objectives and values. They should also strike a balance between what is done (objectives) and how it is done (functions). The principles could be based on:

- International human rights guidelines
- National legal framework for the protection of peoples' and property rights
- The legal and normative framework that supports the creation of the emergency and security system
- The legal framework and the principles of the articulated and related entities

The guiding principles would act as a form of roadmap so that decisions and actions can be carried out in line with the entity's vision, mission, and values, ensuring the well-being of personnel and users who require the services of the emergency and security system.

Some examples of guiding principles are presented below:

- Non-discrimination based on race, color, sex, gender, language, religion, political or other types of opinions, nationality, economic or social position, or any other social condition
- Impartiality
- Cooperation and coordination
- Integration and interoperability
- Accessibility through a single number
- Care provided free of charge

These guiding principles must be expressed in the Code of Ethics and Code of Conduct drafted by the emergency and security system (see Chapter VI of this guide).

2.4 Definition of strategic axes

The strategic axes are the fundamental areas or dimensions that guide all the operations of an emergency and security system. They establish the broad lines of action and help to keep the focus on essential issues. Some examples of strategic axes would be operational excellence, institutional strength, and institutional coordination.

Each axis could be accompanied by a brief description that outlines clearly what it means. Thus, the operational excellence axis could be presented as follows: "Make continuous improvements in processes, systems, infrastructure, and development of human talent to increase the system's levels of quality, efficiency, effectiveness and, as a result, user's satisfaction" (National System of Emergency Answering and Response and Security 9-1-1, 2020).

After establishing the strategic axes, it would be necessary to define the strategic objectives for each of them. In general terms, they should be directed toward guiding and consolidating the actions needed to achieve the expected results.

Table 1: *Example of table for the definition of strategic objectives*

AXIS	STRATEGIC OBJECTIVES	DESCRIPTION
I. Operational Excellence Make continuous improvement in processes, systems, infrastructure, and development of human talent, to increase the levels of quality, efficiency, and effectiveness of the system, and with it, the satisfaction of users.	I.1 Foster a process-based quality management culture.	Effective management set-up, aligned with the vision and focused on integrated processes, for the purpose of creating and maintaining a work culture in line with sustainable quality and the organization's values.
	I.2	
	I.3	

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

2.5 Definition of strategies

Strategies would have to be defined to achieve the proposed objectives. These could be conceived of as actions or activities aimed at achieving the established objectives.

Table 2: *Example of table for the definition of strategies*

AXIS	OBJECTIVE	STRATEGY
I. Operational Excellence Make continuous improvement in processes, systems, infrastructure, and development of human talent, to increase the levels of quality, efficiency, and effectiveness of the system, and with it, the satisfaction of users.	I.1 Foster a process-based quality management culture.	I.1.1 Standardize processes, defining technical standards and procedures for the: Radiocommunication operating model Electrical standard I.1.2 Quality and security integration, by establishing service level agreements with response agencies.
	I.1.	I.1.3. I.1.4. I.1.5.

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

2.6 Action plans

Action or operational plans could be defined as planning products and/or programs framed within the context of a strategy, geared toward achieving objectives, outlining the roadmap. They would also be management tools that could be used to organize, implement, and monitor the tasks necessary to achieve the established objectives. A strategy could be part of one or more action plans.

2.7 System of Indicators and Targets

An essential element of strategic planning would be to measure the degree to which the institutional objectives are met. Thus, in connection with any strategic plan, a set of monitoring and result indicators of the parameterized objectives would also have to be defined. The definition of an indicator would include a description, the unit of measurement, and the calculation formula.

To know whether the established objectives have been met or not, it would first be necessary to establish a baseline against which to compare them.

Table 3: *Example of a system of indicators and targets*

					BASE LINE	TARGETS			
INDICATOR	DESCRIPTION	UNIT	CALCULATION METHOD	ALIGNMENT WITH STRATEGIC OBJECTIVES	BASE YEAR	YEAR 1	YEAR 2	YEAR 3	YEAR 4

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Additionally, it would be necessary to define the frequency with which the indicators would be calculated and, if possible, assign their measurement to the quality management control area. These indicators and targets would also have to become an essential part of the information and technological architecture of the emergency and security system (see Chapter III of this guide.) Having this information updated on an ongoing basis and, if possible, automatically, would make it possible to know whether the strategic objectives of the plan are being met and to make any necessary adjustments along the way.

Responsibility would also have to be assigned for each strategic objective. This assignment of responsibility could rest with a department, unit, team, or individual.

2.8 Budget

Activities related to achieving the system's mission and objectives would have to be accompanied by resources allocated from the budget plan. It is important to differentiate between two types of resources. First, there are annual resources intended to provide users with emergency services and cover operating costs. Second, there are resources allocated to human talent management, infrastructure development to increase coverage in the medium term, or to strengthening the quality management control system. Without this second type of resource, it is almost impossible to execute the strategic plan. Budget execution would have to be consistent with the action plans or programs designed to achieve the system's goals.

Criteria for prioritizing and targeting resources would be critical to budget allocation geared toward development of staff capacities and the technological, functional, and administrative strengthening of the functional areas (see Chapter III, Section 3.2). Likewise, based on these criteria, preference could be given to projects and programs with more significant social impact and institutional value and lower costs.

2.9 Some tools for strategic planning and its execution

Strategic planning would be more advisable than traditional planning as the latter is not designed to respond to significant long-term challenges.

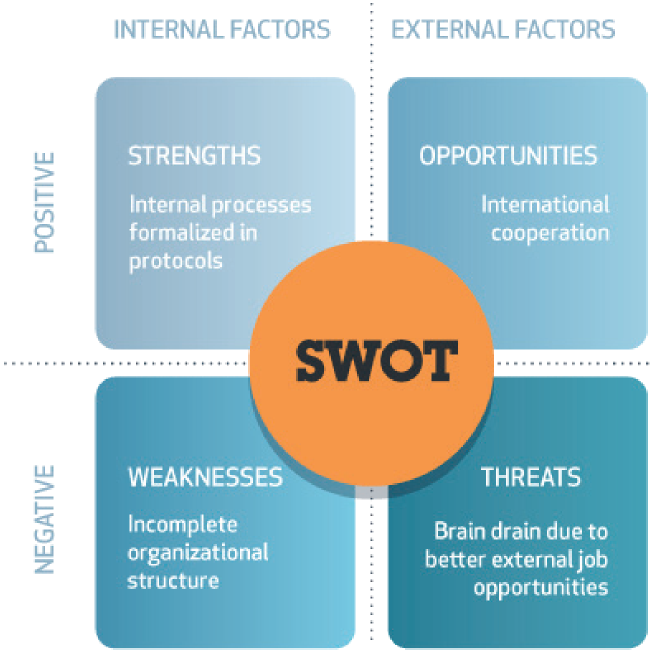
Strategic planning would consist of constructing, developing, and implementing the different action or operational plans the entity would need to formulate to achieve its vision, mission, objectives, and targets.

The strategic planning process could use various tools throughout its development cycle, considering at least three stages: the pre-planning stage, the planning stage, and the post-planning stage.

2.9.1 Pre-planning: SWOT Analysis

As part of this stage, it would be helpful, as an assessment, to identify strengths and weaknesses of the emergency and security system, as well as opportunities and threats related to the services it provides. This exercise could be performed with the SWOT analysis tool.

Figure 4: *SWOT example*


INTERNAL FACTORS
EXTERNAL FACTORS
POSITIVE
NEGATIVE
STRENGTHS
Internal processes formalized in protocols
OPPORTUNITIES
International cooperation
SWOT
WEAKNESSES
Incomplete organizational structure
THREATS
Brain drain due to better external job opportunities

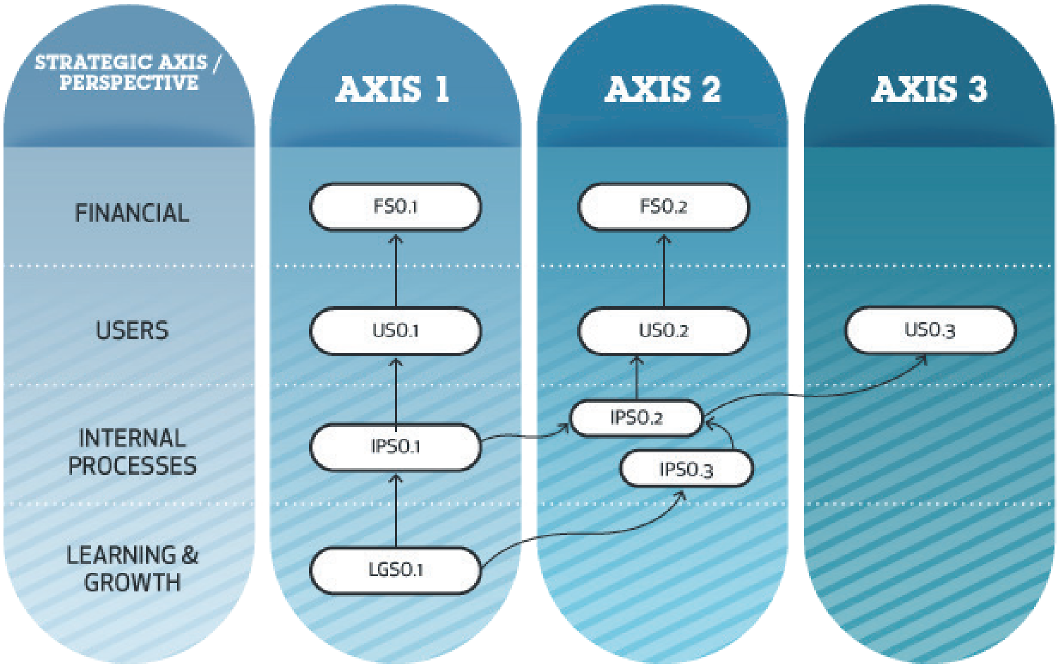
Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

2.9.2 During planning: Strategic Map

A strategic map could visually represent the cause-effect relation between the strategic axes, the established objectives, and the plans and components resulting from planning. A single image could show how public value could be added to the services provided by the emergency and security system.

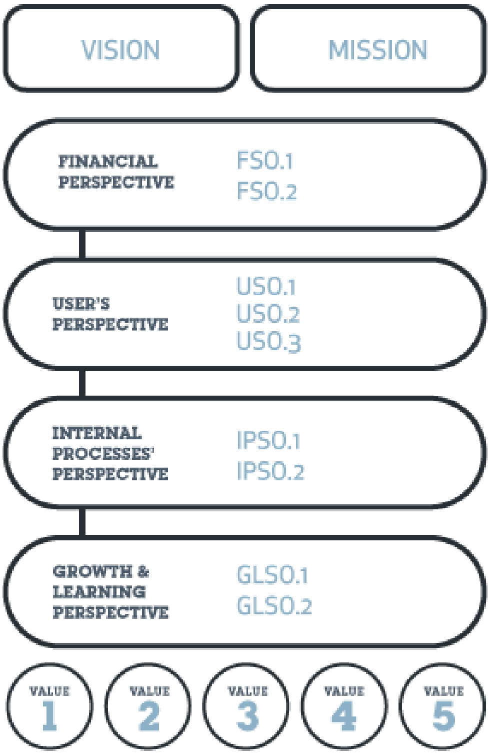
There are several ways to draw strategic maps. Two examples are presented below:

Figure 5: *Strategic Map, Example 1*



Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Figure 6: *Strategic Map, Example 2*



Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Example 1 shows that it is possible to graphically visualize how the strategic objectives interrelate in a cross-cutting manner among the different axes.

In both cases, the strategic map would facilitate tracking of the objectives across the four perspectives in the Balanced Scorecard: financial, user, processes and, finally, learning and growth. It would be advisable to use the strategic map as a tool because, among other advantages, it would help detect possible inconsistencies among the objectives, as well as quickly identify strategies that lack objectives and thus be able to eliminate them.

2.9.3 Post-planning: Balanced Scorecard (BSC)

The Balanced Scorecard (BSC) methodology is helpful for operational strategic management. It is a tool that can be used to monitor and manage strategy implementation, achievement of objectives, attainment of results, and measurement of indicators.

The information it generates is usually easy to understand, communicable, and actionable. Based on this information, the emergency and security system could reformulate and adjust its strategy, improve its analytical capabilities, and reviews its performance.

The Balanced Scorecard (BSC) would facilitate analyzing the entity from various perspectives or points of view.

The traditional BSC has four perspectives:

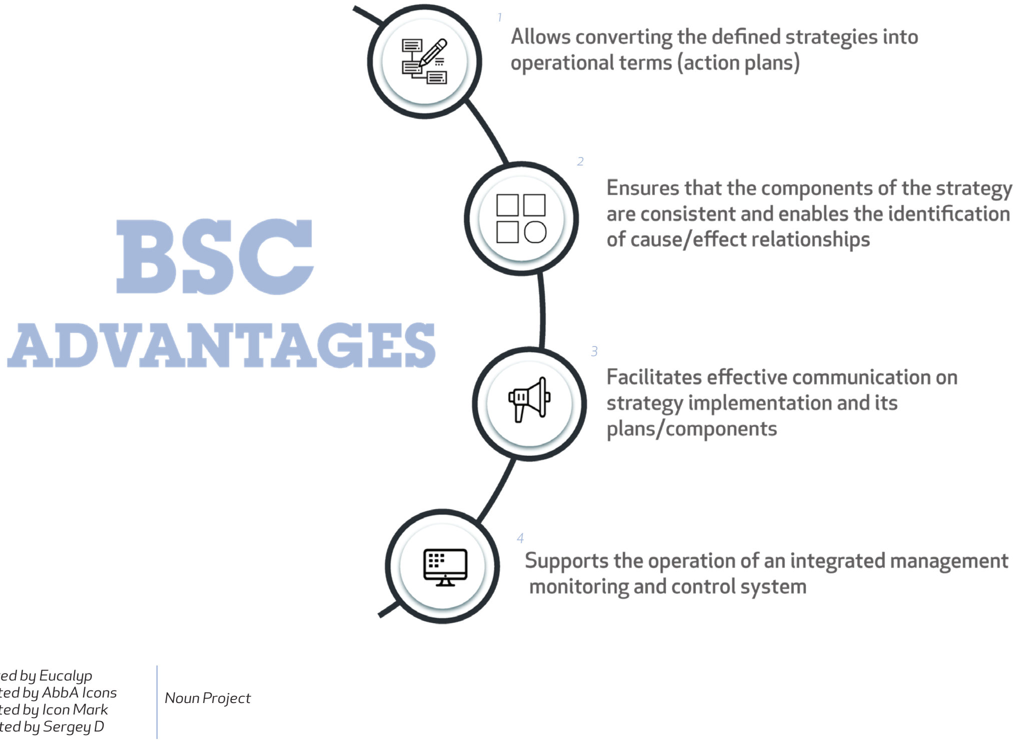
User:
How to strategically position the entity's products and services to satisfy users' needs and meet their expectations.

Internal processes:
Identify and improve critical processes within the entity. Key processes would have to be aligned with the strategic objectives. Efforts would focus on the effectiveness of those key internal processes.

Financial:
From this perspective, the focus would be on the adequate and timely allocation of resources and the minimization of costs.

Learning and growth:
The focus would be on human talent development and strengthening personnel's capabilities.

Figure 7: Advantages of the Balanced Scorecard


BSC
ADVANTAGES
1
Allows converting the defined strategies into operational terms (action plans)
2
Ensures that the components of the strategy are consistent and enables the identification of cause/effect relationships
3
Facilitates effective communication on strategy implementation and its plans/components
4
Supports the operation of an integrated management monitoring and control system
1: Created by Eucalyp
2: Created by AbbA Icons
3: Created by Icon Mark
4: Created by Sergey D
Noun Project

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

The BSC could be used to follow up on the strategic plan, establishing a frequency that allows for the timely detection of any deviation and make the corresponding corrective decisions. From this perspective, the BSC would need to interact and discuss with the functional area in charge of quality control and management of the emergency and security system.

A BSC could contribute with relevant information to prepare an annual report detailing the strategic plan's progress and achievements, and with recommendations for rethinking some strategies (if necessary). If so, these annual reports would have to be included in the reporting system that would, in turn, need to be part of the information architecture of the emergency and security system (see Chapter III of this guide).

2.10 Assumptions of the strategic plan

It is essential to differentiate between conditions and risks for the operation of the emergency and security system and conditions and risks for executing strategic planning. In the first case, the focus would be on the emergency response system, the operations center, or the provision of services (systematic and non-systematic risks). (This topic is developed in Chapter VIII of this guide).

This section addresses the conditions and risks for executing strategic planning. These would also have to be the subject of constant analysis and follow-up. For such purposes, it would be necessary to focus on the underlying assumptions and the internal and external conditions or circumstances, under which such planning and the resulting strategic plan are expected to occur.

The assumptions and conditions for an adequate planning and strategic management process, which seeks to strengthen the emergency and security system, could be categorized according to type or origin. In general, these would be systemic assumptions, referring to primary conditions that could include the following examples:

- Political assumptions:
  The support, willingness, and leadership required to align efforts of the actors involved (internal) and attract the support of interest groups (external).
- Legal assumptions:
  Legal and normative frameworks that facilitate the management and execution of planning, and external and administrative supervision.
- Technical assumptions:
  Management methodologies for the design, execution, monitoring, and evaluation of planning and for adequate risk management.
- Economic-financial assumptions:
  Continuous provision of adequate resources, based on informed estimation and planning validated by the authorities, and supervision of the use of the resources allocated.

Table 8: *Example of a table to define and explain assumptions*

DIMENSION	ASSUMPTIONS
Political	•High-level government support •The interest of internal and external authorities •Leadership required for steering and managing the entity •Support from interest groups (external)
Legal	• Adequate compliance with applicable laws and regulations •General legal framework of the system •Regulations associated with the institutional engineering and the coordination of the entities that make up the system •Powers and responsibilities for the execution of planning, and external and administrative supervision •Inter-agency affairs •Establishment of the Inter-institutional or Inter-sectoral Commission or Committee
Technical	•Creation of multidisciplinary work teams •Management methodologies for the design, execution, monitoring, and evaluation of the processes associated with strategic planning •Planning for the continuity of the system's operation (COOP) •Adequate risk management •Availability of adequate information •Trained teams •Monitoring and quantification/qualification methodologies (Balanced Scorecard)
Economic-financial	•Stable economic situation •Secured financing policy for "normal" operation times as well as for operation in times of disasters •Budget outlined and assigned •Budget evaluation methodology •Analysis of the social impact of the strategic objectives

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Strategic planning means assuming changes in the conditions (and their impacts, based on risks and the probability of damage), under which implementation of the strategic and operational plans was expected to occur. Analyzing how those conditions could affect the course and, consequently, the possibility of achieving the established goals and objectives, and the operation of the emergency and security system would have to be an ongoing task.

Therefore, it would be advisable to carry out analytical exercises of possible as well as prospective scenarios to identify present, emerging, and future conditions under which the strategic plan will be activated and implemented.

Visualizing and projecting these conditions would allow those who lead the planning process to be adequately prepared for possible changes. Furthermore, it would make it possible to distinguish whether changes or distortions observed in the performance of the emergency and security system are due to implementation of the operational plans contained in the strategic plan itself or to changes in the internal and/or external operating circumstances and conditions (environment).

2.11 Critical success factors

Critical success factors (CSF) -in certain contexts also called key success factors (KSF)- are those conditions or goals that would inevitably have to be fulfilled to achieve the strategic objectives.

Although strategic planning produces several goals and objectives, not all can be considered critical success factors.

Below are some of the criteria for goals and objectives to be considered CSF:

- They are vital or essential for the entity
- They benefit the entity
- They can be considered high-level goal
- They are related to the strategic plan

2.12 Risk identification and analysis

All activities have implicit risks. Strategic planning would also involve the identification of risks or contingencies that could affect its implementation. For this reason, it is necessary not only to identify risks but also to evaluate the probability of their occurrence and their potential impact.

There are different methodologies for the identification and estimation of risks, including:

- ISO 21500:2012
  Guidance on project management
- ISO 31000:2018
  Risk management guidelines
- A Guide to the Project Management Body of Knowledge (PMBOK) by the Project Management Institute (PMI)
- The Project Risk Analysis and Management (PRAM) Guide of the Association for Project Management (APM)

Despite the variety of existing methodologies, most of them agree on four stages:

Stage1: Risk Identification This stage would consist of the following fields:

- Priority:
  The priority assigned to the risk event (High, Medium, or Low).
- Risk Status:
  Identifies whether the risk event is Active (if the risk is being actively monitored and controlled) or Inactive (without current effect but could be activated in the future).
- Risk/Opportunity Event:
  Explanation of the risk.
- Symptom or Trigger:
  Situation that indicates that the risk event is about to occur or has already occurred.
- Related Project/s:
  Describe/s the project/s that relate/s to the risk event.
- Category or Functional Aspect:
  Risk category (example: Technical, Project Management, Functional) or Functional aspect (example: Legal, Security).
- Identification Date:
  Date on which the risk event was identified.
- Project phase:
  Project phase during which the risk event is expected to occur.

Table 9: *Example of table for the identification and classification of risks*

PRIORITY	STATUS	ID#	DATE/ STAGE	FUNCTIONAL CATEGORY/ ASPECT	RISK EVENT/ OPPORTUNITY	EVENT DESCRIPTION	SYMPTOM OR TRIGGER	RELATED PROJECT
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(8)
	Active	1	6/27/2016 Execution	Functional	Staff recruitment	Staff recruitment for the expansion of PSAP North	Staff required for the expansion of the North PSAP needs to be hired by Jun.27.2016. • Administrative staff hired by 6/27/2016 • Technical staff hired by 6/27/2016 • Operational staff hired by 6/27/2016 • Staff hired by agencies by 6/27/2016	• Construction work • Furniture • Execute technological bids or donations

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Stage 2: Risk Analysis

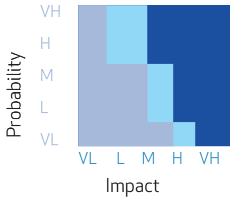
Qualitative Analysis

- Type:
  Area/s impacted by the risk event.
- Probability:
  Qualitative evaluation of the probability of occurrence of the risk event. Valid values could be: Very Low, Low, Medium, High, and Very High.
- Impact:
  Severity of the effect of the risk event on the plan's objectives. Valid values could be: Very Low, Low, Medium, High, and Very High.
- Effects:
  Estimated consequences post-risk event.

Quantitative analysis

- Probability:
  This cell would be recorded automatically based on the qualitative probability assessment. Very low = 10%, Low = 30%, Medium = 50%, High = 70%, and Very High = 90%.
- Impact:
  Evaluation of the impact of the specified risk event in monetary value or days.
- Effect:
  The effect is the product of the probability multiplied by the impact.
- Costs:
  Estimated economic loss.

***Table 10:** Example of table for risk analysis*

QUALITATIVE ANALYSIS				QUANTITATIVE ANALYSIS		
Type	Probability	Impact	Risk Matrix	Probability (%)	Impact ($ or days)	Effect ($ or days)
(9)	(10)	(11)	(12)	(13)	(14)	(15)=(13) x (14)
			 VH H M L VL Probability VL L M H VH Impact			

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Stage 3: Risk Treatment

Strategy: Strategy to be used to respond to the risk event.

Possible values could be:

- For Negative Risks (Threats): Mitigate or Transfer.
- For Positive Risks (Opportunities): Exploit, Share, or Improve.

Response action: Detailed response action to be taken.

Element/s of the affected strategic plan: Design of alternative courses of action as part of the response strategy.

***Table 11:** Example of table for risk treatment*

RESPONSE STRATEGY	
STRATEGY	Response Advantages/ Disadvantages
Mitigate	Monitoring of staff recruitment

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Stage 4: Monitoring and Review

- Responsibility: Name of the area, team, person responsible for managing each of the risks.
- Frequency: How often or at what specific time will the risk status be verified.
- Date, Status, and Review Comments: The date of the last review, the status at the time of the risk review, and any comment derived from the review.

***Table 12:** Example of table for monitoring and reviewing risks*

MONITORING AND CONTROL		
Responsibility (Admin. Task)	Status frequency or Event verification	Date, Status and Review Comments
HH.RR.	Weekly	1/15/2016 Review in progress

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020

Most of the stages would involve conducting workshops, interviews, scenario analysis, surveys, and root cause analysis, among other tools for collecting information and inputs.

An essential tool for risk identification and analysis in strategic planning is the risk matrix. The different types of risk would be placed in a matrix based on an estimate made by comparing different assessment sources (workshops, interviews, surveys, consultations, among others). The matrix would help identify priorities and where to focus the system's resources and efforts.

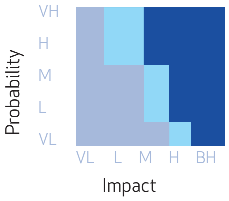
The focus should be on the risk events that end up in the high impact and high probability quadrant. The identification would have to lead to a mitigation plan, including assigning responsibility and designing alternative courses of action.

Below are two examples of risk matrices:

***Table 13:** Risk matrix, Example 1*

RISK MANAGEMENT PLAN

PRIORITY	Assessment							
	Status	ID#	Date/ Stage	Functional Category/ Aspect	Risk Event/ Opportunity	Event Description	Symptom or Trigger	Related Project
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(8)
1	Active	1	2 / 17 /2020 Execution	Technical	Interruption of power suppy/information backup between PSAPs	Interruption of power suppy/ information backup between PSAPs (PSPAP North and PSAP South)	Failure, malfunction or warning alarm of power back-up systems operating in the PSAPs. Failure, malfunction or warning alarm of information backup systems operating in the PSAPs.	N/A

Qualitative Analysis					Quantitative Analysis		
PRIORITY	Type	Probability	Impact	Risk Matrix	Probability (%)	Impact ($ or days)	Effect ($ or days)
(1)	(9)	(10)	(11)	(12)	(13)	(14)	(15)=(13) x (14)
1	Quality Time	High	High				

Response Strategy				Monitoring and control		
PRIORITY	Strategy	Response Advantages/ Disadvantages	WBS elements affected	Responsibility (Admin.Task)	Status frequency or Event verification	Sate, Status and Review Comments
(1)	(16)	(17)	(18)	(19)	(20)	(21)
1	Mitigate	Purchase and install backup and rapid recovery equipment.		Department of Plannings, Logistics and Budget	Weekly	1/15/2016 Review in progress

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

***Table 14:** Risk matrix, Example 2*

RISK IDENTIFICATION	PROBABILITY	IMPACT	MITIGATION	RESPONSIBILITY OFFICIAL(S)
Interruption of funds to finance the program to improve the service management control system	Medium	Reduction of personnel assigned to the detection of good practices and innovation	Containment plan to align internal efforts of the human talent functional area	Department of planning, logistics, and budget

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

2.13 Continuity plan for strategic planning

Ensuring the operational continuity of the emergency and security system should be one of the main objectives of the institutional strategic plan. Therefore, it would be vitally important for the drafting of the continuity plan to be included in the creation of the strategic plan and its subsequent updates.

The development of the continuity plan would have to start with identifying the essential processes and systems for emergency response and assistance in the event of disasters or unplanned events. It should be accompanied by contingency plans that guarantee the operational continuity of the system.

Some important points to consider when creating the continuity plan would be:

- Identify the critical processes and systems for the operation of the system, prioritizing the essential ones.
- Define the indicators and service levels that will be in effect during the contingency.
- Define the plan to return to a "new" normal post risk event once the contingency has been overcome, ensuring the integrity of data and information.

When implementing continuity plans, the following considerations should be kept in mind:

- Determine the scope of a continuity plan based on the assessments of the teams involved in executing the essential activities/services of the emergency and security system.
- Identify alternative mechanisms to accompany the upper and middle administrative levels and the teams in the functional areas.
- Define the crisis management and communication plan.
- Organize awareness and training sessions to ensure staff's support and involvement.
- Define a plan for monitoring internal and external conditions for the execution of strategic planning, testing indicators, and alternative indices in the Balanced Scorecard (BSC).
- Encourage feedback to redefine programs and processes according to the impacts experienced and the effects evaluated.

2.14 Foresight and adaptation

Strategic planning and strategic foresight go hand in hand. Once the strategic plan has been designed and the different operational plans that comprise it have been implemented, it is essential to consider that it is not a static document. The strategic plan should be considered a tool subject to constant revision and updating (to be carried out every 3-5 years), based on a series of factors, including:

- The shifting realities of the environment (e.g., new technologies)
- Institutional developments (incorporation of new services)
- The results of the BSC
- The risk analyzes that have been carried out

In turn, the construction of possible future scenarios makes it easier for the governing body to make more appropriate decisions in the present and to be better prepared for what could lie ahead in the future.

Strategic foresight is based on the analysis of the current situation, the identification of driving forces for change, the determination of the main problems, challenges, and trends, the exploration of possible actions and decisions, and the formation of alliances to build the future desired, avoiding an unwanted one.

CHAPTER

03 SYSTEM DESIGN

Introduction

As a public service, the development of an integrated emergency and security system entails a specific design and work structure based on facilitating the flow of information, the efficient centralization of communications, and the coordination of responses among pertinent organizations, according to the nature of the services required, and the evaluation of processes, operations, and activities (from a quantitative and qualitative perspective).

This chapter addresses three fundamental aspects: the operational model, the structure and organization (institutional architecture), and the functional requirements. The latter includes the infrastructure/technological architecture (hardware and software), the information architecture, the physical infrastructure, and the minimum equipment needed to operate an emergency and security system.

3.1 Operational models

The provision of emergency and security services could be organized based on different operational models, which vary in terms of structure, mechanisms, levels of integration, and collaboration among the participating entities.

Regardless of the name, the system's structure generally reflects an operational model based on a network of nodes, centers, or public safety answering points (PSAP).

The response to an emergency usually includes two stages: the handling/processing stage and the operational stage. Together they encompass six main activities:

Stage 1 Handling/Processing:

1. Geolocation and identification of the incident
2. Information gathering and classification
3. Creation and documentation of the incident
4. Unit assignment

Stage 2 Operations:

5. Unit assistance
6. Documentation and closure of the incident

1. Geolocation and identification of the incident: The user's request is received and automatically, via geographic information systems (GIS) and/or through a series of questions, the place from where the emergency is being reported would be established as accurately as possible. The established protocols would be followed, including a script with a series of standardized questions to determine the type of emergency and risk, the degree of urgency and prioritization, and the type of service to be dispatched. (Stage 1)

2. Information gathering and classification: Background search and verification. The address where the event is occurring, a description of what is happening, and the user's data are captured. The incident is categorized based on a pre-evaluation, classification, and prioritization, in line with the typology of incidents standardized in the computerized system. (Stage 1)

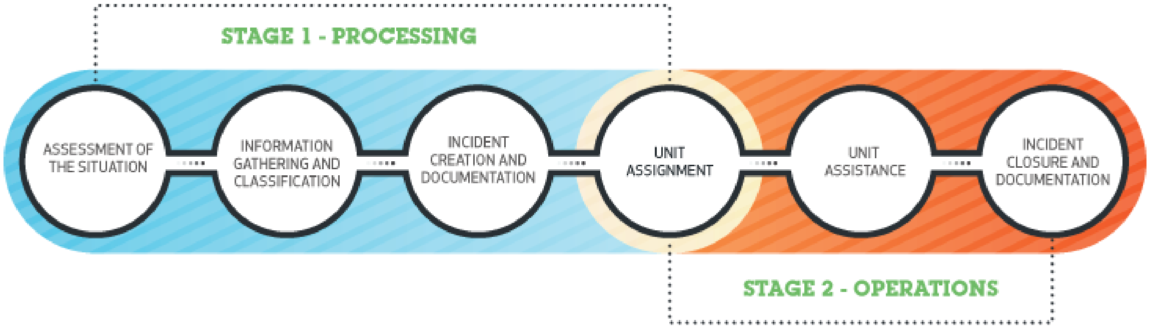
3. Creation and documentation of the incident: A report to notify the response units, according to the classification and prioritization of the event. Once created, it would be advisable for other data to be collected to complete and complement the information on the incident and the scene. (Stage 1)

4. Unit assignment: Notification and dispatch of the unit closest to the event through pre-established means (radio, fleet, platform, or other channels) and assignment of the event. Possibility of requesting support from other first response or support entities and assignment of additional units. (Stage 1)

5. Unit assistance: Follow-up and contact with the response units from the moment of arrival at the incident until they leave, reporting what is happening on-site. (Stage 2)

6. Documentation and operational closure of the event: Documenting the event with all the information gathered, including information collected during dispatch and assistance. Closing of the event in compliance with the established protocols. (Stage 2)

Figure 15: *Six main activities*


STAGE 1 - PROCESSING
ASSESSMENT OF THE SITUATION
INFORMATION GATHERING AND CLASSIFICATION
INCIDENT CREATION AND DOCUMENTATION
UNIT ASSIGNMENT
UNIT ASSISTANCE
INCIDENT CLOSURE AND DOCUMENTATION
STAGE 2 - OPERATIONS

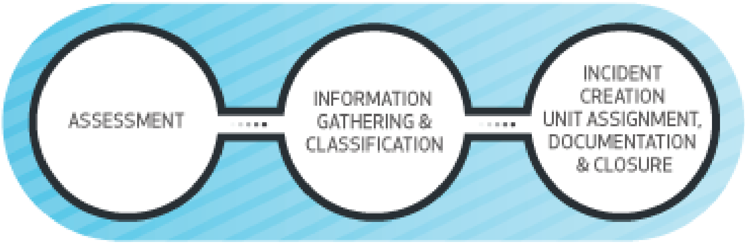
Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

There is no single way to accomplish or combine the six basic activities. At least six operational models have, in fact, been identified. These are differentiated based on the assignment of responsibilities, the degree of concentration, and the institutional placement of the six main activities. These operational models are:

Model A:
Emergency operational entities receive, manage calls, and respond to requests independently. This is an essentially autonomous model covering Stages 1 and 2.

Model B:
There is a single or central call center responsible for receiving emergency requests, calls, and reports, and channeling them to the response institution(s) (Stage 1). Dispatch is under the responsibility of each institution and is independent (Stage 2).

Figure 16: *Model B*

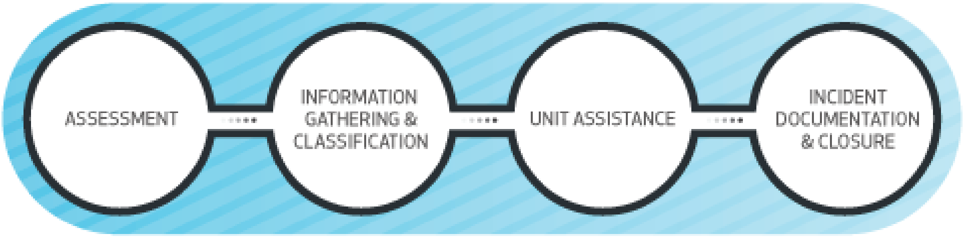

ASSESSMENT
INFORMATION GATHERING & CLASSIFICATION
INCIDENT CREATION UNIT ASSIGNMENT, DOCUMENTATION & CLOSURE

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Model C:

There is a single or central point for receiving requests, calls, and reports, located in a common coordination room (Stage 1) that routes the communication to an operational unit and monitors the service until the case is closed. However, dispatch of the units is done from elsewhere (Stage 2).

Figure 17: *Model C*


ASSESSMENT
INFORMATION GATHERING & CLASSIFICATION
UNIT ASSISTANCE
INCIDENT DOCUMENTATION & CLOSURE

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Model D:

There is a central hub made up of the response institutions, operating from a common room to receive emergency requests, calls, and reports, and for coordination, command, and control, concentrating the six main activities in a single place (Stages 1 and 2).

Model E:

There is an entity independent of the response institutions that manages the system and the resources of the operating entities through an integrated reception/response center or coordination, command, and control hub (PSAP).

Model F:

A network of public safety answering response points (PSAP) is interconnected by an integrated technological system. The network would provide remote services: it would receive emergency requests, calls, and reports, give remote assistance, and follow up on the services until closing, without being directly involved in the dispatch of the units.

3.2 Structure and organization (institutional architecture)

The operational model adopted would require an organizational structure aligned with the system's mission, vision, and strategic guidelines (see Chapter II of this guide).

The organizational structure could be based on functional areas that could be grouped according to two types: core or mission-oriented and support.

Examples of functional areas that could be considered core or mission-oriented:

Operations Management:
Its primary function would be to coordinate and undertake the operations necessary to guarantee the timely, efficient, and effective provision of services to users, as well as institutional and inter-institutional coordination to ensure the interoperability of the system.

Management of Processes and Protocols:
Its primary function would be to ensure the design of each of the processes and their respective protocols, taking into account laws, regulations, and norms or standards that allow the objectives to be achieved.

Quality Management:
Its primary function would be to implement and promote the quality control system and mechanisms, and the tools targeting continuous improvement, as well as the measurement and monitoring of the quality of the services provided, taking into account the feedback from users and support or articulated entities (see Chapter IV of this guide).

Information and Communication Technologies:
Its primary function would be to define the main technological platform, as well as to ensure the availability and functioning of the technological infrastructure that supports the operations of the system, considering information security management, the planned growth of the system's capacity, and contingency plans as pillars of continuity of operations.

Security Management:
Its primary function would be to ensure the security of the system's facilities, personnel, equipment, properties, and visitors, identifying vulnerabilities, threats, and the measures that can be implemented to physically and digitally protect the entity's resources and information (see Chapter VIII of this guide).

Information Management and Analysis:
Its primary function would be to process operational indicators and inputs for administrative management, generating timely and reliable information that serves as the basis for decision-making and improvement of services (see Chapter VII of this guide).

Examples of functional areas that could be considered as support:

Human Talent:
The primary function would be to create policies and manage on a timely basis the human talent that efficiently supports the services provided by the system, through the processes of selection, recruitment, training and continuous evaluation, management of the work environment, and adequate and fair compensation, among other aspects (see Chapter VI of this guide).

Administration and Finance:
The primary function would be to manage, coordinate, and optimize financial and material resources to efficiently support the system's management and continuity of service.

Legal:
The primary function would be to provide specialized and timely legal advice and manage timely responses to the system's legal needs.

Communication:
The primary function would be to design strategies to relate to and engage with the environment (including third ring entities), establish communication channels with the population, and strengthen the system's institutional image by launching campaigns and disseminating activities, among other communication actions (see Chapter IX of this guide).

Strategic and Operational Planning:
The primary function would be to design and monitor the execution of plans implemented to achieve objectives related to the system's strengthening, growth, and continuity of service (see Chapter II of this guide).

Project Management:
The primary function would be to design, execute, and supervise the plans, programs, and projects that support the achievement of the strategies described in the institutional planning.

The organizational structure must be shown in an organizational chart, considering the legal framework and the process map (strategic, mission-oriented, and support processes, among others).

In line with the process map, the work of each functional area should be based on identifying and standardizing processes that could, in turn, be classified as critical or supporting.

Likewise, when setting up functional areas, it would also be relevant to define the technical capabilities each of them would need. This would, in turn, facilitate the identification of the professional profiles necessary for each position (see Chapter VI of this guide).

3.3 Functional requirements

Among the functional requirements of an emergency and security system, at least three could be mentioned:

- Technological infrastructure/ architecture
- Information architecture
- Physical infrastructure and equipment

3.3.1 Technological infrastructure/ architecture

The design of an emergency and security system should consider the technical standards associated with the intensive use of available information and communication technologies.

There are at least four organizations with international influence that issue technical guidelines and standards concerning technologies for emergency response:

- International Telecommunication Union (ITU)
- European Telecommunications Standards Institute (ETSI)
- European Emergency Number Association (EENA)
- National Emergency Number Association (NENA), United States of America

The guidelines and standards of these organizations complement each other. The choice will depend on the system's design and expectations regarding, for example, landlines, mobile telecommunications, radio, convergent systems, broadcast technologies, and the internet.

The technological ecosystem of an emergency and security system would have to include all the hardware and software components necessary to effectively manage the operational and administrative processes linked to the functional areas.

Based on the existing technical standards, the design of the operating system would have to consider the following information and communication technology components:

a. Hardware and web services infrastructure, mail services, file services, network services, database services, and application services, among others.

Additionally, regarding database servers, the following technical features would be recommended:

- High availability (CLUSTER)
- Database replication
- Storage according to operational systems
- Tool for data mining, analysis, and display
- Search and reporting tool
- On-line analytical processing tool (OLAP)
- Executive Information System tool (EIS)
- Decision Support Systems tool (DSS)

b. Highly available infrastructure, based on redundant systems, matrices, networks, and power sources; automatic transfer switch; networking and connectivity equipment, among others.

c. A radio communication system among the areas and entities linked to emergency response. The radio communication network would have to be digital and have specific features such as data encryption. The network's scalability and interoperability with other existing communication systems would allow for expanding the geographic coverage in less time and at a lower cost.

d. Technological compatibility and system integration of the following type:

- Computer telephony integration (CTI)
- System for generation of tokens, codes, and registration numbers
- Telephone number identification system (IP identification)
- Geographic information system (GIS)

- Automatic Vehicle Location (AVL)
- Cameras for personal use or personal video surveillance to monitor what is happening on the ground
- Computer-Aided Dispatch (CAD) system
- Priority Dispatch System (PDS) M*P*F
- Private Automatic Branch Exchange (PABX) or automated private switchboard (routing, forwarding, queuing - erlang, missed calls)
- Computer-Aided Call Handling (CACH)
- Mobile data terminals (MDTs)
- Mobile data computers (MDCs)
- Mobile radio communication system (trunking)
- Radio communications between Public Safety Answering Points (PSAP) and Primary Response Vehicle (PRV) or Ambulance and Advanced Life Support
- Status report of available units/ vehicles
- Action Taken Report (ATR)
- Video surveillance monitoring system and image analysis
- Alert system
- Video wall solution

e. Internet access, website, web services.

3.3.2 Information architecture

An essential element in the design of an information architecture is that it responds to an emergency and security system's information needs, which may be operational, strategic, policy-oriented, and service quality management-related.

This architecture should be linked to the processes and stages directly related to emergency response and assistance, as well as to the controls and indicators established to monitor and evaluate the service provided, the execution and performance of the six main activities (Stages 1 and 2), and the goals and objectives established in the strategic plan.

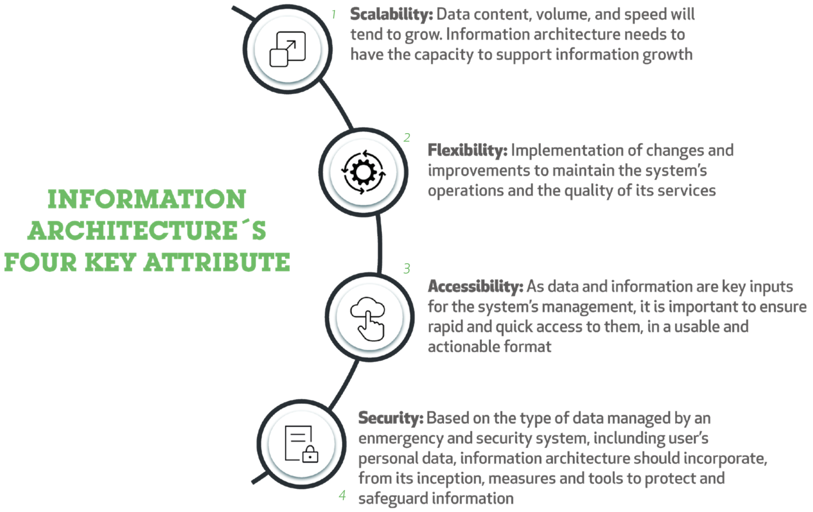
Depending on the operational model of the emergency and security system, the information architecture must be aligned with and support the six main activities, facilitating the recording of data and information, and communication across the board, from the beginning to the end of the incident.

In general, when designing the information architecture, the following aspects should be considered:

- The use of information (what for?), what type of information is required, in what format, for whom, and when should it be gathered and delivered.
- Definition of typologies, classifications, categories, tags, and keywords to structure, organize, and link the information and facilitate its search and retrieval.
- Generation of a common and standardized vocabulary.
- The pathways, channels, or means through which the system will receive emergency alerts: calls, video surveillance, panic buttons, mobile applications, text messaging, among others. If one or more platforms is involved in the handling of an emergency alert, deciding upon information storage, organization, and structure will be different in each case.
- The mechanism for recording emergency alerts.
- The feedback mechanism between field units and the call center.
- Forms to record the information about emergency incidents, seeking to strike a balance between timely recording of information and the information required to understand what is going on at the emergency scene.
- The reports and data display tools generated to provide feedback on the operations and the services provided by the system.
- Sufficient space to store and access data and information captured by the system in its daily operation.

There would be at least four recommended attributes when conceiving the data architecture: scalability, flexibility, accessibility, and security.

Figure 18: *Some recommended attributes for information architecture*



INFORMATION ARCHITECTURE´S FOUR KEY ATTRIBUTE

1 **Scalability:** Data content, volume, and speed will tend to grow. Information architecture needs to have the capacity to support information growth

2 **Flexibility:** Implementation of changes and improvements to maintain the system's operations and the quality of its services

3 **Accessibility:** As data and information are key inputs for the system's management, it is important to ensure rapid and quick access to them, in a usable and actionable format

Security: Based on the type of data managed by an enmergency and security system, including user's personal data, information architecture should incorporate, from its inception, measures and tools to protect and safeguard information 4

1: Created by Adrian Coquet
2: Created by Nhor
3: Created byAdrian Coquet
4: Created by Adrian Coquet

Noun Project

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

3.3.2.1 Incident typology

To ensure an adequate response to emergencies, it would be necessary to establish an incident typology as part of the information architecture, with unique and mutually exclusive categories clearly defined, covering all possible areas, and consistent with existing typologies.

Furthermore, it would also be necessary to establish what will be considered an "incident" for operational purposes, and its relationship with a typology of emergencies. This relationship could be defined on a one-to-one basis, where for each emergency type, there would be an identified incident type that would generate the alert. Another possible relationship is one-to-many, wherein various incidents could be associated with an emergency, based on predefined specifications and associations.

When creating this typology and depending on the operational model, each incident must also be linked to a type of response. The classification and/or regrouping of one or more incidents, according to the specifications and association rules, would determine the type of routing and dispatch, with the possibility of adding other agencies in the response.

As the emergency and security system expands and strengthens, it would be possible to incorporate new types of incidents, as well as changes or adjustments in the definitions. A good practice would be to document these changes, whether they are changes to standards, concepts, or coding.

The incident typology would contain categories and subtypes or subgroups, as well as the classification rules. The typology and the rules must be common to all the entities participating in the system, in Stages 1 and 2. For example, some of these possible general categories are presented below:

- Violence, crimes, and public/citizen security incidents:
  These are events that endanger people's lives and/or property. For example, robberies, fights, domestic violence, gender violence, child abuse, damage to property and other assets.

- Health incidents :
  These are events that immediately endanger the life and physical integrity of people. For example, hemorrhages, knife and firearm wounds, fractures, poisoning, heart attacks, and respiratory distress.

- Mental health Incidents:
  These are events in which the person shows risky behaviors, including suicide attempts, behavioral changes due to substance abuse, depression, mental disorders, or illnesses, among others.

Disasters:
These are high-magnitude events that affect large areas, with several response institutions intervening during prolonged periods of time. Examples are floods, forest fires, fuel spills, tsunamis, hurricanes, earthquakes, and landslides.

Hazard events and crises:
These are geographically concentrated events in which one or more response agencies intervene during prolonged response periods. Examples are explosions, fires, and people being rescued, among others.

Impacts on national and/or State security:
These are events linked to the disruption of public order, which could threaten the nation's integrity, endangering the country's national interests and objectives. An example is terrorist attacks.

Scheduled/programmed events:
These are events whose occurrence is known in advance (for example, the demolition of a building) and for which the emergency and security system expects to receive a high volume of calls.

3.3.2.2 Typology of access channels

Regarding information architecture for emergency management, it would be essential to establish and classify the channels for receiving requests, calls, and reports from users, generating alerts, and communicating with the population.

One of the main channels would be a single telephone number. Its operation would not rule out the activation of other contact or reporting mechanisms, including text messaging (SMS), video surveillance, mobile application, among others.

The design should take advantage of the most recent information and communication technologies (ICTs) and technical standards already developed. The different characteristics and needs of users must also be taken into account, including access for people with disabilities and groups and subgroups in vulnerable situations. TTY devices, panic buttons, and Real-Time Text (RTT) could be incorporated for such purposes.

3.3.2.3. Call typology

Considering the massive number of telephone calls that emergency and security systems usually receive, the information architecture would have to incorporate the classification of the calls, each one with its own definition and pre-established criteria for its handling. Likewise, it would also need a prioritization mechanism and a set of predefined courses of action or protocols for reacting and responding to emergencies in a standardized manner.

The classification could incorporate three criteria to differentiate among the calls, which, in turn, would have to be accompanied by specific protocols for their handling:

- Calls with or without audio
- Appropriate and inappropriate calls
- Calls with or without mobilization of units or resources

In the specific case of appropriate calls, these could be organized based on the following categories, which may need to be adjusted according to the context of each country:

Table 19: *Classification of appropriate calls*

CLASSIFICATION	DESCRIPTION
Emergency	An event that can endanger the life, mental and emotional health, safety, or integrity of individuals or legal persons or property, and that requires immediate assistance.
Urgency	An event that requires immediate attention but is not an emergency and does not represent immediate or imminent danger.
Reports	Notification that a crime or misdemeanor is being committed.
Services and assistance	Calls to request assistance that require the support of a response unit.
Inquiries	Calls to request information on the services offered or inquiries on specific issues managed by the emergency and security system.

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Additionally, appropriate emergency calls could be of different types, depending on the typology of incidents presented above:

- Crimes, violence, and public/citizen security
- Health
- Mental health
- Disasters
- Hazard events/crises
- National security
- Scheduled/programmed events

3.3.2.4. Typology of prioritization levels

Another fundamental tool would be to have a scale for prioritizing the requests, calls, and reports received. Based on the example in Table 19, a prioritization scale could be as follows:

Table 20: *Prioritization scheme*

CLASSIFICATION	PRIORITIZATION
Emergency	1
Urgency	2
Reports	3
Services and assistance	4
Inquiries	5

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Level or Priority 1:

Any situation or event posing an imminent risk to the integrity of people or their property and/or harm to the population or industry and thus requiring immediate assistance.

Requests, calls, and reports that alert about this type of situation, are classified as emergencies and should be managed without delay, immediately activating the most appropriate response resources. They are usually classified as "high priority" or "immediate assistance" and are sometimes displayed in red.

Examples of emergencies would be situations in which life is in danger, serious crimes, such as violence against women, girls, boys, and adolescents, situations in which people's property is in danger, and hydro-meteorological events.

Level or Priority 2:

Any situation or event without imminent risk but that could still affect the integrity of people or their property, the population, or an industry, but nonetheless requires response or assistance as soon as possible.

These types of situations or events would have to receive a response after the resources for Level or Priority 1 emergencies have been dispatched. They are usually classified as "intermediate priority" or "priority assistance" and are usually displayed in orange.

Examples of Level 2 situations would be home accidents, in which no one's life is endangered.

Level or Priority 3:

Any situation or event where there is a "low priority" urgency since no risk is identified for people or property or adverse impact on the population or industry. Therefore, they do not require immediate assistance. These should be dealt with when Level or Priority 1 and Level or Priority 2 incidents are closed and when response units are available.

They are usually labeled as "low priority" or "non-urgent assistance" and displayed in yellow.

Examples of this type of Level 3 situation would be falling trees and falling fences.

Level or Priority 4:

Any situation or event that does not present a sense of urgency but may or may not require the use of resources or could be recorded as helpful information received.

These events would be handled after the previous priorities have been resolved, either in person, by telephone, or remotely.

Level or Priority 5:

Calls to request information about services offered or inquiries regarding specific issues managed by the emergency and security system.

Response to this level of events would be relegated to last place, after all the previous levels have been addressed.

In addition to a numerical scale and qualitative indicators to indicate the prioritization order, the categorization could also be displayed by using a traffic light-inspired color scheme.

Each of these levels or priorities could in turn feature internal subscales.

3.3.2.5. Inappropriate calls

Inappropriate calls lead to misuse of the system's resources. Even when they do not produce any type of response, it would be advisable for the information architecture to include, a classification typology and predefined courses of action for them. This standardized treatment of inappropriate calls would facilitate their subsequent analysis, identification of patterns of service misuse, and design of possible solutions.

Below is an example of a typology for inappropriate calls with possible categories to be considered:

- False emergency call:
  Calls to report fictitious emergencies, which cause the unneeded dispatch of response units.
- Abandoned call:
  When someone calls the call center and hangs up before the call has been taken.
- Hung-up call:
  When someone calls the call center maliciously or accidentally, and the call is interrupted after being answered by the operator.
- Misplaced call (wrong number call):
  Call that is made to the call center by mistake or unintentionally.
- Prank call:
  Obscene, morbid, or insulting call, made for entertainment or fun.

Initially, the following calls could be considered inappropriate:

- Canceled call:
  Call that is terminated because the operator or the caller hangs up or there is some system failure.
- Non-emergency call:
  A call that does not describe a situation that may be classified as an emergency, which may be significant or urgent, but should be addressed through other channels.
- Redundant call:
  Call that has already been reported and is being processed by the response units.
- Silent call:
  Call answered by the operator in which no voice is heard, or no one is speaking.

The above list of calls, however, should be given special treatment to rule out the possibility of their being appropriate calls, i.e., emergency calls. For such purpose, protocols and guidelines should be prepared.

3.3.2.6. Recording incident information

As part of the information architecture, it would be necessary to define the data to be recorded for each request, call, or report received from when the call is received until the case is closed. Determining which inputs to collect would depend on the type of information needed to provide an adequate and timely service. Additionally, it could also respond to the need to generate additional aggregated data to evaluate the operation and quality of the service provided by the system.

There are at least four considerations that could guide this critical step in information architecture design:

- What data/information should be captured, what data/information could be extracted/exported from other databases.
- Timing and frequency with which to upload, extract/export, consolidate and combine the data.
- How to capture data, using protocols and predetermined templates to standardize both the data that is collected as well as the methodology used to do so.
- Where to store, back up, and protect data and information. An IT architecture that includes an exclusive and centralized repository with a single database engine would be recommended for efficient information management.

3.3.2.7. Interoperable and relational databases

Interoperability refers to the functionality of information systems that allows them to exchange different types of data or background information and facilitate their use. Integration that allows for the interoperability of databases is critical for a more effective, efficient, and timely use of information, positively impacting the operation and quality of the service provided.

An emergency and security system would have to develop several databases linked to emergency requests, calls, and reports, unit dispatch, and assistance provided, video surveillance, and other potential services. These databases would contain information on attributes of both the emergencies and the people involved. Whether there is an integrated platform or multiple platforms for responding to emergencies, it would be necessary to define when and how these systems should communicate, exchange, store, and safeguard the information.

Database interoperability and information integration would need to be governed by data protection principles.

3.3.2.8. Data processing, analysis, and display

In addition to the data and indicators resulting from the information architecture designed and the databases developed for data entry, use, and integration, it would be necessary to have a tool for data processing, analysis, and display at the different operating levels of the system (operational, tactical, and strategic).

At least four dimensions that should be defined to configure a system for data processing, analysis, and display are specified below:

- Type of data: structured, unstructured
- Focus of analysis: reports, key performance indicators (KPI), trend analysis, patterns, correlations, models
- Type of analysis: retrospective, descriptive, predictive, prescriptive
- Analysis process: static, comparative, explorative, experimental

3.3.2.9. Generation and use of information

The type of information available within an emergency and security system would largely depend on the information architecture design, including the different incident typologies, classifications and categories, the capture and storage of information, technical standards for integrating databases, and the system's interoperability. Therefore, the information architecture must be designed based on the types of information that will be required and how it will be used.

One of the most frequent uses of information would occur in the field of operations, to guide, in real-time, the response and service provided in an emergency.

Later, it could also be used as input to monitor and evaluate the emergency and security system's operation and the quality of the services provided. Based on identified deviations or deficiencies, it could be used to prioritize areas of intervention and inform the design of measures to continuously improve the system.

Similarly, in its most aggregated form, it would be useful as input and support for the strategic planning process as well as for reporting on progress made with regard to the established goals and objectives.

Additionally, it could also be used beyond the emergency and security system itself, in at least two external contexts or situations:

- For pre-judicial bodies, criminal investigations, and criminal proceedings (see Chapter VII of this guide)
- For the design, monitoring, and evaluation of programs and public policies (see Chapter VII of this guide)

3.3.2.10. Reporting system

Defining the types of reports that an emergency and security system will produce could start by identifying the potential users and the type of information they would need. Then, for each type of report, some features would have to be defined, including objective, format, periodicity, distribution, the area responsible, storage site, and access, among other elements.

The reports could provide information on the system's operation with regard to handling and responding to emergencies, based on a matrix of predefined indicators. This matrix would have to be part of the quality management system and could include indicators of activity, management, processes, and results.

Depending on the information that the system generates, the available tools for data processing, analysis, and display, the technical skills of the personnel, and the uses that will be given to the information, different types of reports could be defined.

For example, at least five types of reports could be considered:

- Reports on the performance and development of human talent
- Management reports (results and productivity)
- Reports on the responses and services provided
- Financial-administrative reports
- Project reports

Depending on the technological architecture/infrastructure available, it could be possible to have platforms for automated report generation and distribution. Other useful functionalities to consider when designing a reporting system would be:

- Common repository
- Search parameters and engine: through specifying keywords or combination of keywords, to find reports quickly
- Standardization of the formats of tables, graphs, and other tools for the presentation and display of data
- Options to send or download in various formats
- Real-time updates
- Display of data on a dashboard or control panel

3.3.2.11. Document management system

As a result of the information architecture and the reporting system it enables, the emergency and security system would have at its disposal a series of documents, both physical and digital.

It would be necessary to define a typology to manage these documents effectively and efficiently, as well as a classification based on their level of confidentiality (for example: confidential, reserved, classified, and public), in line with the legislation of each country, including laws on transparency and access to public information, and the needs of the emergency and security system.

The functional area in charge of document management could also be in charge of standardizing the creation, approval, storage, and destruction of physical and digital material and ensuring compliance.

Below are some activities associated with each of the four processes mentioned:

- Creation:
Establish guidelines for the production of internal documents, including format, identification (numbering/coding), corresponding metadata, and the level of confidentiality, among other elements. In addition, possible uses of the document could be suggested.

- Approval:
Define the steps for document review and validation, for example, who participates, the deadlines, who authorizes the final version of the document, who is in charge of giving it official status. All documentation authorized for internal use would have to be made available to staff members and, depending on the material, disseminated.

- Storage:
Establish a format for saving documents and a methodology for archiving. Also, define the treatment of previous versions of documents and storage deadlines.

- Destruction:
Define the validity of the documentation, the deadlines for filing and destruction of documents, including in the procedure rules, the steps, authorizations, and treatment according to the level of confidentiality, among other aspects.

3.3.2.12. Functional area of information management

Like any functional area, in addition to defining its functions, it would be necessary to establish the scope and position of the information management area within the entity.

Regarding scope, at least three options could be considered:

- Limited scope: could be related to the purely operational.

- Strategic scope: would include support for decision-making at all levels and the development of corporate intelligence.

- Extensive scope: would also involve the communications management of relations with the environment, considering accountability and transparency.

These scopes are not mutually exclusive.

Regarding the positioning of information management within the structure and the organizational chart of an emergency and security system, it could be thought of as an independent area or as part of another functional area that encompasses it.

3.3.3. Physical infrastructure and equipment

The construction and design of the physical spaces that comprise a public safety answering center would have to make human safety their guiding principle. There are some reference documents on the matter, including NFPA 101®, standard ISO 45001-Occupational Health and Safety Management System; OHSAS 18001-Occupational Health and Safety Standard[2]. In this context, the supervision and cooperation of the corresponding agencies in each country are also relevant.

Physical areas could also adhere to lighting and ergonomic design standards, established specifically for work environments, to protect personnel's health and enhance their productivity. To create a healthy and comfortable working environment, it would also be important to think of ways to absorb and reduce noise levels and install heating/cooling systems.

The physical space could be designed based on two large areas: the operations area and the administrative area. In turn, the operations area of a public safety answering center could have the following facilities: call reception room, dispatch room, video surveillance room (if applicable). Additionally, it would be necessary to consider a series of support or common areas, such as a cafeteria, resting area, maintenance area, meeting rooms, and contingency or crisis rooms.

The physical space would have to display the appropriate emergency signage and be adequately equipped to face emergencies. Likewise, alternative workspaces should also be considered in case the facilities could not be used.

Other essential elements to be taken into account concerning the physical space and the equipment would be:

- The location and size of the workstations.
- The equipment of the workstations, including the number of monitors, radio or telephone communication devices, headbands, computers.
- Screens (monitors or TV) to display the turnout of units, according to the type of response, the entity in charge of the service, geographic area, among other characteristics defined in the operational model regarding request, call, or report handling, administration, response coordination, and dispatch-closure.

[2] Please note that OHSAS 18001 has been replaced by ISO 45001 as the new international standard for occupational health and safety management.

CHAPTER

04

COMPREHENSIVE QUALITY MANAGEMENT

Introduction

After planning and design, the emergency and security system would need to start operating. This chapter focuses on managing the operation of an emergency and security system from the standpoint of a quality management model. This quality-based management model seeks continuous improvement to provide the population with a professional and effective service in a sustained and uninterrupted manner.

The quality management model includes four inputs that are described in this chapter: (i) the monitoring and measurement of processes and activities at each point in the service provision chain; (ii) feedback from users; (iii) feedback from first ring or articulated and related institutions or second ring institutions; and (iv) risk management.

Additionally, this chapter also presents two essential tools for conducting quality management of the processes, services, and activities carried out by an emergency and security system. The first would entail identifying and mapping processes and developing protocols for those considered critical for the system's operation and continuity of operations. Compliance with these protocols by personnel would allow the desired quality levels to be maintained. Additionally, comparing these protocols and the actions undertaken would allow the identification of opportunities for improvement.

The second tool entails the definition and calculation of a series of indicators for monitoring and measuring the system's operation in general as well as each of its functional areas and the actions undertaken, particularly regarding handling and responding to emergencies.

Both tools would help to reduce the room for discretion and subjectivity in the operation and management of an emergency and security system. Additionally, they would encourage the professionalism and impartiality that would be needed to carry out the functions and, operational and administrative activities of this type of system. Furthermore, they would provide clear, shared, and uniform parameters and references for all personnel.

4.1. Quality management model

A quality management model is closely linked to the system's governance insofar as it involves everything, from measuring, monitoring, evaluating, and reviewing the quality-of-service delivery to the introduction of the improvements required to make it more efficient, effective, and satisfactory. This cycle would have to be permanent and constantly repeated, as an essential part of the system's operation, with a view to the continuous improvement of the service offered to the population.

A quality management model covers all functional areas (main or mission-oriented and support). It also includes all the levels of operation of a system (strategic, tactical, and operational), with particular emphasis on the delivery of emergency and security services.

Based on the current legal framework and the establishment of standards, protocols, and guidelines, the purpose of the quality management model could be:

- Continuous improvement and innovation of processes and services.
- The satisfaction of users' needs, requirements, and expectations, including groups in vulnerable situations.
- The improvement of efficiency to achieve greater effectiveness.
- Measurement and evaluation of performance.

There are different models of quality management. The model finally adopted would have to be based on the operational model of the emergency and security system, taking into account each critical point in the service delivery chain. Additionally, it would be advisable for the quality management model to be aligned with the most influential international standards on the subject, such as the ISO 9000[3] standards or the EFQM Excellence Model (European Foundation Quality Management)[4].

Despite the variety of quality management models available, four minimum approaches are presented below:

1. Monitoring at each point in the service delivery chain

The first approach is based on measuring and controlling quality in each stage, process, or area of service delivery activity, such as receiving the service request, dispatching, or assigning units, among others.

[3] ISO 9000: Quality Management Systems. Fundamentals and Vocabulary; ISO 9001: Quality Management Systems. Requirements; ISO 9004: Quality Management. Quality of an Organization. Guidance for sustained success. The ISO 9000-2015 family promotes "quality management principles", such as the following: (1) Customer focus; (2) Leadership; (3) Commitment of the people; (4) Focus on processes; (5) Improvement; (6) Decision-making based on evidence; and (7) Relationship management.

[4] The EFQM Model consists of seven criteria aligned with a strategic axis. The three axes of the model structure are the basis of the connection between the purpose and the strategy of an organization and, in turn, guide the actions for the creation of sustainable value for its key interest groups and the generation of outstanding results. These are: Direction: (1) Purpose, vision, and strategy; (2) Organizational culture and leadership; Execution: (3) Involve interest groups; (4) Create sustainable value; (5) Manage the operation and transformation; Results: (6) Interest groups' perception; (7) Strategic and operational performance.

Monitoring would have to be done by comparing general operations and the specific actions carried out to what has been established in regulations, protocols, standards, and guidelines. Additionally, it could be based on the definition and calculation of indicators and the monitoring and measuring of the results obtained, taking pre-set goals and objectives as a reference point.

When doing this first type of monitoring, taking samples from all areas, all types of events, all people, and all entities providing services at different levels would be recommended. This sampling would have to be random and representative, given the volume of incidents handled by an emergency and security system. This would contribute to the objectivity of the exercise and would also redound to the comprehensiveness of the service.

Monitoring could also be carried out through internal audits or management control tools, which require well-defined objectives, targets, and indicators. These could be seen as complementary oversight mechanisms.

Based on the application of these monitoring instruments, if there are differences, gaps, or deviations between practice and the regulations, protocols, standards, and guidelines established or concerning the goals and objectives set, it would be necessary to proceed to the development and implementation of action plans. These would present a set of recommendations to overcome the differences, gaps, or deviations identified.

For the sake of transparency and accountability, the results of the internal audits, as well as the action plans designed to correct the differences, gaps, or deviations identified, could be published on the website of the emergency and security system (see Chapter X of this guide).

2. User feedback

This second approach would consist of establishing consultation mechanisms with users, which would allow for measuring their satisfaction with the service provided, detecting opportunities for improvement, and taking measures to rectify detected deviations. Some of the consultation mechanisms that could be applied are satisfaction surveys, follow-up calls, focus groups, and complaints and suggestions mailboxes (in-person or virtual).

3. Feedback and follow-up regarding articulated institutions (or first-ring institutions)

The third approach would entail the creation of intra- and inter-institutional coordination forums, to include follow-up meetings, technical and exchange panels, as well as the incorporation of tools or techniques such as after-action or ex-post emergency reviews, to:

- Provide feedback to articulated entities about the results of operations based on established monitoring and consultation mechanisms, statistical reports and indicators, trend analysis, after-action reports, among other information.

- Identify situations that could be negatively or positively affecting the operation.
- Regarding the former (negative situations), take corrective action promptly and consider what could be documented as a lesson learned to share with the rest of the staff in order to avoid repeated mistakes.
- Regarding the latter (positive situations), consider what could be documented as a promising or good practice to be shared with the rest of the staff and promote its dissemination and adoption across the system.

These three approaches would consist of the following five steps:

a. Collection of data and information.

b. Data and information analysis to identify possible improvements.

c. Development of plans to address the areas of opportunity identified, which need to be prioritized and aligned with the system's strategic goals and objectives.

d. Establishment of a framework for the implementation of improvement projects:

- Define mechanisms for measuring and monitoring the progress of these plans.
- Analyze their feasibility and budgetary viability.

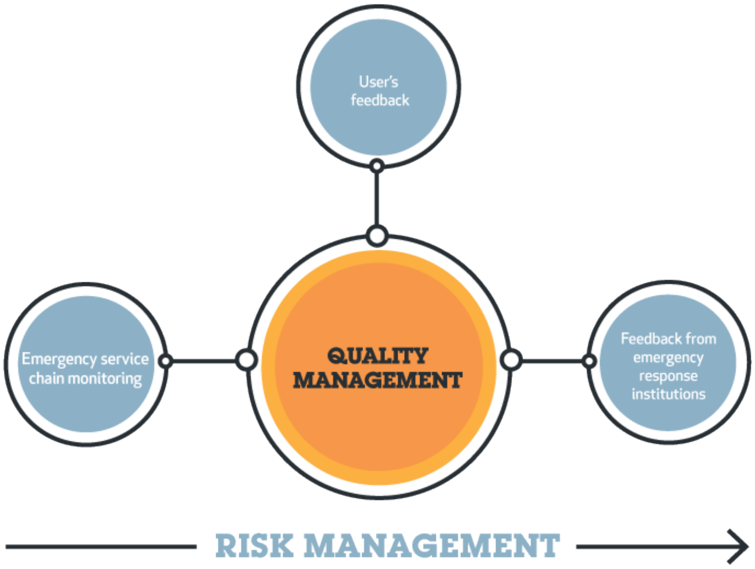
e. Implementation of the activities as defined in the improvement plans and implementation of measurement and monitoring mechanisms.

4. Risk management

The fourth approach focuses on risk management. It starts by identifying and scanning unexpected and foreseeable situations that could harm the system's functioning, seeking to identify the probability of occurrence, level of impact, and existing vulnerabilities.

Based on this assessment, prevention and mitigation actions should be established as part of a risk management plan. This document would have to be updated periodically (see Chapter VIII of this guide).

Figure 21: *Service Quality Management*


User's feedback
Emergency service chain monitoring
QUALITY MANAGEMENT
Feedback from emergency response institutions
RISK MANAGEMENT

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

4.2. Standardization of processes and implementation of protocols

This section focuses on the first tool of a quality management model. The starting point would be to map or outline the general process of emergency response and assistance, and then the specific processes and activities associated with each of the products and services offered.

To map or outline these processes, at least five steps should be taken, bearing in mind: a) functional and performance requirements, and b) applicable legal and regulatory requirements:

- Describe and characterize processes and identify which are the critical ones.
- Develop protocols to standardize processes, particularly those that were identified as critical.
- Develop manuals/procedural guides and action protocols.
- Define process monitoring indicators.
- Set quality parameters and standards.

These five steps would, in turn:

- Serve as a guide and reference for process execution.
- Facilitate personnel training (see Chapter VI of this guide).
- Help verify the compliance of activities carried out by the staff, providing objective parameters for their performance evaluation (see Chapter VI of this guide).
- Enable objective monitoring and evaluation of the system's operation and processes, with a view to its continuous improvement.

The most critical processes for the operation of an emergency and security system include the following seven:

- Receiving requests for assistance and identifying the situation.
- Information collection, classification, and prioritization.
- Incident creation and relay information about the incident.
- Dispatch or assignment of response unit(s).
- Coordination, supervision of communications, and monitoring of response unit(s) at emergency site.
- Operational closure of the incident.
- After-action review of all the above.

Each of these processes or stages of service delivery would merit the development of standards and protocols to ensure efficient, timely, and quality operation of the system.

4.3. Establishing and measuring indicators

This section addresses the second tool in a quality management model, i.e., establishing and measuring a series of indicators to monitor and evaluate the system's operation in general, its functional areas, and actions taken, particularly with regard to emergency response and assistance. Below are some of the indicators that could be considered as part of a quality management model:

- Activity indicators
- Process indicators
- Evaluation indicators
- Management indicators

Each indicator would have to meet all the technical design features, including a factsheet. Indicators would have to be quantifiable, qualifiable, and expressed in a unit of measure, including percentages, indexes, or rates.

The fact sheet for each indicator could include the following fields:

- Name of the indicator
- Description/purpose of the indicator
- Goal, objective, and strategic axis with which the indicator is associated
- Type of indicator
- The formula for calculating the indicator
- The data needed to calculate the indicator, the sources of the data, and who is responsible for those data sources
- Measurement unit and assigned categories
- Ranges and scale
- Frequency of measurement
- Baseline
- Area responsible for calculating and monitoring the indicator (or specify whether the calculation is automated)
- Where that indicator would be available, in which report it would have to be included
- Who would have access to the indicator

These indicators would have to be consistent with the Balanced Scorecard (BSC) (see Chapter II of this guide) and could be grouped, organized, and displayed on a dashboard. They should have been defined, preferably when the system's information architecture was designed (see Chapter III of this guide). In addition, calculation, safeguarding, and storage of indicators must be supported by the technological architecture designed for the operation of the emergency and security system.

4.3.1. Activity indicators

These are indicators that measure the number of emergency requests, calls, or reports received by an emergency and security system. They would have an informative value for assessing the use and allocation of resources, and would also facilitate comparisons with other centers, services, or time periods. Below are some examples of activity indicators:

1) Total number of requests, calls, or reports received

2) Number of requests, calls, or reports received by type of channel

3) Number of requests, calls, or reports by type of incident

4) Number of requests, calls, or reports by location

5) Number of cases handled (service level)

6) Number of operators available per request, call, or report received

7) Number of dispatches made per request, call, or report received

8) Accuracy of geolocation services for emergency requests, calls, and reports [5]

[5] In Mexico, the accuracy of the geolocation that telephone operators provide to CALLE, is measured based on the security and justice collaboration guidelines issued by the Federal Telecommunications Institute (IFT). Based on clearly established parameters and regions, the IFT calculates the measurements on an annual basis. If the minimum required parameters are not met, operators may be penalized.

4.3.2. Process indicators

These indicators would help verify the service's availability, particularly regarding emergency response and assistance, and could be grouped by type of process. For example:

1) Average time spent handling the emergency request, call, or report

2) Percentage of calls beyond the time established, according to type and characteristics of the emergency request, call, or report

3) Time for processing and sending the report to dispatch

4) Average dispatch time of assistance unit

5) Percentage of abandoned calls

6) Percentage of calls on hold

7) Percentage of incidents dispatched that are non-emergency

8) Percentage of unclosed incidents

4.3.3. Evaluation indicators

These could be used to evaluate service provided on a monthly, quarterly, biannual, or annual basis and to identify areas of opportunity based on the responses to emergency requests, calls, or reports received by the system. For example:

1) Percentage of incidents classified correctly

2) Percentage of incidents dispatched

3) Percentage of incidents handled

4) Average time for call processing, according to type and characteristics

5) Average time it takes to dispatch units (from the moment the call is received until the unit is dispatched)

6) Average deployment time (from the moment the dispatcher informs the articulated agency until the unit leaves the facility to go to the emergency site)

7) Average response time (from the moment the request, call, or report is received until the unit reaches the emergency site)

8) Percentage of incidents handled within the time set as a parameter

9) Percentage of requests, calls, and reports that complied with the protocols

4.3.4. Management indicators

These indicators would measure the operation of the service from the standpoint of planning and management of the system and could be grouped by functional area. Some examples are presented below:

4.3.4.1. Human resources:

1) Number of certified operators

2) Average age of operational personnel

3) Number of positions available

4) Number of personnel in training

5) Number of operational personnel about to retire and projected number of employees who would have to be replaced

6) Percentage of absenteeism or punctuality

7) Work environment indicators, which could be formulated based on employees' perceptions regarding:

    - Relationships among colleagues
    - Physical working conditions
    - Compensation and recognition
    - Career development opportunities
    - Equal opportunities
    - Inclusion of people with disabilities, according to functional area

4.3.4.2. Operations

1) Turnover (voluntary and involuntary) of operators

2) Operational capacity (resource availability) by shift and by operator

3) Average or rate of requests, calls, and reports handled by operator

4) Number of cameras available or in operation

5) Number of cameras monitored by video operator (where applicable)

4.3.4.3. Quality

1) Percentage of projects implemented for continuous improvement

2) Percentage of users satisfied with the service provided by the emergency and security system

4.3.4.4. Administration and finance

1) Percentage of the budget assigned by functional area

2) Percentage of budget executed

3) Level of debt as an average percentage of assigned resources

CHAPTER

05

CALL AND INCIDENT MANAGEMENT

Introduction

This chapter provides some general guidelines for addressing the six critical activities presented in Chapter III, which constitute the core of the operation of an emergency and security system:

- Receiving and handling requests, calls, and reports for assistance and identifying the situation
- Information gathering and classification according to the incident, risk, and level of priority
- Event creation and documentation (incident sheet)
- Relaying information and allocation of units
- Unit arrival and assistance
- Documentation and operational closure of the event

This chapter recognizes the need to develop protocols for these six critical activities with a series of clearly defined steps and procedures to guide the actions of operational personnel in an objective, uniform, and institutionalized manner. Accordingly, phases are identified, and a set of considerations and criteria are presented throughout this chapter, aiming to standardize the implementation of these six critical tasks.

The chapter also stresses the importance of standardizing emergency call handling and response in several protocols, from three perspectives:

- Personnel: as a resource for training operational personnel, guiding their actions, and evaluating their performance.
- Management: as a parameter for comparing what has been done and what was expected.
- Quality: as a tool for identifying shortcomings and deviations from what has been established and introducing improvements.

5.1. Handling requests, calls, and reports

The management of emergency requests, calls, and reports would have to be supported by technologies to facilitate data recording and query and other functionalities such as:

- Display of instructions to guide the call
- Activation of an on-line form with classification and prioritization rules, and a typology of incidents from which to select
- Geolocation, addresses, entry points, and geographic reference points
- Identification of the user's phone number or IP, among others

The design of the information architecture and the technological support would have to minimize opportunities for introducing biases and errors during the process of recording personal and incident information on the incident sheet.

The development of standards and protocols for processes, particularly those identified as critical to the mission of the emergency and security system, would also be key to making the task of emergency call handling, response, and closure more objective and consistent.

The operator who receives an emergency request, telephone call, or report would have to have an automated system that generates a registration code and provides instructions or guidelines for filling in the incident sheet with pre-established fields and selection options.

Additionally, the system would have to recognize and display on the screen the basic information on the user, such as the fields listed below:

- Telephone number or call address (IP) (in case it is necessary to call back)
- Address or location of the person (which will not necessarily coincide with the location of the emergency)
- Person's name

The availability of call location data will depend, among other factors, on each country's established telecommunications regulatory framework, including landline and mobile telephone companies.

If the system cannot recognize the three fields listed above, the operator would have to ask a series of questions to capture the person's basic information and location. Likewise, the operator would also have to complete the information based on the Computer-Aided Dispatch (CAD) pre-established fields.

Another important step would be to verify and complete the information on the incident sheet, based on the logs saved in the system's databases. The operator would have to complete the report with information available in the databases, including the number of calls received from that telephone number or IP address and the types of calls (appropriate or inappropriate) made, as well as other information.

Each system would have to define response protocols based on the type of communications channel, type of call (appropriate or inappropriate), and type of incident. These protocols would have to include a script with a series of predefined questions that can be used to guide the communication with the user in a standardized manner, gather information to handle the emergency, and respond to the different types of emergencies promptly and with the appropriate units and resources, based on their complexity and level of priority.

Every public safety answering point (PSAP) would need to have the ability to process an atypical volume of calls that exceeds operational capacity and that could significantly affect the emergency response. To this end, the following recommended mitigation measures could be considered, subject to the availability of a contingency budget that could cover additional costs in extraordinary times:

- Have trained contingency personnel (video surveillance operators and administrative staff)
- Have contingency consoles and the respective technological support
- Enable additional support spaces
- Redirect calls to other public safety answering points

Video surveillance cameras could be another channel through which the system could capture incidents classified as emergencies (priority or level 1). There are at least two ways to accomplish this task: manual or automated. The former would involve relying on video operators, specially trained to monitor and detect emergencies. The latter would depend on the availability of "smart" cameras with the built-in ability to identify critical incidents. Both cases would also have to be governed by specific protocols.

5.2. Risk classification and prioritization

In Chapter III, in the section regarding the information architecture of an emergency and security system, reference was made to the need to define a typology of incidents, with unique and mutually exclusive categories, clearly defined, and covering all possible areas of emergencies.

This typology could be displayed on the operator's screen as a list of incidents from which to select.

A typology of risk levels would also be needed to prioritize the response. Chapter III also introduced an example of possible levels of prioritization.

5.3. General guidelines for drafting protocols

Given the centrality of receiving and handling emergency calls, requests, and reports, and from a quality management perspective, it would be necessary to standardize procedures in protocols that would contribute to the consistency, continuity, and efficiency of the services provided.

This endeavor, operating within the framework of indicators, control mechanisms, and tools to measure the quality of service provided, would facilitate the identification of deficiencies and weaknesses, introduce the necessary changes and updates, and support the continuous improvement of the system. In addition, it could help identify aspects where personnel training and specialization would need to be strengthened.

Below are some basic guidelines that should be considered for the protocol on calls entering the emergency and security system, organized in four phases:

Phase I. Call taking

- Specify the number of times the phone should be allowed to ring.
- Use a standardized greeting, expressed in a clear, cordial, and calm manner. Specify the number of times the greeting should have to be repeated.
- Establish whether the call is in another language and identify the language. If so, indicate with some predefined code and apply the specific protocol for these cases (see below).
- Identify/evaluate whether the call is appropriate/valid or inappropriate/invalid based on a series of predefined criteria/questions.

- If appropriate, ask for the address, and inquire about the location of the incident, including some geographical references, relying on geolocation, and making use of leading questions to facilitate its location. Ask for the user's name, and if not provided, use a code or acronym to record the lack of that information. For example, "NN" could be used. The operator could briefly explain to the user the importance of having the information that is being requested.

- If it is an appropriate call, but the caller does not provide answers, provide him/her assistance through closed-ended questions. Assess the background or context of the situation.

- Conduct a preliminary inquiry about the incident and complete the form generated by the system.

- Check nearby camera(s) to complete and supplement the understanding of the reported situation, if available.

- In the case of inappropriate calls, the corresponding protocol must be applied, depending on the type of invalid call identified. An example of invalid call typology, with possible categories to consider, was presented in Chapter III of this Guide.

The call-taking protocol should take into consideration different situations in which the person who calls or reports an emergency might find himself/herself, including:

- Inability to speak
- Dangerous or high-risk situation
- Disability

Phase II: Call processing

In this phase, the protocol would have to cover at least two aspects:

- Classification of the incident based on predefined categories in the system, and determination of the level of risk and prioritization merited. The system would have to provide the possibility of re-prioritizing the incident and thus changing the level of risk.

- Validation of additional routing of data and data capture, according to the type of incident, which might be useful for the personnel who will be responding to the emergency on site.

Phase III: Incident response

Depending on the system's operational model, information about the incident and the user would have to be sent to the dispatch area or to the articulated institutions (first-ring institutions). If applicable, it would be appropriate to establish the steps to take to further coordinate with related institutions (second-ring institutions).

The development of protocols at this stage would have to set parameters for a differentiated response scheme, depending on the type of incident and the unique needs that the person reporting the emergency might have, among other elements.

In situations that could lead or escalate to a homicide (intentional), including kidnappings, hostage-taking, intimidation, or death threats, among others, the specific action protocol could consider:

- Activating the multi-dispatch tab in the CAD system to coordinate with various first-responder institutions. Collecting basic data and transferring the call to first-responder institutions for online telephone support and, in parallel, activating the dispatch.
- If this type of incident is captured by video surveillance cameras, the activation of the specific protocol could be accompanied by the dispatch process and monitoring of the emergency scene and its surroundings. In addition, and according to the criminal procedural code of each country, the images captured could be forwarded to the judicial entity in charge of the investigation for possible prosecution and trial.

In cases of **gender-based violence, including the risk of femicide, or domestic violence:** The specific action protocol could consider:

- Activating the multi-dispatch tab in the CAD system for coordination with several first-responder institutions. As a developing or ongoing event, immediate coordination with the police and, if necessary, healthcare units would be appropriate. The CAD could be pre-programmed with the articulated and related institutions that would have to be activated in such situations.
- If possible and necessary, psychological assistance could be provided to the victim either by telephone or other available means until the units arrive at the emergency site.
- If there are video surveillance cameras, and according to each country's criminal procedural code, captured images of cases of *flagrante delicto* could be forwarded to the judicial entity in charge of the investigation for possible prosecution and trial.

In cases of people with **mental health problems,** the specific action protocol could consider the following steps:

- During the design of the system's information architecture:
  - Determine the mental health disorder that could have triggered or unleashed an emergency, including suicide attempts, behavioral changes resulting from the use of narcotic and psychotropic substances, shock from a critical incident or hazardous event, among others.
- During the emergency call
  - Ask a series of pre-defined questions to determine the type of situation that first-responders would be confronting.
  - If it is an emergency, apply general guidelines to calm the caller.
  - Activate the ordinary or multi-dispatch tab, as appropriate.
- During dispatch
  - Dispatch the appropriate units and resources needed.
  - Transfer telephone and psychological first-aid support to the appropriate institution.
- During post-closure
  - Deploy additional post-emergency assistance and follow-up actions with institutions that can provide psychological support.

In cases of **persons with disabilities,** the specific action protocol could:

- Identify the type and degree of disability.
- Provide assistance to the person according to the identified disability.
- Activate either the ordinary or the multi-dispatch tab, as appropriate.
- Dispatch the unit and resources needed and provide telephone support, as the case may require.
- Activate additional post-emergency assistance with supporting institutions, and if applicable, with subsidiary actors

The development of action protocols for specific types of incidents, including the four presented previously, would have to be prepared with the participation and contributions of specialized public agencies and civil society organizations. The specific methodology used to develop the protocols will depend on each country and its emergency and security system.

In cases where a different language is used, the specific action protocol could consider:

- Specifying questions to identify the language the user is speaking.
- Contacting someone from a predefined list indicating their respective language skills, who could responsibly act as an interpreter in handling the emergency or linking with an external interpreting service.
- Requesting support for the interpretation, following the established script.
- The incident sheet or report should have a field for recording the fact that the user spoke another language. This could be done by using a predetermined prefix or acronym.

Phase IV: Closing the call

At this stage, a specific script would have to be developed for closing and ending the call. It could contain some of the following elements:

- Confirming data provided on the location for responding to the emergency.
- Providing the caller with a report number.
- Asking if the person needs anything else.
- Incorporating a closing sentence.
- Providing the operator's name and number or code, if applicable.
- Waiting for the user to hang up first.
- Ending the call.

Depending on the type of incident, the unique needs of people reporting an emergency, and the different communication channels available, including web applications, mobile applications, SMS service, voice messages, TTY devices, and help/panic buttons, among others, specific protocols would have to be developed for each of the possible combinations.

5.4. Transfer of information to dispatch services

According to the operational model adopted by the system, the operator would have to relay or route the captured information.

There would be different types of possible transfers:

- Standard (typical) emergency:
  The operator would have to transfer the incident sheet or report to the dispatcher of the institution indicated according to the type of incident. This submission could be performed by the CAD system automatically based on the classification of the emergency that the operator selected.

- An emergency requiring joint action between two or more articulated institutions:
  If necessary, depending on the complexity of the incident, and if the CAD system does not provide for it, the operator would have to forward the information simultaneously to two or more first responders or support institutions for in-the-field coordinated emergency assistance.

- Emergency in progress:
  In this case, the operator would transfer the "basic" information so that the first-responder institution can provide telephone support to the caller until the unit arrives at the emergency site.

- Manual dispatch:
  These are emergencies assigned and communicated directly employing a form, file, or physical record that is hand-delivered to someone responsible for providing dispatch services. This type of dispatch would only be possible when operators and dispatchers are in the same location.

The system would have to consider mechanisms to safeguard the information that has been captured in the incident sheet or report, and transferred to dispatch services, from possible contingencies to avoid information loss. Along those lines, information could be recorded manually or the resend function could be used to forward the information captured digitally once the contingency has been overcome.

5.5. Dispatch and monitoring of units

Based on the operational model, the information architecture of the system, and the characteristics of the computer dispatch system (CAD), the operator or dispatcher could have access to different functionalities to facilitate the coordination of operations with the institutions required to assist in an emergency. Some of the basic functionalities that could be considered are:

Ability to manage/assign. The system would have to allow assigning units or resources based on the operational availability of the first responder institutions and related institutions, if applicable

Ability to cancel/modify. The system would have to have the option to abort or modify the dispatch of units in cases where response operational personnel determine that dispatch is unnecessary or needs to be adjusted.

Ability to scale up. The system would have to allow the possibility of scaling up the handling of the emergency, adding other necessary institutions once the risks and the complexity of the emergency have been verified in the field.

Other additional features to consider would be:

Locating the incident and managing the deployment of dispatched units. The system would have to allow the dispatcher to access the information captured by the operator and dispatch the nearest unit(s) or resource(s) able to reach the incident site in the shortest possible time.

Simultaneous management of multiple services. The system would have to allow the dispatcher to:

- Evaluate emergency information.
- Validate incident information, if required.
- Provide telephone support according to established protocols.
- Identify whether the dispatch of unit(s) and resource(s) is required.
- Assign the available unit(s) and resource(s).
- Record the status of the unit(s) and resource(s) (for example: assigned, on the way, on-site, processing, return, completed).
- Check the arrival of the unit(s) and resource(s).
- Provide feedback to the emergency response system regarding the incident.
- Update the incident information.

Ability to modify the initial incident (re-categorize). The dispatcher/supervisor would have to have the ability to change or re-categorize the initial incident sheet or report, depending on the information reported by the units that arrive at the emergency site through a call or the video operators.

Permanent communication, support, and monitoring of units in the field. Dispatchers should be able to interact with operational personnel assigned to the reported emergency and provide them with all the necessary information to respond adequately to the emergency.

Support provided by video surveillance cameras.[6] The system would need to utilize the video surveillance camera platform to provide needed support and monitor the units deployed in the field.

Depending on the type of cameras available to the emergency and security system, the video operator should be able to:

- Check the operability of the cameras and be able to operate them.
- Monitor assigned cameras.
- Check if the camera has technological support elements (IP speakers, specific software, and sirens, among others).
- Identify the occurrence of incidents based on established protocols for monitoring and analyzing images.
- Record the incident (normal or multi-dispatch), as applicable, identify the response institution(s) that would have to handle the emergency, and send the incident sheet to the dispatcher, based on the established protocols. This flow would depend on the operational model adopted by the system and, among other elements, the type of cameras available.
- Once an emergency has been reported and a unit has been assigned and dispatched, the camera system could be used to provide visual support, accompany, and track emergency assistance in the field, and monitor and protect deployed personnel.

[6] Video surveillance camera networks could also play a deterrent role, focused on preventing the occurrence of offenses, anti-social behaviors, and crimes. They could also be an integral component of the alert system. Having predefined a typology of incidents and depending on the technological sophistication of the cameras available to the emergency and security system, these could help detect the occurrence of certain incidents, including accidents and disasters, and alert the corresponding institutions, according to the adopted operational model.

5.6. Capturing, displaying, and storing data

5.6.1 For the operation

In each request, call, or report received, regardless of the channel or medium used, the recording and entry of the data would have to be done in a standardized manner, depending on the information architecture, the technological support available, and the protocols developed, covering reception, dispatch, and assistance until the closure of the incident.

The information and technological architecture would play a vital role in the accessibility and use of forms to be completed, the availability of supporting tools to complete such a process, as well as the display of such information. Data captured throughout the process would have to be stored on the system's databases and servers.

Some of the minimum fields that would have to be filled out are:

- Name of user
- Address or location
- Geographical reference of the location of the incident
- Phone or IP number
- Incident or emergency type
- Description of the incident
- Assignment and dispatch of unit(s) and resource(s) responding to the emergency.

5.6.2 For evaluation and continuous improvement

Timely and complete data entry from the time the emergency request, call, or report is received until the incident is closed would be essential for service quality management and continuous improvement.

Thus, based on the information architecture devised and the technological support of the system, it should be possible to automatically calculate and record a series of indicators during and after the emergency, based on preset quality controls.

The quality controls should cover the six critical activities that make up the core process of any emergency and security system. They could be carried out by applying quality control templates or matrices, which take into account several predefined categories, criteria, and indicators. These templates or matrices could be applied to incident sheets or reports, recorded audios, and operational activity logs.

If quality control cannot be performed on the total universe of requests, calls, and reports received or dispatches deployed by the emergency and security system, a representative sample could be calculated. The sample's representativeness would have to contemplate the weight or incidence of each type of request, call, and report received, including appropriate and inappropriate ones. Regarding the quality control of dispatches, the sample would have to represent each type of emergency incident responded to and the articulated (or first responder) institutions and related institutions involved in the assistance provided.

As mentioned in Chapter IV, evaluation or control indicators should be able to measure the quality of the service provided, determine the level of compliance with standardized protocols and criteria, and follow up on the goals and objectives established as part of the strategic and operational plan. Regarding users' feedback, other tools mentioned in that chapter were satisfaction surveys, follow-up calls, focus groups, and complaint and suggestion mailboxes (in-person or virtual), among others. In addition, regarding articulated and related institutions, the feedback tools mentioned were, among others: after-action reviews, post-emergency follow-up meetings, and technical panels.

All this quantitative and qualitative information would have to facilitate the identification of deficiencies and weaknesses, and provide the basis for proposing improvements in specific processes and protocols, introducing new standards, and strengthening specific training related to the demonstrated gaps.

Based on the calculation of these indicators, the quality controls applied, and the feedback received from both users and the articulated and related institutions, the system could also generate a series of reports to guide management (at the operational, tactical, and strategic levels), and the process of continuous improvement. Chapter III referred to some of the general reporting requirements that an emergency and security system could consider.

CHAPTER

06

HUMAN TALENT MANAGEMENT

Introduction

The strategy for managing human talent in emergency and security systems should be directed toward skills development. Additionally, it would have to ensure sufficient personnel with the capacity to respond in a timely and appropriate manner to the entity's demands, sustain the continuity of operations, and contribute to the fulfillment of the objectives and goals set out in the strategic plan.

People are an essential resource of any organization, particularly in an emergency and security system. Their work aims at preserving people's lives in stressful and high-pressure situations. Not everyone is prepared to perform the critical tasks inherent to an emergency and security system, particularly regarding the six main activities presented in Chapter III of this guide. A set of specific skills, abilities, knowledge, and aptitudes would be needed for adequate performance in an emergency care center. Therefore, human talent planning and management that involves recruitment, induction, evaluation, training, and retention, emerge as crucial processes.

In the following sections of this chapter, a series of guidelines will be provided on the five stages leading to sound management of human talent from the standpoint of an emergency and security system.

6.1. Planning and management of human talent

Having characterized personnel as one of the primary assets of an emergency and security system, it would be necessary to adopt a planning process that results in an institutional strategy to guide the management of this asset.

The strategic plan (see Chapter II of this guide) and the objectives set in the short, medium, and long term should be considered the starting point for the planning and promotion of human talent. Based on these objectives, it would be necessary to identify the human resources needed to achieve them, establish working models, and define the main processes for human talent management. (Section 6.2 of this chapter presents six possible main processes that characterize the operation of this functional area).

Similarly, planning would have to look at training and career path expectations to strengthen technical skills and abilities, in line with emerging and/or expected changes, innovations, and new challenges. In addition, investing in people's professional growth would serve to promote loyalty, motivate staff, and strengthen a sense of commitment to the entity.

In addition, as part of the planning process, it would be necessary to define specific objectives that should be achieved through the implementation of the human talent management strategy that results from the that planning process. Some of these objectives could be to:

- Attract and retain the best human talent with the skills required for the different job positions.
- Ensure the professional and human quality of personnel who work in the different areas or processes of the emergency and security service.
- Strengthen staff capacities to provide efficient and effective service to the population.
- Identify opportunities for each position and define limitations.
- Maintain a good working environment.
- Encourage team spirit, bonds of trust, and a sense of belonging.
- Anticipate and prepare personnel for risks and possible setbacks that could affect the entity's management and continuity of service.

Human talent planning would have to quantify and qualify the required personnel, by functional areas, projecting the quantity and type of resources needed to meet the entity's personnel requirements.

Qualification would involve defining roles, responsibilities, and profiles for each position, by area, within the entity. This would be one of the most complex and, at the same time, most necessary processes to carry out. It would have to be compatible with the assessment of institutional capacities and the projected demand for services. Based on this modeling, it would be possible to know what kind of talent it would be necessary to attract and, at the same time, foresee what training aspects would need to be developed or strengthened internally.

This process could be divided into two phases:

- Job analysis: the process of gathering information related to the job through various techniques.
- Job description: the process of capturing, in writing, the objectives, main functions, and profile of the job, as a result of the analysis performed in the previous phase.

6.1.1. Job analysis

The analysis of job profiles or positions would seek to identify the functions with the essential skills required and could be carried out through the implementation of various techniques:

- Interviews:
  - With the job incumbent
  - With the person responsible for supervising the job position
- Direct observation of the performance of the functions of the job
- Structured questionnaires to be completed by the job incumbent
- Evaluations
- Journaling by the current incumbent
- Expert groups

It is important to note that it would not be necessary to interview or apply a questionnaire to all those in the same position when multiple positions have the same roles and responsibilities. In these cases, it would be possible to work with a sample.

When this analysis is performed for the first time, and there is no experience in the entity for modeling tasks in each position, it would be possible to resort to expert groups or consult with other emergency and security systems, examining profiles, processes, and functions.

6.1.2. Job descriptions

The job description is the synthesis of the modeling of functions based on the information collected during the previous analysis.

The result would have to be reflected in a document clearly identifying each and every assigned responsibility, obligation, and task.

In that there are various operational models, which were presented in Chapter III of this guide, specific profiles would have to be considered, consistent with four essential operational functions of an emergency and security system: reception, administration, response coordination, and dispatch, which are usually reflected in essential roles such as:

- Call taker
- Video operator
- Dispatcher
- Supervisor/coordinator

In addition, for the configuration or profiling of job positions, it would be possible to follow the guidelines presented in Chapter IV concerning the tasks of the six most essential activities for the operation of an emergency and security system:

- Receiving requests, calls, or reports for assistance and identifying the situation
- Information collection, classification, and prioritization
- Incident creation and referral/ transfer of information
- Assignment and dispatch of response unit(s) and resource(s)
- Coordination, supervision of communications, and monitoring of response unit(s) at the place or site of the incident
- Operational closing of the case

Specifically, the job description or profile could be structured based on the following dimensions:

- Identifying information. Usually found at the top of the document. Presents general information on the job position, including its location and position within the entity's hierarchy. It could include the following fields:
  - Code
  - Name of the job position
  - Position within the entity
  - Administrative or operational unit
  - Role
  - Occupational group
  - Degree
  - Area
  - Source(s) of the information used to develop the analysis of the position and the name of its author

- Dates of preparation and verification of the analysis
- Economic considerations, such as whether the position is exempt or subject to overtime pay

Summary of the position. Brief introductory abstract relating to the obligations, responsibilities, or tasks associated with the position and the skills necessary for its performance, including the emotional ones. It would also indicate the place it would occupy within the organizational hierarchy.

Position interface. Would explain the relationship between the essential activities of the job and internal and external users.

Obligations and responsibilities. In this dimension, the following questions should be answered:

- What is to be done in the position?
- Why should it be done?
- How and with what tools is the work done?
- Where is the job performed?

Answers to these questions should be entered in protocols to guide the position incumbents with regard to their obligations, responsibilities, and tasks to be carried out, and how to do them. These, in turn, would serve as a parameter when evaluating and rating performance.

Specifications and qualifications required for the position. This section would clearly present the necessary skills, experiences, and training to be required of the person to carry out the tasks associated with the position.

Area of knowledge. Technical career of formal instruction required of the person to hold the position.

Work experience required. Level and type of experience required to carry out the tasks associated with the job.

Training required for the position. Topics of training courses and certifications linked to the job that the interested person would have to have.

Technical skills.Skills referring to specific standards linked to the correct performance of positions in a technical area or specific function.

Organizational skills. Basic skills that people who aspire to join the entity would have to possess. They consist of behavioral skills such as a focus on quality, teamwork, innovation-driven, commitment to the values and ethical principles of the entity, among others.

Emotional skills. Personality traits and set of capacities, abilities, and attitudes needed to appropriately process, understand, control, and express emotions and stress levels related to the position.

- Health conditions required for the position. Specify whether some diseases (such as epilepsy) or pre-existing conditions (such as hypertension or diabetes, among others) would be incompatible with the job due to the stress levels and the high emotional burden that the job entails.

Capabilities could be understood as a knowledge, abilities, and skills set that allows for the effective performance of a particular job in the service chain of an emergency and security system and contributes to the achievement of the objectives and goals of the entity. They are used both to define the job profiles and to establish the parameters with which to evaluate the performance of staff.

Capabilities could be regarded as dynamic. They can be acquired and developed throughout a person's professional career. In addition to the technical and organizational capabilities mentioned above, management skills and other skills could also be considered.

The structure and characteristics of the jobs, and the skills needed for each of them would be subject to the internal organization and the human talent management model adopted by each entity.

6.2. Functional area for the management of human talent

The planning and management of human talent would have to be entrusted to a specific functional area. This area would be in charge of implementing and operationalizing the institutional policy guidelines for such purposes, as outlined in a plan that is the result of a planning process.

The functional area would have the mission of supplying the entity with the best possible human resources for each job position, covering the entire work life cycle of an individual's participation in it, from the time a requirement arises for a given position until the end of the employment relationship between the individual and the entity.

The timely provision of the talent needed by an emergency and security system is critical for the smooth functioning of its operations, for maintaining efficiency and quality in its services, and for achieving its objectives and goals.

The functional area would have to be structured and organized to define and manage the following fundamental processes, among others:

- Recruitment and selection
- Induction
- Development (continuous training program)
- Evaluation
- Loyalty and retention
- Departure

All these processes would have to be reflected in protocols. They would also have to be guided by the principle of non-discrimination[7] and a gender perspective, and they should be in line with each country's regulatory framework, and labor and trade union policies.

6.3. Recruitment and selection of human talent

After the assessment, analysis, and definition of the job profiles have been completed, recruitment and selection of the appropriate personnel would proceed.

Recruitment and selection of personnel could be structured based on five phases, within the current legal regulations of each country:

Need: as a first action, it would be necessary to identify the area in which staff must be incorporated or strengthened and to define the skills profile to meet the area's requirements. At this stage, the availability of economic resources and the projected demand for services would have to be analyzed.

Recruitment: this is the phase where the recruitment of candidates would begin, using different sources and channels, according to the defined profile. The job profile would indicate the desired technical skills, capabilities, training, and experience for the position. It would also specify the benefits and compensation that the person interested in the position could expect.

It would be helpful to consider selectivity and prioritization criteria to establish which aspects of the profile are vital and essential and which are important but not decisive for the position.

Depending on the positions or jobs to be filled, the job announcement could be both internal and external. These two approaches are not mutually exclusive. There are many ways to issue the job announcement, including traditional media and social networks, the website of the entity itself, job search platforms, universities with job placement services for their graduates, among others.

Screening and evaluation: phase in which the qualifications of candidates would be verified by conducting tests, interviews, and checking references. It would be helpful in this phase to have predefined criteria for technical admissibility.

Evaluation of candidates would begin at this stage, based on the applicants' resumes, any other supporting material that had been requested, and the requirements established for the position.

[7] Non-discrimination based on race, origin, religion, disability, gender, sexual orientation and/or political affiliation.

To ensure the transparency of the process, it would be necessary to verify compliance with technical and administrative requirements for applying and validate the background history accredited by external entities, including law enforcement, vocational or higher education centers, among others.

After identifying candidates who meet the profile, a series of tests could be conducted to confirm and evaluate skills. To do so, at least three types of tests would be recommended:

- Technical tests: seek to validate the candidate's ability in skills focused on the position, —for example, typing, programming, or language tests.
- Competency testing: aimed at assessing the skills associated with efficient and effective performance in a position.
- Psychometric personality tests: conducted to reveal personality traits consistent with the obligations, responsibilities, and tasks of the job and the levels of stress and emotional burden that the person will have to face.

Basic and/or specialized knowledge and psychometric tests could also be conducted. At this stage, one or more interviewers could conduct a series of interviews with the shortlisted candidates.

Besides measuring and determining job-specific qualifications, capabilities, knowledge, prior training, and experience, it would also be essential to identify early in the process a vocation and attitude for public service among the candidates.

Selection: this is the final phase of the process. From the group of shortlisted candidates, the candidate who best meets the requested requirements and presents the best skills and capacities for performing the tasks inherent to the position would have to be selected.

Hiring: if accepted, the applicant's selection would be notified, and the contract would be drafted according to the current legal framework of each country.

In addition, hiring may be preceded by medical examinations, both physical and mental, and checks on criminal record. Moreover, within the entity's occupational safety and health policy framework, these reviews could be repeated with a predefined frequency, depending on staff members' obligations, responsibilities, workload, emotional burden, and stress levels.

6.4. Induction of human talent

Any staff member who joins the entity would have to go through an induction process. Induction would allow the person who joins the entity to become familiar with it, its mission and vision statement, with the values and principles that guide its decisions and actions, and the objectives it seeks to achieve, among other aspects.

Induction is also an appropriate time to familiarize new staff members with the entity's standards, processes, mechanisms, and operations, among other aspects. It is also the moment to start building a sense of belonging and commitment to the entity and to launch the professional career of each new employee.

A distinction could be made between administrative and technical personnel on the one hand and operational personnel on the other. The latter works directly with call reception, dispatch, and emergency response. The organization, distribution, and degree of centralization of these functions will depend on the model of operation adopted, as already mentioned in Chapter III of this guide.

Depending on the above, at least two induction processes could be considered: general and operational induction.

- General induction: would apply to all new personnel and would include general information on the institution and its mission, vision, values, process map, general policies and regulations, working conditions, and any other general orientation aspect to be added.
- Operational induction: would focus on personnel in areas related to receiving requests, calls, and reports, dispatch, and emergency response in the field, wherein guidance would be provided on protocols and processes, and the use of technological and communication tools and platforms, among other aspects. It would be advisable to include a section focused on physical and mental healthcare and managing work stress, indicating the services and mechanisms available for their treatment.

In contrast, if the operational model is one where the emergency center is the coordinating body among response institutions, each institution would be responsible for the recruitment and training of its personnel. In these cases, it would be advisable to develop a common induction process for field personnel providing emergency assistance. This induction process could focus on the protocols and procedures to be applied across the board, with a view to promoting integration of the service, and mitigating possible clashes between different institutional cultures and work practices.

Some minimum content recommended for this type of operational induction is presented below:

- Components and stages of the service chain, classification procedures, dispatch frameworks, use of technical equipment, specific actions in large-scale emergencies, and other related topics.
- Legal framework, code of ethics and code of conduct, protocols for providing services and managing specific emergencies, including the cases presented in Phase III: Incident response, in Chapter V.
- Effective communication with callers, emergency call processing, ethical and psychosocial aspects of receiving calls, and stress management methods, and other related topics.
- Risk analysis and incident management, coordination of rescue services interventions, among other related topics.
- Teamwork and coordination roles.
- Use of information and communication technologies.
- Learning technical glossary and communication codes with internal users.

If possible, the operational induction process would also have to be linked to the socio-affective process of integrating new staff members with the team or work shift.

In addition to general and operational induction, new employees would also have to receive specific induction to the job position for which they have been hired, in line with the induction and training program established by the entity.

Representatives by area could also be responsible for accompanying new employees during their first days (between 7 and 15 days). This type of support could facilitate their adaptation period and speed up the learning curve. It would be advisable to involve experienced personnel with a high sense of belonging and institutional commitment to act as tutors or mentors.

After the induction process has ended, a trial period could begin in which the person would have to demonstrate that he or she can perform well in the position for which he or she was hired. After that trial period (which could be between 3 and 6 months) has ended, an evaluation would have to be carried out to determine whether the person has adapted to the position or not. If the result is not favorable, the entity would have the ability to not extend the contract, and would restart the recruitment and selection process.

Due to the nature of the work carried out in emergency and security systems, these trial periods allow both parties to determine whether or not the job, the obligations and responsibilities associated with it, and the person initially hired to take them on are compatible.

6.5. Ongoing training to strengthen skills and capabilities

In any emergency and security system, the quality and efficiency of the service provided depend, among other factors, on the level of preparation and experience of its personnel. For this reason, training is one of the pillars of continuous improvement and development of human talent.

Ongoing training would have to follow a learning and specialization program. There are recommendations for developing such programs that could serve as a guide and reference, including those provided by NENA, EENA, IAED, and APCO, to name a few[8]. Training would have to be implemented as a process, in connection with the objectives and goals defined in the strategic plan, and based on a learning and specialization program defined by the entity itself, according to service demands and the need to strengthen personnel's skills.

Such a continuous training program should start from a baseline and the timely identification of gaps and improvement needs. The baseline could be built from assessments at the time of hiring, job adaptation assessments, performance evaluations, among other sources. The program would have to incorporate training and certification courses, with the latter provided by accrediting agencies.

Technological platforms could support training and incorporate different practical experiences, case studies, and, if possible, simulation. Given that not everyone would be able to participate in the trainings, strategies and tools could be put in place to facilitate internal knowledge- sharing and transfer.

[8] EENA: https://eena.org/knowledge-hub/documents/training-of-emergency-calltakers/
NENA: https://www.nena.org/page/trainingguidelines
International Academies of Emergency Dispatch (IAED): https://www.emergencydispatch. org/home
Association of Public-Safety Communications Officials (APCO): https://www.apcointl.org/training-and-certification/

Training would require qualified or certified instructors, up-to-date training materials, logistical supplies, space, and equipment.

Evaluations should be performed at the end of each training session to measure knowledge and goals achieved, based on the established learning objectives. Evaluations would also facilitate the detection of new topics and help track and provide feedback to staff members.

The use of other tools to support the ongoing training program could also be considered, such as:

- A record of the training sessions provided, with a series of systematized data on its organization and participation, among other aspects, and the respective evaluations.
- Trainers' directory, containing information on trainings provided, evaluations received, and other systematized data.
- Indicators to measure impact and implementation of what has been learned in the respective work areas.
- Case management system of personnel files that in addition to the training carried out and certifications received, would include the post-training indicators, the hours and number of training days, the skills, capabilities, and experiences acquired, among other aspects.

The ongoing training program should also be the subject of an evaluation. Efforts to determine the effectiveness of the training provided should identify improvements in processes, products, and services as well as users' satisfaction with the services received.

6.6. Performance evaluation

Performance evaluation is an essential tool at the individual and organizational levels.

At the individual level, it would:

- Provide feedback on the work done.
- Highlight achievements and performance.
- Identify strengths and weaknesses, and propose measures or actions to overcome the latter.
- Suggest or update career and development plans.
- Set goals and communicate the expectations that the entity has for the person.
- Guide promotion as well as layoff decisions.

At the organizational level, the analysis of performance evaluations would facilitate the planning of strategies to guide the staff's professional growth and serve as input to inform the ongoing training program, among other uses.

Such evaluations would have to be reflected in the quality of the service provided and users' satisfaction. For this reason, they must be considered an activity closely linked to comprehensive quality management and continuous improvement of the entity (see Chapter IV of this guide).

Performance evaluation would have to be conducted in a cyclical, ongoing, and objective manner, with the necessary instruments. It is a process that would have to be guided by specific criteria and indicators to rate personnel on their work, performance, and behavior.

Some minimum dimensions that could be considered when evaluating staff performance are:

- Professional performance
    - Meeting established objectives/ goals regarding roles, obligations, and responsibilities associated with the job
    - Quality of work done
- Personal performance
    - Interest in the work done
    - Ability to do teamwork
- Behavior
    - Compliance with standards, protocols, and instructions
    - Attendance and punctuality

6.7. Loyalty and retention of human talent

The steep learning curve and high level of expertise required for emergency and security systems' personnel make it necessary to establish internal strategies and mechanisms to retain human talent and prevent their departure.

The entity would have to create the conditions for people to develop a technical or professional career with prospects for promotion, professional growth, and job opportunities. One of these conditions is the salary that employees receive. The salary amount should be aligned with the responsibilities and functions that the person performs and be as competitive as possible, based on what the labor market offers. Incentives and benefits could also be established to retain qualified staff members. In this line, the entity could, for example, recognize and reward the outstanding performance of its personnel. To that end, it would be necessary to:

- Establish criteria, indicators, and mechanisms to identify those who stand out for their performance.
- Define a recognition and incentives' scheme, according to both individual and group performance areas.
- Systematize outstanding staff performance, communicate, and share these good practices within the entity.

6.8. Departure process

Regardless of the reasons, the process of an employee's departure or termination would have to comply with the legal regulations and internal procedures defined by the entity for such situations.

The departure of a staff member, particularly when retiring or when being professionally appreciated by the entity, may not necessarily mean losing the ability to utilize his/her talent. There are several ways in which the entity could maintain ties with specific people considered to be of high value due to their cumulative knowledge and expertise. The tacit knowledge of these people could be retained through filmed interviews or podcasts available to all personnel. They could also remain linked to the entity as instructors, forming part of its trainer's directory. In addition, in specific situations, they could remain available as experts, to be consulted during specific situations, or as tutors or mentors to guide entry-level and mid-level staff.

6.9. Occupational health and safety

The human talent of the entity could be used to advantage to the extent that the health of staff members is protected and promoted, and a safe and healthy work environment is established and maintained. This would require having and implementing an appropriate occupational health and safety policy, given the nature, dynamics, and working conditions of an emergency and security system.

One of the characteristics of working in an emergency an security system is that employees cope on a daily and continuous basis with traumatic and high-pressure requests, calls, reports, videos, and incidents that generate high stress levels and affect their health. To address this, it would be necessary to establish support services, providing medical support as well as specialized psychological containment, treatment, and follow-up to staff members.

It would also be important to establish mechanisms and tools to detect early symptoms and signs of depression, stress, exhaustion, tension, and other similar conditions arising from traumatic situations experienced by staff members. Early detection would allow cases to be channeled promptly to the specialized support unit and thus prevent them from escalating into more complex situations.

In addition to dealing with some of the job conditions that may affect the physical and mental health of staff, an emergency and security system's occupational health and safety policy would also need to address the following aspects (some of which are addressed in Chapter VIII of this guide):

- Risk factors
- Working conditions
- Work accidents
- Diseases
- Absenteeism
- Epidemiological prevention and surveillance systems

6.10. Code of Ethics and Code of Conduct

A Code of Ethics would have to establish the set of principles and values that guide the actions of the entity and personnel. For its part, a Code of Conduct identifies, prescribes, and prohibits specific individual and interpersonal behaviors. In practical terms, this means that a Code of Ethics would have to be operationalized or translated into a set of behaviors to be avoided/rejected and/or to be followed, which would be reflected in a Code of Conduct. Both should be aligned with the mission and institutional objectives of the emergency and security system.

The principles and values that guide actions considered highly desirable would have to be consistent both with human dignity and human rights, and the public value of the services provided to the population.

Some ethical principles that could be considered are:

- The emergency and security service is an asset for public use.
- Public goods and resources are intended exclusively for the entity's operation.
- A public employee's reason for being is to provide a high-quality service to the population.
- Public interest prevails over individual interests.
- The emergency and security system is accountable to citizens for using public resources entrusted to it and for achieving results.

Some ethical values that could be taken into account when creating the Code of Ethics are:

- Honesty. Act with fairness, discipline, and honor in fulfilling obligations and responsibilities, and when providing institutional services.
- Loyalty. Act with faithfulness, companionship, and respect for personal convictions and the entity's vision, mission, and objectives.
- Solidarity. Act selflessly in dealing with the needs of others.
- Respect. Recognize each person as a unique being with individual interests and needs.
- Collaboration. Demonstrate an attitude of cooperation that allows synergy between knowledge and experience to achieve common objectives.

- Responsibility. Execute tasks with a high level of commitment, efficiency, and effectiveness to meet institutional objectives and contribute to the efficient use of public resources.

- Confidentiality. Do not provide information that is restricted by law, from which undue interest could arise, that could cause serious harm to third parties, or be used to jeopardize the purpose of public service or State assets.

Some desirable behaviors that could be taken into account when developing the Code of Conduct are:

- Respect the policies, rules, protocols, and procedures of the entity.
- Do not participate in or publicly support any group or organization that degrades the entity's vision, mission, objectives, goals, credibility, or reputation.
- Do not provide information that is false, misleading, or that creates false expectations.
- Notify the entity of events that could call into question a person's ability to do his or her duty as an emergency and security system employee.
- Immediately report when an employee is convicted of a crime.
- Do not use certification(s) and knowledge for personal or commercial benefit.
- Respect the laws and privacy rights of users.
- Avoid the use of alcohol, illicit drugs, or any other substance that could affect the capacity of the employee and/or the working environment.
- Prevent, avoid, and eradicate discriminatory practices.

CHAPTER

07 INFORMATION MANAGEMENT

Introduction

Information is one of the main assets of an emergency and security system; it is a resource that could be considered strategic. For this reason, it becomes essential to establish and manage a series of processes that guide the information lifecycle and promote proactive decision-making to achieve the fulfillment of the goals and objectives set out in the strategic and operational plan of an emergency and security system.

In turn, this information cycle would need to take place in a safe environment, with protocols and measures to safeguard information and prevent leaks and misuse (see Chapter VIII on Security Management).

Information emanating from or held by public institutions, agencies, and entities, including emergency and security systems, would have to be ruled by norms governing the use and dissemination of information. The primary safeguard would be to protect users' personal information and avoid breaches of national, public, and the system's security.

This chapter provides guidelines on managing the information of an emergency and security system, proposing an information cycle that would operate based on the iteration of at least seven main activities. The starting point of this cycle would be the development of an information assessment, for which it is suggested that some tools be constructed, including an inventory of resources and a flow chart, among others. The end of the cycle would entail evaluating the management of the entire information cycle, conceived and carried out as an institutionalized process in the interest of quality and continuous improvement of the service.

7.1. Information assessment

A possible starting point for information management would be to develop an information assessment.

Information assessments are recommended because they help identify the information sources, flows, resources, and products or services required and generated by an emergency and security system. This identification, in turn, would be the starting point to better understand and guide what needs to be managed in terms of information.

In addition, the exercise should seek to identify the regulatory, organizational, procedural, material, human and other conditions that have a positive or negative impact on the management of information.

It would also enable recognition of the strengths and weaknesses of the information available in the entity and introduce action plans to overcome the weaknesses identified with a view to continuous improvement.

7.1.1. Sources

Sources of information could be classified into two broad categories: internal and external sources.

Internal sources: These are the sources found within the emergency and security system itself, such as internal databases with a history of services provided, users, operational and administrative personnel, equipment, and budget execution. They also include performance evaluations systematically conducted on personnel and satisfaction surveys answered by users of the system.

External sources: These are found outside the emergency and security system, which has no control over or responsibility for them, although they contain useful information for its operation. These external sources could include databases of other public institutions, websites of state agencies, guides and protocols for large-scale emergencies, publications, public opinion surveys, among others.

7.1.2. Information flows

Chapter I of this guide mentioned that an emergency and security system could operate based on three levels: the strategic, tactical, and operationals levels.

The information would have to flow at each level, as well as between levels. These flows would assume the existence of processes that have been analyzed, planned, modeled, and, if possible, automated.

In addition to internal information flows, flows could also be established from the emergency and security system outwards, as well as from outside into the system. In that sense, it would be possible to consider three types of information flows:

- External flows: formed by information from the external environment that enters the system.
- Internal flows: formed by information that, once it becomes an organizational resource, would circulate and be distributed within the system, to be used and reused internally.
- Institutional flows: formed by the information that the organization shares with other entities and audiences, in the form of information and/or communication products and services.

In any case, identifying these flows would not only make it possible to determine the informational reach of an emergency and security system but would also provide greater clarity regarding what type and how many flows would need to be managed.

Some external and institutional information flows would also involve establishing a network of interrelationships with external actors, including suppliers, users, public agencies, and the media.

For adequate management, the assessment could result in a map of information flows considered crucial for providing support to processes and functional areas deemed essential to the emergency and security system during "normal" times and during critical events.

7.1.3. Information resources

A helpful suggestion would be to identify and record the information resources available to an emergency and security system. Based on this, inventories could be generated, organized by type, name, level of operation, use, area/unit/person responsible, among other categories.

There would be at least two types of information resources that would have to be recorded:

- Tangible information assets: these are physical and digital resources through which data, information, and knowledge of an emergency and security system materialize, become explicit, and become available to a variety of internal and external audiences, and for a variety of purposes, from the delivery of emergency response services to accountability, among other purposes.

- Intangible information assets: These are tacit resources, consisting of strategic and tactical information and knowledge (from experience, lessons learned, good practices to feedback received), and used to support the achievement of objectives and established goals.

Like any resource, these would also have to be managed to obtain their best use and potential.

Information systems used by an emergency and security system could be considered tangible assets. These information systems could be identified and classified according to the operational levels where they are used. Thus, the following could be used at the operational level:

- Emergency Call System
- System for the creation of an incident sheet or report, code, and registration number
- Geographic Information System (GIS)
- Automatic Vehicle Location (AVL)
- Computer Assisted Dispatch (CAD) System
- Mobile radio system (trunking)
- Video surveillance image monitoring and analysis system
- Alert system
- Automated data system for judicial bodies

Those that would be used at the tactical level include:

- Statistics system (data warehouse)
- Quality management system
- Information security system
- Document management system
- Geographic information systems
- Service misuse control system
- Financial information system

One of the systems that could be used at the strategic level would be:

- Balanced Scorecard (BSC).

An emergency and security system requires secure information systems, facilitating the collection, storage, processing, and use of information to support emergency operations, decision-making, administration and control, communication, transparency, and accountability.

7.1.4. Products and services

Information products and services would have to be generated according to the needs and requirements of users, operational staff and the system's managers, and projections for continuous improvement of the service.

In turn, the creation of information products and services would depend on the information and technological architecture with which the emergency and security system was designed (see Chapter III of this guide).

Information products and services should also be recorded as part of the information assessment.

7.2. Information cycle

Once the assessment has been made, there are several models for information management. This section focuses on the management of process-oriented information, based on a continuous cycle of seven interrelated activities:

1. Identification of information needs
2. Obtaining the information
3. Organization and storage
4. Development of information products or services
5. Distribution and access to information
6. Use of information
7. Monitoring and evaluation

For its operation, the information management model of an emergency and security system would, at a minimum, require protocols, procedures, and tools for:

- The classification of information and control of documents
- Information security
- Assigning and controlling different types of access to information
- Acceptable use and the consequences of unauthorized use
- Risk assessment and treatment
- Reviewing, updating, safeguarding, and destroying information

This management model could be used to enhance information resources to support decision-making processes and as input for achieving the objectives and goals set out in the strategic plan.

In addition, it would drive knowledge generation, learning, and adaptation to address a changing environment and facilitate synergy with human talent.

7.3. Information at the functional levels

At each of the three functional levels of an emergency and security system, the strategic level, tactical level, and operational level, sources, flows, resources, products, and information services would be needed to guide decision-making.

Strategic level: Decision-making in this area focuses on defining the broad outlines that guide the management, direction, or re-direction of the system and its positioning.

At this level, decision-making rests with high-level authorities, including in the planning area.

This level acts based on external flows of information, internal information, institutional information, and knowledge generated both from experience and at the tactical level.

Tactical level: At this level, decision-making is focused on planning and developing plans, programs, and projects, for which it uses information from the internal flow and institutional information.

Such decisions would fall to high and mid-level authorities and would use the information and knowledge, or learning acquired at the operational level.

Operational level: Would cover everyday decisions for the system's daily operations. This level would be the source of the data captured through the command-and-control system, which consists of other subsystems, including calls, video surveillance, or other alert mechanisms.

Each functional level would have to have an information cycle consisting of the seven activities mentioned above. Each cycle would have to be embodied in protocols and procedures that, in turn, would enable objective review exercises, adjustments, and improvements, as well as possible audits.

7.4. Identifying information needs

Information needs could be defined based on topics, problems, and contingencies.

There are several mechanisms and tools for identifying information needs, including gap analysis, information audits (see Section 7.9 of this Chapter), performance assessments, and after-action reviews.

***Table 22:** Identifying information needs*

TOPIC	PROBLEM	CONTINGENCY
Timely and reliable information generation	Data generation capability; breach of data generation and transaction systems; data transaction speed; consumption of information, among others.	Propose information plans, programs, and projects, based on the transactional platform of the service.
Interoperability	Consumption of secure information with articulated and related institutions; leaks or unintended dissemination of information; maintenance of the chain of custody; delay in requests for information consumption, among others.	Integrate IT platforms of articulated institutions involved in emergency management or activated for specific emergency cases.
Feedback from emergency response management service	Monitoring of operational and technical standards, among others.	Generate statistical information on emergency response management service.
Response times and variables (articulated institutions)	Identification of response times in the field; number of resources available; heat maps, among others.	Estimate the time and multivariables of hazardous situations linked to the operational management of articulated institutions.
Prioritization levels	Identification of incidents or events; assignment of institutional roles; report of resources in the system, among others.	Estimate the magnitude of hazardous situations linked to operational management of articulated institutions.
Emergency response performance	Compliance with international standards in emergency response, among others.	Evaluate and control the operational management of emergency response.
Hazardous situations (articulated institutions)	Inadequate feedback on situations in the field; status of resources, among others.	Evaluate hazardous situations linked to the operational management of articulated institutions, among others.

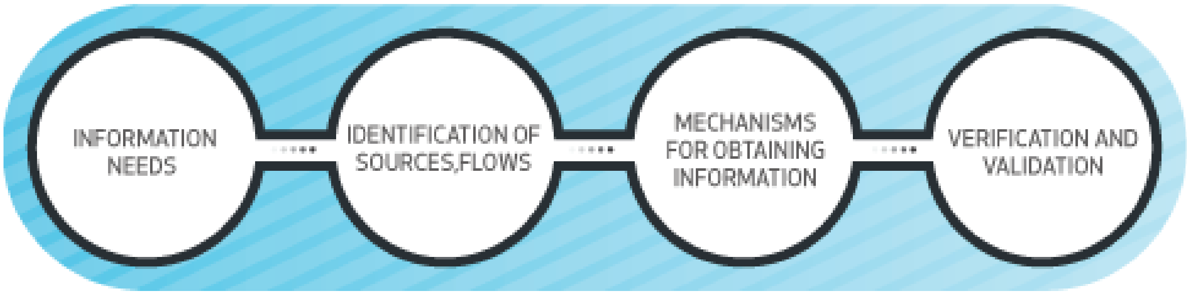
Source: Integrated Security Service ECU-911, 2021.

7.5. Obtaining information

Based on the identified needs, data and information would be gathered accordingly. To do so, it would be necessary to take into account existing information sources, flows, and resources, and to consider incorporating new ones.

The data and information generated would have to be subject to some verification and validation mechanism to ensure minimum quality standards.

Figure 23: *Obtaining information*


INFORMATION NEEDS
IDENTIFICATION OF SOURCES,FLOWS
MECHANISMS FOR OBTAINING INFORMATION
VERIFICATION AND VALIDATION

Source: Integrated Security Service ECU-911, 2020.

7.6. Organization and storage

The organization, storage, and custody of information could be accomplished by creating, maintaining, and constantly updating repositories. These repositories, in turn, would contribute to the institutional memory of the emergency and security system.

For example, the following repositories could be considered: virtual library, reports (including management, emergency services provided, financial, and project implementation), queries or requests for information made by other entities and third parties, among others.

The classification of information in repositories could consider, the ISO/IEC 27001 standard, which simplifies this process in four steps:

- Enter information assets in a repository
- Classification criteria
- Classification by asset (labeling)
- Processing classified information

Information assets in an emergency and security system could be classified according to the following criteria: type, location, retention time, size, storage, security measures, and other attributes. In addition, the person(s) who would serve as custodian(s) or responsible for those assets should be designated, applying principles of rationalization, economics, and screening.

- Asset type
- Location
- Retention times, particularly in terms of documents and archives
- Size
- Storage or support
- Access/Use
- Security
- Responsibility

There would be several criteria for classifying information in terms of access and use. This will depend, among other factors, on current legislation, the reality in each country, as well as the specific needs and circumstances of each emergency and security system.

Despite the above, the criteria for classifying information access should generally be established based on the content of the information and its intended uses. In that sense, the following classification of information could be considered:

- Confidential. Emergency and security systems capture personal information from each user that would need to be safeguarded and protected.
- Reserved or restricted. In general, the reserved classification concerns information related to public and national security.
- Internal use. Accessible solely and exclusively by authorized personnel.
- Interinstitutional use. Accessible for purposes of interacting with other public sector institutions, both in terms of emergency response and as input, as well as inputs for the assessment of problems, the design of public policies to address them, and monitoring and evaluation.
- Public use. Information in the public domain like that found on websites or published through communication and dissemination media for purposes of transparency and accountability. The entity's communication plan should govern this type of information (see Chapter IX of this guide).

Regarding the processing of classified information, particularly when confidential and restricted, it would be advisable to establish security mechanisms to protect it from potential risks, including damage, breaches, leaks, or misuse, among other risks. Some of the most common tools used to safeguard this type of information would be:

- Encrypting information
- Generating and saving backups
- Differentiating and limiting access based on profiles, roles, and responsibilities
- Confidentiality agreements between the entity and other public institutions, as well as between the entity and staff members
- Establishing regulations for inter-institutional information delivery

7.7. Development of information products or services

At this stage of the cycle, the available data and information would be processed, analyzed, and packaged, as appropriate, in products and/or services directed to a variety of internal and external audiences:

- Users in general
- Specific audiences
- Decision makers of the system itself, in the three functional levels
- Decision makers at other state institutions, including Ministries of Health, Ministries of Security, Crime Observatories, and Civil Protection

There are various information services or products that could be developed, for example:

Table 24: *Development of services and/or products*

SPECIFIC NEEDS	SERVICES AND/OR PRODUCTS
Improve the quality of service based on the evaluation and monitoring of emergency response and assistance.	Emergency and security system user satisfaction reports. Statistical reports linked to emergency response and assistance.
Maintain the chain of custody of data that could become evidence in court proceedings.	Provision of information to the judicial branch through the Automated Information Delivery System.
Provide access to public information.	Management reports related to the operation of the emergency and security system.
Improve the level of community readiness, including groups and subgroups in vulnerable situation.	Socio-demographic analysis and identification of risks regarding communities, groups, and subgroups in vulnerable situation, particularly when facing emergencies.

Source: Integrated Security Service ECU 911, 2020.

7.8. Exchange, distribution, access, and use of information

Exchange, distribution, access, and use of information would be subject, among other factors, to:

- Laws and interinstitutional agreements that have been established
- Internal guidelines, protocols, and tools related to the information cycle
- The rating and classification of information in terms of access and confidentiality
- Communication plans, including transparency and accountability components
- Information flows and those responsible for information management

The availability of information in a timely and appropriate format promotes informed decision-making, spurs the learning of the entity itself, facilitates the recognition of new approaches and the disclosure of new problems/solutions. In this way, the emergency and security system could become more resilient, enhancing its capacity to adjust or adapt to changes.

Depending on the intended use of the information, it could be distributed and become accessible in different ways, in various formats, and through various channels or means.

7.8.1. Interoperability and exchange of information

Timely, effective, and automatic availability of data, information, documents, and digital objects among articulated (or first responder) institutions is crucial for providing the population with a quality service.

The recommendation would be for the emergency and security system to have a design that ensures interoperability based on one or more IT platforms that allow the transfer of data and information.

The exchange of information (delivery and use) would have to take into account international and national standards, such as those developed by the International Organization for Standardization (ISO), the National Information Standards Organization of the United States (NISO), or the American National Standards Institute (ANSI).

In addition, internal regulations, protocols, procedures, and interagency collaboration agreements for the exchange of information should also be established, particularly if these are required by law. They would have to specify, among other things, the type of information, format, channels, needs, purposes, and authorizations necessary to enable information requests and deliveries.

7.8.2. Development and continuous improvement of operations

For capacity building, institutional development, and continuous improvement, top executives would need to manage strategic information about the system's operation, including the financial component.

This information could be made available through a dashboard with information on objectives, goals, and indicators. Management, services provided, financial, and project implementation reports could also be made available to top executives through a document management system (repository), sorted by topic and time reference period.

Based on the tools used by the entity to receive feedback, either from users (e.g., satisfaction surveys) and from articulated and related institutions (e.g., after-action review sessions), information inputs for management could be generated. These could be integrated in the document management system, the dashboard, or an information repository linked to quality management and continuous improvement.

7.8.3. Pre-judicial and judicial bodies

The availability and provision of data and information generated or captured by an emergency and security system could serve as critical input for pre-judicial or administrative bodies and judicial bodies.

Regarding the first type of body, the policies, protocols, and procedures established to exchange and deliver interinstitutional information should be used.

For judicial bodies, the legislation of each country could have established mechanisms and procedures for sharing information relevant to the different stages that make up a judicial process. In this context, it would be advisable to provide a specific tool to deliver and share data and information that could serve as evidence in court proceedings. In this way, the authenticity and integrity of the evidence could be safeguarded, thus ensuring its evidentiary value (chain of custody).

The delivery of this type of information should be made through mechanisms that guarantee interoperability, that is, through the development of a platform that allows for the submission *ex officio* or at the request of a party (either the judge or prosecutor), of the information that could serve as evidence concerning alleged punishable acts detected or reported. In this way, the information would be sent directly (point-to-point), encrypted, and without intermediaries. The information would become legible when downloaded by the competent authority (judge or prosecutor), transferring custody, use, and administration to the judicial body. In this way, the risks of leaks, cyberattacks, and viruses could be significantly reduced.

If there is no such platform and no possibilities of developing one, inter-institutional agreements with justice operators could be adopted to define the procedures for delivering information, within the framework established by law. One of the main objectives of these agreements would be to protect the information custody chain, thus preserving the validity of the evidence when it is considered as such in a judicial proceeding.

The tools developed to regulate the treatment and exchange of information with evidentiary value would have to establish the timing and deadlines for responding to requests for information made by justice operators, ensuring the protection and speed of these procedures. Similarly, timetables for information to remain archived within the emergency and security system would have to be defined.

In addition, it would be necessary to introduce legal and technological control mechanisms to keep safe the information that could be used for judicial purposes. These mechanisms would have to be accompanied by clear guidelines for safeguarding the information, to avoid leaks, commercialization, or any other act that could invalidate its use within a judicial process.

7.8.4. Communication, transparency, and accountability

Based on the communication plan (see Chapter IX of this guide), and its objectives, goals, and activities, and the information and IT architecture with which the emergency and security system was designed, the system could produce information of interest, and helpful to the internal public (the system's staff) and external public (general and specific), serving several purposes:

- Informative
- Educational
- Preventive
- Prescriptive
- To generate loyalty and a sense of belonging among staff
- To build trust and legitimacy among the population
- For transparent management and operation of the system, and accountability

There would be several channels or means to distribute and facilitate access to such information, including the intranet, web platform, newsletters (digital and/or printed), reports, and publications (digital and/or printed).

7.8.5. Public policy process

The data and information generated by the emergency and security system, particularly those related to emergency response and assistance, could also become relevant input for other public administration agencies. These agencies could include those working on health, security, domestic violence, and violence against women, natural and man-made disasters, traffic, transport, and mobility, to name a few.

These inputs and the resulting analyses could feed and support the entire public policy cycle, from assessment to design, implementation, monitoring, and evaluation.

There would be several ways to make available the data and information generated by the system based on the emergencies handled. Interoperable systems could be possible between articulated and related entities. If this option is not available, the emergency and security system could generate reports on services provided, with information on emergency response and assistance, prepared monthly, quarterly, every six months, and/or annually. This information would have to be broken down by attributes useful for the design of public policy interventions, including gender, age, type of incident, location of incident, type of incident location, among others.

This type of participation or collaboration that an emergency and security system could provide beyond its direct and immediate field of action, would make it part of public safety governance and, more broadly, public governance.

7.9. Information audits

The seventh activity of the cycle is focused on evaluating information management.

Based on ISO 30401 or similar standards, and the protocols and procedures established for information management, including classification, backup, and protection, it would be advisable to conduct audits to:

- Assess the degree of compliance and enforcement of these instruments
- Measure the effectiveness and efficiency of the information cycle and each of its six activities

As well as to identify:

- Information needs, by levels and areas
- Inconsistencies, duplications, and weaknesses
- New and/or potential information sources, flows, resources, products/services, uses, and users

There would be several types of methodologies for conducting such exercises. The choice would be at the discretion of each emergency and security system, but the following minimum guidelines could be taken into account:

- Clearly present the objectives and purposes of the audit
- Understand the organizational structure, operating levels, information sources, flows, resources, and services/ products, and identify key people with regards to information management
- Design the methodology with which the audit will be conducted: data collection and analysis, interviews, focus groups or any other techniques
- Develop and communicate recommendations
- Follow-up on the implementation of recommendations
- Measure and evaluate changes made based on the recommendations

From a quality management perspective (see Chapter IV of this guide), audits could be considered tools that contribute to the continuous improvement of information management within the entity, overcoming, in a timely and informed manner, any difference, gap, or deviation identified with regard to established standards, protocols, and procedures in this area.

CHAPTER

08

SECURITY MANAGEMENT

Introduction

This chapter presents guidelines on security management that would apply to an emergency and security system. Security could be seen as a critical resource or means for ensuring the delivery of services.

The security management of an emergency and security system should be rooted in the institutional policies, protocols, and tools established for such purpose. International and national security standards in other countries could serve as a reference. These would provide guidelines and parameters to be followed, to be adapted to the realities of each system and each country.

The security of a system that responds to emergencies would have to be addressed from a multidimensional perspective, paying attention to the basic conditions for the functioning of a PSAP and the continuity of services. In this sense, the multiple dimensions of security would encompass: information, communications, IT, physical and infrastructure security, and staff, among other dimensions.

In addition to providing general guidelines for security management and guidelines to ensure the operation of an emergency and security system from multiple dimensions, this chapter also addresses risk and vulnerability analysis to safeguard and ensure operational continuity and the delivery of services in crises.

8.1. Information security

Information security management would find its legal support in all national rules guaranteeing the rights and obligations of individuals and of public institutions providing services. It would also be important to consider the value of information, and of making it available and accessible to the public within the framework of democratic societies and political regimes. This is especially important for conducting monitoring, transparency, oversight, auditing, and accountability exercises (topics addressed in Chapter X of this guide).

Information security would involve the adoption of preventive, proactive, and reactive measures and actions to protect the information of an emergency and security system. It would have to be built on three basic principles: confidentiality, availability, and data integrity.

In addition to being an end in itself, information security would also have to be considered as an ongoing process. As such, it would need to be managed by a specialized team (within the functional area for Security Management referred to in Chapter III of this guide) and guided by a set of policies and protocols established by the entity for such purposes. These should be aimed at preventing unauthorized access, (re)use, disclosure, exchange, interruption, and destruction of the data and information managed by the emergency and security system in different formats, forms, and media.

8.1.1 Information security policies and standards

Security policies and protocols would have to function as guiding tools to shape, standardize, and systematize work in this area. They could adhere to international standards and parameters such as ISO 27000 and the family of standards associated with the certification of Information Security Management Systems (SGSI). They should also be aligned with national standards related to data protection, transparency, intellectual property, among other issues.

In terms of content, they could include general aspects such as:

- Access controls, based on differentiated roles and responsibilities
- Information processing
- Physical and environmental security

More specific aspects that could be addressed and regulated by information security policies and protocols, linked to the functions of an emergency and security system, could include:

- Definition and management of profiles and user accounts (with different degrees/levels of access and security)
- Use and management of access accounts
- Use of messaging services
- Use of software licenses and definition of unauthorized software
- Data protection and privacy
- Physical access control
- Remote access control
- Downloading of files (external/ internal network)
- Record retention and backups
- Use of network services
- Use of mobile computer and communication applications
- Use of cryptographic controls

Information security policies and protocols should be disseminated and publicized among staff members and outsiders visiting the facilities of an emergency and security system.

Based on the policies and protocols adopted by the emergency and security system, the relevant functional area could audit its management in the area of information systems and related technologies. For such purposes, it could use, as a reference, the guidelines established in the Control Objectives for Information and Related Technologies' (COBIT) framework, developed by the Information Systems Audit and Control Association (ISACA).

8.1.2. Treatment of physical and digital documentation

An emergency and security system would have to establish a documented information control process, in line with ISO 15489 and ISO 30301, which establishes instructions and steps for document management.

Procedures would have to ensure secure handling consistent with the importance of internal and institutional information, and applicable at all stages:

- Storage
- Use and reuse
- Access and flow
- Digitization and safeguarding
- Destruction

An emergency and security system would also need to have security measures and protocols for handling information generated or accessed through:

- Office suite
- E-mail messaging
- Portals
- Database systems
- Hard and/or external drives
- Multimedia (voice, video, tape)
- Cloud technologies, or other media

8.2 Security of technology infrastructure for information and communication

One focus of information security management would have to be the IT systems, particularly protecting the IT assets of an emergency and security system. These assets could be classified as:

Hardware: Physical components of the IT system, such as processors, electronics and network wiring, storage media (arrays, disks, DVDs, among others).

Software: A set of programs that run on the hardware, either the operating system itself or its applications.

Data: Logical information processed by the software using the hardware. In general, they will be information structured in databases or information packets exchanged over the network.

Other assets : Such as fungible items used or spent, including ink and paper for printers, DVDs, or other elements. As items external to the IT system, they are not critical to its security.

Of these assets, data are the most critical. Data are stored on the hardware and processed by software applications to support the delivery of services by emergency and security systems. Everything else could be replaced, while data recovery is critical to the operation of the system. Protection protocols would need to be developed to establish the steps and measures to be taken to:

- Recover data in the shortest possible time, and
- Make them usable in the condition closest to when they were lost.

The family of standards associated with the Information Security Management Systems (ISMS) certification also includes basic mechanisms and measures for safeguarding data within an IT system, which could serve as a reference point for emergency and security systems.

8.2.1. Regarding IT systems

IT security policies and protocols should closely follow guidelines to ensure the confidentiality, integrity, and availability of the information handled by the entity. Their implementation would seek to prevent security breaches and keep data safe.

IT security regarding hardware should aim to protect all the physical components that make up a network, using tools to scan and control traffic. These tools could include firewalls, surge protectors, proxy servers, and more.

Servers, printers, firewalls, and proxies would have to comply with the standards and requirements set out in the IT security policies. They would have to be inventoried in physical and electronic formats. Hardware would have to be protected against power supply problems. In addition, the use of external storage devices would have to be subject to standardized protection, control, and security procedures.

Server architecture would have to be designed based on a redundancy and high-availability model. This means that everything housed in its infrastructure would need to be resistant to electrical system outages and failures.

To build a high-availability infrastructure, COBIT Chapter DSS04, particularly section 7 on the management of backup arrangements, could be used as a reference. At a minimum, the following components should be considered:

- Redundant systems
- Redundant disk arrays
- Redundant networks
- Redundant power sources
- Automatic transfer switches (ATS).

IT security regarding software would have to be based on monitoring protocols and frequent testing. Likewise, it would need to consider the validation of security patches and updates, and incorporate antivirus software connected to the internal network. As with hardware, it would be advisable to inventory all software assets such as operating systems, service software, core software packages (office suite, mail client, instant messaging, video conferencing, video editing, database applications, among others).

Some basic mechanisms for the security of IT systems that could be considered are:

- Authentication: Verifies the user's identity, usually when entering the system or network, or accessing a database.
- Authorization: A process that determines what, how, and when an authenticated user can use the entity's resources.
- Administration: Defines, maintains, and eliminates the system's users' authorizations, resources, and user-resource relations.
- Audit: Continuous monitoring of services in production, for which information is collected and analyzed.
- Registration: A mechanism that captures and saves any attempt to violate the security rules established by the emergency and security system on an event database that could then be analyzed.
- Maintaining the integrity of the information: Procedures in place to ensure that files are not changed without authorization and that information sent from a point reaches the indicated destination without having undergone alterations along the way.

8.2.2. Communications security

Emergency and security systems require an increasing number of applications (email delivery systems and browsers, among others) and terminal equipment (phones, central computers, personal computers, and mobile phones) connected to networks. For this reason, the security of communications on data and mobile networks is critical to security management.

The capacity of networks or information systems to withstand accidents or malicious actions that jeopardize the respective services they offer or make accessible depends on the protection and interception of communication traffic and its critical points.

Communications security encompasses storage systems and data processing and transmission systems. These, in turn, consist of transmission mechanisms (cables, wireless links, satellites, routers, and switches, among others) and support services (domain name systems including root servers, caller identification service, and authentication services, among others).

This type of communications-focused security would seek to prevent unauthorized interceptors from accessing telecommunications intelligibly while still delivering the content to the intended recipients. To do so, it could resort to the following mechanisms: crypto-security, transmission security, emissions security, traffic flow security, and physical security of equipment.

It is important to protect classified and unclassified traffic in communications networks, including voice, video, and data. Safe Voice Over Internet Protocol (VOIP) has become the *de facto* standard for securing voice communication, replacing the need for analog equipment.

To safeguard the security of communications, the following guidelines, at a minimum, could be considered:

- Regarding email accounts:
  User names and passwords used to access IT systems would have to be individual and passwords should be created according to a set of criteria to promote higher levels of security.

- Regarding electronic messaging:
  Protection measures would have to be implemented for classified messages, encrypting sensitive content and/or information that could be shared, and monitoring messages.

- Regarding telecommunications:
  Requirements (switches, routers, wireless access points, among others) and servers (web, FTP, mail, and others) could be governed by the ANSI/TIA 942-A standards or some other standard regulated by the specialized body in each country.

8.3. Physical security

Physical security is a subcomponent of facility security, and involves prevention and detection mechanisms to physically protect the system's resources, from physical assets to personnel.

In addition to the technical standards applicable in each country for the design, construction, and approval of working areas for civil servants, the following minimum actions should be considered:

- Assess the current and future condition of the PSAP.

- Periodically analyze and evaluate the operational status and risks the emergency and security system could face in its daily operations.

- Develop, review, and adjust a physical safety plan with measures available to the facility, provide instructions and conduct simulation exercises with personnel.

Regarding physical security, the following minimum elements should be considered:

Physical security and infrastructure:

- Physical security perimeter
- Physical access and exit controls
- Security of offices and facilities
- Protection against external and environmental threats
- Fire protection (see as a reference the NFPA 101 standard), including detection and alarm systems (see as reference the NFPA 72 standard), sprinkler system (see as reference the NFPA 13 standard), installation of fire doors (see as reference NFPA 101), and firewalls (see as reference NFPA 80 standard)
- Evacuation routes and properly marked emergency exits

Security of the equipment:

- Placement and protection of equipment, e.g., against fires, seismic and hydrometeorological events, among others
- Electricity and water supply facilities, among other services
- Wiring safety
- Equipment maintenance
- Off-site equipment safety
- Safe reuse or removal of equipment

Access to authorized facilities and sites

Persons outside the system would have to be properly identified and registered before entering the facility, whether on foot, by vehicle, or by some other means. Registration would have to include, among other elements, the following data: date and time of entry, full name, identity document, the reason for entry, person being visited, as well as the date and time of departure. Photographic records could be taken and credentials or passes generated that would have to be visible while the person is inside the premises.

At entry, visitors could also go through a walk-through or manual metal detector. Additionally, packages could be inspected by an x-ray machine.

Restricted areas would have to be visually identified and access to them would have to be regulated by an internal authorization process, considering personnel's positions and responsibilities.

8.4. Risks and vulnerabilities

Security management would also involve identifying risks or contingencies that could affect an emergency and security system's functions and continuity of operations.

In that regard, implementing processes and tools would be recommended to identify vulnerabilities and potential risks in three of the system's main components:

- Information and communications
- IT support
- Infrastructure

This assessment would serve as input for designing mitigation and contingency, continuity of operations, and recovery plans.

The general recommendation would be to develop a proactive approach to risk management. This approach would require anticipating, reducing, or preventing risks, and taking the necessary preparatory measures to restore the emergency and security system's operations in the shortest possible time, in the event of any of the contingencies identified. For this purpose, at least three essential tools could be considered:

- Risk analysis
- Continuity of operations plan (COOP)
- Disaster recovery plan

8.4.1. Risk analysis

Risk analysis is essential to understanding what prevention, mitigation, and response measures should be introduced so that an emergency and security system can continue to provide its services, regardless of the circumstances. For that purpose, it would be necessary to identify risks that could affect each critical system and service, including the technological and communication equipment supporting and making its operations feasible. It would then be necessary to assess the probability of their occurrence and assess the type and level of their impact. This information could be systematized in a risk matrix.

A risk matrix is a management tool that helps to objectively determine what the relevant risks for safety are. By placing the different types of risk in the matrix, it would be possible to clearly display where the priorities would be and where efforts and resources should be directed. (In Chapter II of this guide, the use of this instrument was linked to the strategic plan.) The following is an example of a risk matrix:

Table 25: Example of a risk matrix

RISK	PROBABILITY	IMPACT	MITIGATION	ASSIGNMENT OF RESPONSIBILITY
Disruption of the power/information backup system between different PSAPs	High in cities on the Pacific coast	Reducing interoperability	Backup equipment	Planning, logistics, and budget department

Source: 9-1-1 National Emergency and Security Response System of the Dominican Republic, 2020.

Risk identification and analysis would have to be accompanied by a plan to contain and mitigate the associated vulnerabilities, with specific actions to be taken, and incorporating the following elements:

- Assignment of responsibility, up to the level of units and teams, so that all parts of the system know how to react and what to do should the identified risks arise
- Budget allocation
- Setting deadlines

8.4.2. Continuity of Operations Plan (COOP)

These plans would help keep support systems, considered essential or critical for the operation of an emergency and security system, available whenever needed, supporting the delivery of services, regardless of the circumstances.

The COOP is an emergency plan that seeks to keep operations at a minimum acceptable level during a contingency or crisis. In the event of such an eventuality, which would negatively impact the system's operations, the plan would have to consider all reaction and recovery measures needed to respond effectively.

The objective of the COOP is to keep the emergency and security system operating. This would entail prioritizing operations deemed critical to maintaining the continuity of operations, at all times, under any kind of contingency being faced.

Some of the benefits and/or advantages of having this type of plan are as follows:

- Early and timely identification of critical processes and assets, prioritizing their protection or ensuring their operation during a crisis
- Definition of critical recovery times and deadlines for returning to the previous status, pointing to contingency plans and protocols
- Prevention and minimization of human and economic losses and adverse effects on personnel working in a PSAP

Recommended steps and aspects that could be considered when designing a COOP include:

- Form a committee and a multidisciplinary work team to anticipate and analyze risks
- Perform risk assessments (probability of occurrence and impact)
- Identify the processes and the criticality of each of these for the operation of the system
- Modularize each critical IT component of the system to ensure the recovery of its operation from any contingency
- Develop and document procedures, indicating objectives and scope, and considering the recovery times for each activity that needs to be executed
- Assign staff member(s) responsible for each action to be executed to ensure nearly immediate continuity
- Develop recovery strategies for potential contingency scenarios where critical processes might be disrupted, including the definition of procedures and roles that would have to be activated to respond and operate in emergencies
- Disseminate and publicize the plan among personnel and train them in functional areas where critical procedures and tasks have been identified. This training would have to be provided regardless of risk mitigation measures carried out, as there will always be residual risks
- Define the crisis communication plan (see Chapter IX of this guide)
- Define the testing and simulation schedule for restoring critical processes based on the disaster recovery plan
- Constantly document and update the plan. Test the plan at least once a year, analyze and document the results, and introduce adjustments and improvements. It would be helpful to create a knowledge database of lessons learned during each test as well as after the actual implementation of the plan during a crisis

8.4.3. Contingency and recovery plans

Contingency planning is a fundamental process for security management in an emergency and security system, and a substantive part of the internal controls established to manage the availability of critical processes and equipment in the event of an outage. The main objective would be to minimize out-of-service time and maximize recovery time. The Business Impact Analysis (BIA) could serve as a reference for contingency and recovery planning.

For the Disaster Recovery Plan (DRP), the guidelines and recommendations regarding the Continuity of Operations Plan (COOP) could be taken into consideration, paying special attention to the following issues:

- Focus on processes and equipment considered critical to the provision of emergency and security services
- Carry out prospective exercises on scenarios that could affect the availability of emergency and security services
- Define the backup actions of the technological and communications infrastructure, which provide support to the critical processes and equipment of an emergency and security system, specifying the frequency and location of those backups
- Define action protocols based on processes and their prioritization
- Define roles and responsibilities
- Define the minimum information required for the emergency and security system to continue operating
- Generate a knowledge database with lessons learned based on plan design, testing, and implementation

8.5. Personnel health and safety

In occupational risk prevention and safety, several professional disciplines come together for the specific purpose of eliminating or reducing the risks associated with work activities. These risks could be causing both occupational illnesses and accidents.

The topic was briefly introduced in Section 6.8 of Chapter VI on Human Talent Management, when reference was made to the occupational health and safety of personnel, which depend on the nature, dynamics, and conditions of work in an emergency and security system. In addition, other aspects that an emergency and security system's occupational health and safety policy might need to address were listed. In this section, those other aspects are briefly presented, including:

- Working conditions: Refer to social, technical, and organizational factors in a workplace and risk factors that could arise in the work environment. These, in turn, could immediately or in the long term have negative or positive consequences for the well-being, health, and safety of staff members.

  International and national regulations provide that the State must establish safe and adequate working conditions for the sound and healthy development of activities.

- Risk factors: An occupational risk factor may be understood as any condition that is present in the performance of a work activity and that could cause accidents, diseases, and even the death of the person carrying out the task.

- Work accidents: Could be defined as any unforeseen and sudden event that arises because of, as a consequence of, or on the occasion of the work activity related to the job, and that causes the person to suffer bodily injury, functional disturbance, disability, or death (immediate or subsequent).

- Occupational illnesses: Could be understood as chronic conditions caused directly by the performance of a job or occupation carried out by the person in the workplace due to exposure to risk factors, and that could lead to inability to work.

  The International Labour Organization (ILO) has produced a list of occupational diseases, organized by cause, that could be used as a reference.

  The key would be to check the cause-and-effect relationship between the work performed and the resulting chronic disease and, if this relationship exists, to introduce measures to eradicate or mitigate the identified causes.

- Absenteeism: The International Labour Organization (ILO) defines it as "the practice of a worker not showing up for work for one or more days, when she/he was expected to be at the workplace, excluding holiday periods, strikes, gestational periods, and deprivation of liberty".

- Epidemiological prevention and surveillance systems: Prevention of diseases that may occur within the workplace and in the performance of work activities is a critical point for preventing occupational risks and protecting personnel's safety and health. In this sense, epidemiological surveillance would be an instrument of vital importance. It would have to be conceived as a dynamic process to identify, measure, and analyze health problems that could affect the workforce. Based on this epidemiological surveillance, information could be generated for decision-making to promote health, prevent diseases, or contain and control health problems once they have already spread within the workplace.

8.5.1. Risk factors

The human factor needs to be recognized as the main factor in a work accident. This could be due to several reasons, including the performance of an unsafe act or an unsafe condition, either due to ignorance when performing the task(s) or over-confidence in performing the task, or technical failures. Consequently, the following steps should be taken into account to ensure success in the prevention of occupational risks:

- Identification and assessment of occupational hazards in the workplace, through internationally endorsed and recognized tools and instruments, including the Colombian Technical Guide (GTC) 45, the Technical Prevention Note (NTP, for its Spanish acronym) 330, Hazard Identification and Risk Assessment (IPER, for its Spanish acronym), among others.
- Assessment of specific risks such as psychosocial risks, ergonomic risks, physical, mechanical, and chemical risks, among others, which could affect the health and well-being of personnel.
- Definition of measures to prevent, mitigate or eliminate such risks, including training based on job positions, existing risks, and how to avoid them.

Among the most common occupational risk factors in an emergency and security system are those associated with three basic operational tasks: answering help requests, calls, or reports, monitoring of video surveillance cameras, and responding to emergencies in the field. Each type of risk would have to be accompanied by several recommendations that could be considered for its mitigation.

Table 26: *Risks and recommendations when answering calls and monitoring cameras*

RISK TYPE: ERGONOMIC	RECOMMENDATIONS
Constant typing on the computer's keyboard and prolonged use of mouse or joystick. Extended periods in a seated position. Prolonged use of screens.	Time assigned for active breaks (rest and stretching exercises) and visual breaks. Provide visual protectors. Adjust height and tilt of the keyboard. Armrests and supports for the palms of the hands. Equip workstations with ergonomic chairs. Correct posture in front of the computer and when sitting down.
RISK TYPE: PSYCHOSOCIAL	**RECOMMENDATIONS**
High levels of responsibility. High levels of stress. Constant alert status. Workload. Difficulty balancing professional and personal life. Long workday, night shift, rotation, overtime, work outside of working hours.	Organize emotional release activities. Improve communication. Psychological follow-up with professionals.

Source: Integrated Security Service ECU 911, 2020.

Table 27: *Risks and recommendations when responding to emergencies in the field*

RISK TYPE: ERGONOMIC	RECOMMENDATIONS
Extended periods driving in a seated position.	Ergonomic seats for vehicles.
RISK TYPE: MECHANICAL	**RECOMMENDATIONS**
Use of vehicles. Ground transportation. Road accidents, entrapments, dismemberments, death.	Regular preventive maintenance of vehicles. Training on traffic laws and related topics. Defensive driving training. Driving awareness.
RISK TYPE: PSYCHOSOCIAL	**RECOMMENDATIONS**
High levels of responsibility. High levels of stress. Constant alert status. Workload. Difficulty balancing professional and personal life. Long workday, night shift, rotation, overtime, work outside of working hours.	Organize emotional release activities. Improve communication. Psychological follow-up with professionals.

Source: Integrated Security Service ECU 911, 2020.

8.6. Continuous improvement

Consistent with the comprehensive quality management model developed in Chapter IV of this guide, improvement measures need to be introduced in all those areas that would contribute to the safety of the emergency and security system. To this end, based on established security policies and protocols, evaluation and measurement mechanisms should be put in place to identify deviations, deficiencies, and weaknesses in current processes and based on those findings, to introduce updates or adjustments that ensure their reliability and safety.

Within the framework of the comprehensive quality management model, the following steps should be considered to generate a continuous cycle of improvements:

- Define monitoring processes that collect and deliver data to measure, process, analyze, and implement improvements in information, IT, communication, physical, and personnel security.
- Design reports that can be used to identify recurring gaps or vulnerabilities and thus adjust existing security policies.
- Identify technological and communication obsolescence.
- Establish a process that can be used to evaluate compliance and constantly measure security policies and protocols.
- Prioritize identified areas of opportunity and produce action plans to address them.

CHAPTER

09

COMMUNICATION MANAGEMENT

Introduction

Communication and information could be considered strategic resources for emergency and security systems, in terms of both institutional and operational communications. The former would be linked to the position, image, and branding of an emergency and security system. It would include a series of communication actions focused on consolidating the relationship with the system's personnel and the external public, from a strategic perspective. The latter would be linked to internal communication within the emergency and security system, and with articulated and related institutions, involved in responding to low and high magnitude emergencies. Thus, its planning and management are essential.

The planning and management of communication would have to be seen as having two axes: a strategic axis, related to institutional communication and another, more operational, axis linked to the daily operation of an emergency and security system. In addition, communication planning and management would have to occur on two levels: within the organization and with its external environment. Finally, communication planning and management would have to be designed for low-intensity emergencies linked to the system's day-to-day operation, and high-intensity emergencies triggered by natural or man-made disasters that affect large numbers of people and geographic areas simultaneously.

As a result of the planning process, a communication plan would need to be developed that could then be used as a roadmap to guide communication management. This chapter presents a series of guidelines to shape the development of a communication plan, taking into consideration its structure, components, and minimum contents.

A number of channels and tools to manage the communications of an emergency and security system are also considered in this chapter, including spokespersons, network use, social media, community relations, as well as prerecorded messages.

The chapter also provides guidelines for planning and managing communication in high-impact crises that affect national, subnational, and local levels. Finally, the chapter concludes with three communication challenges, for which some mitigation measures are proposed.

9.1. Communication planning

Communication actions would have to be part of a structured process of design, execution, and evaluation.

Communication would have to have a comprehensive scope. In turn, communication planning and management would have to be integrated into the overall management of the entity and could have different levels of complexity, depending on the type of operational model adopted by the emergency and security system (these models were presented in Chapter III of this guide).

All communication activity would have to respond to prior planning that helps ensure the achievement of results and impacts sought. In addition, it would have to be aligned with the strategic objectives of the system, the different types of emergencies and operational needs, the information requirements of the population and specific audiences, the media ecosystem, and other aspects.

All these aspects would have to be included in a technical and cross-cutting reference document. The communication plan would serve as a guiding instrument. Planning would have to address two necessary and complementary dimensions of communication activity:

- The organizational/institutional dimension, with a strategic component
- The operational dimension

9.2. Planning organizational communication

In the organizational dimension, communication planning would mean adopting a strategic approach. It is an instrumental activity supporting an entity's strategic plan. It would have to consider communication actions that seek to strengthen the system, taking into account its mission, vision, and stated strategic objectives (see Chapter II of this guide).

Organizational communication would also need to be approached as an integral part of strategic planning, seeking to capitalize on strengths and opportunities, and addressing identified weaknesses and threats. It would need to be guided by its own objectives and targets, aligned with the strategic plan, and incorporate indicators to measure the results achieved.

Different communication strategies would be needed at this level. Each would provide a conceptual and practical framework for responding to a particular situation, applicable at different times. Furthermore, each would result from planning the management of communication flows within the entity, according to its objectives, values, and expectations.

Organizational communication planning would determine how communications should be structured and coordinated, seeking to:

- Integrate communication flows and processes with the strategic objectives outlined during the entity's planning process.
- Establish communication processes and flows that create value, build shared symbols and meanings, develop messages, position the emergency and security system, and generate a sense of belonging with the community, in a systematic and sustained way over time.
- Coordinate and integrate management processes with other organizational processes.
- Involve all personnel in the consolidation, development, and strengthening of the emergency and security system.
- Enhance the transparency and accountability of the system's operations and management (see Chapter X of this guide).

Such planning and its implementation would be the responsibility of the functional area specialized in the subject, consisting of a team of staff members with the necessary training and experience to work in this area.

9.3. Planning operational communication

Communication management in the operational context would have to consider modeling the minimum components of a communication plan to support emergency services delivery and strengthen the system's relationship with users and specific audiences.

Planning operational communication would have to consider at least two dimensions:

- Timing
- The audience

Regarding the first dimension, it would be important to think of communication strategies and objectives for the emergency and security system's "normal" times of operation as well as to plan operational communications for times when high-magnitude and high-impact emergencies occur. (This second temporal dimension is developed in Section 9.6 of this chapter). In particular, this second temporal dimension would have to be linked to the continuity of services before, during, and after critical incidents.

As regards the second dimension, the planning of operational communication activity could be subdivided into two components:

- Internal
- External

The internal component would refer to the communication process that is developed for use by the entity itself. It would involve identifying internal audiences, developing content, designing images, creating products, and identifying and activating communications channels.

These actions would be directed to:

- Sustaining the quality, efficiency, and effectiveness of the services delivered
- Encouraging a good working environment and collaborative working relationships
- Informing and keeping staff updated on decisions made, adoption of new standards, policy and protocol changes, among other issues

The external component would focus on the general population and specific targeted audiences. It would seek to keep them informed about issues related to emergency services provided, scheduled/programmed events, and the operation of the system. This could be done through communication campaigns or other actions. To this end and consistent with the objectives set out in the communication plan, it is essential to formulate messages using simple and direct language, avoiding technicalities, and to determine the channels, timing, and frequency with which the messages will be released.

Scheduled/programmed events are not necessarily linked to operational communication planning. They are events that are expected to occur. They can be national, sub-national, or local in scope. Sometimes they require that emergency and security systems be activated in advance, from a preventive, operational, and communications perspective. This would involve coordination with response entities to monitor video surveillance cameras and deploy units to strategic locations for timely response to possible incidents that could derive from the event, among other actions. Likewise, it would require communication actions to inform the public about the development of the event, using available channels, including press conferences, social media, instant messaging, prerecorded messages, among other means.

9.4. Communication plan

The communication plan could be conceived as a detailed program of the communication activity that an emergency and security system will carry out. It would have to clearly and accurately outline the objectives and goals to be achieved, the communication actions to be implemented, the audiences to which these actions would be directed, the exposure times/frequency, the channels to be used, and the people responsible for each of the tasks.

In addition, the plan would have to be accompanied by an action timeline and its implementation would have to be based on a set of indicators that would seek to measure the results achieved.

To design a communication plan, it would be important to start with at least two steps:

- Understand the traditional and social media ecosystem, including its coverage and penetration, and the frequency and intensity of use among the population.
- Identify and get to know the different types of audiences, their characteristics, needs, and forms of communication to which the communication plan and actions would be directed.

Regardless of the operational model adopted by the emergency and security system, communications should be managed based on a single plan, agreed to by all the actors linked to the system, and with a clear definition of leadership, guidelines, spokespersons, and monitoring and evaluation tools.

The document would have to be prepared annually, considering current state of affairs faced by the emergency and security system. In addition, reviews could be stipulated each month, with a final assessment that allows estimating or measuring the plan's effectiveness, scope, and impact.

Below are some of the minimum components that a communication plan should include:

- Communication assessment, including environmental analysis and contextualization
- Communication objectives
- Segmentation of audiences
- Creative strategy and key messages
- Media strategy
- Design and production of communication and advertising pieces and products
- Communication actions
- Timing, frequency, and duration
- Budget
- Control and evaluation

Each communication plan would include a series of communication actions that should be implemented so as to achieve the proposed communication objectives, based on the creative strategy and key messages, the specified communication channels, and the communication and advertising pieces or products designed.

Below are examples of communication actions that could be considered:

- Campaigns
- Media tours
- Events with community and authorities' participation
- School visits or tours
- Emergency response drills on public spaces

When designing campaigns, there are some basic parameters that could be considered:

- They should be informative
- Language should be simple and straightforward
- They should be based on the issues or problems detected by the analysis generated by the emergency and security system from its own data (see Chapter VII of this guide)

If the plan includes communication actions with traditional media, it would be advisable to approach leading media outlets and to build and maintain relationships with them.

The corresponding functional area would be responsible for the development of the communication plan, which would then have to be validated and approved by the highest authority of the emergency and security system prior to implementation.

Below is an example of a communication plan's proposed structure and minimum content:

***Table 28:** Template for the development of a Communication Plan*

INSTITUTIONAL PRESENTATION	
Name	[Of the emergency and security system]
Mission	Manage emergency responses, reported by the population through a unique number (if such number exists) and those generated by video surveillance, monitoring of alarms, or some other means. The response consists of dispatching specialized response resources, from public and private entities linked to the system, to continuously contribute to the achievement and maintenance of safety.
Vision	To be a leading and model institution in coordinating emergency and security services, using state-of-the-art technology in systems and telecommunications, committed to quality, safety, occupational health, and the environment, providing a high-quality service to the population, in a continuous and sustained manner.
Sector	Security
INTERNAL AND EXTERNAL CHANNELS	
Channel	Description
Facebook	The use of photographs and videos could be considered communication products that are able to increase the appeal, interest, activity, and interaction within the account and among followers.
Twitter	It offers the ability to publish straightforward, short, and timely messages. Another valuable feature of this social network is the immediacy with which messages are published. All the features mentioned above make it an appealing source of information for traditional media. The use of hashtags would allow for grouping contents according to specific events or situations, facilitating their search for them and, in cases of important news or events, for positioning messages and trends.
YouTube	Official account where videos produced by the institution are kept and organized, according to their content, facilitating navigation and the search for information by the population and specific audiences. The institution could produce documentary-type videos, programs on successful cases, news summaries, interviews, and other genres. These could also be produced with the support of an external agency. The videos could be used to supplement the information provided to the public. Links to the videos could be inserted in other social media platforms. This is particularly useful when social media have a maximum capacity and character limit.

Instagram	The content on Instagram would have to be visual. Photographs or videos would need to be of high-quality, self-explanatory, and sufficiently interesting/eye-catching to generate interactions. Short descriptions, complemented by a hashtag, could provide an idea of the content being shared.
Website:	It can provide more detailed information, with official data from entities involved in the coordination of an emergency. Written content could be supplemented with photos and videos. It could be used to publish and make available to the public administrative and operational information, contributing to transparency in the management and operations of an emergency and security system.
Screens in service areas:	Specify quantity and places where they are positioned (malls, government agency waiting rooms, bus or train stations, among other possible strategic locations).
Media or communication programs:	Radio or radio program in FM or digital. Open signal TV channel or program (public, private, or community). Newspaper or opinion column/article (weekly or monthly). Magazine or opinion column/article, according to its publication schedule or based on a pre-established frequency.

COMMUNICATION PLAN

JUSTIFICATION (Question to be answered: Why is it relevant to have a communication plan?)

To publicize and position the emergency and security system's services among the population, contact methods to access the services, and the need to make responsible use of the services.

The possibility of facing minor- and large-scale emergencies makes it necessary to prepare people and groups in situations of vulnerability so they know what to do and how to respond in these situations.

It would also be necessary to generate consistent, continuous, and reliable communication, regardless of the operational model adopted. A communication plan becomes even more important in crises in order to limit anxiety, uncertainty, and confusion among the population and counteract misinformation (false information), erroneous information, and malicious information.

OBJECTIVES (This part would have to describe what is to be achieved with a communication plan. Question to be answered: What for?)	
General objective:	Project a positive and credible image of the emergency and security system among the population.
Specific objectives:	Positively attract the attention of national and international strategic partners. Strengthen the relationship with media outlets and increase institutional presence in the media. Create a sense of belonging among the institution's personnel. Position the emergency and security system as a reference center/model in the response to high-impact incidents. Make the management and operation of the emergency and security system's transparent.
Communication actions:	Social media campaigns. Interventions in traditional media. Visits to schools. Guided tours for schools, Emergency response drills on public spaces.

Source: Integrated Security Service ECU 911, 2020.

9.5. Communication management

An emergency and security system faces different types of emergencies. These do not have specific hours or days, except for scheduled/programmed incidents. Most emergencies are unexpected and surprising; therefore, communication planning and actions should be able to adapt to this intrinsic nature of emergencies, seeking to provide the population with helpful information to preserve life and safety at all times. The communication of and for emergencies should be a dynamic process and able to adjust to the characteristics of events that occur.

In an emergency, the ability to provide practical, up-to-date, valid, and ongoing information will depend on the communication planning and preparation carried out by the emergency and security system prior to the incident.

Depending on the nature and dynamics of emergencies, emergency communications would have to occur in near real-time. This is one of the main reasons why communication should be based on six basic guidelines:

- Make it clear
- Make it simple
- Make it concrete
- Make it concise
- Make it consistent
- Make it timely

A functional area specifically focused on the subject should be responsible for the communication plan's implementation and the daily management of communication. This area would have to consist of a team of professionals with specialized training, specific capabilities, and a set of attitudes needed to perform in positions related to the subject.

Communications in emergencies should be handled through different channels and tools:

9.5.1. Spokespersons

Due to the characteristics and dynamics of an emergency and security system, it would be advisable to have one or more spokespersons.

Spokespersons could be understood as people specifically appointed to fulfill the function of communicating; they represent the official voice and image of the entity.

It would be important to clearly define the roles of spokespersons and the skills and attitudes sought for that job profile. In that regard, they would at a minimum have to:

- Know how the emergency and security system works
- Be informed about the situation and developments in responding to emergencies
- Express themselves clearly and straightforwardly

Those who respond to emergencies should always be in contact with the spokespersons and the communication team. Their integration and the complementarity of their work could make a difference in the performance and image of the emergency and security system. The spokesperson role takes on particular importance in large-scale, high-impact emergencies.

If possible and depending on changes in the communication ecosystem and the emergencies themselves, it would make sense to consider including a spokesperson specialization/refresher course or workshop in the entity's continuous training program (see Chapter VI on Human Talent Management).

9.5.2. Networks

Below are two types of networks (external and internal) that emergency and security systems could utilize as part of their communication plans and actions. Networks would have the following advantages, to mention just a few:

- They increase the visibility and scope of actions and messages
- Contents can be updated frequently at no great cost
- They communicate information instantly, directly, and simultaneously to many people

9.5.2.1. Web platform (external)

The website should be considered the emergency and security system's digital presentation, which would provide internet users with the following items of information relating to the system's communications:

- Institutional information, including vision, mission, objectives, year of creation, work team, management and operational models adopted
- Presentation and description of the services it provides
- Ways to contact for emergencies and consequences of misuse of the system
- Communication actions and press releases
- Past and future events
- Open data, statistical data and bulletins, and reports
- Institutional contact and social media accounts' information

Several of these information items could also be used in traditional and social media.

The design and maintenance of the website would have to satisfy some basic criteria. It would need to:

- Be user-friendly and easy to navigate
- Provide reliable and high-quality information, constantly updated, and presented in a clear and structured way
- Use high-resolution images and videos to illustrate and supplement written information

- Have an inclusive approach, from a technological point of view (in terms of connection type, speed or bandwidth, browser, and operating system, and other features), and one that considers internet users' disabilities
- Be compatible for viewing and browsing from mobile devices
- Meet protection and safety requirements in line with the policies and protocols established by the emergency and security system (see Chapter VIII of this guide on Security Management).

9.5.2.2. Intranet (internal)

The intranet is one of the communication and information mechanisms or channels intended for both administrative and operational personnel in an emergency and security system. In this internal digital space, staff members could find up-to-date information about the entity's performance, news, developments, events, and activities, as well as administrative and operational tools that could facilitate the system's management and operations (including current, new, or updated policies and protocols; forms; explanations of how to carry out specific internal tasks or procedures, among other resources).

The following are some guidelines that could be suggested for the structure and content of an emergency and security system's intranet:

- Allow different access levels and content according to staff's different responsibilities and positions
- Facilitate the two main types of internet services or applications:
  - Those that allow communication, including suggestion mailbox; instant messaging; audio and video calls; international, national, local, and institutional news; internal discussion groups; and real-time image and audio player.
  - Those that allow for information search and organization: shared files; directories with contact information; internal and external database access and query, and search engine.

9.5.3. Media

Media outlets are channels for reaching the public. They transmit messages that are broadcasted to many receivers simultaneously using different techniques and technologies. Each has specific characteristics with regard to audience type, coverage, advertising forms, advantages, and costs.

9.5.3.1. Traditional media

The relationship with traditional media would involve institutional liaison with editors, journalists, interviewers, and reporters. This relationship would have to be seen as a strategic alliance, as it can be used to highlight an emergency and security system's actions and performance on a mass scale and to reach different audiences simultaneously, according to the planned communication objectives. These objectives could be associated with external communication at the operational level, as well as with organizational communication, intended to impact public perception of the value of the services provided, credibility, transparency, and accountability of the emergency and security system.

Messages should be geared toward informing and raising public awareness. The communication approach could be preventive, educational, or prescriptive.

9.5.3.2. Social Media

Social media would have to be considered a channel for direct communication with the population. There are currently several social media platforms, including Twitter, Facebook, Instagram, among others.

Through social media, it would be especially important to share useful information with the population such as road status, accidents, or the development/status of relevant events (information reports, pictures, and videos).

They could also be utilized to disseminate campaigns designed to provide information, recommendations, reminders about important dates or events, raise awareness of specific risks or the proper use of the system, among other actions, and to do so in a timely and cost-effective manner.

To feed social media accounts and keep them active and relevant, it would be preferable to choose the information most "attractive" or interesting to the public. Audiovisual content generally has greater impact and tends to generate more interactions.

Unlike traditional media, social media enable horizontal, two-way (an even in some cases multi-directional) communication. Through social media, the public could also express their satisfaction or dissatisfaction with the service.

Below are some general guidelines for an emergency and security system to consider when managing social media accounts:

- Avoid engaging in discussions with anyone
- Any message on behalf of the institution would require authorization from the person in charge of the entity's communications
- Avoid syncing the institution's official accounts with any app, personal Twitter account, or any game or program that could automatically post content
- Avoid posting personal opinions in the institution's name
- Post photos and videos with prudence, caution, and respect

9.5.4. Public and community relations

Regarding its engagement with the surrounding environment, an emergency and security system should consider two components: building a relationship with the public and communities on the one hand and incorporating a monitoring and early warning component on the other.

The purpose of the public and community relations component would be to mobilize and consolidate people's involvement and interaction with the emergency and security system. Messages, events, and other communication actions using this component would need to reflect and address specific concerns, opinions, problems, and risks of the population and communities being targeted. In this way, useful and tailored information would be provided so that they can make better decisions when dealing with emergencies.

An additional purpose of this component could be to mobilize the community to introduce positive changes in behavior and habits, helping to improve people's health, well-being, and safety.

Building and maintaining a relationship with the population and the community could have short-, medium-, and long-term objectives. For example, short term objectives of public and community relations could be intended to:

- Raise people's awareness regarding proper use of the service, particularly children, adolescents, and young people who will become potential users of the system in the medium and long term
- Train people on how to act and how to deal with different types of emergencies
- Instruct people on how to prepare for and act in response to high-impact incidents

In the medium and long term, public and community relations could be guided by the objective of strengthening the emergency and security system's image and legitimacy.

Public and community relations should be based on at least four premises:

- Respect in treating users and the general population
- Empathy and sensitivity toward people who, individually or collectively, might be facing dire situations and problems
- Closeness and constancy in the bond with people and communities
- Professionalism in the service provided to the population, demonstrating preparedness, coordination, efficiency, and effectiveness

These premises would also help to build trust and a sense of belonging with the emergency and security system, in line with the medium- and long-term objectives mentioned above.

Ties can be developed face-to-face with the implementation of programs and projects according to the conditions and needs of each community and virtually with the use and expansion of social media platforms.

Constant interaction with the population and communities would, in turn, be linked to the monitoring and early warning component. This second component could be seen as a two-way listening process managed by the emergency and security system and would include the analysis, monitoring, and collection of information on the population and communities regarding:

- Needs, problems, and challenges they face in terms of emergency assistance. This information would serve as an input for proposing proactive and timely solutions.
- Rumors and false information about potential risks and dangers that could adversely affect the work of the emergency and security system. These situations could be contained and counteracted with information campaigns based on data, facts, and evidence.
- The peoples' and communities' knowledge and satisfaction levels, opinions, and perceptions regarding the emergency and security system. This information could serve as input to guide the introduction of changes and improvements in line with the comprehensive quality management approach (presented in Chapter IV of this guide).

9.5.5. Prerecorded messages

In addition to the channels and tools already presented, prerecorded messages could be an efficient option for communicating with and informing the population about ongoing emergencies and scheduled/programmed events. These would have to be configured based on each system's technological capacity and each State's regulatory telecommunications framework.

9.6. Communication planning and management in large-scale emergencies

Large-scale emergencies are scenarios of high technical, political, and social sensitivity, where the operation of an emergency and security system would have to be accompanied by a crisis communication plan. Such a plan must include articulated (or first responder) and related entities and must be directed to the general population and the specific audiences/groups identified.

In large-scale emergencies, information is a highly valuable resource for decision-making. Communicating available information is key to mobilizing national and international resources and allows for a timely and appropriate response.

Crisis communication is a strategic component of planning communication activities as well as a component of risk management. Just as most large-scale incidents and risks can be analyzed and anticipated, communication management would have to consider planning and preparing for large-scale events.

Crisis communication planning and preparedness would have to result in a communication plan. This plan could be part of the comprehensive or master communication plan or could be developed as a separate plan but linked to the master plan. In both cases, it would allow communication actions to be managed and guided under exceptional circumstances. Crisis communication should support large-scale emergency responses. Additionally, it would have to be in line with the risk matrix, the continuity of operations plan (COOP), and the disaster recovery plan (see Chapter VIII of this guide).

The plan should contain at least the following components:

- The steps needed to develop press releases in times of crisis
- Communication and messaging strategies
- Evaluation of the plan, after the crisis is over

Crisis communication planning would enable emergency and security system authorities to have established guidelines, processes, and procedures to effectively communicate to the general population and specific audiences about the nature, status, and evolution of risk. The design of targeted and segmented communication, using the various communication channels available and based on the needs of the identified audiences, could contribute to the assertiveness and receptiveness of the message.

The dissemination of emergency alerts at the national, subnational, or local levels is a timely instrument in high-impact situations. These alerts are mass, instantaneous, and rapidly disseminated messages that require the support of the telecommunications sector to guarantee the simultaneous availability of the various communication channels.

Alert messages would have to vary depending on the predefined incident type. This forecast would allow the advance preparation of message templates.

It is highly likely that in such large-scale and high-impact situations not only will first-response or articulated entities be activated but supporting or related agencies will also be involved. Due to the increased number of entities, response and communication coordination becomes even more essential. Standardized messages to be disseminated to the population and the need for all entities involved in the emergency response to handle the same information, become more important, increasing the need for a single crisis communication plan.

All entities would have to align themselves with the communication actions envisaged in the crisis communication plan, avoiding conflicting messages or media competition. In this way, it becomes possible to maintain consistent messages and a constant and continuous flow of up-to-date, valid, and credible information.

Crisis communication planning would also have to consider the operational aspect of the response. In that regard, it would have to establish a set of guidelines, processes, and procedures to facilitate communication for interaction, information exchange, and coordination at different levels among authorities, articulated and related entities, emergency teams, and interested audiences (including scientists, academics, public health professionals, and communicators, among others).

Regarding crisis communication management, the following guidelines could be considered:

- Establish a centralized communications center or node responsible for handling all requests for information and preparing releases for media outlets, social media, other institutions, the public, and specific audiences.
- Define the authorization chain for the communication and dissemination of information.
- Set up a communication calendar.
- Develop message templates or scripts.

Message templates or scripts could be based on the following three components:

- Audience(s) being targeted
- Main message
- Instructions for more information

The Incident Command System (ICS), specifically the communication chapter, could provide guidelines and standards to be followed for emergency communication. Additionally, other reference sources could be the "Crisis Communications Planning Guide" and the "Tips for Communicating with Stakeholders During a Crisis," both developed by Mission Critical Partners (2020).

9.7. Communication challenges

Communication during emergency management can change every day and at any time due to the very nature of the incidents. In addition to this challenge, communication of and about emergencies faces at least three additional challenges.

Challenge 1: Groups in vulnerable situations

Emergency assistance and response measures would have to consider the specific needs of people in situations of vulnerability, marginality, or disability.

Failure to consider difficulties using communication channels and devices, and the social, physical, and cultural distance of these groups emerge as real obstacles when providing protection, assistance, and response in an emergency.

To address this challenge when planning communication actions, an emergency and security system could consider the following steps:

- Identify which groups are in vulnerable situations (including illiterate people, people in marginal conditions, ethnic groups with customs and languages different from the dominant or official culture, and people with physical or mental disabilities). Understand their sociodemographic characteristics, geographic location (if applicable), and communication needs in low and high-intensity emergencies.
- Analyze advantages and opportunities in the use of different communication channels.
- Design communication actions and messages targeting at each group, in order to reduce their vulnerability and increase the effectiveness of emergency assistance and response efforts.

Challenge 2: Misinformation

- False, erroneous, or misleading information (misinformation)
- Incomplete, inaccurate, or manipulated information (disinformation)
- Assertions that are no longer based on objective facts and data, factual information, and evidence and instead, appeal to the emotions, beliefs, or desires of the public (post-truth)

In a post-truth context, where false and manipulated information flows, there is an increased chance of "information disorders" that, in turn, could lead to social unease and despair. To address this scenario, an emergency and security system could consider the following guidelines for communication management:

- Avoid improvisation or half-truths
- Avoid trying to get the public's attention by publishing sensationalist images
- Establish emergency data verification mechanisms before sharing data with the media outlets
- Have communication and information dissemination guidelines
- Take care with the system's style of communication, respecting victims' human dignity above all

Challenge 3: Increasing incidence of high-impact disasters or catastrophes

Given the increase in the frequency and intensity of high-impact disasters caused by climate change and man-made actions, emergency and security systems are increasingly more likely to face these types of situations. In light of this scenario, some additional guidelines for communication planning and management are shown below:

- Strengthen the planning and review of communication plans, particularly related to the preparedness component
- Establish mechanisms for cooperation, sharing lessons learned and good practices, and joint exercises with other entities on how to respond to such events
- Adopt tools to broadcast emergency alerts[9] (if possible), monitor communications, and evaluate communication plans and actions

[9] See Common Alerting Protocol (CAP).

CHAPTER

10 TRANSPARENCY AND ACCOUNTABILITY

Introduction

Transparency and accountability could simultaneously be considered values and principles to be upheld, objectives to be achieved, and processes to be followed. In any case, these three approaches are essential in and for democratic governance and policies related to public management, including in the field of safety, and emergency response.

Given that emergency response services are provided by the State and their focus is to protect and safeguard human life, it would be necessary to facilitate accountability for the system's management and achievements. Making data and information available to public institutions, the media, the academic and private sectors, civil society, and the population facilitates the legitimate exercise of horizontal and vertical controls. Doing so would not only bring the emergency and security system in line with the laws of each country, its internal rules and policies but it would also help to increase the system's level of approval, trustworthiness, and legitimacy among the population.

Given the nature of the content and the purpose pursued, transparency and accountability would have to be part of the design of any emergency and security system and strategic planning for its strengthening. This would involve creating protocols, processes, and mechanisms to proactively provide information on the operations and management of the system and facilitate access to information that allows for oversight, knowledge generation, the creation of public value, and innovation.

This chapter addresses transparency and accountability from a planning perspective, linking it with strategic planning (Chapter II of this guide) and organizational communication planning (Chapter IX of this guide). It then describes a set of specific mechanisms and tools for the exercise of transparency and accountability, including inquiries and requests for public information, quantitative data, indicators and open data, the reporting system, public procurement and acquisition of goods and services, internal/external audits, and the entity's communication plan.

The communication plan (covered in Chapter IX of this guide) is presented as a key tool for incorporating communication objectives, goals, outcomes, and actions related to transparency and accountability, utilizing information available through the above-mentioned mechanisms and tools.

Finally, the chapter refers to two additional instruments: the Code of Ethics and the Code of Conduct (introduced in Chapter VI of this guide). These codes, accompanied by induction and training sessions and an incentive and penalties scheme to support compliance, would seek to instill transparency and accountability as values and guiding principles of the emergency and security system's actions and its personnel.

10.1. Planning for transparency and accountability

Planning to ensure high levels of transparency and accountability in an emergency and security system could begin with the rationale for them. Thus, it could explain why an emergency and security system would seek transparent action and accountability for its activities vis-à-vis other public entities, specific audiences, and the population in general.

For example, these reasons could be linked to:

- Ensuring the effectiveness and efficiency of the system, contributing to its governance
- Respecting people's right to access public information
- The need to ensure the integrity of the system's operations and management and to prevent and address corruption

A planning process would also allow for the definition of the objectives to be achieved, such as:

- Achieving a high level of trust and credibility among the population
- Becoming a national (and international) reference or source of reliable and up-to-date information

It would also allow systematic consideration and establishment of the goals and performance indicators that could be agreed upon to measure progress and achievements in meeting the objectives set for transparency and accountability. This could in turn be used for the communication, proof, and publication of results, and accountability for goals and successes achieved, as well as those not achieved.

Planning could result in a plan that, for its implementation, would require a set of processes, procedures, and mechanisms. The plan would have to align with national transparency and access to public information laws, open government plans in effect in each country, and other (strategic and operational) plans developed by the emergency and security system.

Depending on the objectives and goals that have been set, a system could consider implementing several internal and external mechanisms or tools to achieve them, including:

- Inquiries and requests for public information
- Quantitative data, indicators, and open data
- Reports
- Publication of public procurement and contracting procedures
- Internal/external audits
- Communication plan

10.2. Inquiries and requests for public information

An emergency and security system would need to have established processes and mechanisms for receiving inquiries and requests for information from the population and specific audiences, in line with the existing legal framework in the country.

Below are some considerations to bear in mind for standardizing and facilitating inquiries and requests for information:

- Enable multiple channels or means, including phone, email, face-to-face, or the emergency and security system's website. It would be important to make a clear distinction between these channels and those used to report emergencies.
- Design a form (on paper and digital) so that the public can make inquiries or request the information they need.
- Define an internal procedure for processing queries and information requests, including:
  - Classify the type of information that can be shared and disclosed.
  - The format in which the requested information will be presented.
  - Deadlines to respond to the query or request for information.
  - Authorizations required to deliver the requested
  - Script for answering such calls.
  - Preset email templates to automatically respond to such inquiries or requests.
  - Certification (on paper or digital) stating that the query was answered, and the requested information was delivered. If not, it would be advisable to provide an explanation consistent with the country's legislation or the entity's regulatory framework.
- Emergency and security system personnel specifically trained and dedicated to carrying out this type of tasks.

Since an emergency and security system handles personal data, it would be essential to strike a balance between transparency and accountability and the privacy and confidentiality of users' identifiable information. It would also be important for the information generated and managed by an emergency and security system to be subject to a classification typology and process (see Chapters III and VII of this guide).

The information classification typology should be consistent with the parameters established in the laws of each country. It should also consider internal security issues such as the non-disclosure of data that could generate some type of risk, including compromising the operation of the emergency and security system, generating vulnerabilities in the entity's IT and communications systems, and compromising the physical integrity of staff, among other aspects.

In addition, in line with the policies and protocols established by the entity regarding information security, communication, and IT systems, personal data should also be protected to prevent their misuse and leakage of information. (On this subject, refer to Chapter VIII of this guide).

10.3. Quantitative data, indicators, and open data

It is essential that public services, including an emergency and security system, make information available to interested parties to assess the operation of the system, the services provided, and the results achieved.

Thus, an emergency and security system could initially make available to the public two main types of data and indicators, already processed or with some degree of human intervention:

- Quantitative data and indicators on the use of public funds: payroll, budget, balance sheet, among other topics.
- Quantitative data and indicators on the operation and services provided: cases served, number of people served (broken down by sex and age), type of events handled, areas served, among other variables.

Thereafter, a more recent approach would have to be taken into account; this approach focuses on open data, i.e., data that can be freely used, reused, and redistributed by anyone, and is only subject, at the most, to two requirements: acknowledging authorship and sharing the data in the same format in which they were digitally published.

The emergency and security system would have to regularly publish open data to facilitate and promote their use, reuse, and distribution by the public and specific audiences, without imposing restrictions based on copyright or reproduction rights.

For open data, it would be important to define, for example:

- Their source, how, and where they were obtained
- The frequency of publication of up-to-date and comprehensive data
- The format, including attributes such as being machine-readable, interoperable, and comparable
- How the source should be cited
- The place within the emergency and security system's website where they could be published

In addition to promoting transparency and accountability, open data would encourage public participation and knowledge generation based on the processing and analysis of data made available to the public. In addition, they could contribute to the emergency and security system's governance and trust. Furthermore, they could be sources of innovation for addressing common problems and challenges that require informed solutions.

10.4. Reporting system

Based on the information architecture used to design the emergency and security system, the IT systems that support its operation, and the databases that have been created (see Chapter III of this guide), a series of useful reports could be available for accountability purposes.

These could include:

- Management reports. These would account for the system's administrative functions, the use of economic resources, compliance with strategic and operational planning, and the results achieved. They could be prepared on a bi-annual and/or annual basis.
- Service reports. These would provide information on the services provided by the emergency and security system. They could be developed monthly, quarterly or every four months, biannually, and/or annually.
- Financial reports. These are based on income and expenditure budgets. They would provide an implementation and degree of compliance balance sheet. They could be prepared on a quarterly or every four months, biannually, and/or annually.
- Project reports. These would present the level of progress made in active projects, estimated closing dates, projects' levels of financial execution, among other relevant information. They could be published quarterly or every four months.

These reports, in turn, could be part of the entity's communication plan. They could be disclosed through different channels or means, including the website, social media accounts, face-to-face or virtual events, and publications. (On communication management for an emergency and security system, go to Chapter IX of this guide).

10.5. Government purchasing and contracting of goods and services

Transparency would also need to be incorporated in all goods and services procurement processes, complying with the standards established in each country and ensuring the same opportunities for all suppliers.

To ensure transparency in purchasing and contracting processes, it would be advisable to:

- Have a section within the emergency and security system's website where all tenders are published, detailing the requirements, conditions, and deadlines. This information could also be published in other media, as required by law in each country.
- Have a purchasing team that reviews goods and services procurement processes and approves only those consistent with the provisions of the law and its procedures, and published requirements and specifications. It would be advisable for this team to consist of the senior authority in the entity, a legal adviser, an official in the planning area, an official in the administration and finance area, and, if any, an official in charge of transparency and accountability issues.
- Call upon technicians and experts specialized in specific goods or services subject to a purchasing or contracting processes to provide recommendations and an informed opinion regarding requirements and specifications and suppliers' compliance with them.

Through the web platform (external), the emergency and security system could publish the results of purchasinge and contracting processes (including tenders). It could also consider conducting and publishing technical evaluations of suppliers and goods and services purchased or contracted.

10.6. Internal/external audits

Another mechanism available to demonstrate transparency and institutional management is the periodic execution of audit processes. These would allow for timely identification of both financial and operational deviations, and for formulating corrective measures, and implementing them through action plans.

Audits could be both internal and external. Internal audits would have to be conducted by a specialized technical area within the organization. External audits would have to be conducted by a regulatory body or company hired for such purposes. The purpose of this process would be to objectively demonstrate compliance with the legal and regulatory provisions that apply to the entity as well as its performance and the extent of its achievement of the stated objectives. This audit could involve various perspectives: financial, technological, institutional management, data and security management, among others.

It would be important for the entity to transparently publish the results of the audits, as part of the actions stipulated in the plan, taking into account the classification of institutional information. This would facilitate the process of horizontal and vertical control, including oversight by the people, civil society organizations, and other specific audiences, with regard to the emergency and security system management.

10.7. Communication plan

The communication plan for an emergency and security system, particularly in terms of its organizational component, would have to incorporate objectives, goals, results, and communication actions linked to transparency and accountability.

It would have to exploit the use of networks (external web platform and intranet), the media (traditional and social), and other channels available so that, based on the data and reports produced by the emergency and security system, it would be able to communicate and disseminate them with a view to institutional transparency and accountability.

In line with the above, and as an example, the web platform could be used to publish and make digitally available data and indicators, reports (management, service, financial, and projects), purchasing and contracting processes (from start to finish, going through and accompanying all stages, including supplier and contractor evaluations), audit results, institutional conferences and press releases, among other content relevant to the transparency and accountability of the emergency and security system.

Traditional and social media could be used to provide the population with balance sheets on management, services provided, results of tenders and audits carried out, among other possible communication actions.

In any case, the communication plan could be another mechanism for promoting transparency and accountability on the part of an emergency and security system

10.8. Additional mechanisms

In addition to these specific processes and mechanisms contributing to the transparency and accountability of an emergency and security system, at least two more tools could be mentioned:

- The Code of Ethics and the Code of Conduct (both introduced in Chapter VI of this guide)
- Training of employees based on these two Codes to promote professional conduct and actions based on ethical values, linked to honesty, integrity, and transparency

Transparency and accountability would have to be applied to the operations of the system on a cross-cutting basis. To this end, it would be relevant to have a Code of Ethics that consolidates the principles and values that would have to guide actions considered highly desirable by the emergency and security system. In addition, there should be a Code of Conduct that defines desirable behaviors at the individual level and in interpersonal relations among those working for an emergency and security system.

These Codes could be part of the induction process for new employees, regardless of their type of contract or position, so that they know the purposes and contents of both instruments, as well as the consequences of non-compliance. Throughout the professional career of the staff members of an emergency and security system, it may be necessary to update, refresh, or deepen training in ethical values, including courses on value-based leadership. Additionally, both Codes could be available to employees through the intranet and to the public through the web (external) platform.

Guide for the Establishment and Strengthening of National Emergency and Security Systems