

**Guide for the Establishment and Strengthening of National Emergency and Security Systems
in the Member States of the Organization of American States (OAS)**

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 origin, 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.

Copyright © (2021) General Secretariat of the Organization of the American States (GS/OAS). This work is subject to a Creative Commons IGO 3.0 Attribution-Noncommercial-No Derivative Works license (CC-IGO 3.0 BY-NC-ND) (<http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) and can be reproduced for any non-commercial use, granting the respective recognition to the GS/OAS. Derivative works are not allowed.

Any dispute related to the use of the works of the GS/OAS that cannot be resolved amicably will be submitted to arbitration in accordance with the current Arbitration Rules of the United Nations Commission on International Trade Law (UNCITRAL). The use of the name of the GS/OAS for any purpose other than the respective recognition and the use of the logo of the Organization of American States (OAS), are not authorized by this CC-IGO license and require an additional license agreement. Note that the URL link includes additional terms and conditions of this license.

Dedication

With respect and admiration to all the officials and public servants in the emergency and security systems of the Member States, and first responders who, in a professional, technical, and fully committed way, answer to emergencies and respond to **various dangerous situations on top of the traditional and emerging threats that arise in each of the jurisdictions**. To all those who, despite the 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**.

Acknowledgements

The production of this Guide was possible due to the collaboration, contributions, effort, and dedication of a group of officials of emergency and security systems and related agencies that work in the region. All of them came together within the Subsidiary Technical Group on Emergency and Security Systems (GTS-SES).

All of those who participated in this process, did so without knowing each other, working remotely, and within the context of one of the most serious pandemics that 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 who were involved in the drafting process of the chapters that made possible the production 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 GTS-SES 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 officials who participated in the process of preparing, reviewing, and validating this Guide. To all of them 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, Operative Logistics Coordinator

Luis Fernando Alfaro Ubico, Legal Counselor

Carolina Jiménez Rodríguez, Planning Coordinator

Guiselle Mejía Chavarría¹

911 National Emergency and Security Response System of the Dominican Republic



Brigadier General Vicente Mota Medina, ERD, Executive Director

Lieutenant Colonel Pedro

Lourdes Florentino, Planning and Development Director

Teresa Garcés, Head of the

Luis Ferrand, Operations Director

Tammy Ramírez, Head of the Emergency Reception

Alfredo Arredondo, Technology Director²

Luis Reyes, Head of System Development

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 process 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 time doing so, they contributed to the writing of the chapters assumed by the 9-1-1 National Emergency and Security Response System of the Dominican Republic.

| | | | |
|---|--|---|--|
| Ventura Chang, FARD, Head of Plant Security | Management Quality Department Agustín Jiménez, Head of the Institutional Development Department | Department Misael Ventura, Head of the Emergency Dispatch Department | and Implementation Department ² Mabely Díaz, Director of Data Processing, Analysis and Management of Information ² |
|---|--|---|--|

National Information Center of Mexico



| | |
|--|--|
| David Pérez Esparza, Head | Oscar Laguna Maqueda, Deputy Director of Area |
| Hernán Salgado, Head of Office | |
| Juan Salazar Dominguez, Area Director | 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 SIS ECU-911 and Chairman of the GTS-SES | Gary Almeida, National Regulatory Director in Emergencies of the SIS ECU-911 |
| Marco Garnica, Doctrine Technical Deputy Director of the SIS ECU-911 | Celia Gómez, National Regulatory Emergency Specialist of the SIS ECU911 |
| Bolívar Tello, Operations Technical Deputy Director of the SIS ECU-911 | Elisa Bravo, Director of Processes and Quality Control of the SIS ECU-911 |
| Angélica Buñay, Operations Analyst of the SIS ECU911 | Wilfrido Muñoz, National Director of Social Communication of the SIS ECU-911 |
| Rosana Malta, Health and Occupational Security Specialist of the SIS ECU-911 | Cassandra Arciniegas, Interinstitutional Coordination Specialist of the SIS ECU-911 |

9-1-1 Emergency System in Paraguay



| | |
|--|----------------------------------|
| Liliana Díaz, General Director | Carlos Román, Technical Support |
| Daniel Rojas, Strengthening Coordinator | Nilse Molinas, Technical Support |

Likewise, it is necessary to acknowledge the valuable support provided by two of the most prestigious associations in supporting, advising, and accompanying the emergency answering and response systems, such as EENA and NENA in Mexico-Latin America. Their participation in the external validation process meant a second quality control check, strengthening even more the technical rigor of this Guide's contents.



Cristina Lumbreras, Technical Director



Leonardo Dorony, President

A word of appreciation for Patricio Tudela's professional excellence, thoroughness, and intellectual fortitude who, as an external consultant, accompanied the review, editing and validation stages of this guide, even making substantial contributions in many of its chapters.

The planning and production of this Guide was under the responsibility of the Public Security Information and Knowledge Section Chief of the OAS Department of Public Security, Karen Bozicovich.

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 under the responsibility of the Integrated Security Service ECU-911 of Ecuador.

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

©OAS

May 2021.

General editors: Karen Bozicovich and Patricio Tudela

Design and layout: Giovanny Guzmán

English translation: CABI Interpreters and Translators

Table of Contents

| | |
|---|-----------|
| ACRONYMS..... | 13 |
| GLOSSARY | 15 |
| PROLOGUE BY THE GENERAL DIRECTOR OF THE SIS ECU-911, JUAN ZAPATA SILVA | 21 |
| PROLOGUE BY THE OAS SECRETARY GENERAL, LUIS ALMAGRO | 22 |
| PRESENTATION | 24 |
| INTRODUCTION | 27 |
| CHAPTER I: CREATION AND ESTABLISHMENT..... | 30 |
| INTRODUCTION..... | 30 |
| 1.1 INSTITUTIONAL AND POLITICAL SUPPORT..... | 30 |
| 1.2 LEGAL FOUNDATIONS AND REGULATORY FRAMEWORK | 30 |
| 1.3 INSTITUTIONAL ANCHORING | 31 |
| 1.4 IDEATION | 31 |
| 1.5 STRUCTURE | 32 |
| 1.5.1 First response actors (or articulated institutions) | 32 |
| 1.5.2 Supporting actors (or liaison institutions) | 33 |
| 1.5.3 Subsidiary actors | 33 |
| 1.6 OPERATION LEVELS | 33 |
| 1.7 COORDINATION AND COOPERATION | 33 |
| 1.8 STRATEGIC TARGETING..... | 34 |
| 1.9 EXECUTIVE DIRECTOR (OR SIMILAR POSITION)..... | 35 |
| 1.10 FINANCING AND SUSTAINABILITY | 35 |
| CHAPTER II: STRATEGIC PLANNING | 36 |
| INTRODUCTION..... | 36 |
| 2.1 STRATEGIC PLANNING | 36 |
| 2.2 FUNDAMENTAL COMPONENTS OF A STRATEGIC PLAN | 36 |
| 2.3 GUIDING PRINCIPLES | 37 |
| 2.4 DEFINITION OF STRATEGIC AXES..... | 37 |
| 2.5 DEFINITION OF STRATEGIES..... | 38 |
| 2.6 ACTION PLANS | 39 |
| 2.7 INDICATORS AND GOALS SYSTEM..... | 39 |
| 2.8 BUDGET..... | 39 |
| 2.9 SOME TOOLS FOR BUDGET PLANNING AND ITS EXECUTION..... | 40 |
| 2.9.1 Pre-planning: SWOT Analysis..... | 40 |
| 2.9.2 During planning: Strategic Map | 40 |
| 2.9.3 Post-planning: Balanced Scorecard (BSC)..... | 41 |
| 2.10 THE PREMISES OF THE STRATEGIC PLAN | 42 |
| 2.11 KEY SUCCESS FACTORS | 44 |
| 2.12 RISK IDENTIFICATION AND ANALYSIS..... | 44 |
| 2.13 CONTINUITY PLAN FOR STRATEGIC PLANNING | 47 |
| 2.14 FORESIGHT AND ADAPTATION | 48 |
| CHAPTER III: SYSTEM DESIGN..... | 49 |
| INTRODUCTION..... | 49 |
| 3.1 OPERATING MODELS | 49 |
| 3.2 STRUCTURE AND ORGANIZATION (INSTITUTIONAL ARCHITECTURE) | 51 |
| 3.3 FUNCTIONAL REQUIREMENTS..... | 52 |
| 3.3.1 Infrastructure/technological architecture | 52 |
| 3.3.2 Information architecture | 54 |
| 3.3.2.1 Incident typology..... | 55 |
| 3.3.2.2 Typology of access channels | 56 |

| | | |
|--|---|-----------|
| 3.3.2.3 | Call typology..... | 57 |
| 3.3.2.4 | Typology of prioritization levels | 58 |
| 3.3.2.5 | Inappropriate calls..... | 59 |
| 3.3.2.6 | Recording incident information..... | 60 |
| 3.3.2.7 | Interoperable and related databases..... | 60 |
| 3.3.2.8 | Data processing, analysis, and visualization | 60 |
| 3.3.2.9 | Generation and use of information | 61 |
| 3.3.2.10 | Reporting System | 61 |
| 3.3.2.11 | Document management system | 62 |
| 3.3.2.12 | Information Management functional division | 63 |
| 3.3.3 | Physical infrastructure and equipment | 63 |
| CHAPTER IV: INTEGRAL QUALITY MANAGEMENT | | 65 |
| INTRODUCTION..... | | 65 |
| 4.1 | QUALITY MANAGEMENT MODEL | 65 |
| 4.2 | STANDARDIZATION OF PROCESSES AND PROTOCOL APPLICATION | 68 |
| 4.3 | SETTING AND MEASURING INDICATORS | 69 |
| 4.3.1 | Activity Indicators | 70 |
| 4.3.2 | Process Indicators..... | 70 |
| 4.3.3 | Evaluation indicators | 71 |
| 4.3.4 | Management indicators | 71 |
| 4.3.4.1 | Human Resources | 71 |
| 4.3.4.2 | Operations | 72 |
| 4.3.4.3 | Quality | 72 |
| 4.3.4.4 | Administration and finance..... | 72 |
| CHAPTER V: CALL AND INCIDENT MANAGEMENT | | 73 |
| INTRODUCTION..... | | 73 |
| 5.1 | RECEIVING REQUESTS, CALLS AND REPORTS | 73 |
| 5.3 | GENERAL GUIDELINES FOR DRAWING PROTOCOLS | 75 |
| 5.4 | TRANSFER OF INFORMATION TO DISPATCH SERVICES | 78 |
| 5.5 | DISPATCH AND MONITORING OF UNITS | 79 |
| 5.6 | CAPTURING, VISUALIZING, AND STORING DATA | 80 |
| 5.6.1 | For the operation | 80 |
| 5.6.2 | For evaluation and continuous improvement | 81 |
| CHAPTER VI. HUMAN TALENT MANAGEMENT | | 82 |
| INTRODUCTION..... | | 82 |
| 6.1 | PLANNING AND MANAGEMENT OF HUMAN TALENT | 82 |
| 6.1.1 | Job analysis..... | 83 |
| 6.1.2 | Job descriptions..... | 83 |
| 6.2 | FUNCTIONAL DIVISION FOR HUMAN TALENT MANAGEMENT | 86 |
| 6.3 | RECRUITMENT AND SELECTION OF HUMAN TALENT | 86 |
| 6.4 | INDUCTION OF HUMAN TALENT | 88 |
| 6.5 | ONGOING TRAINING TO BUILD CAPACITIES AND FUNCTIONS | 89 |
| 6.6 | PERFORMANCE ASSESSMENT | 90 |
| 6.7 | LOYALTY OF HUMAN TALENT | 91 |
| 6.8 | DEPARTURE PROCESS..... | 92 |
| 6.9 | OCCUPATIONAL HEALTH AND SAFETY | 92 |
| 6.10 | CODE OF ETHICS AND CODE OF CONDUCT | 93 |
| CHAPTER VII. INFORMATION MANAGEMENT | | 95 |
| INTRODUCTION..... | | 95 |
| 7.1. | INFORMATIONAL DIAGNOSIS | 95 |
| 7.1.1 | Sources | 95 |
| 7.1.2 | Information flows..... | 96 |
| 7.1.3 | Information resources..... | 96 |
| 7.1.4 | Products and services..... | 97 |

| | | |
|---|---|------------|
| 7.2. | INFORMATION CYCLE | 98 |
| 7.3. | LEVELS OF INFORMATION OPERATION | 98 |
| 7.4. | IDENTIFYING INFORMATION NEEDS | 99 |
| 7.5. | ACQUISITION OF INFORMATION | 100 |
| 7.6. | ORGANIZATION AND STORAGE..... | 100 |
| 7.7. | DEVELOPMENT OF INFORMATION PRODUCTS OR SERVICES | 102 |
| 7.8. | DISTRIBUTION, ACCESS AND USE OF INFORMATION | 102 |
| 7.8.1. | Interoperability and exchange of information | 103 |
| 7.8.2. | Continuous development and improvement of operations | 103 |
| 7.8.3. | Pre-judicial and judicial instances..... | 103 |
| 7.8.4. | Communication, transparency, and accountability | 104 |
| 7.8.5. | Public policy process..... | 105 |
| 7.9. | INFORMATION AUDITS | 105 |
| CHAPTER VIII. SECURITY MANAGEMENT..... | | 107 |
| INTRODUCTION..... | | 107 |
| 8.1. | INFORMATION SECURITY | 107 |
| 8.1.1 | Information security policies and standards | 107 |
| 8.1.2 | Treatment of physical and digital documentation | 108 |
| 8.2. | SECURITY OF TECHNOLOGY INFRASTRUCTURE FOR INFORMATION AND COMMUNICATION | 109 |
| 8.2.1. | Regarding computer systems | 109 |
| 8.2.2. | Communications security | 110 |
| 8.3. | PHYSICAL SECURITY | 111 |
| 8.4. | RISKS AND VULNERABILITIES..... | 112 |
| 8.4.1 | Risk analysis..... | 112 |
| 8.4.2 | Continuity of Operations Plan (PCO) | 113 |
| 8.4.3 | Contingency and recovery plans..... | 114 |
| 8.5. | PERSONNEL’S HEALTH AND SAFETY | 115 |
| 8.5.1 | Risk factors | 116 |
| 8.6. | CONTINUOUS IMPROVEMENT..... | 117 |
| CHAPTER IX. COMMUNICATION MANAGEMENT | | 118 |
| INTRODUCTION..... | | 118 |
| 9.1. | COMMUNICATION PLANNING | 118 |
| 9.2. | PLANNING ORGANIZATIONAL COMMUNICATION..... | 119 |
| 9.3. | PLANNING OPERATIONAL COMMUNICATION..... | 119 |
| 9.4. | COMMUNICATION PLAN..... | 120 |
| 9.5. | COMMUNICATION MANAGEMENT | 124 |
| 9.5.1. | Spokesperson | 124 |
| 9.5.2. | Networks | 125 |
| 9.5.2.1 | Web platform (external) | 125 |
| 9.5.2.2 | Intranet (internal) | 126 |
| 9.5.3. | Media | 126 |
| 9.5.3.1 | Traditional media..... | 126 |
| 9.5.3.2 | Social Media..... | 127 |
| 9.5.4. | Establishing relationships with the population and communities..... | 127 |
| 9.5.5. | Prerecorded messages | 129 |
| 9.6. | PLANNING AND MANAGEMENT OF COMMUNICATION IN LARGE-SCALE EMERGENCIES | 129 |
| 9.7. | COMMUNICATION CHALLENGES..... | 130 |
| CHAPTER X. TRANSPARENCY AND ACCOUNTABILITY | | 132 |
| INTRODUCTION..... | | 132 |
| 10.1. | PLANNING FOR TRANSPARENCY AND ACCOUNTABILITY..... | 132 |
| 10.2. | INQUIRIES AND REQUESTS FOR PUBLIC INFORMATION..... | 133 |
| 10.3. | QUANTITATIVE DATA, INDICATORS, AND OPEN DATA..... | 134 |
| 10.4. | REPORTING SYSTEM | 135 |
| 10.5. | PROCUREMENT AND ACQUISITION PROCESSES FOR GOODS AND SERVICES..... | 135 |
| 10.6. | INTERNAL/EXTERNAL AUDITS..... | 136 |

| | | |
|-------|-----------------------------|-----|
| 10.7. | COMMUNICATION PLAN..... | 136 |
| 10.8. | ADDITIONAL MECHANISMS | 137 |

Table and Figures Index

| | |
|--|-----|
| Table 1: Example of Table for the definition of strategic objectives..... | 38 |
| Table 2: Example of Table for the strategic definition..... | 38 |
| Table 3: Example of a Indicators and Goals System | 39 |
| Figure 4: SWOFT example | 40 |
| Figure 5: Example 1 of Strategic Map Figure 6: Example 1 of Strategic Map | 41 |
| Figure 7: Advantages of the Balanced Scorecard | 42 |
| Table 8: Example Table to define and explain the assumptions | 43 |
| Table 9: Example of a Table for the Identification and Classification of Risks..... | 45 |
| Table 10: Example of Table for Risk Analysis | 46 |
| Table 13: Example 1 of Risk Matrix..... | 47 |
| Table 14: Example 2 of Risk Matrix..... | 47 |
| Figure 15: Six Basic Operational Tasks | 50 |
| Figure 16: Model B..... | 50 |
| Figure 17: Model C..... | 50 |
| Figure 18: Some recommended attributes for information architecture | 55 |
| Table 19: Classification of appropriate calls | 57 |
| Table 20: Prioritization scheme | 58 |
| Figure 21: Service Quality Management..... | 68 |
| Table 22: Identification of Information Needs..... | 99 |
| Figure 23: Acquisition of information | 100 |
| Table 24: Development of Services and/or Products | 102 |
| Table 26: Risks and recommendations when receiving calls and monitoring cameras | 116 |
| Table 27: Risks and recommendations in responding to emergencies on the field..... | 117 |
| Table 28: Template for the development of a Communication Plan | 122 |

Acronyms

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

| | |
|------|-------------------------------------|
| VMS | <i>Video Management Software</i> |
| VOIP | <i>Voice Over Internet Protocol</i> |

Glossary

| | |
|----------------------------|--|
| Alert | Notification, call or signal regarding an incident that has occurred, is occurring or is about to occur, and that enters the emergency and security system through any of the established communication paths, channels or means. |
| Appropriate call | A call that is 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) | Management approach and methodology for strategic planning, which translates into action the strategy and vision of the organization. It converts objectives, goals, and activities into a set of indicators to track and measure the overall performance of the organization, which are 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 a component of it, 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 that are applied in the protection and securing of 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 | 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 that are activated in the event of a contingency that affects the operation of an emergency and security system to minimize downtime and maximize recovery time. |
| Continuous improvement | Systematic process of collecting, analyzing, using, and documenting information to follow up on actions aimed at producing a product or providing a service, with the purpose of identifying 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 that covers the data, hardware and software considered as critical and essential for the operation of an emergency and security system, so that it can resume operations if it has been affected by a contingency. |

| | |
|---|--|
| Dispatcher | Person in charge of assigning units and resources for the timely assistance of an emergency, contingency or incident that generates an alert to the emergency response service. |
| Dispatch of resources | Unit or activity that involves choosing and assigning the available and necessary resources in response to an emergency, contingency, or incident, according to its type. It is usually performed by means of a technological system or platform (see definition of computer-assisted dispatch). Additionally, dispatch of units is also used. |
| Emergency | 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 types of 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 | Message transmitted by the entities that provide and manage emergency services, through any means, platform, or technology. This message can be transmitted massively at national, subnational, or zonal level, or to a group of people, depending on the type of emergency and the situation that arises. |
| 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 the structure of an emergency and security system. They can be classified into two types of main functional or mission areas. Since both their activity and the work they perform are critical for the fulfillment of the aim of an emergency and security system. Among the main functional or mission areas, the following could be considered: Operations Management, Process and Protocol Management, Quality Management, Information and Communication Technologies, Security Management, and Information and Analysis Management. The second type of functional areas are those that act as supporting units, including: Human Resources, Administration and Finance, Legal, Communication, Strategic and Operational Planning, and Project Management. |
| Geographic Information System | Software for entering, integrating, analyzing, sharing, visualizing, retrieving, and storing geographically referenced or spatially referenced data and information. It is often a key software tool for the location, response, and management of emergencies. |

| | |
|----------------------------|--|
| High availability | A design protocol that when implemented indicates the technological infrastructure of an emergency and security system 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, which 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 attention or displacement of units or resources of the articulated response institutions. |
| Information | Information is one of the most important 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 oriented to the use of information at each of the three operational levels of an emergency and security system (strategic, tactical, and operational) to guide decision making and meet established objectives. It comprises of a series of stages, guided by regulations, standards, and procedures, and streamlined or facilitated using software. |
| Information security | A set of preventive, proactive, and reactive measures applied with the purpose of preserving the confidentiality, integrity and availability of information. |
| Interoperability | Ability 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 involved stakeholders. |
| Misuse of the Service | Requests, calls and reports received by the emergency and security system, which are due to improper, malicious, or fraudulent use, or which entail the obstruction and unnecessary use of the System's material and human resources. |
| Multidispatch file | Electronic tool of the system that requires mandatory fields to be filled out by the operator in an electronic form that allows for simultaneous transfers to two or more response institutions. |
| Operator | Person in charge of receiving, categorizing, inquiring, assessing, and addressing, based on established guidelines and procedures, requests, calls or reports that enter the emergency and security system. |
| Operations continuity plan | Emergency plan that, based on the identification and analysis of risks, and the identification of critical and essential processes for the operation of an emergency and safety system, establishes the processes, steps, and actions to be undertaken, as well as the assignment of responsibilities, to guarantee and recover the operation of the system in the event of any contingency. |
| Ordinary file | Electronic system tool that requires mandatory fields to be filled out by the operator in 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 emergency situations or scheduled events. One of the main reasons for the use of this type of messages is to avoid congestion of the line and other channels to report an emergency. |
| Prioritization levels | Categorization linked to the risk estimation of requests, calls and reports received by the emergency and security system, based on the characteristics and complexity of the incident or contingency, and resulting in a prioritization of attention. |
| Process map | Graphic representation of the processes of the emergency and security system, allowing to identify and focus attention on those considered critical for its 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 that take place in the main or mission-oriented functional divisions of an emergency and security system, without which it would not be able to attend 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 administrative functions of the system. |
| Programmed events | Events whose occurrence is known in advance and that require the early activation of emergency and security systems to inform and communicate to the population about the status and evolution of these events, and to prevent and act in a timely manner 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 the provision of a service, fulfillment of a task or performance of an activity. |
| Quality management | Management and organizational culture approach aimed at satisfying the requirements and needs of users 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 reports the characteristics and circumstances related to an emergency. |
| Response resources | These are the components of an emergency assistance and response service, consisting of people, vehicles, and tools. |
| Risk analysis | A study to identify and evaluate potential hazards and threats and understand their possible consequences, effects, impacts or damages, either on the planning process and plan, 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 an analysis, which tends to be presented in matrices, and both (the analysis and the risk matrix) are used for management of risk. |
| Risk management | Processes established and managed in a comprehensive manner 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 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 operation (processes and services) and its facilities; and 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 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 fulfilled for the provision of these services. |
| Strategic map | A tool used to visualize and follow up on 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, which participate in a complementary manner and seek to create conditions and capacities for the functioning of an emergency and security system. Some examples of subsidiary actors are: international agencies, civil society organizations, the business sector, the academic sector, the media sector, among others. |
| 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, as well as the quality of the service provided, based on the established protocols and reference 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 of priority or specific attention; entities in charge of providing basic 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 under his/her charge, to detect and categorize possible incidents that require immediate |

| | |
|-----------------|---|
| | response or assistance, and to analyze, evaluate and direct 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 potential negative effect. |

Prologue by the General Director of the SIS 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 a great opportunity to disseminate and propose alternatives on a common topic: the prevention and fight against 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 basic 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, the issue of emergency preparedness and response was addressed, promoted by Ecuador through the Integrated Security Service ECU- 911 (SIS ECU-911).

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

During difficult times, product of the global health crisis caused by COVID-19 and its multiple impacts, wherein emergency answering and response systems have played a key role, we hope that this Guide will serve as a useful and actionable tool to provide guidance during the creation or strengthening processes for this type of services within the member states of the Organization.

The making of this Guide is the product of international cooperation. Therefore, we value the support and commitment of countries such as: Costa Rica, Mexico, Paraguay, and the Dominican Republic. Each of the countries that support this initiative has provided the experiences of their own 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 aimed at 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 of sharing it with other OAS Member States opens the opportunity to share experiences and knowledge to face common emergencies and threats. It also provides a space to standardize good practices regarding responses and interventions aimed at safeguarding and protecting people's lives and integrity.

Thus, the commitment we took on is ratified and we trust that in the short-term we will be able to execute agreements that allow 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.

Important actions have been undertaken, but many additional initiatives remain to be promoted 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 answering points and response. There are also various levels of progress among the countries in the region regarding their integration of services and interoperability, territorial coverage, the standardization and protocolization of operational processes, information and communication technological infrastructure, and IT support, among other aspects. In addition, not all countries have a single number for receiving emergency assistance requests from the population.

This asymmetry and wealth of experiences within the hemisphere opens an interesting and necessary workspace at the inter-American level and from a multilateral context.

Emergency assistance and response is a new and recently incorporated topic within the framework of the Organization of American States. Ecuador, through its Integrated Security Service ECU-911 (SIS ECU-911), was one of the main promoters of incorporating this issue at the regional level, in the various OAS forums and in the work of the General Secretariat of the OAS, particularly in its Department of Public Security.

The foundational event that initiated the trajectory of emergency and security systems on the hemispheric security agenda and within the Organization was the International Seminar on Cooperation Mechanisms and Tools for Emergency Services in the Region, organized by SIS ECU-911 in April 2019. It was on that occasion that a series of consensus proposals were presented, including the creation of a Subsidiary Technical Group on Emergency and Security Systems (GTS-SES), and the preparation of 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 that they approved in their Seventh Meeting, held in Quito, Ecuador in October 2019.

It is based on these recommendations and within the framework of the Subsidiary Technical Group on Emergency and Security Systems (GTS-SES) that, with the leadership of the SIS ECU-911 and the technical support offered by the Department of Public Security, the basic conditions necessary to enable the drafting of this Guide were met.

This Guide is aimed to all the countries of the region, either for the creation of integrated national emergency and security systems or for the strengthening of existing ones. It is precisely due to the existing asymmetries and differences between the countries in terms of emergency assistance and response services that this Guide hopes to contribute to reducing some of these gaps, facilitating the best possible integration between systems.

The development of this Guide is a milestone that deserves to be celebrated for several reasons. First, 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, Mexico's National Information Center, the Integrated Security Service ECU-911, and the 911 Emergency System of Paraguay, each of them contributing, from the standpoint of their knowledge and experience, with the drafting of roughly one to four chapters each. Second, because this Guide was developed in the context of an unprecedented pandemic in the last 100 years of human history, which placed all the first responders and health personnel in a situation of permanent alert, care, and service, to try to save as many lives as possible. Despite this challenge and its associated responsibility, these five institutions managed to make this Guide. Third, because it means a concrete, valuable and useful contribution for the other countries and systems in the region. They have created a regional public good

that is made available to everyone who works in emergency assistance and response to establish, improve, or strengthen the services they provide to the population.

Likewise, the production of this Guide revalues and enhances the existing collective workspaces, as part of the operational and technical structure of the OAS. It is from these multilateral places, 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 SIS ECU-911 and the making of this Guide, the Subsidiary Technical Group on Emergency and Security Systems is off to a promising and productive start. From the OAS General Secretariat, we hope that this will be one of many products that will guide the countries in the region in leveling the capacities of emergency and security systems for the sake of greater quality, excellence, and professionalism in providing this kind of services, with sights on a scenario of greater cooperation and integration between them.

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) was born as a proposal from the Integrated Security Service ECU-911 (SIS ECU-911) of Ecuador. The proposal was presented within the framework of the International Seminar on Cooperation Mechanisms and Tools on Emergency and Security Services of the Region, which took place in the city of Quito, Ecuador on April 25th and 26th, 2019. In that opportunity, an index proposal with 10 chapters was presented, which was submitted to the consideration of the participating delegations.

The International Seminar resulted in a consensus proposal document, among which the Subsidiary Technical Group on Emergency and Security Systems (STG-ESS) was entrusted to develop the Guide.

The consensus proposals document was transmitted to the preparatory process for the Seventh Meeting of Ministers Responsible for Public Security in the Americas through the Hemispheric Security Committee. Thus, the proposals agreed in the framework of the International Seminar were incorporated into the Quito Recommendations for Strengthening International Cooperation in the area of Public Security Matters for the Prevention and Fight against Crime, approved on October 31st, 2019. Among the 19 recommendations approved by the Ministers Responsible for Public Security in the Americas on that occasion, the planning of the STG-ESS work by the Department of Public Security (DPS) was included, with special emphasis on the objective of completing the Guide for the Establishment and Strengthening of National Emergency and Security Systems in the OAS Member States.

This way, once the STG-ESS was established under the presidency of the SIS ECU-911, a first planning meeting was organized on March 3rd, 2020 during which it was agreed that the DPS would prepare a Work Plan. On March 13th, the DPS presented an activity plan for the STG-ESS with four activities, including the development of the Guide. It was decided to work collectively and collaboratively on the Guide, inviting other Emergency and Security Systems, and related institutions, to participate in the process, collaborating in the drafting of one or more chapters.

However, the categorization of the coronavirus disease as a pandemic by the World Health Organization (WHO) on March 11th, meant delaying the start of the drafting process of the Guide, and redirecting the efforts of the STG-ESS to provide some kind of response, accompaniment and support to the Emergency and Security Systems of the region in the fight against COVID-19.

Faced with this new scenario, the SIS ECU-911, as chair of the STG-ESS, and the Public Security Department, in its capacity of Technical Secretariat, took the initiative to create a Virtual Community, 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 to respond 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 conversations. In 2020, as part of that series, four conversations were organized for the members of the Community, on issues related to the pandemic.

The development of the Guide was resumed in June 2020. Thus, on June 8th, the authorities of Costa Rica, Mexico, Paraguay, and the Dominican Republic, linked to emergency assistance and response, were invited to participate in the drafting process of the Guide, asking them to choose one or more chapters to work on. As said authorities responded to the invitation letters sent, the 10 chapters of the Guide ended up being distributed between them.

On June 19th, a coordination meeting between the SIS ECU-911 and the OAS DPS (DPS/OAS) was held. In that meeting, the allocation of the 10 chapters among the five participating institutions was presented: 911 Emergency System of Costa Rica (Chapter 1), the 9-1-1 National Emergency and Security Response System of the Dominican Republic (Chapters 2, 3, 8 and 10), Mexico's National Information Center (Chapters 4 and 8), Integrated Security Service ECU-911 (Chapters 5, 7, 8 and 9) and the 911 Emergency System of Paraguay (Chapter 6).

At that meeting, the DPS made a series of proposals for consideration by the SIS ECU-911, including: a 7-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 writing style and the document format and saving, among others. Additionally, a shared folder was created on Google Drive, giving access to all the officials involved in the production process of the Guide. All documents related to the Guide's elaboration process were made available in that shared folder, including the general and planning guidelines, and the successive versions of the chapters.

Once the SIS ECU-911 endorsed the proposals made by the DPS/OAS, they were presented to the participating institutions at a planning meeting held on July 1st, 2021. This meeting can be conceived as the starting point of the collective and joint production process of the Guide, thus activating its first stage. As part of this first stage, individual meetings were held with the five participating institutions to review the index of the assigned chapter(s), reach agreements upon the contents that were expected to be covered in each chapter, review the general guidelines, and answer any doubts that the teams may have had regarding the Guide and the production process.

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

Once a first draft of the Guide was obtained, an internal review process was organized with the participating institutions themselves (third stage). In this stage, having read the entire Guide as an integrated product, each country team was able to share and submit their comments and suggestions to 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 the scrutiny of EENA and NENA Mexico-Latin America. In addition to receiving their comments in writing, two working meetings were organized with two representatives of the aforementioned organizations, so that they could also give virtual feedback to all the participating institutions. This way, an exchange and learning space was created between all those involved.

After incorporating all the contributions resulting from the review and validation stages, the second draft of this Guide was produced. This second draft went through a brief editing stage (fifth stage) to be 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, headed by SIS ECU-911. The meeting took place on May 6th and 7th, 2021, virtually, 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. Likewise, the representatives of EENA and NENA

Mexico-Latin America, and the external consultant who accompanied and provided technical support throughout the entire making process of the Guide were present.

Having been well received by the Member States, who highlighted the fact that it is a jointly developed product, based on the coordination, participation, effort, and experience of the region's own 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

The implementation of strategies and concerted actions to promote and strengthen the necessary capacities for the prompt provision of quality emergency and security services, and to increase their effectiveness, is a recent objective in the hemisphere. This objective arises in response to a growing demand by the population for protection and response regarding the agencies responsible for providing assistance, both in frequent incidents and daily contingencies as well as in situations of greater danger and complexity.

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

In times of crisis and deep transformations, the need to model and have Systems to protect and more effective services to help people, breaks the molds of the paradigms used until now and, likewise, to innovate in the design of public services, particularly concerning the interaction between authorities, institutional actors and users or beneficiaries. This represents an opportunity to encourage and coordinate the 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, either to install or to strengthen capacities in prevention and reaction to emergencies and incidents associated with public and citizen security, as well as when facing situations of greater magnitude and complexity. All these situations require greater or lesser levels of coordination and collaboration between different immediate response institutions, and, in some cases, the support of specialized institutions might also be needed.

The public and critical nature of the work conducted explains the need to promote joint actions by public authorities at different levels and contexts, facing obstacles and improving the conditions for emergency assistance and response, including those related to security, conceived as a vehicle for a better quality of life. That is why the approval of laws, the assignment of resources, and the design and implementation of public policies and programs that support this type of services are necessary.

At the hemispheric level, support came from the Subsidiary Technical Group on Emergency and Security Systems (STG-ESS) and was materialized in this Guide for the Establishment and Strengthening of National Emergency and Security Systems in OAS Member States. It presents a systematization of guidelines and recommendations, organized in 10 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, which allows to shed light and guide decision-making regarding the design and operation of an emergency and security system. It is not a Guide that explains how to do things, nor a single recipe with the 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 considerations on components, areas, processes, and tasks that could be considered for the creation, strengthening and sustainable operation of this type of service.

Regarding the creation and establishment of an emergency and security system that is addressed in **Chapter I**, a shared observation is the relevance of a systemic, integrated and joint responsibility approach on horizontal cooperation and coordination. The governance of the System 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 such as the one presented in **Chapter II**, it will hardly be possible to provide timely and quality assistance to the requirements of people at risk. The configuration of an effective model, during the design of the emergency and security system, involves choosing between different operational alternatives, which vary in structure, mechanisms, integration levels and areas of collaboration between articulated entities or institutions (first response) and related institutions (complementary), which shall comprise it. These questions and decisions intrinsic to the design stage of an emergency and security system are introduced in **Chapter III**.

This entails focusing on reducing one of the main weaknesses observed, such as -in some cases- the insularity of organisms, the asymmetries, and gaps in effective capacities, and strengthening those determining factors that are at the basis of information and communication interoperability. There is no doubt that this challenge goes beyond improving coordination, and involves efforts for the integration of existing subsystems, and planning of interoperable technological and information architectures, sufficient infrastructure and resources, coverage and availability of units in the various territories, among others

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

The development achieved in information and communication technologies makes it more likely that OAS Member States will have tools that make processes more efficient. However, among the functional areas, management of calls and response to incidents are essential functions that deserve special attention, through the provision of continuously updated and validated protocols, procedures, and standards. That is why **Chapter V** of this Guide focuses on the reception, treatment and response of the assistance requests, calls and reports received. It is in this area where collective intelligence, organizational engineering and the exchange of experiences and lessons become indispensable.

As the experiences on State modernization show, management of human talent involves an important effort to increase the main asset of any public organization. That is why, in this Guide, **Chapter VI** places special interest in lines of action to guarantee the professional quality of the staff, from recruitment and selection, induction and continuous training, to evaluation and departure. Likewise, it also focuses on the well-being of the personnel through a series of criteria focused on promoting occupational health and security, as well as creating a safe and healthy work environment.

Information management is considered a main process for the strategic objectives of the System and to provide support and guidance to the delivering of services. It is for this reason that in **Chapter VII** information management is linked to the organizational strategy and to the levels of operation of an emergency and security system. As information is one of the main assets of this type of Systems, it is also suggested to have a cycle of processes, which optimizes a series of stages related to obtaining, organizing and storing, distributing, accessing, and using this resource for the development of products that support decisions in the different instances and moments associated with interoperability flows in the assistance and response to emergency requests, calls and reports.

In a System that assists and responds to emergencies, security management must be approached from a multidimensional perspective, paying special attention to both the conditions for the operation of a center and to the continuity of services. That is why **Chapter VIII** not only suggests courses of action for the protection of information, communications, computer systems, physical and infrastructure security, and

personnel security, but also addresses the analysis and management of risk. To this end, the Chapter presents guidelines for developing at least two basic tools: continuity of operations plans and disaster recovery plans.

A central element in emergency management, as well as during high intensity incidents or larger crises, is communication management, both institutional and operational. Faced with these situations, **Chapter IX** outlines the minimum elements that need to be considered when preparing a communication plan. This tool serves as a roadmap for managing communications, using different channels and tools, including spokespersons, the use of networks, traditional and social media, engagement with the population and communities, and prerecorded messages. Towards the end of the Chapter, some orientations are also postulated to guide the planning and preparation of crisis communication.

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 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, as well as the organizational communication. The Chapter proposes a series of tools and mechanisms to proactively provide information on the operation, management, and results of the System, as well as 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 I: CREATION AND ESTABLISHMENT

Introduction

This Chapter presents the basic 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 purposes, its position within the structure of the State, institutions that comprise it, responsibilities and functions, services it would provide, resources that it would have, among other foundational elements, and (c) financing.

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

There would be at least three types of actors that could be considered to form the structure of an emergency and security system. The Chapter emphasizes the need for coordination and cooperation between the actors, advocating a systemic approach that allows the parties to collaborate with each other to deliver quality products and services with high public value. 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 strategic direction while the second would be responsible for tactical and operational issues

1.1 Institutional and political support

For the creation of an emergency and security system, will, leadership and political support at the highest level are essential, guided by a vision of what type of system to create and how to create it. This would have to manifest itself into political-technical consensus and inter-institutional agreements, including service level agreements (public/private).

It would also be important to have the involvement of all entities deemed necessary due to their direct and indirect role in Emergency and Security Response. This involvement would have to be from the beginning, to generate a common identity, a feeling of ownership and the empowerment of those who make it up. Likewise, it would help to 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 services for emergency answering, aimed at protecting and saving 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.

They outline powers and responsibilities, functions, and roles, as well as supra and inter-institutional instances for the coordinated articulation of institutions, bodies and any other entity related to the products and services provided by an emergency and security system.

It is considered that the ideal legal instrument for the creation of an emergency and security system would be through an Act, due to the Legislative and Executive support that this entails, in addition to the fact of it being a rule of a higher rank.

Additionally, it may be necessary to establish agreements between the participating institutions that promote, at least, the guidelines for coordination, collaboration, co-production, and co-responsibility.

In any case, the legal instruments by which the creation of an emergency and security system is conceived, would have to explicitly specify, the mandatory participation of the institutions related to emergency response in each country.

1.3 Institutional Anchoring

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

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

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

A third possibility is that the emergency and security system is constituted under the protection of a decentralized public institution

In any anchoring scheme, the standard would have to fully establish what are the responsibilities, powers, 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.

To maintain coordination and collaboration among the member institutions, as well as impartiality and uniformity in operational actions, it is recommended that the System is not institutionally anchored within a preexistent entity.

1.4 Ideation

Based on a strategic vision, the System could be conceived as a public policy or as an instrument thereof, a management model or a network of cooperating entities for the provision of emergency answering services. This service network would have to respond to the need to improve interoperability between the components, through integration and value addition. That is why the integration 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 that is articulated and operates in a context of interoperability, with other institutions that deal with incidents and emergencies that affect the population. Its strategic objectives would have to be aimed at favoring collective interests and achieving greater impact and quality in the service provided to the population.

The nature of the entity that is eventually formed, would imply that the competencies allotted to any bodies comprising it would have to form an organic entity. All of them would have to act in an integrated manner, contributing with their skills and resources to achieve not individual objectives for each institution, but rather collective ones, related to the effective and quality answering of emergencies.

1.5 Structure

The creation of an emergency and security system would have to be translated into a structure that, in turn, would be presented as an opportunity to seek synergy among the member institutions at a national and subnational level.

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

- First response actors (or articulated institutions or institutions of the first ring)
- Supporting actors (or related institutions or institutions of the second ring)
- Subsidiary actors (or third ring institutions)

1.5.1 First response actors (or articulated institutions)

First response actors would be responsible for carrying out essential functions in an emergency and security system. Among which, appear the following:

- Receive, process and answer to applications, calls and help reports, and the coordination of responses in emergency situations, with coverage throughout the country.
- Enable and maintain multiple means of communication between people and the emergency and security system, including mobile and land lines, text messaging (SMS), applications, help buttons (panic) and social media, among others.
- Serve as a Coordination, Command and Control Center for Emergency Responses and manage the video surveillance monitoring centers.
- Prepare, update, and validate common action and answering protocols.
- Develop and maintain high availability technological and communications infrastructure for the coordinated provision of services.
- Serve as an operational entity for the national risk and disaster management system, when appropriate.
- Maintain a backfield registration system for the traceability of cases and the analysis of procedures, management audits and the measurement of the effectiveness of services and, likewise, periodic accountability exercises

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

- **Transit and mobility:** First response institutions would be in charge of answering to emergencies related to vehicular traffic issues or traffic problems on the country's roads.
- **Citizen/public security:** First response institutions would be in charge of answering to emergencies related to the prevention and mitigation of crime, the preservation of security and the maintenance of public order.
- **Health (physical and mental) care:** First response institutions would be in charge of answering emergencies, related to events that threaten the life and health of people.
- **Fire and incident management:** First response institutions would be in charge of the prevention, care, mitigation, control, investigation and evaluation of fires. Likewise, they would be responsible for rescuing trapped or lost people.
- **Care and prevention of risks and disasters:** First response 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 liaison institutions)

According to the types of emergencies and the needs of groups in situations of vulnerability and/or critical risk, the possibility that first response institutions may have to coordinate with other state agencies shall be considered. These would act as support entities (also referred to as second-ring institutions). 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 sectional services could be wide or narrow, depending on the institutional engineering of each country, the 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: Ministries, Technical Secretariats, Departments, Directorates, Special Commissions, and municipalities, among others.
- Entities in charge of specific segments of the population, such as those related to children, women, the elderly, people with disabilities and minorities, among others.
- Entities in charge of the attention of tourists and foreigners: those that provide multilingual attention and guide people who visit and stay temporarily in the country and with a status different from that of citizen or resident.
- Entities in charge of providing basic services: drinking water, electricity, food provision, education, health, among others.

1.5.3 Subsidiary actors

There is a third type of actors that could be called subsidiary entities or third-ring institutions, and that would seek to generate conditions and capacities for the operation of the system.

Some examples of subsidiary entities would be: international organizations, civil society organizations, the business sector, the academic sector and the media sector, among others, with whom it would be possible to sign agreements or negotiate specific support to contribute to the improvement of the service.

1.6 Operation levels

There would be at least three levels of operation to consider concerning emergency answering:

- Strategic level:** The space where long-term objectives and interaction with other entities are determined, and decisions that affect the System are made, its organization and structure, with a vision oriented towards the future and the sustainability of services.
- Tactical level:** Related to the development and execution of action plans for the main service areas and activities, the coordination, supervision, and evaluation (with a quantitative and qualitative perspective) of operations and goals to be achieved. This level is made up of a series of internal processes that provide support for the operation of the System.
- 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 response entities (first ring), supporting entities (second ring), and subsidiary entities (third rings) would need to be aligned around shared purposes, objectives, and goals, within the framework of strategic planning (See Chapter II of this Guide).

The proper functioning of the System would also require coordination and cooperation between the entities that make it up, to generate a quality service and public value.

Particularly among first response entities, it would be suggested to work based on a dynamic of horizontal cooperation between peers, with communication channels and flows and mechanisms to facilitate the exchange of resources, information, ideas, and personnel.

The regulations of each of them would have to be respected under the assumption that they are all under the same or similar condition. Additionally, all of them would have to respect and adhere to the regulations of the emergency and security system. The latter could be considered as complementary, contributing to the creation of a common identity and purpose, and the generation of a work environment based on collaboration for the provision of a public service.

Coordination and cooperation between the entities that make up a System could assume different modalities:

- Collaborative networks and networks of topics or themes
- Horizontal peer cooperation
- Promotion of mechanisms for the exchange of information and knowledge (systematized experiences and good practices)
- Collaboration in design and evaluation processes
- Creation of effective alternatives for the exchange of study results or research products
- Promotion of public-private partnerships, universities, and international organizations
- Periodic training and professionalization instances
- Cooperation in the training of human talent and professional specialization, 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, in the norm that sets forth its creation, the formation of an Inter-institutional or Inter-sectoral Commission or Committee.

Meeting periodically, and extraordinarily whenever necessary, said Commission or Committee could have some of the following functions:

- Define and approve inter-institutional processes, policies, procedures, and protocols.
- Supervise compliance with the guidelines defined as necessary so that the emergency and security system, as well as the offices of each institution or member organization, meet the objectives established by law.
- Establish the parameters and ensure the quality and efficiency in the attention of requests, calls and emergency reports.
- Establish quality-of-service parameters (with a quantitative and qualitative perspective) of the emergency and security system from the moment the emergency request, call or report enters the PSAP until the moment the emergency incident is closed.
- Create the commissions it deems necessary for its proper functioning.

In some cases, this instance could exist temporarily, to lead and accompany the design and installation. In others, it could be constituted for the supervision of the emergency and security system, once installed and in operation. In this second scenario, it would assume a more permanent character.

It is possible that this Commission, depending on its position and legal status, is made up of the heads of the entities that make up the System, and chaired by the highest authority of the corresponding Ministry.

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

1.9 Executive Director (or similar position)

The regulation that establishes the emergency and security system would have to define the selection process and the profile for the position of an executive director, in accordance with the framework for hiring public officials in each country.

The Director is the one who concentrates the operational-tactical execution of the provision of services, so it is considered appropriate that the profile of the position incorporates the skills, abilities, knowledge, and experiences necessary for the management of an emergency system and security.

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

- A technically defined competence profile in the field of security and risk and incident management.
- The professional experience necessary to lead a strategic, tactical, and operational process.
- The suitability required for all public servants

1.10 Financing and sustainability

The financing would have to consider, in the first instance, the resource for the creation and establishment of an emergency and security system, which could come from a loan or international cooperation agreement. Then, in a second instance, funds would be required to guarantee its functioning and the continuity of operations of the System. These funds could come from at least two sources: a national budget (annual or multi-year) and, in addition, a specific tribute or tax.

As we refer to fiscal resources, the exercise would be subject to the application and execution of the Public Sector Budget Act (or similar) of each country. The resources would be subject to a control, auditing, or oversight process.

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

In line with the above, an additional source of financing could be generated from the sale of the services of the System itself, subject to the requirements and conditions established in the legislation that stipulates its creation and operation.

CHAPTER II: STRATEGIC PLANNING

Introduction

This Chapter presents strategic planning as a tool and as a process. In its conception as a management tool, the minimum components that would have to comprise it are presented herein. Regarding the process, its standardization and institutionalization is accomplished through the definition of protocols, procedures, and instruments. The latter are presented in terms of three stages inherent to the planning process: the pre-planning stage, in-planning, and post-planning.

Planning as a tool, which is, the results from the planning process, would be a strategic plan. Regarding this, the Chapter focuses on making the assumptions explicit, 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 objectives and established goals.

Strategic planning is presented in this Chapter as a different tool compared to traditional planning. This is because the former would be focused on addressing the largest mid and long-term challenges, incorporating prospective analysis and the consideration of possible future scenarios, and adapting to internal and external changes that an emergency and security system may experience.

2.1 Strategic planning

The strategic plan could be considered as a management tool, which brings together a set of objectives, goals and activities established by an organization, with a view to achieving them and carrying them out within a specified period. Additionally, it could also be considered as a product that results from the culmination of a planning process, commonly known as strategic project or plan. In this process, all the functional areas, the highest decision-making levels and the key actors of an emergency and security system would have to be included. Throughout the process, it is important to stimulate strategic thinking, as well as to gather valuable information and different approaches to set forth objectives.

This exercise could be executed by the planning and strategic management department of the emergency and security system itself or with the support of an external consultancy, with extensive and recognized experience in 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 duly formalized, defined by a series of procedures, steps, and tools so that it can be carried out continuously and systematically.

2.2 Fundamental components of a strategic plan

The essential components that must be part of a strategic plan would be the following:

- **Vision:** It is the long-term definition of what the entity intends to be. It is how this is visualized in the future. It is the reference that guides the System to achieve the desired objectives. It usually relies on emotions and serves as an inspiring force.
- **Mission:** It describes the fundamental objective of the entity, establishing its purpose and its actions to achieve the vision. A mission statement constitutes a fundamental element to motivate the team towards the achievement of the objectives and goals, by providing them with a clear sense of direction and strategic intent.
- **Values:** Beliefs, virtues, or qualities by which the entity is governed. They reflect the standards, evoke its essence, and express its identity. The values of an emergency and security system

should be related to 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 service, among others. These values must be enshrined in the Code of Ethics and the Code of Conduct guiding the entity's personnel (see Chapter VI of this Guide).

- **Objectives:** Measurable results that the entity wants to achieve; they could be short, mid 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 as essential guidelines that lead the performance of an emergency and security system, which must be consistent with the objectives and values of said entity. They would also have to keep a certain balance between what is done (objectives) and how it is done (functions). The principles could be built on:

- International human rights guidelines
- National legal framework for the right to protection of people and their assets
- 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 model so that decisions and actions can be carried out in line with the vision, mission, and values of the entity, ensuring the well-being of personnel and users who require the services of the emergency and security system.

Here are some examples of guiding principles:

- Non-discrimination based on race, color, sex, gender, language, religion, political opinions or of any other nature, nationality, economic or social position, or any other social condition.
- Impartiality
- Cooperation and coordination
- Integration and interoperability
- Accessibility through a single dialed number
- Gratuity

These guiding principles must be expressed in the Code of Ethics and the Code of Conduct that guides 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 on which all actions of an emergency and security system are founded and developed. They establish the greater routes 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, among others.

Each axis could be accompanied by a brief description that clearly demarcates what it is about. Thus, the axis of operational excellence could be presented as follows: Conduct continuous improvements in processes, systems, infrastructure, and development of human talent, to increase the levels of quality, efficiency, and effectiveness of the System, and with it users' satisfaction (9-1-1 National Emergency and Security Response System 9-1-1, 2020).

After establishing the strategic axes, it would be necessary to define the strategic objectives for each of them. These should be aimed at directing and consolidating the actions to achieve the expected results.

Table 1: Table example for defining strategic objectives

| AXIS | STRATEGIC OBJECTIVES | DESCRIPTION |
|---|--|--|
| I. Operational Excellence Conduct continuous improvement of processes, systems, infrastructure, and development of human talent, to increase the levels of quality, efficiency and effectiveness of the System, and with users' satisfaction. | I.1 Foster a process-based quality management culture. | Set-up of effective management, one that is aligned with the vision and focused on integrated processes, to create and maintain a work culture aligned to quality in a sustainable way and to the values that govern the organization. |
| | I.2 | |
| | I.3 | |

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

2.5 Definition of strategies

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

Table 2: Table example for defining strategies

| AXIS | OBJECTIVE | STRATEGY |
|--|--|---|
| I. Operational Excellence Conduct continuous improvement of processes, systems, infrastructure, and development of human talent, to increase the levels of quality, efficiency and effectiveness of the System, and with it users' satisfaction. | I.1 Foster a process-based quality management culture. | I.1.1. Standardize processes, defining technical standards and procedures such as: <ul style="list-style-type: none"> • Radio communication functions model • Electrical technical standard I.1.2. Quality and Security Integration, setting-up Service Level Agreements (ANS) 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, oriented towards the achievement of objectives, outlining the roadmap. They would also be management tools that would allow organizing, implementing, and controlling the set of tasks necessary to achieve the goals. A strategy could be part of one or more action plans.

2.7 Indicators and goals system

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

To know whether the established goals have been met, first it would be necessary to establish a comparison baseline.

Table 3: Example of an Indicators and Goals System

| Indicator | Description | Unit | Calculation Method | Strategic Objectives Alignment | Base Line | Goals | | | |
|-----------|-------------|------|--------------------|--------------------------------|-----------|--------|--------|--------|--------|
| | | | | | 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, the periodicity with which the indicators would be calculated would have to be established and, if possible, incorporate the measurement of these indicators in the quality management control Functional division and they 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 continuously, on an ongoing basis and, if possible, automatically, would allow knowing whether the strategic objectives of the Plan are being met, to make any necessary adjustments along the way.

Each strategic objective would also have to have an allotment of responsibility. This allotment could fall onto a department, unit, team or individual.

2.8 Budget

Activities related to the achievement of the mission and objectives, would have to be accompanied by the allotted resources from the budget plan. It is important to differentiate between two types of resources. First, the annual resources, destined to the provision of emergency answering services aimed at users as well as their operating costs. Second, the resources allotted to managing human talent, developing the infrastructure to increase coverage in a medium term, or strengthening the quality management control system. Without this second type of resources, it is almost impossible to execute the strategic plan. Budget execution would have to be consistent with the programs and action plans to achieve the goals.

Criteria for prioritizing and targeting resources would be key, regarding budget allocation, personnel's capacities development and 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 greater social impact and institutional value, and lower cost

2.9 Some tools for budget planning and its execution

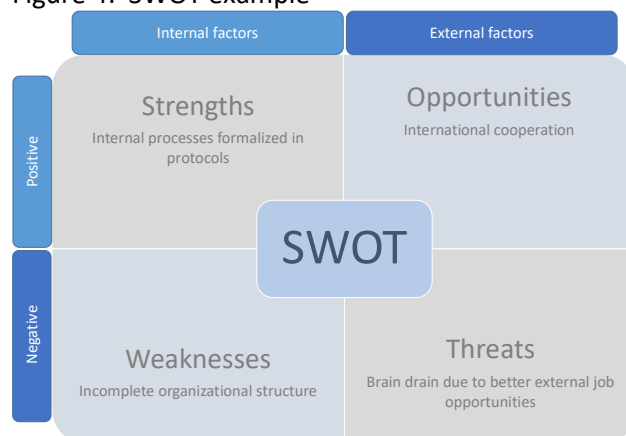
Strategic planning would be more encouraged than traditional planning since the latter is not designed to respond to massive long-term challenges. It entails the construction, development and implementation of the various action or operational plans for the entity to achieve its vision, mission, objectives, and goals.

The strategic planning process could use a series of 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 useful to, as a diagnosis, to identify strengths and weaknesses of the emergency and security system, as well as opportunities and threats for the services the System procures. This exercise could be performed with the SWOT analysis tool.

Figure 4: SWOT example



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 would visually represent the cause-effect relation that exists between the established objectives and strategic axes, and the plans and components that would result from such planning. In a single image, it makes it possible to visualize the value for the public that could be added through the service provided by the Emergency Answering and Response and Security System.

There are several ways to draw strategic maps. Below are two examples:

Figure 5: Strategic map Example 1

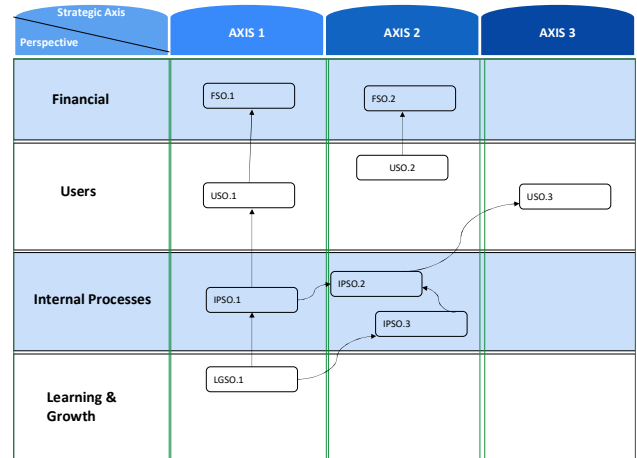
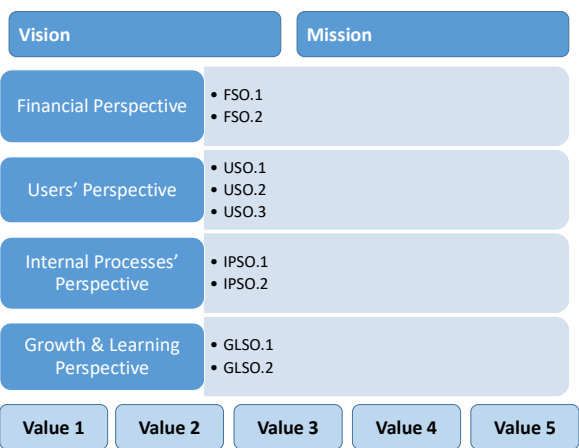


Figure 6: Strategic map Example 1



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

Example 1 shows it is possible to graphically see how the strategical objectives transversally interrelate, among the different axes.

In both cases, the strategic map would facilitate following up on the objectives of 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 to detect possible inconsistencies between the objectives, as well as to quickly identify the strategies that lack objectives and thus proceed to their elimination.

2.9.3 Post-planning: Balanced Scorecard (BSC)

The methodology of the *Balanced Score Card* (BSC) is useful for strategic operational direction and management. It is a tool to monitor and manage strategy implementation, achievement of objectives, attaining of results and indicator measurement.

The information it generates is usually easy to understand, communicable and actionable. It is from this information that the emergency and security system reformulates and adjusts its strategy, improves its analysis capability 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:** attention must be directed to how to strategically position the entity's products and services to meet the needs of users and meet their expectations
- **Internal processes:** would seek to identify and improve key processes within the entity. Key processes would have to be aligned with the strategic objectives.

Attention would have to focus on the effectiveness of those key internal processes

- **Financial:** from this perspective, attention must be focused on the adequate and timely allotment of resources, and the minimization of costs.
- **Learning and growth:** the focus would be on human talent development and the strengthening of personnel skills.

The BSC could be used to follow-up on the strategic plan, establishing a periodicity that allows for the timely detection of any deviation, to then take the corresponding corrective decisions. Discussions with the functional area in charge of quality control as well as management of the emergency and the security system would be undertaken from this perspective.

The use of a BSC could contribute with relevant information in the preparation of an annual progress and achievements report of the strategic plan, with recommendations for rethinking some strategies (if necessary). If so, these annual reports must be included in the reporting system that would therefore be designed as part of the information architecture of the emergency and security system (see Chapter III of this Guide).

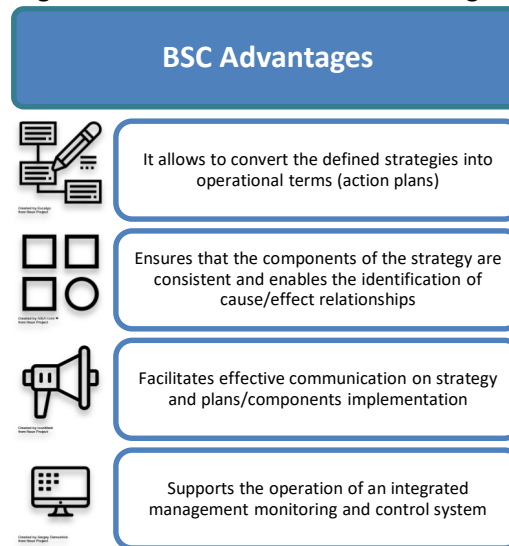
2.10 The premises of the strategic plan

It is important to differentiate between conditions and risks for the operation of the emergency and security system, and those conditions and risks for the execution of the planning strategy. In the first case, the focus would be on the emergency answering system, in the operations center or in 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 purpose, the attention must be focused on the starting premises and the conditions or circumstances, internal and external, under which such planning and the resulting strategic plan are expected to take place.

The premises and conditions for an adequate planning and strategic management process, which seeks to strengthen the emergency and security system, could be ordered according to type or origin. In general,

Figure 7: Balanced Scorecard Advantages



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

these would be systemic premises, which refer to those basic conditions, which, for example, could be distinguished from the following:

- **Political assumptions:** Support, willingness and leadership required to align efforts of the actors involved (internal) and attract the support of interested groups (external).
- **Legal assumptions:** Legal and normative bases that authorize the conduction and execution of planning, external and administrative supervision.
- **Technical assumptions:** The management methodologies for the design, execution, monitoring and evaluation of planning; and for proper risk management.
- **Economic-financial assumptions:** Provision of adequate and continuous specific resources, subject to an estimation and planning validated by the authorities and supervision in the use of the allotted resources.

Table 8: Example of table to define and explain premises

| Premises | Hypothesis |
|--------------------------------|---|
| Political assumptions | <ul style="list-style-type: none"> • Government authority support • Interest of internal and external authorities • Leadership required for leading • Support from interest groups (external) |
| Legal assumptions | <ul style="list-style-type: none"> • Adequate compliance with applicable laws and regulations • General legal framework of the System • Regulations associated with the institutional engineering and coordination of the entities that make up the System • Powers and responsibilities in the execution of planning, external and administrative supervision • Inter-agency affairs • Formation of the directive committee |
| Technical assumptions | <ul style="list-style-type: none"> • Formation of multidisciplinary work teams • Management methodologies in the design, execution, monitoring and evaluation of the processes associated with strategic planning • Planning for continuity of the operations of the System • Adequate risk management • Availability of adequate information • Trained human teams • Monitoring and quantification methodologies (Balanced Scorecard) |
| Economic-financial assumptions | <ul style="list-style-type: none"> • Stable economic situation • Secured financing policy • Outlined and allotted budget • 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 involves foreseeing changes in the conditions (and their impacts, depending on the risks and probability of damage), under which it was thought that the implementation of the strategic and operational plans would take place. Analyzing on how they could affect the course and, consequently, the possibility of achieving the established goals and objectives, and the operation of the emergency and security system must be a permanent task.

Therefore, it would be advisable to carry out analysis exercises of possible and prospective scenarios to identify present, emerging, and future conditions under which it could be foreseen that the strategic plan could be implemented and would work.

Visualization and projection of these conditions would allow those who lead the planning process to be properly prepared for possible changes. Furthermore, it would facilitate the possibility of distinguishing whether the changes or distortions observed in the performance of the emergency and security system are due to the 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 Key Success Factors

Key Success Factors (KSF), in certain contexts also called Key Success Factors, are those conditions or goals that would inevitably have to be fulfilled to achieve the strategic objectives.

Although strategic planning produces several objectives and goals, not all of them can be considered Key Success Factors. Below are some of the criteria for objectives and goals to be considered as KSF:

- They are vital or essential for the entity
- Benefit the entity
- Can be considered high-level goals
- Are related to the strategic plan

2.12 Risk identification and analysis

All activities imply risks. Strategic planning would also imply the identification of risks or contingencies that may affect its implementation. That is why it is not only necessary to identify risks, but also to evaluate the probability of their occurrence and the impact they could have.

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

- ISO 21500:2012 Standard - Orientation on project management
- ISO 31000:2018 Standard - Risk Management
- Project Management Body of Knowledge (PMBOK) by the Project Management Institute (PMI),
- The PRAM Guide of the Association for Project Management (APM), etc.

Despite the variety of existing methodologies, most of them converge in four stages:

- i. **Risk Identification Stage.** This phase would consist of the following fields:
 - a. **Priority:** It is the priority allotted to the risk (High, Medium or Low).
 - b. **Risk Status:** Identifies if the risk is Active (that is, if the Risk is being actively Monitored and Controlled) or Inactive (Does not have an effect at this time but could be activated in the future).
 - c. **Risk/Opportunity Event:** Risk Explanation.
 - d. **Symptom or Trigger:** Situation that indicates that the risk event is about to occur or has already occurred.

- e. **Related Project (s):** Describe the projects that relate to risk.
- f. **Category or Functional Aspect:** Risk Category (example: Technical, Project Management, Functional) or Functional Aspect (example: Legal, Security).
- g. **Identification Date:** Date in which the risk was identified.
- h. **Project stage:** Project phase during which the risk is expected to occur

Table 9: Example of a 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 Jun. 27, 2016. Technical staff hired by Jun. 27, 2016. Operational staff hired by Jun. 27, 2016. Staff hired from agencies by Jun. 27, 2016. | <ul style="list-style-type: none"> • Construction work • Furniture • Excute technological bids or donations |

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

ii. Risk Analysis stage

- Qualitative Analysis
 - a. **Type:** Risk impacted area/a.
 - b. **Probability:** Qualitative evaluation of the occurrence probability of the risk event. Valid values could be: Very Low, Low, Medium, High, and Very High.
 - c. **Impact:** Severity of the effect of the risk on the project objectives. Valid values could be: Very Low, Low, Medium, High, and Very High,
 - d. **Effects:** Estimated consequences to be faced post-risk
- Quantitative analysis
 - a. **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%.
 - b. **Impact:** Evaluation of the impact of the specified risk in monetary value or days.
 - c. **Effect:** The effect is the product of the probability multiplied by the impact
 - d. **Costs:** Estimate of economical 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) |
| | | | | | | |

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

iii. **Risk Treatment stage** (Table 11: Example of Table for Risk Treatment)

| Response Strategy | |
|-------------------|-----------------------------------|
| Strategy | Response Advantages/Disadvantages |
| (16) | (17) |
| Mitigate | Monitoring of staff recruitment |

- Strategy:** Strategy to be used to respond to risk. Possible values could be:
 - For Negative Risks (Threats): Mitigate, Transfer or Avoid.
 - For Positive Risks (Opportunities): Exploit, Share or Improve.
- Response Action:** Detailed response action to be taken.
- Element/s of the Affected strategic plan/s:** Element/s of the strategic plan to be modified as part of the response strategy

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

iv. **Monitoring and Review stage** (Table 12: Sample Table for Monitoring and Reviewing Risks)

| Monitoring and Control | | |
|---------------------------|--|----------------------------------|
| Responsible (Admin. Task) | Status frequency or Event verification | Date, Status and Review Comments |
| (19) | (20) | (21) |
| HH.RR. | Weekly | 1/15/2016 Review in progress |

- Responsibility:** Name of the division, team, official 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:** It is the date of the last review, the status at the time of the risk review and any comment derived from the review performed.

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.

A basic tool for risk identification and analysis in strategic planning is the risk matrix. The different types of risk would be positioned in a visualization matrix based on an estimate reached through the comparison of different sources of appreciation (workshops, interviews, surveys, consultations, among others). The matrix would help identify what the priorities would be, and where efforts shall be directed.

The focus shall be on the high impact and high probability of occurrence quadrant. The identification would have to lead to a mitigation plan, which would include responsibility and alternative courses of action.

Below are two examples of risk matrices:

Table 13: Risk Matrix Example 1

| Risk Management Plan | | | | | | | | | | | | | | | | | | | | |
|----------------------|--------|------|------------------------|----------------------------|---|---|--|----------------------|---------|-------------|--------|---|-----------------|---------------------|---------------------|----------|--|------------------------|--|--|
| Assessment | | | | | | | | Qualitative Analysis | | | | Quantitative Analysis | | | Response Strategy | | | Monitoring and Control | | |
| Priority | Status | ID # | Date/Stage | Functional Category/Aspect | Risk Event/Opportunity | Event Description | Symptom or Trigger | Related Project | Type | Probability | Impact | Risk Matrix | Probability (%) | Impact (\$ or days) | Effect (\$ or days) | Strategy | Response Advantage/Disadvantage | WBS elements affected | Responsible (Admin, Tech) | Status Frequency or Event verification |
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) | (13) | (14) | (15) | (16) | (17) | (18) | (19) | (20) | (21) |
| 1 | Active | 1 | 2/17/2020 Execution | Technical | Interruption of power supply/information backup between PSAPs (PSAP North and PSAP South) | Interruption of power supply/information backup between PSAPs (PSAP North and PSAP South) | Failure, malfunction or warning alarm of power back-up systems operating in the PSAPs. | NA | Quality | High | High |  | | | | Mitigate | Purchase and install back-up and rapid recovery equipment. | | Department of Planning, Logistics and Budget | Weekly |

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 | Responsible 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 functional area for human talent | 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

Guaranteeing the operational continuity of the Emergency Answering and Response and Security System shall be one of the main objectives of the institutional strategic plan. In line with the above, it would be vitally important that the development of the continuity plan be included in the creation and subsequent updates of the strategic plan.

The elaboration of the continuity plan would have to start with the identification of the essential processes and systems for the emergency answering and response, in case of disaster or unplanned event. It shall 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” normality post-risk event once the contingency has been overcome, guaranteeing the integrity of the data or information.

When implementing continuity plans, it would be important to keep the following considerations in mind:

- Determine the scope of a continuity plan based on the assessment of the teams involved in the execution of the essential activities/services of the emergency and security system.
- Identify alternative mechanisms to accompany the upper and middle administrative levels, as well as the teams of the functional areas.
- Define the crisis management and communication plan.
- Organize socialization and training sessions for personnel to ensure their support and involvement.
- Define a plan for monitoring internal and external conditions in the execution of strategic planning, testing of 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 important to consider that it is not a static entity. The strategic plan shall be understood as a tool in constant review and update (to be carried out every 3-5 years), depending on a series of factors, including:

- The shifting realities of the environment (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 present 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 desired future and avoid the unwanted future.

CHAPTER III: SYSTEM DESIGN

Introduction

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

This Chapter addresses three fundamental aspects: the operating model, the structure and organization (institutional architecture) and the functional requirements. The latter revises the infrastructure/technological architecture (hardware and software), the information architecture, the physical infrastructure, and the minimum equipment necessary for the operation of an emergency and security system.

3.1 Operating models

The provision of emergency and security services can be organized based on different operating models, which vary in terms of structure, mechanisms, levels of integration and areas of collaboration between the different entities that comprise it.

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

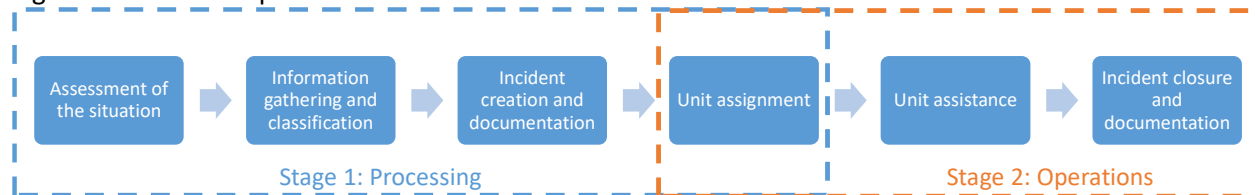
The response to an emergency usually includes two stages: the processing stage and the operational phase, each of which composed of six main activities:

- Stage 1 Processing:
 - a) Geolocation and identification of the situation
 - b) Information gathering and classification
 - c) Creation and documentation of the incident
 - d) Unit assignment
 - Stage 2 Operations:
 - a) Unit assistance
 - b) Documentation and closure of the incident
- a) **Geolocalization and identification of the situation:** The request of the user is received and automatically, via geographic information systems, and/or through a series of questions, the place from where the emergency is being reported would be established, with the greatest possible precision. The established protocols would be followed, including a script with a series of standardized questions, aimed at determining the type of emergency and risk, the degree of urgency and prioritization, and the type of service to be dispatched. (Stage 1)
- b) **Information gathering and classification:** Background search and verification. The address where the event is occurring, what is happening, and the user's data are identified. The incident is typified based on a pre-evaluation, classification, and prioritization (Filter 1), according to the typology of incidents parameterized in the computerized system. (Stage 1)
- c) **Creation and documentation of the event:** A report to notify the response units that they would have to attend the scene, according to the parameterization of the incident. Once created, it

would be convenient for other data to be collected to complete and supplement the information about the incident and the scene. (Stage 1)

- d) **Unit Allotment:** Notification and dispatch of the unit closest to the event through the pre-established means (radio, fleet, platform, or other channel), and allotment of the event. Possibility of requesting support from other first response or support entities and allotting additional units. (Stage 1)
- e) **Unit assistance:** Follow-up and contact with the response units from the moment of arrival at the scene of the incident and until their withdrawal, reporting what is happening in the place. (Stage 2)
- f) **Documentation and operational closure of the event:** Documenting the event with all the information collected, including information collected during dispatch and attendance. Closing of the event complying with the established protocols. (Stage 2)

Figure 15: Six basic operational tasks



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

There is no single way to accomplish or combine these operational tasks. In fact, at least six operating models have been identified. These are differentiated from each other based on the assignment of responsibilities and the degree of concentration and the institutional location of those six operational tasks. These operating models are:

Model A: Emergency operating entities receive, manage calls independently, and respond to requests independently. It is an essentially autonomous model comprising Stages 1 and 2.

Model B: There is a central office for receiving requests, calls and emergency reports that channels them to the response institution(s) (Stage 1). The office is under the responsibility of each institution and is independent (Stage 2).

Figure 16: Model B



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 reception of requests, calls and reports in a coordination room (Stage 1), which routes communication to an operational unit, following up on the service until the operational closing of the case, but the dispatch of the units is done from elsewhere (Stage 2).

Figure 17: Model C



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

Model D: There is a hub integrated by the response institutions, which operates from a room for receiving requests, calls, and reports, and for coordination, command, and control, concentrating the 6 basic operational tasks in one single place (Stages 1 and 2).

Model E: There is an entity independent of the response institutions, which manages the System and the resources of the operating entities, through an integrated reception/response center or hub, command, and control room (PSAP).

Model F: There is a network of care centers or emergency and security answering and response points (PSAP) interconnected by an integrated technological system. This would provide remote services: it would receive, give remote assistance and follow-up on the service until closing, without being directly involved in the dispatch of units

3.2 Structure and organization (institutional architecture)

The functions model adopted would require an organizational structure that is aligned with the mission, vision and strategic guidelines set forth herein (see Chapter II of this Guide).

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

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

- **Operations Management:** Its main function is to coordinate and undertake the operations necessary to guarantee the timely, efficient, and effective provision of the service to the user, as well as institutional and inter-institutional coordination to ensure the interoperability of the System.
- **Management of Processes and Protocols:** Its main function is to ensure the design of each of the processes and their respective protocols of action and interaction for incident response, considering laws, regulations as well as norms or standards that regulate the fulfillment of the objectives.
- **Quality Management:** Its main function would be to implement and promote the quality assurance system and mechanisms, and the tools that direct towards continuous improvement, as well as the measurement and monitoring of the quality-of-service provision, considering the feedback from the users and the support or articulated entities (see Chapter IV of this Guide).
- **Information and Communication Technologies:** Its main function is to define the main technological platform, as well as to guarantee the availability and operation of the technological infrastructure that supports the operations of the System, considering information security management, capacity growth planning and contingency plans as the pillars of service continuity.
- **Security Management:** Its main function is to ensure the security of the facilities, personnel, equipment, properties, and visitors of the System, identifying vulnerabilities, threats and the measures that can be conducted to physically and digitally, protect the resources and information of the institution (see Chapter VIII of this Guide).
- **Information Management and Analysis:** Its main function is the processing of operational indicators and inputs for administrative management, generating timely and reliable information that serves as the basis for decision-making and service improvement (see Chapter VII of this Guide).

Examples of functional areas that are considered as support:

- **Human Talent:** Its main function would be to create policies and manage, in a timely manner, human talent that efficiently supports the service, through the processes of selection, recruitment, training and continuous evaluation, work environment management and compensation management, among others. (See Chapter VI of this Guide).
- **Administration and Finance:** Its main function is to manage, coordinate and optimize the use of financial and material resources to efficiently support the management and continuity of the service.
- **Legal:** Its main function is to provide specialized and timely legal advice, as well as to manage timely responses to the legal proceedings of the System.
- **Communication:** Its main function is to design relationship strategies towards the environment (including the entities of the third ring), establishing communication channels with the population and strengthening the institutional image, by launching campaigns and dissemination activities, among other actions communications. (See Chapter IX of this Guide).
- **Strategic and Operational Planning:** Its main function is to design and monitor the execution of development plans to achieve the objectives of service reinforcement, growth, and continuity assurance. (See Chapter II of this Guide).
- **Project Management:** Its main function is to design, execute and supervise the plans, programs and projects that support the achievement of the strategies described in the institutional plan.

The organizational structure must be shown in an organizational chart, considering the regulatory 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 must be supported by the identification and formalization of processes which may be classified as critical or support.

Likewise, when setting up functional areas, it may also be pertinent to define the technical capabilities required by each of them. This would 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:

- Infrastructure/technological architecture
- Information architecture
- Physical infrastructure and equipment

3.3.1 Infrastructure/technological architecture

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

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

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

The standards of these organizations complement each other. The choice will depend on the design of the System and its expectations, for example, around hardwired telephone, cellular, radio, convergent systems, broadcast technologies and the Internet.

The technological ecosystem of an emergency and security assistance and response center 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 service, file services, network services, database services and application services, among others.

Additionally, regarding database servers, it is recommended to have the following technical features:

- High availability (CLUSTER)
 - Database replication
 - Storage according to operational systems
 - Tool for data mining, analysis, and visualization
 - Search and report tool
 - On-line analytical processing tool (OLAP)
 - Management Information Tool (*Executive Information System*, EIS)
 - Decision Support Systems tool (DSS)
- b. Highly available infrastructure, based on the existence of redundant systems, matrixes, network, and power sources; automatic transfer switch; networking and connectivity equipment, among others.
 - c. Radio communication system between the areas and entities linked to the response. The radio communication network would have to be digital and have certain features such as data encryption. The network scalability and its interoperability with other existing communication systems would allow offering greater 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 the generation of token, code, and registration number

- Telephone number identification system (IP identification)
- Geographic information system (GIS)
- Automatic Vehicle Location (AVL)
- Computer-Aided dispatch system (CAD)
- Cameras for personal use or personal video surveillance to monitor what is happening on the ground
- Priority Dispatch System M*P*F (PDS)
- Private Automatic Branch Exchange PABX or automatic private central (routing, bypass, 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 centers (PSAP) and Primary Response Vehicle (PRV) or Ambulance y Advanced Life Support.
- Status report of available units/PRVs
- Action Taken Report (ATR)
- Video surveillance image analysis and monitoring system
- Alert System
- Video *wall* solution

e. Internet access, website, web services

3.3.2 Information architecture

One of the most important elements for an information architecture adapted to the needs of the Public Safety Answering Centers is that its design responds to information needs, which can be operational, strategic, public policy and service quality management related.

The aspects that make up this architecture must be linked to the processes and stages directly related to the answering and response of emergencies, as well as to the controls and indicators established to monitor and evaluate service provided, operation and performance in the six basic operational tasks (Stages 1 and 2), as well as the goals and objectives established in the strategic plan.

Depending on the functions model of the emergency and security system, the information architecture must be aligned with and provide support to the six basic operational tasks, facilitating the recording of data and information and communication across the board, from the beginning to the end of the event.

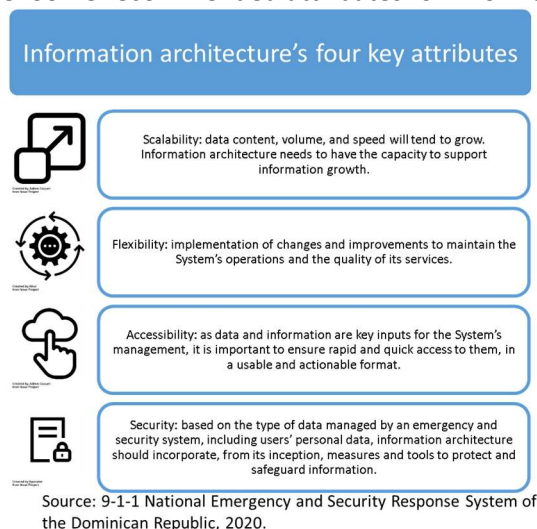
In general, when designing information architecture, the following aspects must be considered:

- The uses that will be given to the information (what for?), what type of information is required, in what format, for whom and at what time (is it collected and delivered?).

- The definition of typologies, classifications, categories, tags, and keywords to structure, organize and match the information, to facilitate its search and retrieval.
- The generation of a common and standardized vocabulary.
- The pathways, channels or means through which the service center will receive emergency alerts: call, video surveillance, panic button, mobile application, text messaging, among others. If one or more platforms interact at the reception of the emergency, deciding upon information storage, organization and structure must be different according to each case.
- The mechanism for recording emergency alerts.
- The feedback mechanism between field units and the response center.
- The forms for the information capture, trying to find a balance between the capture time and the information requirements.
- The means for information input, trying to find a balance between input time and information requirements.
- The reports and data visualization tools that will be generated to provide feedback on the operations of the center.
- Sufficient space to store and access the data and information captured

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

Figure 18: Some recommended attributes for information architecture



3.3.2.1 Incident typology

To guarantee adequate answering and response to emergency events, it is necessary to establish an incident typology in the information architecture, with unique and mutually exclusive categories, clearly defined, covering all possible areas, and being consistent with existing typologies.

Furthermore, it would also be necessary to establish what will be considered as an “incident” for operational purposes and its relationship with the emergency typology. 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 operations 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 give as a result the type of routing and dispatch, with the possibility of adding other agencies in the response.

As the emergency answering and response 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 made to standards and concepts, or to 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. As an example, some of these possible general categories are presented as follows:

- **Crimes and public security incidents:** These are events that endanger people's lives and/or property. For example, property thefts, fights, domestic violence, gender violence, child abuse, property, and assets damage, among others.
- **Health care incidents:** These are events that immediately endanger the life and physical integrity of people. For example, hemorrhages, knives and firearm wounds, fractures, poisoning, heart attacks and respiratory distress, among others.
- **Incidents of mental health care:** These are events in which the person shows risky behaviors, including suicide attempts, behavior alteration due to substance abuse, depression, mental disorders, and illnesses, among others.
- **Disasters:** These are magnitude events that affect large territorial areas, and several response institutions intervene during prolonged response periods. For example, floods, forest fires, fuel spills, tsunamis, hurricanes, earthquakes, and landslides, among others.
- **Accidents and crises:** These are focused events in which one or more response agencies intervene during prolonged response periods. For example, explosions, fires, and people rescue, among others
- **Impacts on national and/or State security:** These are events linked to the alteration of public order, which could threaten the integrity of the nation, endangering the continuity of its national interests and objectives. For example, terrorist attacks
- **Scheduled events:** These are events that are already known in advance to occur (for example, the blowing up 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 emergency management information architecture, it is essential to categorize the channels to receive requests, calls and reports from users, generate alerts and establish communication mechanisms with the population.

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

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

3.3.2.3 Call typology

Taking into account the massive number of telephone contacts that public safety answering points usually receive, the information architecture would have to incorporate a classification of the calls, each one with its respective definitions. Likewise, it would also need a prioritization mechanism and a set of predefined courses of action or action protocols to react and respond to emergencies.

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

- 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, or others that could arise according to the context of each country:

Table 19: Classification of appropriate calls

| Classification | Descriptions |
|--------------------------------|--|
| Emergency | Event that can endanger the life, safety, or integrity of natural or legal persons, or property, and that requires immediate assistance. |
| Urgency | Circumstance or event that requires immediate attention, but is not an emergency, and does not represent immediate or imminent danger. |
| Complaint | Notification that a crime or infraction is being committed. |
| Services and assistance | Calls to request assistance that require the presence of a response unit. |
| Consultation | Calls to request information on the services offered or inquiries on specific issues handled by the emergency answering and response system. |

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

Additionally, appropriate calls from emergencies could be of different types, depending on the type of incidents already presented:

- Crimes, violence, and public/citizen security
- Health
- Mental health
- Disasters
- Casualties/crisis
- National security
- Scheduled events

3.3.2.4 Typology of prioritization levels

Another fundamental tool would be to have a scale to prioritize the requests, calls and reports received. Along with the example on Table 1, a prioritization scale. could be as follows:

Table 20: Prioritization Scheme

| Classification | Prioritization |
|-------------------------|----------------|
| Emergency | 1 |
| Urgency | 2 |
| Complaints | 3 |
| Services and assistance | 4 |
| Consultation | 5 |

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

- **Level or Prioritization 1:** It is any type of situation or event in which there is an imminent risk to the integrity of people or their property and/or damage to the population or industry, therefore requires immediate attention.

Requests, reports, and calls that alert this type of situation are classified as emergency and shall be managed without delay, immediately activating the most appropriate response resource. They are usually classified as “high priority” or “immediate attention” and are sometimes displayed in red.

Examples of emergency situations 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 Prioritization 2:** It is any type of situation or event without imminent risk but that could affect the integrity of people or their property, the population, or the industry but that, nevertheless, requires response or attention as soon as possible.

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

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

- **Level or Priority 3:** Concerning any type of situation or event in which there is an urgency of “low priority” since no risk is identified for people or their property, nor impact on the population or industry. Therefore, they do not require immediate attention. These will be dealt with when Level or Priority 1 and Level or Priority 2 are closed, when response units are available.

They are usually labeled as “low priority” or “non-urgent response” and displayed in yellow.

Examples of this type of Level 3 situations would be: falling trees and falling fences, among others.

- **Level or Priority 4:** Concerning any type of situation or event that does not present an urgency but may or may not require a resource for its resolution; or it could be recorded as useful information provided.

These events must receive response 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 must be relegated until the end, and after a response has been provided to the previous levels.

In addition to a number scale to indicate the order of prioritization and qualitative indicators, the categorization could also be accompanied by a traffic light.

Each of these levels or priorities could be the subject of an internal subscale.

3.3.2.5 Inappropriate calls

Inappropriate calls lead to a misuse of the System's resources. Even when they do not give rise to an emergency response, urgency, complaint, services and assistance or consultation, it would be advisable to incorporate a typology and predefined courses of action, as part of the information architecture. This standardized treatment of inappropriate calls would facilitate their subsequent analysis, identification of patterns of misuse of the service, and design of possible solutions.

Below is an example of a typology scale for inappropriate calls with possible categories to consider:

- **False emergency call:** Calls to report fictitious emergency situations, which cause the response units to be displaced.
- **Abandoned call:** When someone calls the call center and hangs up before the call has been served.
- **Hung-up call:** When someone calls the call center maliciously or accidentally, and the call is interrupted after being answered by the operator.
- **Canceled call:** Call that is terminated because the operator or the caller hangs up, or due to some system failure.
- **Wrong call:** Call that is made to the call center by mistake, or unintentionally.
- **Prank call:** obscene, morbid, or insulting calls, made for entertainment or fun.

Initially, the following calls could be considered as inappropriate:

- **Canceled call:** Call that is terminated because the operator or the caller hangs up, or due to some system failure.
- **Non-emergency call:** A call wherein a situation that may be classified as an emergency is not described, which may be important or urgent, but must be processed through other response resources.
- **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 directly.

Such calls, however, should be given special treatment to rule out the possibility of them being appropriate calls. For such purpose, the action protocols set forth in this regard are essential.

3.3.2.6 Recording incident information

As part of the information architecture, it would be necessary to define the data to be recorded into the system for each request, call or incident report, from the moment of reception to the closing of the case. The determination of which inputs to collect would have to address the information needed for an adequate provision of the service. Additionally, it could also respond to the need to generate more aggregate data to evaluate the operation and quality of the service provided by the System.

There are at least four questions that could guide this important step in information architecture design:

- What data/information to input, what data/information could be extracted/exported from other databases.
- Time/s to input, extract/export, consolidate and combine the data.
- How to input, using predetermined protocols and templates to standardize both the data that is collected, and the methodology applied to do so.
- Where to store, how to back up and protect data and information. It is recommended, for an efficient information management, a computer architecture that includes an exclusive and centralized repository with a single database engine.

3.3.2.7 Interoperable and related databases

Interoperability refers to the functionality of information systems to exchange data or prior history of a different nature to facilitate usage. An integration that allows for interoperability of databases is key for a more effective, efficient, and timely use of information, having a positive impact on the operation and the quality of the service provided.

In an emergency and security system, several databases would have to be created, linked to requests, calls and emergency reports, linked to unit dispatch and assistance provided, to video surveillance, and to other potential services provided. These databases would contain information on attributes of both, the emergencies, and the people, whether there is an integrated platform or multiple platforms for responding to emergencies, it would have to show where and how these systems could communicate with each other and exchange, store and safeguard the information.

Database interoperability and information integration shall be governed by the data protection guidelines.

3.3.2.8 Data processing, analysis, and visualization

In addition to the data and indicators produced by the structure designed, and the databases developed for their input, use and integration, it would be necessary to have a tool for data processing, analysis, and visualization at the different operating levels of the System (operational, tactical, and strategic).

Below, we set forth at least four dimensions that must be defined to configure a system for data and statistics processing, analysis, and visualization:

- **Data type:** structured, unstructured
- **Analysis focus:** reports, key performance indicators (KPI), trend analysis, patterns, correlations, models
- **Analysis type:** retrospective, descriptive, predictive, prescriptive
- **Analysis process:** static, comparative, explorative, experimental

3.3.2.9 Generation and use of information

The type of information that would be available within the emergency and security answering and response centers would largely depend, on the way the information architecture is configured, including the different types of incidents, requests, calls and reports, the categorizations and classifications, the input and storage of information, the technical standards for the integration of databases and the system's interoperability. Therefore, the information architecture must be designed based on the types of information required and the uses given to such information.

One of the most frequent uses of information would take place immediately, on the field of operations, to guide, in real time, the response and service provided in an emergency.

Later, it could also be useful to monitor and evaluate the operation of the emergency and security system, and the quality of the services provided. Based on identified deviations or deficiencies, it would be useful to prioritize intervening areas and to inform the design of measures to continuously improve the system.

Likewise, it would be useful, in its most aggregated form, to feed and support the strategic planning process, as well as to account for the progress made in relation to the established objectives and goals.

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

- For pre-judicial instances, criminal investigations and criminal proceedings (see Chapter VII of this Guide); and,
- For the design, monitoring and evaluation of programs and public policies (see Chapter VII of this Guide).

3.3.2.10 Reporting System

To define the types of reports that the emergency and security system will produce, one 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, division responsible, place of storage and access, among other elements.

The reports could provide information on the operation of the System regarding the answering and response 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 or administration, processes, and results, among others.

Depending on the information that the System generates, the available tools for data processing, analysis and visualization, the technical skills of the personnel, and the uses that will be given to the information, different types of reports could be defined. As an example, at least five types of reports could be considered:

- Performance human talent development report
- Management report (results and productivity)

- Response report (linked to the services provided)
- Financial-administrative report
- Project report

Depending on the technological possibilities, it would be necessary to have platforms for automated report generation and sending. Other useful functionalities to consider when designing a reporting system would be:

- Common repository
- Parameters and search engine: by means of specifying keywords or combinations, to find reports quickly
- Standardization of the format of charts, tables, graphs and other instruments for the presentation and visualization of data
- Options to send or download in various formats
- Real-time updates
- Visualization of data on a dashboard or control panel environment

3.3.2.11 Document management system

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

In order to manage these documents effectively and efficiently, it would be necessary to define a typology, 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 transparency and access to public information, and the needs of the emergency and security system.

The Functional division in charge of document management could also be in charge of standardizing the processes of 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 the guidelines for the production of internal documents, including format, identification (numbering/coding), corresponding metadata and the level of confidentiality, among other elements. The creation could also be accompanied by a proposal regarding the uses given to the document.
- **Approval:** define the steps for document review and validation, for example, who participates, what are the deadlines, who authorizes the final version of the document, who is in charge of giving it authorized status. All the documentation authorized for internal use would have to be made available to the personnel and, depending on the type of material, disseminated.
- **Storage:** Establish a format for saving documents and methodology for archiving. Also define the treatment of previous versions of documents and 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 level of confidentiality, among other aspects.

3.3.2.12 Information Management functional division

Like any functional division, in addition to defining its functions, it would be necessary to establish its scope and position 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**, it would also involve the communications management of relations with the environment, considering accountability and transparency

These scopes are not mutually exclusive.

Regarding the positioning within the structure and the organizational chart of an emergency and security system, it could be thought of as an independent division or as part of another functional division containing it.

3.3.3 Physical infrastructure and equipment

The construction and design of the physical spaces that comprise a public safety answering center shall 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; OSHA 18001- Occupational Safety and Health Administration. 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, that contribute to personnel health and productivity. In order to create a healthy and comfortable working environment, it would also be important to think of ways to absorb and reduce noise levels, and to install an air conditioning system.

The physical space could be comprised by 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 areas, such as: canteen area, rest area, maintenance area, meeting rooms and contingency or crisis rooms.

The physical space would have to be properly marked and equipped to face emergency situations. Likewise, alternative workspaces should also be considered in case the facilities cannot be used.

Other important elements, to be taken into account in relation to 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 view the concurrence of units, according to type of response, entity in charge of the service, geographic area, among other characteristics defined in the functions model on reception, administration, response coordination and dispatch-closure.

CHAPTER IV: INTEGRAL QUALITY MANAGEMENT

Introduction

After planning and design, the emergency and security system would have to be commissioned. This chapter focuses on how to manage 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, ongoing, 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 coordinated and liaison institutions, and (iv) risk management.

Additionally, in this Chapter, at least two key tools are also introduced to conduct quality management of the processes, services and activities conducted by an emergency and security system. The first would entail identifying and mapping processes and formalizing those considered critical for the operation and continuity of operations of the System. Compliance with these protocols by personnel would allow the desired quality levels to be maintained. Additionally, the contrast between these protocols and the actions undertaken would allow identification of improvement opportunities.

The second tool would be related to definition and calculation of a series of indicators to monitor and measure the operation of the System in general, as well as for each of its functional areas and the actions undertaken, particularly regarding attention and response to emergencies.

Both elements would contribute to reduce discretion and subjectivity margins in the operation and management of the emergency and security system. Additionally, they would add professionalism and impartiality which are essential elements of all the functions and operational and administrative activities of this type of Systems. Furthermore, they would provide clear, common, and uniform parameters and references for all personnel.

4.1 Quality management model

A quality management model is closely linked to the governance of the System, insofar as it involves everything, from measuring, monitoring, evaluating, and reviewing the quality of the service provision, down to the introduction of 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 operation of the System, contributing 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 the levels of operation of a System (strategic, tactical, and operational), with special emphasis placed on the provision of emergency services and security.

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

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

There are different models of quality management. The model adopted would have to be based on the functions model chosen by the emergency and security system, taking into account each critical stage in the service chain. Additionally, it would be convenient for it to be aligned with the most influential international standards on the subject, such as the ISO 9000² standards or the EFQM Excellence Model (*European Foundation Quality Management*)³.

Despite the diversity of quality management models available, four essential and minimal approaches that could be considered are the following:

i. Monitoring at each stage of the service delivery chain

A first approach is based on the measurement and control of quality on each stage, process, or area of activity of the provision of the service, for example: the reception of the service request, the dispatch or assignment of units, among others.

Monitoring would have to be done by comparing general operation and the actions conducted with the provisions of specific regulations, protocols, standards, and guidelines. Additionally, it could be based on the definition and calculation of indicators, as well as monitoring and measuring results obtained, taking pre-set objectives and goals as a point of reference.

When doing this first type of monitoring, it is recommended to take samples from all areas, all types of events, all people and all entities providing the service at different levels. This sampling would have to be random and representative, by virtue of the volume of events served by an emergency and security system. This would contribute to the objectivity of the exercise and would also respond 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.

From the application of these monitoring instruments, if there are divergences, gaps or deviations between practice and the regulations, protocols, standards, and guidelines established, or in relation to the goals and objectives set, it would be necessary to proceed to the elaboration and implementation of action plans. These would present a set of recommendations to overcome the divergences, 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 divergences, gaps or deviations identified, could be published on the website of the emergency and security system (see Chapter X of this Guide).

² 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.

³ The EFQM Model consists of 7 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 of 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

ii. User feedback

This second approach entails 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 complaint and suggestion boxes (face-to-face or virtual), among others.

iii. Feedback and follow-up to articulated institutions

The third approach would entail the creation of instances of intra- and inter-institutional coordination, including: follow-up meetings, technical and exchange tables, among others; and the incorporation of tools or techniques such as, for example, analysis after the action or ex-post served emergencies, to:

- Provide feedback to articulated entities about operations results, based on established monitoring and consultation mechanisms, statistical reports and indicators, trend analysis, post-action reports, among other information.
- Identify situations that may be negatively or positively affecting the operation.
- Regarding the former, take corrective action in a timely manner and consider what could be documented as a lesson learned to share with the rest of the personnel, to avoid repeated mistakes.
- Regarding the latter, consider what could be documented as a promising practice or good practice to share with the rest of the staff and promote its dissemination and adoption across the board within the System.

These three approaches would be comprised by the following 5 steps:

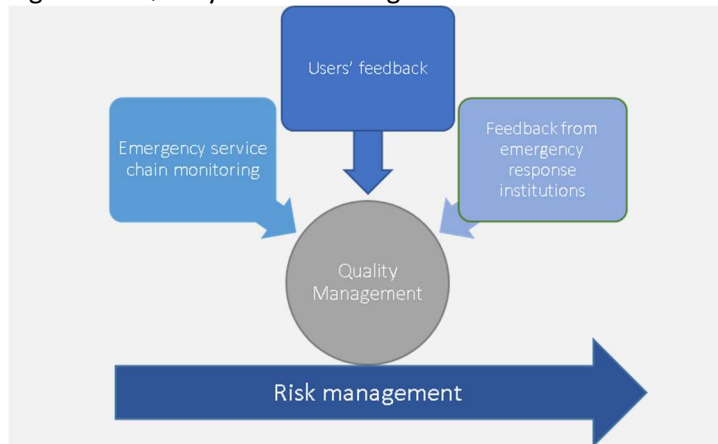
- a. Collection of data and information.
- b. Data and information analysis to identify possible improvements.
- c. Development of plans to address the areas of opportunity identified. These plans must be prioritized and aligned with strategic goals and objectives.
- d. Establishment of a framework for the implementation of improvement projects.
 - Define mechanisms for measuring and monitoring the progress of these plans.
 - Analyze factual and budgetary feasibility of improvement plans.
- e. Implementation of the activities defined on the improvement plans, and implementation of measurement and monitoring mechanisms.

iv. Risk management

A fourth approach focuses on risk management. Its deployment starts from the identification and survey of unexpected and foreseeable situations that could harm the functioning of the System, seeking to identify probability of occurrence, level of impact and existing vulnerabilities.

Based on this diagnosis, 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: Quality Service Management



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

4.2 Standardization of processes and protocol application

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

In order to prepare this map or process schematic, at least five steps would have to be conducted, taking into account: a) functional and performance requirements, and b) applicable legal and regulatory requirements:

- i. Describe and characterize processes, and identify critical processes
- ii. Standardize and formalize processes, particularly those that were identified as critical
- iii. Develop manuals/procedural guides and protocols of action
- iv. Define process monitoring indicators
- v. Set quality parameters and standards

These five steps, in turn:

- Would serve as a guide and reference for process execution
- Would facilitate personnel training (see Chapter VI of this Guide)
- Would help to verify or verify the suitability of the activities carried out by the staff, providing objective parameters for their performance evaluation (see Chapter VI of this Guide).
- Would enable objective monitoring and evaluation of the system's operation and its processes, to maintain continuous improvement.

Among the most important processes for the operation of an emergency and security system are the following seven:

- i. Receiving requests for assistance and identification of the situation
- ii. Information collection, classification, and prioritization
- iii. Incident creation and dissemination/communication of information

- iv. Dispatch/allotment to response unit(s)
- v. Coordination, communications monitoring, and response unit(s) follow-up, at the place or site of the event
- vi. Operational closure of the case
- vii. Retrospective or post-mortem evaluation of all of the above

Each of these processes or stages of service delivery would merit standardization and formalization to ensure an efficient, timely and quality operation of the System

4.3 Setting and measuring indicators

This section addresses the second tool of a quality management model, relating to the establishment and measurement of a series of indicators to monitor and evaluate the functioning of the System in general, its functional areas and actions undertaken, particularly regarding to attention and response to emergencies. 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 data sheet. Indicators would have to be quantifiable and expressed in a unit of measure, which may include percentages, indexes, or ratios, among others.

The data sheet for each indicator must include the following fields:

- Indicator name
- Description/purpose of the indicator
- Goal, objective, and strategic axis to which the indicator would be associated
- Type of indicator
- Formula for calculating the indicator
- The data that would be needed to calculate it, the sources where that data would be available, and whom such data source depends on
- Measurement unit and allotted categories
- Ranks and scale
- Measuring frequency
- Baseline
- Responsible person for measuring and monitoring (or if the calculation is automated)
- Where would that indicator 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 visualized through a dashboard. Its definition must have been made, preferably, when designing the information architecture of the system (see Chapter III of this Guide). Furthermore, calculation, safeguarding and storage must be supported by technological architecture configured for the operation of the emergency and security service.

4.3.1 Activity Indicators

Indicators that measure the number of requests, calls or distress reports received by the emergency and security service. They have an informative value in assessing resource usage and allotment and would also allow comparisons between centers, other services, or other time periods. As an example:

- 1) Total number of requests, calls, or reports received
- 2) Number of requests, calls, or reports received per answering and response channel
- 3) Number of requests, calls, or reports by incident type
- 4) Number of requests, calls, or reports per location
- 5) Number of cases served (service level)
- 6) Number of operators available on requests, calls, or reports received
- 7) Number of dispatches made on requests, calls or, reports received
- 8) Accuracy of geolocation services for emergency requests, calls and reports⁴

4.3.2 Process Indicators

These indicators would help to verify the availability of the service, particularly regarding emergency answering and response, and could be grouped by process type. As an example:

- 1) Average time of attention to the request, call or report
- 2) Percentage of calls out of the established time, according to type and characteristics of the request, call or report
- 3) Time for processing and sending the report to dispatch
- 4) Average dispatch time of the 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 In Mexico, the measurement of the accuracy of geolocation delivered by telephone routers to the STREET, is done based on the security and justice collaboration guidelines issued by the Federal Telecommunications Institute (IFT). Based on clearly established parameters and regions, such entity performs the measurements on an annual basis. If the minimum required parameters are not met, operators may be sanctioned.

4.3.3 Evaluation indicators

These are used to evaluate the service provided on a monthly, quarterly, biannually or on an annual basis, and to identify areas of opportunity in responses to requests, calls or distress reports received by the System. As an example:

- 1) Percentage of incidents classified correctly
- 2) Percentage of incidents dispatched
- 3) Percentage of incidents served
- 4) Average time for call processing, according to type and characteristics
- 5) Percentage of time for units' dispatch (from the moment the call is received and until the unit is dispatched)
- 6) Percentage of deployment time (from the moment the dispatcher informs the articulated service and until the unit leaves the facility to go to the emergency site)
- 7) Percentage of response time (from the moment the request call, or report is received and until the arrival of the unit to emergency site)
- 8) Percentage of incidents fulfilled in the time set as parameter
- 9) Percentage of requests, calls, and reports that complied with the protocols

4.3.4 Management indicators

These indicators measure the operation of the service from the point of view of the planning and management of the System and are grouped by functional area. Some examples are presented below:

4.3.4.1 Human Resources

- 1) Number of certified operators
- 2) Average age of operations personnel
- 3) Number of positions available
- 4) Number of personnel in training
- 5) Number of operations personnel about to retire and forecast of the number of people who would have to be replaced
- 6) Percentage of absenteeism or punctuality
- 7) Occupational atmosphere indicators which could be formulated based on the perceptions of the personnel regarding:
 - Relationships between colleagues
 - Physical working conditions
 - Compensation and recognition
 - Career development opportunities

- Equal opportunities
- Integration of people with disabilities, according to the activity to be performed

4.3.4.2 Operations

- 1) Turnover (voluntary and involuntary) of operators
- 2) Operational capacity (resource availability), per shift, per operator
- 3) Average or rate of requests, calls and relief reports fulfilled by each System operator
- 4) Number of cameras available or in operation
- 5) Number of cameras monitored by each person (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 budget executed
- 2) Percentage of budget assigned by functional division
- 3) Level of debt as an averaged percentage of assigned resources

CHAPTER V: CALL AND INCIDENT MANAGEMENT

Introduction

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

- i. Receiving requests, reports, and calls for assistance and identification of the situation
- ii. Information collection and typification according to incident, risk, and priority
- iii. Event creation and documentation (response sheet)
- iv. Dissemination/communication of information and allotment of the unit
- v. Unit arrival
- vi. Documentation and operational closure of the event

This approach arises from the need to formalize these six operational tasks in a series of clearly defined steps and procedures to guide the actions of the operations personnel in an objective, homogeneous and institutionalized manner. Therefore, throughout this Chapter, stages are identified as well as considerations and criteria are presented to be taken into account in order to standardize the conduction of these six operational tasks.

The Chapter also stresses the importance of standardizing emergency answering and response in several protocols, from three perspectives:

- i. Personnel: as a resource to train operational personnel, guide their actions and evaluate their performance
- ii. Management: as a parameter to compare between what has been done and what is expected
- iii. Quality: as a tool to identify deviations from what has been established and introduce improvements

5.1 Receiving requests, calls and reports

The management of requests, calls and distress reports must be supported by technologies to facilitate data input and access, and other functionalities such as:

- Visualization of guidelines to guide calls
- The activation of a form to fill out, in line with classification and prioritization rules, and a typology of incidents to select from
- Geolocation, addresses, accesses, 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 must aim at minimizing opportunities to introduce biases and errors during the process of recording person and incident information in the response sheet.

Standardization and formalization of 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 answering, response and closure more objective and consistent.

The operator or recipient of a request for help, telephone call or report would have to have an automated system that generates a registration code, and that provides indications for filling in the response file with pre-established fields and selection options.

Additionally, the system would have to recognize and display on the screen, the basic information of 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 the regulatory framework that each State has established in the field of telecommunications, including hard line and mobile telephone companies.

If the system cannot recognize the three fields listed above, the operator would have to ask the corresponding questions to input the basic information about the person and their location. Likewise, the person would also have to fill in the information based on pre-established fields on Computer Aided Dispatch (CAD).

Another important step would be to verify and complete the information on the response sheet, from the logs saved in the system's databases. It is from this computer support that the report will be supplemented with the information available in its databases, including: the number of calls received from that telephone number or IP address and the types of calls (appropriate or inappropriate) made, among others.

Each Center would have to define answering and response protocols based on the type of access 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 will allow to conduct communication with the user in a standardized way, collect information that might be necessary for emergency answering and to respond to the different types of emergencies in a timely manner and with the appropriate units and resources, depending on their complexity and prioritization.

Every call reception center would have the ability to process an atypical volume of calls that exceed operational capacity, and that could significantly affect emergency answering and response. To this end, it is recommended to consider the following mitigation measures, subject to the availability of a contingency budget to 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 centers

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 first would involve relying on video operators, specially trained to carry out the monitoring and detection of emergency situations. The second 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 protocols.

5.2 Risk classification and prioritization

In Chapter III, in the section regarding the information architecture of the 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 to select from.

It would also require a typology of risk levels to prioritize attention. Chapter III also introduced an example of possible levels of prioritization.

5.3 General guidelines for drawing protocols

Given the centrality of the reception and treatment of emergency calls, requests, and reports, and from a quality approach, it would be necessary to standardize the procedure in a protocol of action that allows for consistency, continuity and efficiency for the service provided.

This formalization, operating within the framework of a series of indicators, controls, and tools to measure the quality of service provided, would allow the identification of deficiencies and weaknesses, introduce the necessary changes and updates, and support the continuous improvement of the System. In addition, it could facilitate the identification of aspects where personnel training and specialization would need to be strengthened.

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

Phase I. Call Reception

- Specify the number of times the phone shall rang.
- Standardized greeting, express it in a clear, cordial way, with pauses. Specify the number of times that greeting would have to be repeated.
- Set whether the call is in another language and identify the language. If so, indicate with some preset code and apply the specific protocol of action for these cases (see below).
- Identify/evaluate whether the call is appropriate/inappropriate from several preset criteria/questions.
- If so, ask directions and inquire about the location of the incident, including some geographical reference, relying on geolocation, and making use of guide questions to facilitate its location. Ask for the user's name, and if not provided, use any code or acronym to record the lack of data. As an example, "NN" could be used. The operator may briefly explain to the user the importance of having the information that is being requested.
- If it is an appropriate/valid call but the caller is not providing answers, provide him assistance, through closed questions, so that he can do so. Assess the background or context of the situation.
- Pre-check the incident and complete the file generated by the emergency answering and response system.
- Check nearby camera(s) to complete and supplement the understanding of the situation being reported, if available.

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

This protocol shall take into account different situations in which the caller or whoever reports an emergency might find himself, including:

- Inability to speak
- Danger or high-risk situation
- Any kind of disability of the user

Phase II: Call Processing

The protocol at this stage 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 that it entails. The system would have to provide the possibility of re-prioritizing the incident and, so, changing the level of risk.
- Validation of additional routing and data input depending on the type of incident, which might be useful to the personnel who will be responding to the emergency on the field.

Phase III: Incident response

From the operation model of the System, information about the incident and the user would have to be sent to the dispatch division or to the articulated institutions and, if applicable, it would be appropriate to establish the steps to complete for further coordination with connected institutions.

Formalization at this stage would have to set parameters for a differentiated schematic of attention, depending on the type of incident and the special needs that the person reporting the emergency might have, among other elements.

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

- Activate the multi-dispatch tab in the CAD system to coordinate with various response institutions. An event in process would require inputting basic data and transferring communication to response institutions for online telephone support and, in tandem, activating dispatch.
- If this type of incident is evidenced by video surveillance cameras, in addition to activating the specific protocol, they could accompany the dispatch process and monitor the place of the emergency 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.

In cases of **gender-based violence, including risk of femicide**: The specific protocol of action might consider:

- Activating the multi-dispatch tab in the CAD system for coordination with several first-response institutions. Being a developing or ongoing event, the immediate coordination with the police and, if necessary, healthcare units would be necessary and adequate. At the CAD level, the

institutions in coordination that would have to be activated in such situations, could already be pre-programmed.

- If possible and necessary, psychological assistance shall be provided to the affected person by telephone or other available means, until the units arrive at the site of events.
- In the event of video surveillance cameras, and in accordance with each country's criminal code, images of the flagrant actions captured by such cameras could be forwarded to the judicial entity in charge of the investigation for possible prosecution.

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

- i. During the design of the information architecture
 - Determine the mental health illnesses that could happen during an emergency situation, including: suicide attempts, behavioral alterations resulting from the consumption of narcotics and psychotropic substances, shock from a critical incident or hazardous event, among others.
- ii. During the inquiry of the emergency call
 - Ask a series of pre-defined questions to determine the type of situation being dealt with.
 - If such is the case, apply general guidelines to placate the caller.
 - Activate the ordinary or multi-dispatch file, as appropriate.
- iii. During dispatch
 - Dispatch the appropriate units and resources.
 - Transfer telephone support and psychological first aid to the corresponding institution.
- iv. During post-closure
 - Deploy complementary post-emergency attention and response and follow-up actions with psychological support institutions.

In cases of **persons with disabilities**: The specific protocol of action might consider:

- Identifying the type and degree of disability.
- Providing care 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 be.
- Activate complementary post-emergency telephone and response actions with support institutions and with subsidiary actors, if applicable

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

In cases of a different language: The specific protocol of action might consider:

- Asking questions to identify the language the user is speaking.
- Contacting the person who could responsibly act as an interpreter in the answering and response to the emergency, from a predefined list of operators indicating their respective language skills or linking with an external interpreting service.
- Requesting support for the interpretation, following the established script.

- The incident sheet or report shall state the fact that the user spoke another language. This could be done, for example, with the use of a prefix or preset acronyms.

Phase IV: Closing the call

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

- Confirming location data provided for emergency answering and response.
- Providing a report number generated from the request or assistance.
- Ask 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 incidents, the special needs of people reporting an emergency and the different access channels available, including web applications, mobile applications, SMS service, voice messages, TTY devices and help 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 functions model adopted by the System, the operator would have to transfer or route the captured information.

There would be different types of possible transfers:

- Standard (normal) emergency:** The operator would have to transfer the report or response sheet 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 the operator selected.
- Emergency requiring joint action between two or more coordinated 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 transfer the information simultaneously to two or more first-response or support institutions for coordinated, on-the-field emergency care and response.
- Emergency in process:** In this case, the operator would transfer the "basic" information so that the first-response institution can provide telephone support to the caller, until the unit arrives at the emergency site.
- Hand dispatch:** These are emergencies assigned and communicated directly by means of a form, file or physical record that is hand-delivered to a person responsible for providing dispatch services. This type of dispatch would be possible when operators and dispatchers are in the same center.

For both the information in the response sheet and for its submission to dispatch services, the System would have to consider safeguarding mechanisms for possible contingencies and to avoid losses of

information. Subsequently, the sender could opt for filling out the record manually, or for using the re-send function to forward the information captured digitally once the contingency has been overcome.

5.5 Dispatch and monitoring of units

According to the functions model, the information architecture of the system and the characteristics of the dispatch system (CAD), the operator or dispatcher could have access to different functionalities to facilitate operations coordination with the institutions required for emergency answering and response. Some of the basic features that might be considered are:

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

Possibility to cancel/modify. The system would have to have the option to abort or modify the dispatch of units, in such cases where response operations personnel determine that such dispatch is not necessary or that it needs to be adjusted.

Possibility of escalation. The system would have to allow for the emergency answering and response to be scaled up, adding other necessary institutions once the risks and the complexity of the emergency on the field have been identified.

Other additional features to consider would be:

Location of the incident and deployment management of dispatched units. The system would have to allow the dispatcher to access the information captured by the operator and dispatch the nearest unit or resource that can 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 resource dispatch is required.
- Assign the available resource(s).
- Record the status of the resource (as an example: assigned, on the way, on site, processing, return, completed).
- Check the arrival of the resource(s).
- Feedback regarding the incident in the emergency answering and response system.
- 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 tab, depending on the information that was reported by the units that arrive at the emergency site, through call or video operators.

Permanent communication, support, and monitoring of units in the field. Dispatchers shall be able to interact with the operations personnel assigned to the reported emergency response and provide them with all the information necessary to provide proper care.

Support video surveillance cameras.⁵ The system would need to be able to leverage the video surveillance camera platform to provide the necessary support and monitor the units deployed on the field.

Depending on the type of cameras available to the emergency and security system, the video operator would have to have the possibility to:

- Check the operation of the cameras and be able to operate them.
- Monitor assigned cameras.
- Check if the camera has technological support elements (IP public address, 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 the case may be, identify the response institution(s) that would have to attend to the emergency and send the incident response sheet to the dispatcher, based on the established protocols. This flow would depend on the functions model adopted by the System, as well as, 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 answering and response on the field, and monitor and protect deployed personnel.

The system would have to be able to take advantage of the video surveillance camera platform to provide the necessary support and monitor the units deployed on the field.

Depending on the type of cameras that the emergency and security system may have, the video operator would have to have the possibility of:

5.6 Capturing, visualizing, and storing data

5.6.1 For the operation

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

The information and technology and architecture would play a key role in the ease of access and use of the forms fill out, as well the support tools available complete such process, in addition to everything related to the visualization 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 entered are:

- Username

⁵ Video surveillance camera networks could also play a deterrent role, focused on preventing the occurrence of offenses, anti-social behaviors and crimes. Additionally, they could also be an integral element 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, accordingly to the adopted functions model.

- 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 the emergency resources

5.6.2 For evaluation and continuous improvement

Timely and complete data entry from the reception of the assistance request or distress call to the closure of the incident is essential for service quality service management and continuous improvement purposes.

Then, based on the information architecture devised and the technological support of the System, it would be necessary to calculate and record, automatically, a series of indicators both during and after the emergency, based on preset quality controls.

Quality controls would have to go through the six critical tasks that make up the main process of any emergency answering and response care system. They could be carried out from the application of quality control templates or matrixes, which cover several predefined categories, criteria, and indicators. These arrays could be applied to assistance files, recorded audios, and operational activity logs.

If quality control cannot be performed on the universe of requests, calls and reports received or dispatches deployed by the emergency and security system, a representative sample could be calculated. The representativeness of the sample would have to contemplate the weight or incidence of each type of request, call and report received, including those appropriate and inappropriate. Regarding the quality control of dispatches, the sample would have to be representative of each type of emergency incident responded to, as well as the coordinated (or first-response) institutions and related institutions involved in the care provided.

As mentioned in Chapter IV, evaluation or control indicators shall allow 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 operations plan. Other tools mentioned in this Chapter were, concerning user feedback: satisfaction surveys, follow-up calls, focus groups, and complaint and suggestion mailboxes (face-to-face or virtual), among others. In addition, regarding coordinated and liaison institutions, among the feedback tools, were mentioned: methodologies or techniques for post-action analysis, post-emergency follow-up meetings and technical tables.

All this quantitative and qualitative information would have to facilitate the identification of deficiencies and weaknesses, to propose improvements in certain processes and protocols, introduce new standards, and strengthen training in certain aspects related to the gaps evidenced.

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

CHAPTER VI. HUMAN TALENT MANAGEMENT

Introduction

In the following sections of this Chapter, a series of guidelines will be provided on the five stages leading to good management of human talent, from the perspective of a public safety answering center.

The strategy to manage human talent in emergency and security systems should be directed towards 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 own demands, sustain the continuity of operations, and contribute to the fulfillment of the objectives and goals set out in the strategic plan.

People are the most important resource of any organization, particularly in a public safety answering center. Its work would be aimed at preserving people's lives in situations of high pressure and tension. Not everyone would be prepared to perform the critical tasks inherent to a public safety answering center, particularly those six basic operational tasks presented in Chapter III of this Guide. Several specific skills, abilities and knowledge would be needed for proper performance in a public safety answering center. Therefore, planning and management of human talent that encompasses attraction, induction, evaluation, training, and loyalty are vital.

6.1 Planning and management of human talent

Having characterized personnel as one of the main resources in any public safety answering center, it would be necessary to adopt a planning process that results in an institutional strategy to guide the management of this asset.

For the planning and promotion of human talent, the institutional strategic plan (see Chapter II of this Guide) and the objectives set in the short, medium, and long term should be taken as a basis. Based on these objectives, the human resources necessary to achieve them would have to be identified and, additionally, work models should be established as well as defining the main processes for human talent management. (Section 6.2 of this Chapter presents six possible main processes that characterize the functioning of this operational area).

Similarly, planning would have to look at training and expectations about the career path of the personnel, to strengthen their technical skills regarding changes, innovations and new challenges that may arise and/or project. In addition, investing in personnel in terms of their professional growth would serve as a loyalty mechanism, element of motivation, and incentive to strengthen the sense of commitment to the entity.

Likewise, as part of the planning process, the specific objectives that would be achieved through the implementation of the human talent management strategy resulting from that process would have to be defined. Some of these objectives could be:

- Attract and retain the best human talent with the skills required for the different jobs.
- 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 an adequate working environment.
- Encourage team spirit, bonds of trust and a sense of belonging.

- Prevent and prepare personnel against risks and possible setbacks that could affect institutional management and ensure maintenance and continuity of service.

Human talent planning would have to quantify and qualify the required personnel, depending on the functional division, projecting the quantity and type of resources that will be needed to meet the requirements of the personnel.

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 diagnosis of institutional capacities and the projection of demand for services. It is from this definition that one could model and know what kind of talent would need to be attracted and, at the same time, foresee what formative aspects would need to be developed or strengthened internally.

This process could be divided in two phases:

- a) Position analysis: is the collection of information related to the job through various techniques.
- b) Job Description: it is the process of reflecting, in writing, the objectives, main functions and profile of the job, product of the analysis previously carried out in the previous phase.

6.1.1 Job analysis

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

- Interviews:
 - With the occupant of the job
 - With the person responsible for overseeing the job
- Direct observation of the execution of the functions of the job
- Structured questionnaires to be completed by the occupant of the job
- Evaluations
- Logs
- Expert groups

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

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 centers, 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 one of the assigned responsibilities, obligations, and tasks.

There were various functions models, which were addressed in Chapter III of this Guide, specific profiles consistent with four essential operational functions of an emergency and security system would have to be considered: reception, administration, response coordination and dispatch, which usually result in essential roles such as:

- Call receiver (call taker)
- Video surveillance operator (video operator)
- Dispatcher (dispatcher)
- Supervisor/coordinator

In addition, for the configuration or profiling of jobs, please follow the guidelines presented in Chapter IV concerning the tasks associated with the six most important operations tasks for the operation of an emergency and security system:

- Receiving assistance and identification requests for the situation
- Information collection, classification, and prioritization
- Incident creation and derivation/communication of information
- Dispatch/ assignment of response unit/s
- Coordination, monitoring of communications and response unit(s) at the place or site of the event
- Operational closure of the case

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

- **Identification information.** Usually located at the top of the document. Presents general position data, including where would the entity be located: place and in hierarchy. It could provide the following information:
 - Code
 - Name of the job
 - Position within the entity
 - Administrative or operative unit
 - Role
 - Occupational group
 - Degree
 - Area
 - Source of the information with which the analysis of the position was prepared and 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.** It is a small introductory synthesis 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 to be occupied within the organizational hierarchy.
- **Position interface.** It would explain the relationship of the essential activities of the job in relation to internal and external users.
- **Obligations and responsibilities.** In this dimension, the following questions should be answered:
 - What is to be done in the position?
 - What is there to do?
 - How and with what tools is the work done?
 - Where does the job get done?

Answers to these questions should be entered in protocols that guide the occupiers of the positions regarding their obligations, responsibilities, or 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 part would clearly set out the necessary skills, experiences, and training to be required of the person to carry out the tasks associated with the position.
- **Area of knowledge.** It is the technical career of formal instruction that would be required of the person to take up the position.
- **Work experience required.** This is the level and type of experience that would be required to carry out the tasks associated with the job.
- **Training required for the position.** It defines the themes of the trainings and certifications linked to the job that the interested person would have to possess.
- **Technical capacities.** They are those that would refer to specific standards, linked to the correct performance of positions in a technical area or specific function.
- **Organizational capacities.** These are basic skills that people who aspire to join the entity would have to possess. They are composed of behavioral competencies such as orientation to quality, teamwork, interest in innovation, commitment to the values and ethical principles of the entity, among others.
- **Emotional skills.** Personality traits and set of capacities, abilities, and attitudes to process, understand, regulate, and express in an appropriate way the emotional phenomena and the stress levels related to the position.
- **Health conditions required for the position.** Specify if 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.

Competences could be understood as a set of knowledge, abilities and skills that allow the efficient performance of a certain job in the chain of services of a Center and, in this way, contribute to the achievement of the objectives and goals of the entity. They serve both to define the job profiles as well as to establish the parameters on which to evaluate the performance of the staff.

Competences could be regarded as dynamic. They can be acquired and developed throughout a person's professional career. In addition to the technical and organizational competences already mentioned above, psychological and management skills, among others, could also be considered.

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

6.2 Functional division for human talent management

The planning and management of human talent would have to fall into a specific functional area. This area would be in charge of implementing and operationalizing the institutional policy guidelines for such purposes, set forth in a plan, as a product of a planning process.

The functional area would have the mission of supplying the entity with the best possible resource for each job, 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 answer and response center is critical for the smooth function of its operations, for maintaining efficiency and quality of its services, and for the achievement of 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
- Departure

All these processes would have to be formalized. They would also have to be guided by the principle of non-discrimination⁶ and a gender approach, and in line with each country's policy framework and labor and trade union policies in each country.

6.3 Recruitment and selection of human talent

After the diagnosis, analysis, and definition of the profile of the jobs has been completed, the recruitment and selection process of the appropriate personnel would be carried out.

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

⁶ Non-discrimination based on race, origin, religion, disability, gender, sexual orientation and/or political affiliation.

- a) **Need:** as a first action, it would be necessary to identify the area in which staff are required to be incorporated or strengthened, as well as to define the skills profile to meet the requirements of the area in question. At this stage, the availability of economic resources and the projection of demand for services would have to be analyzed.
- b) **Recruitment:** this is the phase where the recruitment of candidates would begin through different sources and channels, according to the defined profile. This would indicate the desired technical skills, competencies, training, and experience for the position. Additionally, it would also specify the benefits and compensation that the person interested in the position might expect.

It would be useful 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.

The call, depending on the positions or jobs to be filled, could be both internal and external. These two fronts are not mutually exclusive. The means to make the call are multiple, including media and social media, the website of the entity itself, job search platforms, universities with job placement service for its graduates, among others.

- c) **Selection and Evaluation:** phase in which the qualifications of candidates would be verified, through the application of tests, interviews, and validation of references. It would be useful for this phase to have predefined criteria for technical admissibility.

At this stage, we would initiate the process of evaluating candidates based on the applicants' resume, any other support material that had been requested, and according to the requirements established for the position.

To ensure the transparency of the process, it would be necessary to verify compliance with technical and administrative requirements for the application and validate the history accredited by external entities, including law enforcement and police, 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 the competencies identified. To do this, it would be recommended to carry out at least three types of tests:

- **Technical tests:** these are those that seek to validate the candidate's ability in skill competencies focused on the position. For example, a typing, programming, or language test.
- **Competency testing:** aimed at assessing the skills associated with efficient and effective performance in a position.
- **Psychometric personality tests:** they are applied to reveal personality traits in accordance with the obligations, responsibilities and functions of the job, and the levels of stress and emotional burden that the person must face.

Basic and/or specialized capability assessments and psychometric tests could also be performed. It is at this stage that, in addition to, a series of interviews with the shortlisted candidates could be conducted, either by one or more interviewers.

Also, besides measuring and determining job-specific qualifications, competencies, knowledge, prior training, and experience, it would be essential to be able to identify inclinations and attitude for public service early among candidates.

- d) **Selection:** this is the final phase of the process where from the group of shortlisted candidates, the candidate who best meets the requested requirements and presents the best applications to perform the functions inherent in the position would have to be selected.
- e) **Recruitment:** if accepted, the declaration of selection of the applicant would be published, and the contract would be made in accordance with the current legal framework of each country.

In addition, hiring may be preceded by medical examinations, both physical and mental, and consultation about criminal history. Moreover, within the framework of the occupational safety and health policy established by the entity, these reviews may be repeated on a certain frequency, depending on the obligations, responsibilities, and workload of officials in an emergency answering and response and response center.

6.4 Induction of human talent

Any official who joins the entity would have to go through an induction process. The induction would allow the person who enters the entity, to become familiar with it, with its mission and vision statement, with the values and principles that guide its decisions and actions, and the objectives it tries to achieve, among other matters.

Induction is also an excellent time to familiarize new officials with the standards, processes, mechanisms, and operation, among other aspects, of the entity. This is when we could start building a sense of belonging and commitment to the entity and start the career of each person who enters.

In an emergency answering and response center, there could be a difference between administrative and technical personnel on the one hand, and operations personnel on the other. The latter is the one who works directly with the reception of calls, dispatch and emergency answering and response. The organization, distribution, 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 types of induction processes could be considered: general and operations induction.

- **General induction:** it would apply to all the new personnel, containing general information of the institution on its mission, vision, values, process map, policies and general regulations and working conditions, among other general orientation aspects to be added.
- **Operations induction:** this would be aimed at personnel of the areas related to the receipt of requests, calls, and reports, dispatch and emergency answering and response on the field, wherein guidance is provided on protocols and processes, the use of technology and communication tools and platforms, among other aspects. It would be advisable to include a section focused on the management of work stress, indicating the services and mechanisms available for its treatment.

If, on the other hand, the model of operation is such that the response center is the coordinating body between response institutions, where each of them would be responsible for the recruitment and training of its personnel, it would be recommended to prepare an induction for personnel who will be providing emergency answering and response on the field. This induction could focus on the protocols and procedures to apply across the board, to promote integration to the service and mitigate a possible clash of different institutional cultures and work habits.

Below are some minimum recommended contents for this type of operational induction:

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

In addition to the general and operations induction, the new official would also have to receive a **specific induction** to the job for which he/she was hired, in line with the induction and training program established by the entity.

Representatives could also be considered by area, responsible for accompanying new officials during their first days (which could be between 7 and 15 days). This type of support could facilitate their adaptation period and speed up the learning curve. To do this, 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 has ended, a trial period could be activated, in which the person would have to demonstrate that he or she has the ability to perform in the position for which he/she was hired. After that testing period (which could be between 3 and 6 months), an evaluation would have to be carried out determining whether the person has adapted to the position or not. If the result is not favorable, the entity would have the possibility of not extending the contract which would restart the recruitment and selection process.

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

If possible, the operations induction would also have to be linked to an accompaniment of the socio-affective process of integration of the new official to the team or work shift.

6.5 Ongoing training to build capacities and functions

In any emergency and security system, the quality and efficiency of the service provided depends, among other elements, on the level of preparation and experience of the personnel. That is why training is one of the pillars of continuous improvement and the development of human talent.

Ongoing training would have to follow a learning and specialization program. There are guidelines for the development of such programs that could serve as a guide and as a reference, including those provided by NENA, EENA, IAED and APCO, to name a few⁷. Training would have to be implemented as a process, in

⁷ EENA: <https://eena.org/knowledge-hub/documents/training-of-emergency-calltakers/>
 NENA: <https://www.nena.org/page/trainingguidelines>

relation to the objectives and goals defined in the strategic plan, and on the basis of a learning and specialization program defined by the entity itself, according to the demands of service and the needs to strengthen the skills of its personnel.

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

Technological platforms could be used to support training, as well as incorporate different practical experiences, case studies and, if possible, simulation. Given the possibility that not everyone can participate in the trainings, it would be important to develop strategies and tools to share and transfer the knowledge acquired internally, to the rest of the corresponding personnel.

Training would require qualified or certified instructors, up-to-date training materials, logistical inputs, space, and equipment needed for their development.

At the end of each training, assessments should be made to measure capacities and goals achieved, according to established learning objectives. Evaluations would also facilitate the detection of new topics and help track and provide feedback to the personnel.

In addition to the ongoing training program, it would be optimal to consider the use of other support tools, such as:

- Registration of the trainings provided, with a series of systematized data on their achievements and participation, among other aspects, and their respective evaluations.
- Trainers' directory, containing, among other systematized information, the trainings provided, and the evaluations received.
- Indicators that allow measuring the impact and application of what has been learned in the respective areas of work.
- System of files per person, where in addition to the trainings carried out and certifications received, the post-training indicators, the hours and number of training days, the skills, competencies, and experiences acquired, among other aspects, are included.

In addition, we recommend that the ongoing training program should also be the subject of an evaluation. The determination of the effectiveness of the trainings provided, would have to try to establish the following from improvements in processes, products and services, and the satisfaction of users with the attention and services received.

6.6 Performance assessment

Performance assessment is a key tool at the individual and organizational level.

At the individual level it would allow:

- Provide feedback on the work done.
- Highlight achievements and performances.

- Identify strengths and weaknesses and propose measures or actions to overcome them.
- Suggest or update career and development plans.
- Set goals and communicate the expectations that the entity has for the person.
- Guide promotion decisions, as well as layoff decisions.

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

The conduction of such evaluations would have to be reflected in the quality of the service and in the satisfaction of the users. It is for this reason that it must be considered as an activity closely linked to management for the integral quality and continuous improvement of the entity (see Chapter IV of this Guide).

The performance assessment 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 qualify personnel for their work, performance, and behaviors.

Minimum dimensions to bear in mind to assess personnel performance may include:

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

6.7 Loyalty of human talent

The learning curve and high level of expertise required for emergency answering and response center personnel make it necessary to establish internal strategies and mechanisms to retain human talent and prevent their departure.

To do this, 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 the civil public servants receive. The salary amount should be in line with the responsibilities and functions that the person performs, and be as competitive as possible, depending on what the labor market offers. It could also establish incentives and benefits to retain qualified officials. In line with the above, it could, by way of example, recognize and reward the outstanding performance of its personnel. In that line, it would be necessary to:

- Establish criteria, indicators, and mechanisms to identify those who stand out for their performance.

- Define a recognition scheme and incentives according to both individual and group performance areas.
- Systematize outstanding performance of personnel; communicate and share these good practices within the entity.

6.8 Departure process

Regardless of the reasons, the process of departing or disengaging an official would have to comply with the legal regulations and internal procedures defined by the entity for such situations.

The disengagement of an official, particularly when the person departs while being professionally appreciated by the entity, may not necessarily mean losing the possibility of taking advantage of his/her talent. There are several ways in which the entity could be linked to certain people considered to be of high value due to the accumulated knowledge and experience. The topical knowledge of these people could be retained through filmed interviews or podcasts available to all personnel. They may also be linked to the entity as instructors, forming part of its trainer directory. In addition, in specific situations they may be available as experts, to consult during or before instances, or as tutors or mentors to guide entry-level and mid-command officials.

6.9 Occupational health and safety

The human talent of the entity may be harnessed to the extent that the health of officials 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 answering and response center.

One of the characteristics of working in an emergency answering and response center is that officials live on a daily and continuous basis with traumatic and high-stress requests, calls, reports, videos, incidents, generating high levels of stress and health impacts. Therefore, it would be necessary to establish a parallel service, providing medical support, as well as specialized containment, treatment, and psychological follow-up to personnel.

It would also be important to establish mechanisms and tools to detect early symptoms and signs of depression, stress, exhaustion, tension, and other similar ailments arising from traumatic situations experienced by the personnel. Early detection would allow cases to be channeled in a timely manner to the specialized support unit to 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 workers, an emergency response center's occupational health and safety policy would also need to address the following aspects (some of them 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 behaviors and in interpersonal relationships. In other words, a Code of Ethics would have to be operationalized or translated, in practical terms, into a set of conducts to be avoided/rejected and/or to follow, 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 with both human dignity and human rights as well as the public value of the services provided to the population.

Ethical principles that might be considered include:

- The emergency and security service is an asset for public use.
- Public assets and resources are intended exclusively for the functions of the entity.
- The reason to have a public official is to provide a high-quality service to the population.
- Public interest prevails over particular interest.
- The emergency and security system holds citizens accountable for the use of the public resources entrusted to them and for the results of the management team.

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

- Honesty. To act with fairness, discipline, and honesty in fulfilling obligations and responsibilities, and in the provision of institutional services.
- Loyalty. Act with faithfulness, companionship and respect for personal convictions and the vision, mission, and institutional objectives.
- Solidarity. Act selflessly in the face of 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 experiences to achieve common objectives.
- Responsibility. Execute functions with a high level of commitment, efficiency, and effectiveness, in order to meet institutional objectives and contribute to the good use of public resources.
- Confidentiality. Failure to provide information that is reserved by law, from which undue interest could arise, could cause serious harm to third parties, or could be used to jeopardize the purpose of the public service or state assets.

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

- Respect for the policies, rules, protocols, and procedures of the entity.
- Avoiding participation or publicly supporting any group or organization that degrades the vision, mission, objectives, goals, credibility, or reputation of the entity.
- Not providing information that is false, misleading, or that creates mistaken expectations.

- Notifying the entity of events that could call into question a person's ability to do his or her duty as an emergency answering and response center official.
- Immediately notifying if an official is convicted of a crime.
- Not using certification(s) and knowledge for private or commercial benefit.
- Respecting the laws and privacy rights of users.
- Avoiding the use of alcohol, illicit drugs or any other substance that could affect the capacity of the official and/or the working environment.
- Preventing and eradicating discriminatory practices.

CHAPTER VII. INFORMATION MANAGEMENT

Introduction

Information is one of the main assets of an emergency and security system; 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, in order 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 cycle of information would have to occur in a safe environment, with protocols and measures to safeguard information and prevent leakage and misuse (see Chapter VIII on Security Management).

Information emanating from or in the possession of institutions, agencies, public entities, including emergency and security systems, would have to be governed by rules governing the use and dissemination of information. The main safeguard that should be had in doing so is to protect the personal information of users, as well as not transgressing national or public security or system security.

This Chapter provides guidelines on how to manage the information of an emergency and security system, proposing a cycle of information that would work from the iteration of at least six main activities. The starting point of this cycle would be the development of an informational diagnosis, for which building some tools will be suggested, including an inventory of resources, a flow chart, among others. Until reaching the end of the cycle, it would mean evaluating management, conceived, and carried out as an institutionalized process for the sake of quality and continuous improvement of the service.

7.1. Informational diagnosis

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

Such diagnosis would be recommended because it would identify the sources, flows, resources, and informational products or services required and generated by an emergency and security system. This identification, in turn, would be the starting point for better understanding and guiding what needs to be managed in terms of information.

In addition, the exercise should be aimed at identifying the normative, organizational, procedural, material, and human conditions, among others, 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 for the sake of continuous improvement.

7.1.1 Sources

Regarding sources of information, these could be classified into two broad categories: internal and external sources.

- **Internal sources:** These are the sources within the emergency and security system itself, for example: internal databases with a history of response provided, users served, operational and administrative personnel, equipment, and budget execution. Performance assessments systematically conducted on personnel and satisfaction surveys answered by users of the system.
- **External sources:** These are sources that are outside the emergency and security system and over which it has no control or responsibility, but which contain useful information for its operation.

These external sources could include databases of other public institutions, websites of state agencies, guides, and protocols for events of magnitude, publications, public opinion surveys, among others.

7.1.2 Information flows

Chapter I of this Guide mentioned that an emergency and security system could work based on three levels: the strategic level, the tactical level, and the operations level.

Information would have to flow at each level, as well as between levels. These flows would involve the existence of processes analyzed, planned, modeled and, if possible, automated.

In addition to internal information flows, outward flows could also be established from the emergency and security system, as well as from the outside towards the System. Therefore, it could be possible to consider three types of information flows:

- **External flows:** Formed by information from the external environment and entering the entity.
- **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 publics/audiences in its environment, materialized in informational and/or communication products and services.

In any case, identifying these flows would allow not only to establish the information scope of an emergency and security system, but also to have greater clarity of what type and the number of flows to be managed.

Some of the 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 proper management, diagnosis could result in a map of the information flows considered key, to provide special support those processes, and functional areas considered critical for the emergency and security system in “normal” times as well as during critical events.

7.1.3 Information resources

A useful suggestion would be to identify and record the information resources available to an emergency and security system. From the moment of recording, inventories, organized by type, name, level of operation, usage, responsible, among other categories, could be generated.

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

- **Tangible information assets:** These are physical and digital resources wherein 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 purpose resources, that encompass from providing emergency answering and response services down to accountability, among others.
- **Intangible information assets:** These are tacit resources, composed of strategic and tactical information, and knowledge (derived from experience, lessons learned, good practices, feedback received, among others), that support the scope of the objectives and the fulfillment of the 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 answering and response center could be considered tangible assets. These systems could be identified and classified according to the operation levels where they apply. In this way, at the operational level the following would be necessary:

- Emergency Call Reception System
- File, code, and registration number generation system
- Geographic Information System (GIS)
- Automatic Vehicle Location (AVL)
- Computer Assisted Dispatch System (CAD)
- Mobile radio system (trunking)
- Video surveillance image monitoring and analysis system
- Alert system
- Automated data system for court instances

Those that would be used at the tactical level:

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

One of the systems to be used at the strategic level would be:

- Balanced Scorecard (BSC)

An emergency and security system requires secure information systems, supporting 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

Informational products and services would have to be generated according to the needs and requirements of users, operations officials and those who manage the System, and the projection of the continuous improvement of the service.

In turn, the development of these would depend on the information and technological architecture with which the emergency and security system has been designed (see Chapter III of this Guide).

These should also be recorded as part of the informational diagnosis.

7.2. Information cycle

Once the diagnosis was made, there would be several models for information management. This section focuses on the management of process-oriented information, based on a continuous cycle of related activities:

1. Identifying information needs
2. Acquisition of 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 model for the management of the information of an emergency and security system would require, at a minimum, protocols, procedures, and tools aimed at:

- The classification of information and control of documentation
- Information security
- Assigning and controlling differentiated accesses to information
- Acceptable use of assets and the consequences of unauthorized use
- Risk assessment and treatment
- Reviewing, updating, safeguarding, and destroying information

This management model would enhance information resources to support decision-making processes and as input to achieve the objectives and goals set out in the strategic plan.

In addition, it would drive knowledge generation, learning and adaptation in the face of a changing environment, and facilitate synergy with human talent.

7.3. Levels of information operation

At each of the three levels of operation of an emergency and security system: strategic level, tactical level and operations 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 great guidelines that guide the management, direction or re-direction of the System, and its positioning.

Decision-making rests with high-level authorities, including officials in the planning area.

This level acts based on external flows of information, internal information and institutional information, and knowledge that would have been 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 the high and mid-level authorities and they would use the information and knowledge, or learning produced at the operations level.

- **Operations level:** It would cover the decisions made daily in line with the everyday functions of the System. This level, would produce the data entered into the command-and-control system, composed of other subsystems including call, video surveillance, or other alert mechanisms.

Each of these operating levels would have to have an information cycle, consisting of the six 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 eventual audits.

7.4. Identifying information needs

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

Table 22: Identifying Information Needs

| Theme | Problem | Contingency |
|---|---|--|
| Timely and reliable information generation | Data generation capability; breach of data generation and transaction systems; data transaction rate; consumption of information, among others. | Propose plans, programs, and information projects, based on the transactional platform of the service. |
| Interoperability | Consumption of secure information with articulated and liaison institutions; Leakage or unintended dissemination of information; maintenance of the chain of custody; delay in requests for consumption of information, among others. | Integrate IT platforms of articulated institutions associated with emergency management or related in specific cases. |
| Feedback from emergency answering and response service management | Monitoring of operational and technical standards, among others. | Generate statistical information on emergency answering and response service management. |
| Attention times and variables (Articulated Institutions) | Identification of response times based on territory; number of resources available; heat-maps, among others. | Estimate the time and multi-variables of hazardous situations linked to the operations management of articulated institutions. |
| Prioritization levels | Identification of incidents or events; assignment of institutional roles; report and resources in the System, among others. | Estimate the magnitude of the hazardous situations linked to the operational management of articulated institutions. |

| | | |
|---|--|---|
| Emergency answering and response performance | Compliance with international standards in emergency answering and response, among others. | Evaluate and control the operational management of emergency answering and response. |
| Hazardous situations (articulated institutions) | Unsuitable feedback of situations on the field; state of resources, among others. | Evaluate hazardous situations linked to the operational management of articulated institutions, among others. |

Source: Integrated Security Service ECU-911, 2020.

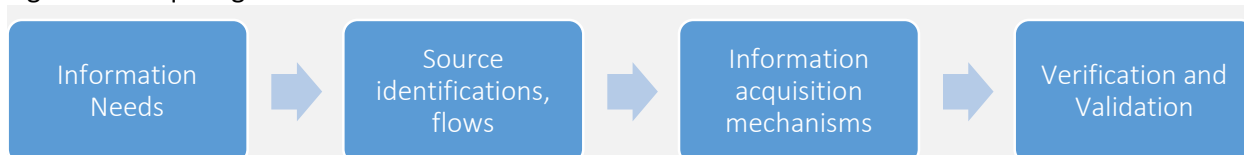
There would be several mechanisms and tools for identifying information needs, including gap analysis, information audits (see Section 7.9 of this Chapter), performance assessments and post-action reviews, among others.

7.5. Acquisition of information

Based on the identified needs, we would proceed to collect all the data and information required to solve such needs. This should take into account existing sources, flows and information resources and consider incorporating new ones.

The data and information generated would have to be subject to some form of verification and validation mechanism that ensures the minimum quality aspects.

Figure 23: Acquiring the information



Source: Integrated Security Service ECU-911, 2020.

7.6. Organization and storage

The organization, storage, and custody of information could be done by creating, maintaining, and constantly updating repositories. These repositories, in turn, would contribute to the institutional memory of the emergency and security system.

As an example, the following repositories could be considered: virtual library, reports (management, attention, financial, projects), queries or requests for information made by other entities and third parties, among others.

For the classification of information in repositories, the ISO/IEC 27001 standard that simplifies this process could be taken into account in four steps:

- i. Entering assets into a repository
- ii. Classification criteria
- iii. Classification by asset (labeling)
- iv. 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 specified, applying principles of rationalization, economics, and purging.

- Asset type
- Location
- Retention times, particularly in terms of documents and archives
- Size
- Storage or support
- Access/Use
- Safety
- Responsibility

There will be several criteria for classifying information in terms of access and use. This will depend, among other factors, on the current legislation, the reality of each country, as well as the specific needs and circumstances of each emergency and security system.

Despite the foregoing, in general terms, the criteria for the classification of information regarding access, should be established based on the content of the information and the uses that will be given to it. Therefore, one might think about the following classification of information:

- **Confidential.** Emergency and security systems capture personal information from each person 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 of the System.
- **Inter-institutional use.** Accessible to interact with other public sector institutions, both in terms of emergency answering and response, as well as input for the diagnosis of problems, the design of intervention policies to address them, and monitoring and evaluation.
- **Public use.** Public domain information such as information found on the website or published by means of communication and dissemination for the purpose of transparent management and accountability. This should be governed by the entity's communication plan (see Chapter IX of this Guide).

Regarding the processing of classified information, particularly as confidential and restricted, it would be desirable to establish security mechanisms to protect it from potential risks, including damage, leakage or misuse, among others. Some of the most common tools used to safeguard this type of information would be:

- Encrypting information
- Generate and save backups
- Differentiate and limit access based on profiles and functions

- Confidentiality agreements between the entity and other public institutions, as well as between the entity and staff.
- Regulate the delivery of inter-institutional information.

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 aimed at a variety of internal and external audiences:

- Users in general
- Specific audiences
- Decision makers of the System itself, in the three levels of operation
- Decision makers at other state institutions. These could include the Ministries of Health and Safety, Crime Observatories and Civil Protection, among others.

There would be a variety of services or informational products that could be developed, by way of example:

Table 24: Development of Services and/or Products

| Specific Needs | Services and/or Products |
|--|---|
| Improve the quality of service from the evaluation and monitoring of emergency answering and response. | Emergency system and safety system user satisfaction reports. Statistical reports linked to emergency answering and response. |
| Maintain the chain of custody of data that could become evidence in court proceedings. | Provision of information through the Automated Information Delivery System to the judicial function |
| Provide access to public information. Improve the level of community readiness, including vulnerable groups and subgroups. | Management reports related to the operation of the emergency and security system. Socio-demographic analysis of the population and identification of risks of the population, groups and subgroups in a situation of vulnerability to emergencies. |

Source: Integrated Security Service ECU-911, 2020.

7.8. Distribution, access and use of information

Distribution and access to information would be subject, among others to:

- Laws and inter-institutional 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, and
- Information flows and information managers, among others.

The availability of information in a timely and in the appropriate format, promotes informed decision-making, catalyzes the learning of the entity itself, facilitates the recognition of new approaches and the revelation of new problems/solutions. This way the emergency and security system could become more resilient, with greater ability to adjust or adapt to changes.

Depending on the use that is intended to give to the information, it could be distributed and become accessible in different ways, in a variety of formats and making use of various channels or media.

7.8.1. Interoperability and exchange of information

Timely, effective, and automatic availability of data, information, documents, and digital objects among articulated (or first-response) institutions is a key functionality to provide 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 Organization of National Information Standards of the United States (NISO) or the American Institute of National Standards (ANSI).

In addition, internal regulations, protocols, and procedures, as well as inter-agency collaboration agreements for the exchange of information, should also be established. They would have to specify, among other things, the type of information, format, channels, need, purposes, and authorizations necessary to enable orders and information transfers.

7.8.2. Continuous development and improvement of operations

For capacity building, institutional development and continuous improvement of the entity, management staff would need to manage strategic information about the operation of the System, including the financial component.

This information could be made available through a dashboard with information on objectives, goals, and indicators. Management, service, financial and project reports could also be at the management level through a document management system (repository), sorted by topic and time reference period.

From the tools used by the entity to receive feedback, either from users (e.g., satisfaction surveys) and from articulated and liaison institutions (e.g., post-action review sessions), information inputs for management could be generated. These could be integrated into the document management system, the dashboard or an information repository linked to quality management and continuous improvement.

7.8.3. Pre-judicial and judicial instances

The availability and delivery of data and information generated or entered into an emergency and security system could serve as key inputs for pre-judicial or administrative instances and judicial authorities.

Regarding the first type of instance, the policies, protocols, and procedures that had been established for the exchange and delivery of inter-institutional information should be used.

For judicial authorities, 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. Within this framework, 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 indication

could be safeguarded and thus contribute to ensuring the evidentiary quality of the indication (chain of custody).

In this regard, it would be recommended that the delivery be made through the mechanisms that guarantee interoperability, that is, to provide for the development of a platform that allows the submission of a motion, or at the request of a party (either the judge or prosecutor), of the information that could serve as evidence in relation to 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. The risks of leaks, cyberattacks and viruses would be reduced.

If a specific platform is not or cannot be developed, under the law, inter-institutional agreements with justice operators could be adopted to define the procedure for the delivery of information. One of the main objectives of these agreements would be the precaution of the chain of custody of the information and therefore preserve the validity of the evidence at the time of it being considered as evidence in a judicial process.

In these instruments which are issued to regulate the processing and exchange of information of considered as evidence, the times, deadlines, or terms of response to requests for information made by the operators of justice should be established, ensuring protection and speed in the different procedures. Similarly, timetables for information to remain archived within the emergency and security system should be defined.

In addition, it would be necessary to introduce legal and technological control mechanisms in order to keep safe the information that could be used for judicial purposes. These mechanisms would have to be accompanied by clear guidelines for their safeguarding, avoiding unintended dissemination, commercialization or any other act that could result in the invalidation of the information within a judicial process.

7.8.4. Communication, transparency, and accountability

Based on the communication plan being developed (see Chapter IX of this Guide), and the objectives, communication goals and activities that would have been set forth in it, and based on the information and computer architecture with which the emergency and security system has been designed, it could produce information of interest and usefulness to the internal public (officials of the System itself) and the external public (general and specific), taking into account a varied range of purposes:

- Informative
- Educational
- Preventive
- Binding
- To generate loyalty and sense of belonging among the personnel
- To build trust and legitimacy among the population
- For transparency purposes regarding the management and operation of the System, and for accountability purposes.

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), among others.

7.8.5. Public policy process

The data and information generated by the emergency and security system, particularly those related to emergency answering and response, could also become relevant inputs for other public administration units. These units could include those working on health, safety, domestic and women's violence, natural and anthropic disasters, traffic, transport, and mobility, to name a few.

These inputs and analyses derived from them could feed and support the entire public policy cycle, from diagnosis to design, implementation, and monitoring, to evaluation.

There would be several ways to make available the data and information generated by the System from the emergencies received and served. Regarding articulated and liaison entities, one might think about having interoperable systems. If this is not possible, the emergency and security system may generate service reports, with information on emergency answering and response, prepared monthly, quarterly, or biannual and/or annually. This information would have to be classified by useful attributes for the design of public policy interventions, including gender, age, location of incidents, type of incident location and type of incident, among others.

This type of participation or collaboration that could provide an emergency and security system beyond its direct and immediate area of action would place it as part of governance for public safety and, more broadly, public governance.

7.9. Information audits

The sixth activity of the cycle is focused on evaluating information management.

That is why, based on ISO 30401 or similar standards adopted, and the protocols and procedures been established for the management of information, including classification, support, and protection, it would be advisable to carry out 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 or potential sources, flows, resources, products/services, uses and users who might have the information.

There would be several types of methodologies for carrying out 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.
- Know the organizational structure, operating levels, sources, flows, resources, and information services/products and identify key people in the information organization.

- Design the methodology with which the audit will be carried out: data collection and analysis, interviews, focus groups, among other techniques.
- Develop and communicate recommendations.
- Follow up on the implementation of recommendations.
- Measure and evaluate the changes generated from them.

Audits could be considered as tools for, from a quality management approach (see Chapter IV of this Guide), to contribute to the continuous improvement of information management within the entity, overcoming, in a timely and informed manner, any divergence, gap or deviation identified regarding the standards, protocols and procedures established on in this field.

CHAPTER VIII. 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 key resource or means of ensuring the provision 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 of other countries could serve as a reference. These would provide guidelines and parameters to be followed, adapting them to the realities of each System and each country.

The security of a system that serves and responds to emergencies would have to be addressed with a multidimensional approach, paying attention both to the basic operating conditions of an operational center and to the continuity of services. In this sense, the multiple dimensions of security would cover information, communications, computer systems, physical and infrastructure security, and staff security, among others.

This chapter, in addition to providing general guidelines for security management and guidelines to ensure the operation of an emergency answering and response center from multiple dimensions, also addresses risk and vulnerability analysis to safeguard and ensure operational continuity and delivery of services in crisis situations.

8.1. Information security

The legal basis for information security management would have to be referred to all national rules guaranteeing the rights and obligations of individuals and public institutions for the provision of a service. The value of the information could also be considered, made public and accessible within the framework of democratic political societies and regimes. This is especially relevant for conducting monitoring, transparency, observance, auditing, and accountability exercises (topics addressed in Chapter X of this Guide).

Information security would involve preventive, proactive and reactive measures, and actions to protect the information of the emergency answering and response center. It would have to be built on three basic principles: confidentiality, availability, and data integrity.

In addition to being an end on itself, information security would have to be considered as an ongoing process. As such, it would need to be managed by a specialized team (within the functional division for Security Management referred to in Chapter III of this Guide) and guided by a set of policies and protocols established by the entity itself for such purposes. These should be aimed at preventing unauthorized access, (re)use, disclosure, exchange, interruption and destruction of the data and information handled by the emergency and security system, in different formats, forms and means.

8.1.1 Information security policies and standards

Security policies and protocols would have to function as guiding tools to guide, 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), among others. They would also have to align themselves 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 operation of an emergency answering and response center, 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 courier services
- Use of *software licenses* and definition of unauthorized *software*
- Data protection and privacy
- Physical access control
- Remote access control
- Downloading files (external/internal network)
- Record retention and backups
- Use of network services
- Use of computing and communications in mobility
- Using cryptographic controls

Information security policies and protocols should be disseminated and socialized among the personnel, as well as external persons visiting the facilities of an emergency answering and response center.

Based on the policies and protocols that are designed and implemented, the functional division responsible for the security of an emergency answering and response center, could audit its management in terms of information systems and related technologies. For such purpose, it could use, as a reference, the guidelines established in the guide: Control Objectives for Information and Related Technologies (COBIT), developed by the Information Systems Audit and Control Association (ISACA).

8.1.2 Treatment of physical and digital documentation

The emergency and security system would have to establish a documented information control process, in line with ISO 15489 and ISO 30301, which sets forth instructions and steps for document management.

Procedures would have to be treated safely and consistent with the importance of internal and institutional information, applicable at all stages: (a) storage, (b) use and reuse (c) access and flow, (d) digitization and safeguarding, and (e) destruction.

They would also need security measures and protocols for handling information generated or accessed through: (a) office suite, (b) e-mail messaging, (c) portals, (d) database systems, (e) hard and/or external disks, (f) multimedia (voice, video, tape) and (g) cloud technologies, or other media.

8.2. Security of technology infrastructure for information and communication

One of the focuses of information security management would have to be computer systems, particularly the protection of the computer assets of the emergency answering and response system. These could be classified into:

- **Hardware:** physical elements of the computer 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, whether it is the operating system itself or the applications installed on it.
- **Data:** Logical information that processes the software using the hardware. In general, they will be information structured in databases or information packets that are exchanged over the network.
- **Others,** for example: fungible items, which are those used or spent, including ink and paper for printers, DVDs or other media. Being external elements to the computer system, they are not critical to their security.

Among these, the most critical is the data. Data is stored on the hardware and processed by software applications to support the provision of emergency answering and response system services. Everything else could be replenished, 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 them in the shortest possible time and,
- Make them usable, in the state closest to the time of loss.

The family of standards associated with the Certification of Information Security Management Systems (SGSI) also includes a set of basic mechanisms and measures to safeguard data within a computer system, which could serve as a reference for an emergency answering and response center.

8.2.1. Regarding computer systems

Computer security policies and protocols should closely follow guidelines to ensure the confidentiality, integrity and availability of the information handled by the entity. Its implementation would aim to avoid security breaches and keep data safe.

Computer security regarding hardware should be aimed at protecting all the physical elements that make up a network, using tools to scan and control traffic. These tools could include firewalls, proxy servers, and more.

Servers, printers, firewalls, and proxies would have to comply with the standards and requirements set out in computer security policies. They would have to be inventoried in physical and electronic formats. Hardware would have to be protected against power problems. In addition, the use of external storage devices would have to be subject to standardized protection, control, and security procedures.

In relation to servers, their architecture would have to be designed based on a model of redundancy and high availability. This means that everything that is housed in its infrastructure would be resistant to electrical system outages and failures.

To build a high-availability infrastructure, COBIT Chapter DSS04, particularly section 7, associated with the management of backup agreements, could be referenced. At a minimum, the following components should be considered: redundant systems, arrays, network, power source, automatic transfer switches (ATS).

Computer security regarding software would have to be based on periodic surveillance and testing protocols. Likewise, patch and update validation and the incorporation of antivirus software that is connected to the internal network would also need to be considered. As with hardware, *it* would be advisable to inventory all software assets such as operating systems, service software, base software packages (office software, mail client, instant messaging, video conferencing, video editing, database applications, among others).

Some basic mechanisms for the security of computer systems that could be considered would be:

- **Authentication:** Verify the user's identity, usually when entering the system or network, or accessing a database.
- **Authorization:** A process through which it is determined what, how, and when, an authenticated user can use the entity's resources.
- **Administration:** Defines, maintains, and eliminates the authorizations of the System, its resources, and its 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 answering and response system, on an event base that could then be analyzed.
- **Maintaining the integrity of the information:** Procedures in place to prevent or control that the files are not changed without authorization and that the information sent from a point reaches the indicated destination, without having undergone alterations along the way.

8.2.2. Communications security

Emergency assistance and response systems are increasingly demanding a growing number of applications (email delivery systems and browsers, among others) and terminal equipment (phones, central computers, personal computers, and mobile phones, among others) connected to networks. That is why the security of communications on data and mobile networks is critical to security management.

The capacity of networks or information systems to withstand malicious accidents or actions that jeopardize the corresponding services they offer or become 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 system including root servers, identification service for calls and authentication services, among others).

This type of security, focused on communications, would seek to prevent unauthorized interceptors from accessing telecommunications in an intelligible way, while still delivering the content to the intended recipients. This could include 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. Voice over Secure Internet Protocol (VOIP) would have become the de facto standard for securing voice communication, replacing the need for analog equipment.

For these purposes related to safeguarding the security of communications, the following guidelines could be considered:

- **Regarding email accounts.** The username and password used to access computer systems would have to be individual, and passwords created according to several criteria to promote higher levels of security.
- **Regarding electronic messaging.** Protection measures would have to be implemented for classified messages, encrypting content and/or sensitive 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) may be governed by the ANSI/TIA 942-A standards or others 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 resources, from physical assets to personnel.

In addition to the technical standards for the design, construction and commissioning of areas and units for the work of public officials in force in each country, at least the following actions should be considered:

- Diagnose the current and future state of the operational center.
- Periodically analyze and evaluate the operating status and risks the emergency and security system could face in its daily operation.
- Develop, review, and adjust a physical safety plan with measures available to the facility, and instructions and drill exercises for the personnel.

Regarding physical security, the following elements should be considered at a minimum:

i. 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 firewall (see as reference NFPA 80 standard).
- Evacuation routes and properly marked emergency exits

ii. 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

iii. Access to authorized facilities and sites

Persons outside the System would have to be properly identified and registered before entering the facility, either 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, reason for entry, person to visit, as well as the date and time of departure. Photographic records and generating credentials or passes that would have to be visible while the person is inside the premises could also apply.

At entry, visitors could also go through a detector arc or a 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 the personnel's positions and responsibilities.

8.4. Risks and vulnerabilities

Security management would also involve identifying risks or eventualities that could affect the operation and continuity of operations of an emergency and security system.

In this sense, it would be recommended to implement processes and tools to identify vulnerabilities and potential risks on the System's main three components: information and communications, IT support and infrastructure. This diagnosis would serve as an input to design mitigation and contingency plans, continuity of operations and recovery.

The recommendation would be to develop a proactive approach to risk management. This approach would demand to anticipate, reduce, or avoid risks and take the necessary priority measures to restore emergency and security system operations in the shortest possible time, in the event of any of the identified contingencies. To do this, there would be at least three key tools that could be considered: risk analysis, an operations continuity plan (PCO), and a disaster recovery plan.

8.4.1 Risk analysis

Risk analysis is key to knowing what prevention, mitigation, and response measures to take so that the emergency and security system can continue to provide its services, regardless of the circumstances.

To do this, it would be necessary to identify risks that could affect each of the critical systems and services, including the technological and communication equipment that supports and makes its operation feasible. It would then be necessary to assess the possibility of them occurring, and to assess the type and level of impact they would have. This information could be systematized on a risk matrix.

The risk matrix is a management tool that helps to objectively determine what the safety-relevant risks are. By positioning the different types of risk in the matrix, you could clearly visualize where the priorities would be, and where efforts and resources should be directed. (In Chapter II of this Guide, the use of this instrument linked to the strategic plan was addressed.) The following is an example of a risk matrix:

Table 25: Example of risk matrix

| Risk | Probability | Impact | Mitigation | Head(s) |
|---|-------------------------------------|---------------------------|------------------|---|
| Disruption of the electrical/information backup system between different response centers | 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 that includes the following elements:

- The appointment of managers, up to the level of units and equipment, so that all parts of the System know how to react and what to do in the event of the occurrence of the identified risks,
- The budget allotment and,
- Setting deadlines.

8.4.2 Continuity of Operations Plan (PCO)

Such plans would help to make support systems, essential or critical, for the operation of the emergency answering and response center available when necessary, supporting the provision of services, regardless of the circumstances of the context.

The PCO is an emergency plan that aims to maintaining functionality to a minimum acceptable level during a contingency or crisis. In the event of such an eventuality, which would have a negative impact on the operations of the System, that plan would have to consider all reaction and recovery measures in order to respond effectively.

The goal of the PCO is to maintain the emergency answering and response center. This would result in the need to prioritize operations that are critical to maintain the continuity of their operation, at all times, under any kind of contingency that is being faced.

Some benefits and/or advantages of having this type of plan would be as follows:

- Early and timely identification of critical processes and assets, giving priority to their protection or guarantee of operation during a crisis.
- Definition of critical recovery times and deadlines to return to the previous state, pointing to contingency plans and protocols.
- Prevention and minimization of human and economic losses, and of affectation of personnel working in a Center.

For the design of the PCO it would be advisable to consider the following steps and aspects:

- Form a multidisciplinary committee and team to anticipate and analyze risks.
- Perform risk assessments (probability of occurrence and impact).
- Identify the processes and criticality of each of these for the operation of the System.

- Modulate each critical computer component of the System, in order to ensure the recovery of the operation from any contingency.
- Develop and document procedures, indicating the objective and scope, considering the recovery times for each activity to be executed.
- Assign responsible for each action to be executed, to ensure near-immediate continuity.
- Develop recovery strategies for potential contingency scenarios where critical processes are disrupted, including the definition of procedures, and roles that would have to be activated to respond and operate in emergency situations.
- Disseminate the plan among the personnel and train them in functional areas where critical areas and procedures have been identified. This training would have to be provided regardless of the risk mitigation that may have taken place, as there will always be residual risk.
- 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 useful to create a knowledge base of lessons learned during testing, as well as after their implementation in the face of a crisis.

8.4.3 Contingency and recovery plans

Contingency planning is a basic process for security management in an emergency answering and response system, and a substantial part of internal control to manage the availability of critical processes and equipment in the event of an outage. The main goal would be to minimize time out of service and maximize recovery time. A reference model for contingency planning and recovery could be Business Impact Analysis (BIA).

For the Disaster Recovery Plan (PRD), the guidelines and recommendations relating to the Continuity of Operations Plan (PCO) could be considered and particular attention should be paid to the following points:

- Focus on processes and equipment considered critical to emergency and security services.
- Develop 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 support the critical processes and equipment of the emergency and security services, specifying the frequency and location of those backups.
- Define protocols of action based on processes and prioritization thereof.
- Define roles and responsibilities.
- Define the minimum information that is required to continue operating.
- Generate a knowledge base with lessons learned from plan design, testing, and implementation.

8.5. Personnel's health and safety

In occupational safety and risk prevention, several professional disciplines would be combined with the specific purpose of eliminating or reducing the risks associated with work activities. These risks could be causing both illnesses and occupational 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 the personnel, depending on the nature, dynamics and working conditions in an emergency answering and response center. In addition, other aspects that an occupational health and safety policy of an emergency answering, and response center could address were listed, which are briefly presented in this section, including:

- **Working conditions:** These refer to social, technical, organizational factors in a workplace, and to risk factors that may arise in the work environment. These, in turn, could, immediately or in the long term, have negative or positive consequences on the well-being, health and safety of civil servants.

International and national regulations provide that it is the obligation of the State to establish safe and adequate working conditions for the correct and healthy development of activities by civil servants.

- **Risk factors:** It is determined as an occupational risk factor as any condition that is present in the development of a work activity and that could cause accidents, diseases and even death of a person.
- **Work accidents:** They 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 in the person body injury, functional disturbance, disability, or death (immediate or subsequent).
- **Occupational illnesses:** These could be understood as chronic conditions, caused in a direct way by the exercise of the job or occupation carried out by the person in the workplace and as a result of exposure to risk factors, and which could lead to incapacity to work.

The International Labor Organization (ILO) has produced a list of occupational diseases, organized for cause, that could serve as a reference for this item.

The key would be to check the cause-and-effect relationship between the work performed and the chronic disease, and if so, introduce measures to eradicate or mitigate the identified causes.

- **Absenteeism:** The International Labor Organization (ILO) defines it as "the practice of a worker of not appearing to work for a period of one or more days that he was supposed to attend, excluding holiday periods, strikes, gestational periods and deprivation of freedom."
- **Epidemiological prevention and surveillance systems:** Prevention of diseases that may occur within the workplace and in the performance of work activities are an important point for the prevention of occupational risks, the safety and health of personnel. In this sense, epidemiological surveillance would be an instrument of vital importance. It would have to be conceived as a dynamic process used to identify, measure, and analyze health problems that could affect the working population. It is from this epidemiological surveillance that information could be generated for decision-making aimed at promoting health, preventing disease or, otherwise, containing and controlling health problems that have already been presented within a workplace.

8.5.1 Risk factors

It is necessary to start from the recognition that the main factor for a work accident is the human factor. This could be due to several reasons, including: the execution of an unsafe act or an unsafe condition, either out of ignorance at the time of execution of the task(s), over-confidence in the execution of the task(s), or technical failures. Thus, the following steps would have to 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, technical standard of prevention (NTP) 330, Hazard Identification and Risk Assessment (IPER), among others.
- Assessment of specific risks such as the assessment of psychosocial risks, ergonomic risks, physical, mechanical, and chemical risks, among others, that could affect the health and well-being of the personnel.
- Definition of measures to prevent, mitigate or eliminate such risks, including job-specific training, existing risks, and how to avoid them.

Among the most common occupational risk factors in an emergency answering and response center are those associated with three basic operational tasks: receiving help requests, calls or reports and monitoring of video surveillance cameras, and emergency answering and response on the field. Each type of risk would have to be accompanied by several recommendations that could be considered for mitigation.

Table 26: Risks and recommendations for receiving calls and monitoring cameras

| Risk Type: Ergonomic | Recommendations |
|---|--|
| <ul style="list-style-type: none">• Constant operation of the keyboard and prolonged use of mouse or joystick.• Remaining seated for extended periods of time.• Prolonged use of screens | <ul style="list-style-type: none">• Time allotment for active breaks (rest and stretching exercises) and visual breaks.• Endowment of visual protectors.• Adjusting the height and tilt of the keyboard.• Armrests and supports for the palms of the hands.• Equipped with ergonomic chairs.• Correct positions in front of the computer and when sitting |
| Risk Type: Psychosocial | Recommendations |
| <ul style="list-style-type: none">• High responsibility.• High levels of stress.• Constant alert status.• Workload.• Difficulty balancing professional and personal life.• Workday, night work, rotation, overtime, work outside of working hours. | <ul style="list-style-type: none">• Emotional discharge activities.• Improved communication.• Psychological follow-up with professionals. |

Source: Integrated Security Service ECU-911, 2020.

Table 27: Risks and recommendations in response to emergencies on the field

| Risk Type: Ergonomic | Recommendations |
|--|---|
| <ul style="list-style-type: none"> • Posture seated for a long-time during driving activity. | <ul style="list-style-type: none"> • Ergonomic seats for vehicles. |
| Risk Type: Mechanical | Recommendations |
| <ul style="list-style-type: none"> • Use of vehicles. • Displacement in land transport. • Road accidents, entrapments, dismemberments, death. | <ul style="list-style-type: none"> • Preventive maintenance of vehicles on a regular basis. • Training on traffic laws and related topics. • Defensive management training. • Awareness behind the wheel. |
| Risk Type: Psychosocial | Recommendations |
| <ul style="list-style-type: none"> • High responsibility. • High levels of stress. • Constant alert status. • Workload. • Difficulty balancing professional and personal life. • Workday, night work, rotation, overtime, work outside of working hours. | <ul style="list-style-type: none"> • Emotional discharge activities. • Improved communication. • Psychological follow-up with professionals. |

Source: Integrated Security Service ECU-911, 2020.

8.6. Continuous improvement

In line with the comprehensive quality management model developed in Chapter IV of this Guide, improvement actions would need to be established in all aspects to make the emergency system safe. 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, as a result, introduce updates or adjustments that keep them reliable and safe.

Within the framework of the comprehensive quality management model, to generate a continuous circle of improvements, it would be necessary to consider the following steps:

- i. Define monitoring processes that collect and deliver data to measure, process, analyze, and implement improvements in information, computing, communication, physical security, and personnel security.
- ii. Design reports to identify recurring gaps or vulnerabilities to adjust existing security policies.
- iii. Identify technological and communication obsolescence.
- iv. Establish a process with which compliance and constant measurement of security policies and protocols can be evaluated.
- v. Prioritize identified areas of opportunity and generate action plans to address these findings.

CHAPTER IX. COMMUNICATION MANAGEMENT

Introduction

Communication and information could be considered as strategic resources for emergency and security systems, both in terms of institutional and operational communication. The first would be linked to the positioning, image and "branding" of an emergency and security system. It would include a series of communication actions aimed at the relationship with personnel as well as the external public from a strategic perspective. The second would be linked to communication within the emergency and security system, and this with actors from the environment, in answering and response to low and high magnitude emergencies. That is why its planning and management are essential.

The planning and management of communication would have to be thought of in two axes: a strategic axis, related to institutional communication, and another more operational axis, linked to the operation of the emergency and security system in emergency answering and response. In addition, the planning and management of communication would have to take place on two levels: within the organization and in relation to the environment. Finally, communication planning and management would have to be designed for low-intensity emergencies, relating to the daily operation of the System, and high-intensity emergencies, related to natural or anthropic disasters that simultaneously affect many people and geographical areas.

As a result of the planning process, a communication plan would have to be developed to guide the management of communications. This Chapter presents a series of guidelines to guide the structure, components and minimum content that could be considered to develop a communication plan.

Then some channels and tools that could be taken into account for the management of communications in an emergency and security system are set forth, including: spokespersons, the use of networks, media and social media, and the connections with the population and communities as well as prerecorded messages.

The Chapter also provides guidelines to guide the planning and management of communication in high-impact crisis situations, that affect at a national, subnational and zone level. Finally, the Chapter concludes with the presentation of three communication challenges, to which some mitigation measures are proposed.

9.1. Communication planning

Communication actions would have to be part of a structured design, execution, and evaluation process.

Communication would have to have a comprehensive scope. In turn, the planning and management of communication would have to be integrated into the overall management of the entity and could have different levels of complexity, depending on the type of functions 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 results and impact 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, the different specific audiences, and the media ecosystem, among other elements.

All these aspects would have to be endorsed in a technical and cross-reference document. The communication plan would serve as a driving instrument. Planning would have to address two necessary and complementary dimensions of communication activity: organizational/institutional activity, with a strong strategic and operational component.

9.2. Planning organizational communication

In the organizational dimension, communication planning would involve taking a strategic approach. It is an instrumental activity to support an entity's strategic plan. It would have to consider the communication actions that seek the strengthening of the System, taking into account the mission, vision and strategic objectives herein (see Chapter II of this Guide).

Organizational communication would also need to be addressed as an integral part of strategic planning, trying to capitalize on strengths and opportunities, and addressing identified weaknesses and threats. It would have to be guided by its own objectives and goals, aligned with the strategic plan, and incorporate indicators to measure the results achieved.

Different communication strategies would be necessary at this level. Each would provide a conceptual and practical framework for responding to a particular situation, applicable at different times. In addition, each would be the result of a planning of 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:

- Integration of communication flows and processes with the strategic objectives profiled during the planning process of the entity.
- Establishment of communication processes and flows that allow to create value, build shared symbols and meanings, develop messages, position the emergency and security system and generate a closeness/belonging relationship with the population, in a systematized and sustained way over time.
- Involvement and coordination between the management process and the other organizational processes.
- Participation of all personnel in the consolidation, development and strengthening of the emergency and security system.
- Transparency and accountability of the operation and management of the System (see Chapter X of this Guide).

Such planning, as well as its implementation, would be the responsibility of the functional division specialized in the subject, composed of a team of officials with the necessary training and experience to perform in the area.

9.3. Planning operational communication

Communication management in the operational field would have to consider modeling the minimum elements of a communication plan, aimed at supporting the provision of services in emergency answering and response, and strengthening the System's relationship with the user population and the various identified audiences.

Planning operational communication would have to consider at least two dimensions: temporality and the audience.

Regarding the first dimension, it would be important to think of communication objectives and strategies for "normal" times of operation of the emergency and security system. In addition, it would also be relevant to plan operational communication for large and high impact emergency times. (This second

temporal dimension is developed in Section 9.6 of this Chapter). In particular, it would have to be linked to the continuity of services, before, during and after critical incidents.

In relation to the second dimension, the planning of operational communication activity could be subdivided into two components: one internal component and one external component.

Internal communication would refer to the communication process that is developed for consumption of the entity itself. It would involve identifying internal audiences, developing content, designing images, and processing products, and identifying and activating media/communication channels.

These actions would be aimed at:

- Sustain the quality, efficiency and effectiveness of the services provided.
- Promote a good working environment and collaborative working relationships.
- Inform and keep staff up to date on decisions made, adoption of new standards and policy and protocol changes, among other topics of interest.

External communication would be aimed at the general population and the different audiences identified. It would seek to keep them informed about issues related to the answering and response to emergencies and the functioning of the System itself, through campaigns and other communication actions. To this end, it is indispensable that, in accordance with the objectives set out in the communication plan, messages are formulated, the channels, times and frequency with which they will be disclosed are chosen, and understandable and simple language is used, avoiding technicalities

Regarding scheduled events, these are not necessarily linked to operational communication planning. These are events that are expected to occur. They can be national, sub-national or zonal in scope. Sometimes they require that the emergency and security system be activated in advance, from a preventive, operational and communicational approach. It would imply coordination with the response entities for the monitoring of video surveillance cameras and the deployment of units in strategic places for the timely attention of possible incidents that could derive from the event, among other actions. Likewise, it would demand communication actions to inform the public about the development of the event, using the 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 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 designed, the audiences to which these actions would be directed, the exposure times/frequency, the channels/means to be used, and the people responsible for each of the tasks.

In addition, the plan would have to be accompanied by an action schedule and its implementation would have to be based on a set of indicators with which the results achieved would be measured.

In order to be able to design a communication plan, it would be important to start with at least two steps:

- Understand the structure of traditional and social media and be clear about their coverage and impact, as well as the frequency and intensity of use among the population.
- Identify and know which are the different types, characteristics, needs and forms of communication of the audiences to which the communication plan and its actions would be directed.

Regardless of the functions model adopted by the emergency and security system, it is important that communication in the emergency and security system is handled based on a single plan, agreed by all the actors articulated to the System, and with a clear definition of leadership, guidelines of action, spokespersons, and monitoring and evaluation tools.

The document would have to be prepared annually, considering the situation through which the emergency and security system is going through. In addition, reviews could be stipulated each month, with a final assessment that allows estimating or measuring their effectiveness, scope, and impact.

The minimum elements that a communication plan would have to have, could include:

- Communication diagnostics, including environment 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
- Opportunity or timing, frequency, and duration
- Budget
- Control and evaluation

Each communication plan would include a series of communication actions that would have to be implemented to try to achieve the communication objectives proposed, based on the creative strategy and key messages, specifying the mechanisms and communication media to be used, and making use of the communicative and advertising pieces or products designed.

In terms of communication actions, the following examples could be considered:

- Campaigns
- Media agendas and tours
- Events in the participation of the community and authorities
- School visits or school-receiving tours
- Public road drills for emergency answering and response

Regarding campaigns, here are some basic parameters that could be considered when designing them:

- The campaigns would have to be informative.
- Language would have to be simple and clear.
- They should be based on the topics or problems detected from the analysis of the information that the emergency and security system itself has generated (see Chapter VII of this Guide).

If the plan includes actions with traditional media, it would be recommended to approach with the main media and keep contacts and relationships with them up to date.

The development of the communication plan would have to be under the responsibility of the corresponding functional area and then validated and approved by the highest authority of the emergency and security system for its implementation.

The following, as an example, a proposal for structure and content, while on a communication plan:

Table 28: Template for the development of a Communication Plan

| INSTITUTIONAL PRESENTATION | |
|--------------------------------|---|
| Name: | [From the appropriate emergency and security system] |
| Mission: | Manage the response of the emergency situations of the population, reported through a unique number (if any) and those generated by video surveillance, monitoring of alarms or some other means, by dispatching specialized response resources, belonging to public and private bodies articulated to the System, to contribute, on a permanent basis, to the achievement and maintenance of security. |
| Vision: | To be a leading and model institution in the coordination of emergency and security services, using state-of-the-art technology in systems and telecommunications, committed to quality, safety, occupational health, and the environment, which allow to provide a high-level service to the population, continuously and sustained. |
| Sector axis: | Security |
| INTERNAL AND EXTERNAL CHANNELS | |
| Channel | Description |
| Facebook: | The use of photographs and videos could be communication products with the possibility of generating greater attraction, interest, activity, and interaction within the account and among followers. |
| Twitter: | <p>It provides the possibility to publish simple, short, and timely messages.</p> <p>Another valuable feature of this social network is the immediacy with which messages are published.</p> <p>All the features mentioned above make it a possible source of information for traditional media.</p> <p>The use of hashtag tags would allow for grouping content according to specific events or situations, facilitating their search and in cases of news or important events, positioning messages and trends.</p> |
| YouTube: | <p>Having an official account where to host and organize the videos produced by the institution, according to their content, would facilitate the navigation and search for information by the specific population and audiences.</p> <p>The videos could be documentary type, programs about successful cases, news summaries, interviews, among other genres, produced by the institution itself or supported by an external agency.</p> |

| | |
|---|--|
| | The videos could be used to complement the information you want to show the public. Additionally, on other social media, links to the videos could be placed. This is particularly useful when social media have a maximum capacity and character limit. |
| Instagram: | <p>The content on Instagram would have to be visual. Photographs or videos with quality and self-explanatory ability, and interesting/eye-catching enough to generate interactions.</p> <p>Short descriptions, complemented by a hashtag, could be used to provide an idea of what is happening and wants to be released.</p> |
| Website: | <p>It allows to provide information in detail, with official data from entities involved in the coordination of an emergency or relevant case.</p> <p>Written content could be supplemented with photos and videos.</p> <p>It could be used to publish and make available to the public information of an administrative and operational nature that account and contribute to transparent the management and operation of an emergency and security system.</p> |
| Screens in service areas: | Specify quantity and places where they are positioned (malls, waiting rooms or attention rooms of public entities, bus, or train stations, among other possible strategic locations). |
| Own media or communication programs: | <p>Radio or radio program in FM or digital.</p> <p>Channel or open signal tv show (public, private or community).</p> <p>Newspaper or contribution (weekly or monthly) through a column/opinion article.</p> <p>Review or contribution through a column/article, according to the periodicity of publicity of the medium or at a preset frequency.</p> |

COMMUNICATION PLAN

JUSTIFICATION (Must answer the question: Why is it relevant to have a communication plan?)

To publicize and position the emergency and security system services among the population, the contact forms to access the services, and the need to make responsible use of them.

Faced with the possibility of facing low- and high-scale emergencies, it would be necessary to prepare people and vulnerable groups to know what to do and how to respond to these situations.

It would also be necessary to generate a consistent, continuous, and reliable communication, regardless of the functions model adopted. A communication plan becomes even more relevant in crisis situations to contain anxiety, uncertainty, and confusion among the population, and to 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. The question that would have to be answered would be: what for?)

| | |
|-----------------------------|---|
| General objective: | Position positive and confiding image of the emergency and security system among the population. |
| Specific objectives: | <ul style="list-style-type: none"> Positively attract the attention of national and international strategic partners. Strengthen the relationship with the media and increase institutional presence in the media. Create a sense of belonging in the institution's officials. |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Consolidate the emergency and security system as a reference center within the framework of high impact incidents. • Transparent the management and operation of the emergency and security system. |
| Communication Actions: | <ul style="list-style-type: none"> • Social media campaigns. • Interventions in traditional media. • Visits to schools. • Guided tours of schools. • Public road drills for emergency answering and response. |
| 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 incidents. Most emergencies are unexpected and surprising, therefore planning and communication actions should be able to adapt to this nature of emergencies, seeking to provide the population with useful information to preserve life and safety, at all times. The communication of and for emergencies should be practiced as a dynamic process and adjustable to the characteristics of the events that occur.

In an emergency, the ability to provide useful, up-to-date, valid, and ongoing information will depend on the planning and communication preparation previously developed by the emergency and security system.

Depending on the nature and dynamics of emergencies, emergency communication would have to be made in near real time. This is one of the main reasons why communication should be based on six basic premises:

- Make it clear
- Make it simple
- Make it concrete
- Make it concise
- Make it consistent
- Make it timely

From the communication plan, its implementation, and the daily management of communication, they would have to fall into a functional division specifically dedicated to the subject. The area would have to be composed of a team of officials with specialized training, certain predefined competences, and several attitudes necessary to be able to perform in the positions related to the subject.

Communication in emergency situations could be handled through different channels and tools:

9.5.1. Spokesperson

Due to the characteristics and dynamics of an emergency and security service, it would be appropriate to have one or more spokespeople.

Spokespeople could be understood as specifically appointed persons to fulfill the function of communicating; they represent the official voice and image of the entity.

It would be relevant to clearly define the roles of spokespeople, as well as the skills and attitudes to be sought for that position profile. That sense would minimally have to:

- Know the operation of the emergency and security system.
- Be informed about the situation and developments regarding emergency answering and response.
- Express themselves in a simple and clear way.

Those who attend, articulate, and respond to emergencies should always be in contact with the spokespeople and communication team. The integration and complementarity of their work could make a difference in the performance and image of the emergency and security system. The role of voice work takes on particular importance in high-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 in the entity's ongoing training program (see Chapter VI on Human Talent Management), a course or workshop of specialization/updating in communication, particularly linked to the emergency sector.

9.5.2. Networks

Below are two types of networks (external and internal), which could be leveraged by the emergency and security system as part of their communication plans and actions. Networks would have the advantage:

- Expanding the visibility and scope of actions and messages,
- Frequent updating of contents at no higher cost, and
- The ease of communicating information immediately, directly and to a large number of people simultaneously, to mention only one of them.

9.5.2.1 Web platform (external)

The website should be considered as the digital emergency and security system presentation "card". It is there that internet users can find at the very least, the following informational elements, from the communication point of view of the System:

- Institutional information, including vision, mission, objectives, year of creation, team, management, and operational model adopted
- Presentation and description of the services it provides
- Forms of contact for emergencies and consequences for misuse of the System
- Communication actions and newsletters
- Events held and those to come
- Open data, data and statistical bulletins and reports
- Institutional contact and social media account information

Several of these informational elements could also be used in traditional and social media.

The design and maintenance of the website would have to meet some basic criteria, including:

- Simple and easy-to-navigate web site scheme.
- Reliable and quality information, constantly updated, presented in a clear and orderly manner.
- Use high-resolution images and videos to illustrate and supplement written information.
- Inclusive approach, from a technological point of view (connection type, speed or bandwidth, browser, and operating system, among others) and from the point of view of the disabilities of internet users.
- Support for viewing and browsing from mobile devices.
- Protection and safety requirements in line with the policies and protocols established by the emergency and security system (see Chapter VIII of this Safety Management Guide).

9.5.2.2 Intranet (internal)

The intranet is one of the mechanisms or channels of communication and information aimed at the administrative and operational personnel of an emergency and security system. In this internal digital space, the personnel could find up-to-date information, related to the performance of the entity, news and events and activities, as well as administrative and operational tools that could facilitate the management and operation of the System (including: current, new or updated policies and protocols; forms; explanation of how to carry out certain internal tasks or procedures, among others).

Among the guidelines that could be proposed for the structure and contents of an intranet for an emergency and security system would be the following:

- Allow different contents and access levels according to the different functions and positions of the personnel.
- 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 sound player.
 - Those that allow the search and organize information: shared files; directories with contact information; access and query internal and external databases and search engine.

9.5.3. Media

The media are channels to reach the general public. They transmit messages that are disseminated to many receivers simultaneously, through different techniques and technologies. Each has specific characteristics in relation to: audience type, coverage, advertising forms, advantages and costs, among others.

9.5.3.1 Traditional media

The relationship with traditional media would involve institutional liaisons with editors, journalists, interviewers, and reporters. This relationship would have to be conceived as a strategic alliance, as it allows actions and the design of the emergency and security system to be massively evident and reach different types of audiences simultaneously, in accordance with the communication objectives set out.

These objectives could be associated with external communication at the operational level, as well as organizational communication, aimed at working on public perception of the value of services, trust, transparency and accountability of the emergency and security system.

Messages should be geared towards informing and raising public awareness. The communication approach could be preventive, educational, or binding.

9.5.3.2 Social Media

Social media would have to be considered as a channel of direct communication with the population. There are currently several social media, including Twitter, Facebook, Instagram, among others.

Through social media it would be especially important to share useful information for the population such as the status of roads, accidents, evolution/status of relevant events (information sheets and images), among others.

Similarly, they could also be leveraged to disseminate campaigns designed to provide information, recommendations, reminders about highlighted dates or events, raise awareness of certain risks or the proper use of System, among other actions, and do so in a timely and low-cost manner.

To feed social media accounts, keep them active and relevant, it would be preferable to choose the most "attractive" or interesting information for the population. Audiovisual content generally has a greater impact and tends to generate more interactions.

Unlike traditional media, social media enables horizontal and dual (and even, in some cases, multi-way) communication. Through social media, the public may also express their conformity or nonconformity with the service.

Here are some general guidelines to consider for managing social media accounts by an emergency and security system:

- Do not engage in discussions with anyone.
- Any message on behalf of the institution would have to have the authorization of the person in charge of the communication of the entity.
- Avoid syncing the institution's official accounts with any app, personal Twitter account, or any game or program that might automatically post content.
- Avoid posting personal opinions on behalf of the institution.
- Post photos and videos with caution and respect

9.5.4. Establishing relationships with the population and communities

In linking with the environment, an emergency response and assistance system would have to consider a component of relationship with the public and communities, and another component of early monitoring and warning.

The purpose of the public and community relationship component would be to activate and consolidate their involvement and interaction with the emergency and security system. Messages, events, and other communication actions taken as part of this component would need to reflect and address specific concerns, opinions, problems and risks of the population and communities to which they would be addressed. In this way, useful and targeted information would be provided so that they can make better decisions when dealing with emergencies.

In addition, this linkage could also aim to mobilize the community to introduce positive changes in behavior and habits, leading to preserving people's health, well-being, and lives.

The objectives of the relationship with the population and the community could be raised in the short, medium, and long term. By way of example, in the short term, the linkage with the population and communities could be aimed at:

- Raising awareness of the good use of the service, particularly children, adolescents, and young people who, in the medium and long term, will become potential users of the system.
- Train on how to act and how to deal with different types of emergencies.
- Instruct on how to prepare and act on high-impact incidents.

In the medium and long term, the objectives of the linkage with the population and the community could be raised in terms of strengthening the image and social legitimacy of the emergency and security system.

The link with the population and communities should be based on at least four premises:

- Respect for the treatment given to users and the general population.
- Empathy and sensitivity to situations and problems that people, individually or collectively, might be facing.
- Closeness and constancy in the bond with people and communities.
- Professionalism in the service provided to the population, demonstrating preparation, coordination, efficiency, and effectiveness.

These premises would contribute to building trust and membership with the emergency and security system, in line with the medium and long-term objective mentioned above.

The linkage can be face-to-face, through the implementation of programs and projects according to the conditions and needs of each community; as well as virtual, facilitated by the use and expansion of social media.

In turn, constant interaction with the population and community would be linked to the early monitoring and alerting component. This second component could be conceived as a two-way listening process, including the analysis, monitoring and collection of information by the emergency and security system regarding the population and communities on:

- Needs, problems and challenges they face in terms of emergency answering and response. This information would serve as an input to propose assertive 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 faced with information campaigns based on data, facts, and evidence.
- The level of knowledge and satisfaction, and the kind of opinion and perception that the population and communities have regarding the emergency and security system. This information could serve as input to guide the introduction of changes and improvements in the logic of 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 to communicate and inform the population about ongoing emergency situations and scheduled events. These would have to be configured according to the technological capacity of each System and adjust to the regulatory framework that each State has established in the field of telecommunications.

9.6. Planning and management of communication 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 communications plan, including articulated (or first-response) and related entities, and which is aimed at the general population and the specific audiences identified.

In high-scale emergencies, information is a valuable resource for decision-making. Communicating available information is key to mobilizing national and international resources and provides a timely and appropriate response to the population.

Crisis communication is a strategic component of the planning of communication activities and also a component of risk management. Just as most incidents of magnitude and risks can be analyzed and anticipated, communication management would have to consider planning and preparing for events of magnitude.

The planning and preparation of crisis communication would have to be crystallized into a communication plan. This plan could be part of the comprehensive or master plan, or it could be developed as a separate plan but linked to the first. In both cases, it would allow communication actions to be managed and guided in exceptional circumstances. This communication crisis task would have to support the large-scale emergency response. Additionally, it would have to be in line with the risk matrix, the continuity of operations plan, and the disaster recovery plan (see Chapter VIII of this Guide).

The plan should contain at least the following elements:

- The steps needed to develop crisis communiqués
- Communications and message strategies
- Evaluation of the plan, having overcome the crisis

Crisis communication planning would enable emergency and security system authorities to have established guidelines, processes, and procedures in place to effectively communicate to the general population and specific audiences about the nature, status and evolution of risk. In this sense, the design of targeted and segmented communication actions, making use of different communication channels available and close to the needs of the identified audiences, could contribute to the assertiveness and receptivity of the message.

A timely instrument for situations of great affectation, at the national, subnational or zone level, is the dissemination of emergency alerts. This type of alerts are messages of massive, instantaneous, and rapid dissemination, which require the support of the telecommunications sector to guarantee the simultaneous availability of the different communication channels. Alert messages would have to vary depending on the predefined incident type. The anticipation of this would allow the elaboration, in advance, of message templates for their eventual use.

In addition, in the context of such high-scale and impact situations, it is highly likely that not only articulated but linked entities will be activated as well. Due to the increased number of entities, coordination in response and communication become even more crucial. The approval of messages to

disseminate to the population and the need for all entities involved in the emergency response to handle the same information, become more relevant and make it even more necessary to have 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 and communication 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 field of the response. In this sense, it would have to establish a set of guidelines, processes and procedures that facilitate communication for interaction, exchange of information and coordination at different levels, including: authorities, articulated and related entities, emergency teams and interested audiences (scientists, academics, public health professionals and communicators, among others).

With regard to the management of communication in crisis, the following guidelines could be considered:

- Establish a centralized communications center or node, in charge of handling all requests for information and preparing releases for media, social media, other institutions, the general public, and specific audiences.
- Define authorization chain for the communication and dissemination of information.
- Set a communications calendar.
- Develop pre-assembled message templates or scripts.

The latter could be designed based on the following three components:

- Audience(s) to which they are targeted
- Main message
- Instructions for more information

The Incident Command System (SCI), specifically the communication chapter, could provide guidelines for emergency communication. Additionally, other sources of references could be: the "Crisis Communications Planning Guide" and the "Recommendations for Communicating with Interested Parties during a Crisis," both developed by *Mission Critical Partners* (2020).

9.7. Communication challenges

Communication in emergency and security management can change every day and at all times due to the very nature of the incidents. In addition to this challenge, communication from and for emergencies faces at least three additional challenges.

i. Challenge 1: Vulnerable groups

Emergency answering and response measures would have to consider the specific needs of persons with some sort of vulnerability, marginality or with some type of disability. The lack of consideration of the difficulties of interaction with the media and communication devices, and the social, physical, and cultural distance of these groups, emerge as real obstacles when providing protection, emergency answering and response.

Faced with this challenge, in the planning of communication actions, an emergency and security system could consider the following elements:

- Identify vulnerable groups (including: illiterate, marginal groups belonging to ethnicities with different customs and languages to that dominant or official and people with physical or mental disabilities, among others). Understand what their sociodemographic characteristics are, its geographical location (if applicable) and its needs in relation to communication aspects in low and high intensity emergencies.
- Analyze advantages and opportunities in the use of different media.
- Design communication actions and messages aimed at each of the identified special audiences, to reduce the vulnerability of those people and increase the effectiveness of emergency answering and response efforts.

ii. Challenge 2: Misinformation

- False, erroneous or misleading information (misinformation)
- Incomplete, inaccurate, or misrepresented/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 "informational disorders" that, in turn, could lead to misinformation and social unrest. In the face of this scenario, an emergency and security system might consider the following guidelines for communication management:

- Avoid improvisation or half-told truths.
- Avoid trying to get the public's attention by publishing sensationalist images related to emergency situations.
- Establish emergency data verification mechanisms before handing them over to the media.
- Have communication guidelines and information for dissemination.
- Take care of the way we communicate, respect above all the human dignity of victims.

iii. Challenge 3: Higher incidence of high-impact disasters or catastrophes

Given the increase in the frequency and intensity of high-impact disasters, for example caused by climate change and anthropic origin, emergency and security systems are increasingly more likely to face these types of situations more frequently. In the face of this scenario, some guidelines for communication planning and management are presented:

- Strengthen the planning and review of communication plans associated with preparation.
- Establish mechanisms for cooperation, exchange of lessons learned, good practices and training together with other entities on how to act in the face of such events.
- Adopt communications monitoring and evaluation tools for communication plans and actions

CHAPTER X. TRANSPARENCY AND ACCOUNTABILITY

Introduction

Transparency and accountability could simultaneously be seen as values and principles to be sustained, objectives to be achieved and processes to be followed. In any case, the three approaches are substantive in and for democratic governance and policies associated with public management, including in the field of security and emergency answering and response.

This type of service, being provided by the State and being focused on the protection and safeguarding of human life, would require facilitating accountability for the management and results obtained, making available to public institutions, means of communication, academic and private sectors, civil society and the population, a series of data and information for the legitimate exercise of horizontal and vertical control. 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 would also contribute to increasing its level of approval, trust and legitimacy among the population.

Because of the nature of the content and the purpose it pursues, transparency and accountability would have to be part of the design of the System and the strategic planning oriented to its strengthening. This would involve the creation of protocols, processes, and mechanisms to proactively provide information on the financing and management of the System, as well as to facilitate access to information that contributes to the observation, knowledge generation, public value creation and innovation.

This Chapter addresses transparency and accountability from the perspective that they need to be subjected to a planning process, 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: consultations and requests for public information, quantitative data, open indicators and data, reporting system, procurement and public procurement of goods and services, internal/external audits and the entity's communication plan.

The communications 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, leveraging information available through the above mechanisms.

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, accompanied by induction and training sessions, as well as an incentive and sanctions scheme to support compliance or non-compliance, would seek to instill transparency and accountability as values and guiding principles of the action of the emergency and security system as well as its personnel.

10.1. Planning for transparency and accountability

Planning to ensure high levels of transparency and accountability by an emergency and security system could begin with a justification. This could set out the reasons why an emergency and security system would seek transparent action and accountability for activities carried out with other public entities, specific public, and the population in general.

By way of example, these reasons could be linked to:

- It ensures the effectiveness and efficiency of the System, contributing to governance,
- Respect the right to access public information of individuals, and

- The need to ensure the integrity of the operation and management of the System, and to prevent and address corruption.

A planning process would also define the objectives to be achieved, for example:

- Achieve a high level of trust and credibility on behalf of the population.
- Become a national (and international) reference or source of reliable and up-to-date information.

It would also enable to think and establish systematically the goals and performance indicators that could be agreed upon to measure progress and achievements on the objectives set for transparency and accountability. This in turn could serve for the communication, demonstration and publication of results, and accountability for the goals and achievements accomplished, as well as for those not achieved.

Planning could result in a plan that, for implementation, would require several processes, procedures, and mechanisms. The plan would have to be aligned with both national transparency and access to public information laws, the open government plans valid in each country, and the other (strategic and operational) plans developed by the emergency and security system.

Depending on the objectives and goals set, a System could consider implementing several internal and external mechanisms to meet them, including:

- Inquiries and requests for public information
- Quantitative data, indicators, and open data
- Reporting (reports)
- Publication of procurement and acquisition processes
- Internal/external audits
- Communication plan

10.2. Inquiries and requests for public information

An emergency and security system would have to have stipulated processes and mechanisms for receiving inquiries and requests for information from the population and specific audiences, in line with the legal framework in force in the country.

Some considerations to keep in mind for standardizing and facilitating query and request for information processes:

- Enable multiple channels or media, including: by phone, email, face-to-face or through the emergency and security system website. It would be important to clearly differentiate these channels from those used to report emergencies.
- Design a physical and digital form so that the public can make their inquiries or request the information they need.
- Define an internal procedure for processing that query or request for information, 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 the request for information made.

- Authorizations required to deliver the requested information.
 - Script for the attention of such calls.
 - Pre-assembled mail templates to automatically respond to such orders or requests.
 - Physical and digital certification stating that the query was served, and the requested information was delivered. If not delivered, it would be suggested to provide an explanation under the country's legislation or the entity's regulatory framework.
- Emergency and security system officials specifically trained and dedicated to fulfilling these types of tasks.

Since an emergency and security system handles personal data, it would be important to strike a balance between transparency and accountability, and the privacy and confidentiality of users' identifiable information. It would also be important if the information generated and managed by an emergency and security system is also subject to a classification typology and process (see Chapter III and VII of this Guide).

The typology of classification of information should be in line with the parameters established in the laws of each country, also considering internal security issues such as the non-disclosure of data that could generate some kind of risk, including: compromising the operation of the emergency and security system, generating vulnerabilities to the computer systems and communications of the entity, and compromising the physical integrity of officials, among other aspects.

In addition, in line with the policies and protocols established by the entity regarding information security, communication and computer systems, personal data would also have to be protected to prevent 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 available to interested parties, information for the assessment of the operation of the System, the services provided, and the results achieved.

That is why, at first, an emergency and security system could make available to the public two large types of data and indicators, already processed or with some degree of 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 (disaggregated by sex and age), type of events served, areas of care, among other variables.

Secondly, a more recent approach, which places particular interest in open data, would have to be considered, i.e., data that can be freely used, reused, and redistributed by anyone, and which are subject, at most, to the attribution requirement and to be shared in the same way that it was digitally published.

The emergency and security system would have to regularly publish open data to facilitate and promote its use, reuse and distribution by the general public and specific audiences, without imposing restrictions based on copyright or reproduction.

For open data, it would be important to define, for example:

- The origin, how and where they were obtained

- The frequency of publication of up-to-date and comprehensive data
- The format, including to be machine readable, interoperable, and comparable
- How the source should be cited
- The place within the emergency and security system website where they could be published

In addition to promoting transparency and accountability, open data would encourage public participation and knowledge generation through the processing and analysis of publicly available data. In addition, they could contribute to governance and trust in the emergency and security system. Moreover, they could be sources for innovation in the face of common problems and challenges that require informed solutions.

10.4. Reporting system

Based on the information architecture with which the emergency and security system has been designed, the computer 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.

These could include:

- **Management reports.** They would account for the administrative functioning of the System, the use of economic resources, compliance with strategic and operational planning, and the results achieved. These could be developed on a bi-annual and/or annual basis.
- **Service reports.** They would provide information on emergency answering and response. They could be developed monthly or quarterly, biannual and/or annually.
- **Financial reports.** Based on income and expenditure budgets. They would provide an implementation balance sheet and degree of compliance. They could be developed on a quarterly or biannual and/or annual basis.
- **Project Reports.** They would present the level of progress of the active projects, estimated closing dates, its levels of financial execution, among other relevant information. They could be published quarterly.

These reports, in turn, could be part of the entity's communication plan. They could be disclosed through different media or channels, including: the website, social media accounts, face-to-face or virtual events and posts, among others. (On communication management for an emergency and security system, go to Chapter IX of this Guide).

10.5. Procurement and acquisition processes for goods and services

Transparency would also need to be incorporated into all procurement processes of goods and services, complying with the standards established in each country and ensuring the same opportunities for all suppliers.

To transparent the procurement and acquisition processes it would be advisable to:

- Have a section within the website of the emergency and security system where all tenders are published, detailing the requirements, conditions, and deadlines. This information may also be published in other media, as required by law in each country.
- Have a purchasing team that reviews the procurement processes of goods and services and approves only those that are in line with the provisions of the law and its published procedures, requirements, and bases. It would be advisable for this team to consist of the

highest authority of 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.

- Use technicians and experts specialized in each good or service subject to a purchase or contracting process, so that they can provide recommendations and an informed opinion on requirements and specifications, and their compliance by suppliers.

Through the web platform (external), the emergency and security system could publish the results of the purchase and contracting processes (including tenders). In addition, it could be considered to carry out and publish technical evaluations of suppliers and goods and services purchased or hired.

10.6. Internal/external audits

Another mechanism available to demonstrate transparency and institutional management is the periodic execution of audit processes. These would enable timely identifying both financial and operational deviations, formulating correction measures and implementing them through action plans.

Audits could be both internal and external. Internal ones would have to be carried out by a technical area of the organization, specialized in the subject. External audits would have to be carried out 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 the performance and degree of fulfillment of the objectives set out. This verification could be financial, technological, of educational management, data management and security, among others.

It would be important for the entity, in a transparent manner, to publish the results of the audits as part of the actions stipulated in the plan, considering the classification of institutional information. In this way, the process of horizontal and vertical control would be facilitated, including the observers on behalf of the population, civil society organizations and other specific audiences, regarding the management of the emergency and security system.

10.7. Communication plan

The communication plan for an emergency and security system, particularly regarding its organizational component, would have to incorporate objectives, goals, results, and communication actions linked to transparency and accountability.

It would have to take advantage of the use of networks (external web platform and intranet), the media (traditional and social) and other channels available to, based on the data and reports produced by the emergency and security system, be able to communicate and disseminate them for the sake of transparency and institutional accountability.

In line with the above, and as an example, the web platform could be used for the publication and digital availability of data and indicators, reports (management, service, financial and projects), procurement and acquisition processes (from the beginning to the end, going through and accompanying all its stages, including the evaluation of suppliers and contractors), the results of the audits carried out, institutional conferences and press releases, among other content relevant to the transparency and accountability of the emergency and security service.

Traditional and social media could provide the population management balances and regarding the services provided, the 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 by an emergency and security system

10.8. Additional mechanisms

In addition to these specific processes and mechanisms to contribute 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)
- The training of civil servants based on these two Codes, in order to promote professional conduct and actions based on ethical values, linked to honesty, integrity and transparency

The application of transparency and accountability would have to be cross-cutting to the functioning of the System. 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, a Code of Conduct should also be available that defines desirable behaviors at individual level and with regard to interpersonal relationships, between those working for an emergency and security system.

These Codes could be part of the process of induction of new officials, regardless of the type of contract or position, so that they know the purposes and contents of both instruments, as well as the consequences of not respecting them. It may be necessary throughout the professional career of officials of an emergency and security system to update, refresh or deepen training in ethical values, including leadership courses based on high values. Additionally, both Codes may be available to the personnel through the intranet as well as to the general public, through the web (external) platform.