Guía para el Establecimiento y Fortalecimiento de Sistemas Nacionales de Emergencia y Seguridad en los Estados Miembros de la Organización de los Estados Americanos (OEA)

Acerca de la OEA

La Organización de los Estados Americanos (OEA) es el principal foro político de la región, que reúne a todas las naciones independientes del hemisferio occidental para promover conjuntamente la democracia, fortalecer los derechos humanos, fomentar la paz, la seguridad y la cooperación y avanzar en el logro de intereses comunes. Desde su origen, la OEA ha tenido el objetivo principal de prevenir conflictos y proporcionar estabilidad política, inclusión social y prosperidad en la región a través del diálogo y acciones colectivas como la cooperación y la mediación.

Dedicatoria

Con el respeto y la admiración para todos/as los/as funcionarios/as y servidores/as de los sistemas de emergencia y seguridad de los Estados Miembros, y primeros respondientes que, de forma profesional, técnica y comprometida, atienden las emergencias y dan respuesta a las **diferentes situaciones de peligro, además de las amenazas tradicionales y emergentes que se presentan en cada una de las jurisdicciones**. A todos/as aquellos/as que, aún a pesar de los riesgos, siguen dando lo mejor de cada uno/a para mantener a salvo y proteger la vida de las personas que requieren auxilio, **las 24 horas del día los 365 días del año**.

Agradecimientos

La realización de esta Guía fue posible gracias a la colaboración, los aportes, el esfuerzo y la dedicación de un grupo de funcionarios/as de los sistemas de emergencia y seguridad, y agencias afines que trabajan en la región. Todos/as ellos/as se nuclearon en el seno del Grupo Técnico Subsidiario sobre Sistemas de Emergencia y Seguridad (GTS-SES).

Todos/as quienes participaron en este proceso, lo hicieron sin conocerse, trabajando en modalidad virtual, y en el marco de una de las más graves pandemias que ha tenido que enfrentar la humanidad. A pesar de todo lo anterior, asumieron la tarea de redactar esta Guía de manera desinteresada y comprometida. Es por ello que a continuación, en señal de agradecimiento, se reconoce a las personas que estuvieron involucradas en la redacción de los capítulos y que hicieron posible producir esta Guía.

Gracias a su esfuerzo y tesón, el Grupo Técnico Subsidiario sobre Sistemas de Emergencia y Seguridad ha dado cumplimiento a una de las recomendaciones emanadas de la Séptima Reunión de Ministros en Materia de Seguridad Pública de las Américas. De manera colaborativa, colectiva y concertada, el GTS-SES ha elaborado un bien público regional que será de utilidad para todos los países miembros de la Organización de los Estados Americanos (OEA).

A continuación, se presentan las agencias, países y nombres de los/as funcionarios/as que participaron en el proceso de elaboración, revisión y validación de esta Guía. A todo/as ellos/as un reconocimiento especial por el trabajo realizado.

Sistema de Emergencias 9-1-1 de Costa Rica (SE9-1-1 CRI)

Elena Amuy Jiménez, Directora	Carolina Jiménez Rodríguez, Coordinadora Planificación,	
Johnny Hidalgo, Coordinador Logística Operativa	Guiselle Mejía Chavarría[1]	
Luis Fernando Alfaro Ubico, Asesor Legal		

Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1 de República Dominicana

Gral. de Brigada Vicente Mota Medina, ERD, Director Ejecutivo	Lourdes Florentino, Directora Planificación y Desarrollo	Luis Ferrand, Director de Operaciones	Alfredo Arredondo, Director Tecnología[2]
		Tammy Ramírez, Encargada	

[1] Al momento de la publicación de esta Guía, Guiselle Mejía Chavarría ya no forma parte del Sistema de Emergencias 9-1-1, pero mientras se desempeñó como Directora de la entidad, brindó su apoyo, liderazgo y experiencia en el proceso de elaboración de este documento.

[2] Al momento de la publicación de esta Guía, Alfredo Arredondo, Luis Reyes y Mabely Díaz ya no se desempeñan en los cargos señalados, sin embargo, mientras lo hicieron, colaboraron en la redacción de los Capítulos asumidos por el Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1 de República Dominicana.

	Tte. Cnel. Pedro Ventura Chang, FARD, Encargado Departamento Seguridad de Planta	Teresa Garcés, Encargada Departamento de Calidad en la Gestión Agustín Jiménez, Encargado Departamento Desarrollo Institucional	Departamento Recepción de Emergencias Misael Ventura, Encargado Departamento Despacho de Emergencias	Luis Reyes, Encargado Departamento Desarrollo e Implementación de Sistemas[2] Mabely Díaz, Directora Procesamiento de Datos, Análisis y Gestión de Información[2]
	Centro Nacional de Información de México			
SECRETARIADO EJECUTIVO DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA CNI CENTRO NACIONAL DE INFORMACIÓN	David Pérez Esparza, Titular Hernán Salgado, Jefe de Oficina Juan Salazar Dominguez, Director de Área	Oscar Laguna Maqueda, Subdirector de Área Moisés Salas, Subdirector de Área Laura Álvarez Susano, Subdirectora de Área		
	Servicio Integrado de Seguridad ECU-911 de Ecuador			
ECU 911 SERVICIO INTEGRADO DE SEGURIDAD ¡línea única para emergencias!	Juan Zapata, Director General del SIS ECU-911 y Presidente del GTS-SES Marco Garnica, Subdirector Técnico de Doctrina del SIS ECU-911 Bolívar Tello, Subdirector Técnico de Operaciones del SIS ECU-911 Angélica Buñay, Analista de Operaciones del SIS ECU911 Rosana Malta, Especialista de Salud y Seguridad Ocupacional del SIS ECU-911	Gary Almeida, Director Nacional Regulatorio en Emergencias del SIS ECU-911 Celia Gómez, Especialista Nacional Regulatorio en Emergencias del SIS ECU911 Elisa Bravo, Directora de Procesos y Control de Calidad del SIS ECU-911 Wilfrido Muñoz, Director Nacional de Comunicación Social del SIS ECU-911 Cassandra Arciniegas, Especialista de Coordinación Interinstitucional del SIS ECU-911		
	Sistema de Emergencias 9-1-1 de Paraguay			
EMERGENCIA 911 POLICIAL	Liliana Díaz, Directora General Daniel Rojas, Coordinador de Fortalecimiento	Carlos Román, Soporte Técnico Nilse Molinas, Soporte Técnico		

Asimismo, es necesario reconocer el valioso apoyo brindado por dos de las asociaciones más prestigiosas en apoyar, asesorar y acompañar a los sistemas de atención y respuesta a emergencias como los son el EENA y el NENA México-Latinoamérica. Su participación en el proceso de validación externa significó un segundo control de calidad, fortaleciendo aún más la rigurosidad técnica de los contenidos de la Guía.

Cristina Lumbreras, Directora Técnica

Leonardo Dorony, Presidente

La excelencia, la rigurosidad y el temple de Patricio Tudela quien, como consultor externo, acompañó las etapas de revisión, edición y validación de la Guía, inclusive haciendo aportes sustantivos en varios de sus capítulos, también merecen ser reconocidos.

La planificación y elaboración de esta Guía estuvo a cargo de la Jefa de la Sección de Información y Conocimiento del Departamento de Seguridad Pública de la OEA, Karen Bozicovich.

Este documento fue elaborado por el Departamento de Seguridad Pública de la OEA con las contribuciones del Sistema de Emergencias 9-1-1 de Costa Rica (SE9-1-1 CRI), el Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1 de República Dominicana, el Centro Nacional de Información de México, el Servicio Integrado de Seguridad ECU-911 de Ecuador y el Sistema de Emergencias 9-1-1 de Paraguay. La orientación técnica general del documento estuvo a cargo del Servicio Integrado de Seguridad ECU-911 de Ecuador.

Los lineamientos, sugerencias y recomendaciones expresados en este documento corresponden a los/as autores/as de cada capítulo y no reflejan necesariamente las posiciones oficiales de los países miembros de la OEA.

Mayo 2021.

Editores generales: Karen Bozicovich y Patricio Tudela
Diseño y diagramación: Giovanny Guzmán

Índice de Contenidos

Índice de Tablas y Figuras

Acrónimos

ANS		Acuerdo de Niveles de Servicio
ANSI	*American National Standards Institute*	Instituto Estadounidense de Estándares Nacionales
APCO	*Association of Public-Safety Communications Officials*	Asociación de Oficiales de Comunicaciones de Seguridad Pública
APM	*Association for Project Management*	Asociación para la Gestión de Proyectos
ATR	*Action Taken Report*	Reporte de Decisiones Adoptadas
ATS	*Automatic Transfer Switch*	Tablero de Transferencia Automática
AL	*Automatic Vehicle Location*	Localización vehicular automatizada
BSC	*Balanced Score Card*	Cuadro de Mando Integral (CMI)
BIA	*Business Impact and Analysis*	Análisis de Impacto en el Negocio
CACH	*Computer Aided Call Handling*	Manejo de Llamadas Asistido por Computadora
CAD	*Computer Aided Dispatch*	Despacho Asistido por Computadora/Sistema de despacho asistido computarizado
CAES		Centro de Atención de Emergencia y Seguridad
COBIT	*Control Objectives for Information Technologies*	Objetivos de Control para la Información y Tecnologías Afines
CTI	*Computer Telephony Integration*	Sistema de Recepción de Llamadas de Emergencias
DSS	*Decision Support System*	Sistema de Apoyo para Decisiones
EENA	*European Emergency Number Association*	Asociación Europea del Número de Emergencia
EFQM	*European Foundation Quality Management*	Fundación Europea para la Gestión de la Calidad
EIS	*Executive Information System*	Sistema de Información Ejecutiva
ETSI	*European Telecommunications Standards Institute*	Instituto Europeo de Normas de Telecomunicaciones
FCE		Factores Claves para el Éxito
FTP	*File Transfer Protocol*	Protocolo de Transferencia de Archivos
GIS	*Geographic Information System*	Sistema de Información Geográfica
GPS	*Global Positioning System*	Sistema de posicionamiento global
IAED	*International Academies of Emergency Dispatch*	Academia Internacional de Despachado de Emergencia
IFT		Instituto Federal de Telecomunicaciones
IP	*Internet Protocol*	Protocolo de Internet
ISACA	*Information Systems Audit and Control Association*	Asociación de Auditoría y Control de Sistemas de la Información
ISO	*International Organization for Standardization*	Organización Internacional para la Estandarización
KPI	*Key Performance Indicator*	Indicadores Claves de Gestión
MDC	*Mobile data computers*	Equipos de comunicación móvil de datos
MDT	*Mobile data terminals*	Equipo de comunicación móvil
NENA	*National Emergency Number Association*	Asociación Nacional del Número de Emergencia
NFPA	*National Fire Protection Association*	Asociación Nacional de Protección contra el Fuego de Estados Unidos
NISO	*National Information Standards Organization*	Organización de Estándares Nacionales de Información de Estados Unidos
NOC	*Network Operation Center*	Centro de Control de Redes
OIT		Organización Internacional del Trabajo
OLAP	*On-line analytical processing*	Procesamiento analítico en línea

PABX	*Private Automatic Branch Exchange*	Central Privada Automática
PCO		Plan de Continuidad de las Operaciones
PMBOK	*Project Management Body of Knowledge*	Conjunto de Conocimientos sobre la Gestión de Proyectos
PMI	*Project Management Institute*	Instituto para la Gestión de Proyectos
PRAM	*Project Risk Analysis and Management*	Guía de Análisis y Gestión de Riesgos
PRD		Plan de Recuperación ante Desastres
PRV	*Primary Response Vehicle*	Reporte de Estado de Unidades/Vehículos Disponibles
PSAP	*Public Safety Answering Point*	Punto de Respuesta de Seguridad Pública
SCI		Sistema de Comando de Incidentes
SIG		Sistemas de Información Geográfica
SGSI		Sistemas de Gestión de la Seguridad de la Información
SMS	*Short Message Service*	Servicio de Mensajes Cortos
TIA	*Telecommunications Industry Association*	Asociación de la Industria de Telecomunicaciones de Estados Unidos
TIC		Tecnologías de la Información y la Comunicación
TTY	T*eletypewriter*	Dispositivo/Teletipo
ITU	*International Telecommunication Union*	Unión Internacional de Telecomunicaciones
VMS	*Video Management Software*	Software de Gestión de Video
VOIP	*Voice Over Internet Protocol*	Voz Sobre Protocolo de Internet

Glosario

Actores de apoyo (Instituciones vinculadas o Instituciones del segundo anillo)	Organismos/instituciones estatales o del sector privado y asociaciones de la sociedad civil que actúan como entidades de apoyo y que resultan vitales en situaciones críticas o para el aseguramiento de la continuidad de servicios esenciales. Estas pueden ser entidades encargadas de segmentos específicos de la población o especializadas en temáticas puntuales, como aquellas relacionadas con las personas adultas mayores, personas con discapacidad y violencia de género, entre otros sectores de atención prioritaria o específica; entidades encargadas de la prestación de servicios básicos, incluyendo: agua potable, electricidad, provisión de alimentos, educación, entre otras.
Actores para la primera respuesta (Instituciones articuladas o Instituciones del primer anillo)	Organismos/instituciones estatales o del sector privado responsables de llevar a cabo las funciones esenciales de un sistema de emergencia y seguridad, que atienden directamente y responden a los diferentes tipos de emergencias (tránsito y movilidad; seguridad ciudadana/pública; atención de salud física y mental, sanitarias; gestión de incendios, siniestros y desastres).
Actores subsidiarios (Instituciones del tercer anillo)	Organismos/instituciones estatales y una diversidad de actores públicos, privados y de la sociedad civil, que tienen un rol complementario y procuran generar condiciones y capacidades para el funcionamiento de un sistema de emergencia y seguridad. Ejemplos de actores subsidiarios serían: organismos internacionales, organizaciones de la sociedad civil, sector empresarial, sector académico, sector de medios de comunicación, entre otros.
Acuerdo de prestación de servicio	Contrato o decisión entre las partes que conforman un sistema de emergencia y seguridad, que define qué servicios proporcionará cada una de las entidades y los estándares que se deberán cumplir para la prestación de estos.
Alerta	Aviso, llamada o señal sobre un incidente que sucedió, que está ocurriendo o que está por suceder, y que ingresa al sistema de emergencia y seguridad por cualquiera de las vías, canales o medios de comunicación establecidos.
Alerta de emergencia	Mensaje dirigido por las entidades que brindan y gestionan la atención de servicios de emergencias, a través de cualquier medio, plataforma o tecnología. Dicho mensaje puede ser dirigido de forma masiva a nivel nacional, subnacional o zonal, o a un grupo de personas, dependiendo del tipo de emergencia y de la situación que se presente.
Alta disponibilidad	Es un protocolo de diseño que, al ser implementado, denota que la infraestructura tecnológica de un sistema de emergencia y seguridad puede

	ser resistente a las interrupciones y fallas del sistema eléctrico, y seguir funcionando y prestando servicios a la población.
Análisis de riesgo	Estudio para identificar y evaluar peligros y amenazas potenciales y comprender sus posibles consecuencias, efectos, impactos o daños, enfocado ya sea en la planificación, un proyecto, un proceso, un servicio, el personal o una instalación, con el objeto de establecer medidas de prevención, protección y mitigación. Una de las herramientas típicamente utilizada para el análisis de riesgo es la matriz de riesgo.
Áreas funcionales	Forma de agrupar y organizar actividades de carácter homogéneo e interrelacionadas, que corresponden a la estructura de un sistema de emergencia y seguridad. Pueden clasificarse en dos tipos. Áreas funcionales principales o misionales porque su actividad y el trabajo que realizan resultan críticos para cumplir con la razón de ser de un sistema de emergencia y seguridad. Entre las áreas funcionales principales o misionales se podrían considerar las siguientes: Gestión de Operaciones, Gestión de Procesos y Protocolos, Gestión de Calidad, Tecnologías de la Información y la Comunicación, Gestión de Seguridad y Gestión de Información y Análisis. El segundo tipo de áreas funcionales son aquellas que fungen de apoyo o de soporte, incluyendo: Talento Humano, Administración y Finanzas, Jurídica, Comunicación, Planificación Estratégica y Operativa, y Gestión de Proyectos.
Cuadro de Mando Integral (CMI)	Enfoque y metodología de gestión para la planificación estratégica, que traslada la estrategia y visión de la organización en acción. Convierte los objetivos, metas y actividades en un conjunto de indicadores para dar seguimiento y medir el desempeño total de la organización, y por perspectivas, incluyendo: la perspectiva financiera, perspectiva de clientes/usuarios, perspectiva de procesos internos y perspectiva de aprendizajes para el crecimiento.
Cadena de custodia	Conjunto de actividades y procedimientos secuenciales que se aplican en la protección y aseguramiento de los indicios y/o evidencias físicas y digitales, desde la recepción de la llamada o el registro de video vigilancia, la localización en la escena del delito o lugar de los hechos, hasta su presentación ante la instancia judicial.
Ciclo de la información	Proceso orientado al aprovechamiento de la información en cada uno de los tres niveles de funcionamiento de un sistema de emergencia y seguridad (estratégico, táctico y operativo) para orientar la toma de decisiones y cumplir con los objetivos establecidos. Está compuesto por una serie de etapas, guiadas por normas, estándares y procedimientos, y agilizadas o facilitadas por el empleo de *software*.

Confidencialidad	Calificación de la información que restringe el acceso, uso, disponibilidad y divulgación a personas, organismos o entidades no autorizados.
Despachador/a	Persona encargada de la asignación de unidades, recursos o dispositivos para la atención oportuna de una emergencia, contingencia o incidente que genera una alerta al servicio de atención de emergencias.
Despacho asistido por computadora	Sistema computarizado para recibir llamadas, despachar los recursos necesarios para la atención de emergencias al lugar donde están ocurriendo y según el tipo de incidente, proporcionar actualizaciones periódicas sobre el estatus de la emergencia a partir de las acciones que se están llevando a cabo en terreno, y analizar, de manera integral, los servicios prestados. Comúnmente se lo conoce y denomina con el acrónimo CAD (*computer assisted dispatch*).
Despacho de recursos	Unidad o actividad que involucra elegir y asignar el recurso disponible y necesario para la atención de una emergencia, contingencia o incidente, según el tipo. Suele realizarse por medio de un sistema o plataforma tecnológica (ver definición de despacho asistido por computadora). Adicionalmente, también se utiliza despacho de unidades y despacho de dispositivos.
Emergencia	Situación imprevista, contingencia o incidente reportado al sistema de emergencia y seguridad por diferentes vías, canales o medios de comunicación establecidos, que afecta o pone en peligro la vida o integridad de las personas y/o los bienes, y que por lo tanto requiere una respuesta inmediata y efectiva. Existen diferentes tipos de emergencias, incluyendo de seguridad pública/ciudadana, salud física y mental, sanitaria, desastres y siniestros, seguridad nacional y eventos programados. También se utilizan palabras como evento, contingencia o incidente para referirse a una situación de emergencia.
Eventos programados	Eventos cuya ocurrencia se conoce con antelación y que requieren de la activación anticipada de los sistemas de emergencia y seguridad para informar y comunicar a la población sobre el estado y la evolución de estos, y prevenir y actuar de manera oportuna ante posibles incidentes que se pudieran desprender del evento.
Ficha multidespacho	Herramienta electrónica del sistema que requiere llenar campos obligatorios por parte del/a operador/a en una ficha o formulario electrónico y que permite su envío simultáneo a dos o más instituciones articuladas de respuesta.
Ficha ordinaria	Herramienta electrónica del sistema que requiere llenar campos obligatorios por parte del/a operador/a en una ficha o formulario

	electrónico para luego ser enviada al despachador/a de una institución articulada específica.
Gestión de la calidad	Enfoque de gestión y de cultura organizacional dirigido a la satisfacción de los requerimientos y las necesidades de los/as usuarios/as a través de la mejora continua de los servicios que brinda un sistema de emergencia y seguridad con base en estándares internacionales y nacionales definidos para tales fines.
Gestión de riesgos	Procesos establecidos y administrados de manera integral para la identificación, análisis de vulnerabilidades, de probabilidad e impacto y el diseño de respuestas frente a factores de riesgo emergentes, presentes y futuros, que pudieran amenazar la implementación del plan estratégico, el funcionamiento de un sistema de emergencia y seguridad, la prestación de los servicios, la vida y la seguridad del personal y las instalaciones. Podría formar parte o contribuir a la gestión de calidad de un sistema de emergencia y seguridad.
Información	Uno de los activos más importantes de un sistema de emergencia y seguridad que puede manifestarse de diversas formas: textual, numérica, gráfica, tabular, cartográfica o narrativa, y en cualquier medio: magnético, papel, electrónico, audiovisual y otros. La clasificación, protección, acciones de monitoreo y control de la información pueden seguir las pautas establecidas por estándares internacionales y nacionales definidos para tales fines.
Interoperabilidad	Capacidad de los sistemas de información, y de los procedimientos que le dan soporte, de compartir datos e intercambiar información sin restricciones y/o limitaciones, bajo la administración y control de las partes interesadas.
Línea de base (o línea basal)	Es el primer paso del monitoreo y la evaluación. Permite dar cuenta de la situación/estado inicial en que se encuentra el sistema, o un componente de este, antes de iniciar una intervención, reforma o cambio. Se suelen utilizar una serie de variables e indicadores para establecerla.
Llamada efectiva/ procedente	Llamada que está asociada a una emergencia y como tal, amerita su atención y, cuando corresponda, la movilización de recursos, unidades o dispositivos a terreno, y la coordinación oportuna con las instituciones articuladas.
Llamada no efectiva/ no procedente	Llamada que no obedece a una emergencia, que puede ser de broma, marcación incorrecta o no intencionada, consultas no relacionadas a emergencias, mal uso del servicio de emergencias o problemas de comunicación, que no requieren de la atención o desplazamiento de

	recursos, unidades o dispositivos de las instituciones de respuesta articuladas.
Mal uso del servicio	Solicitudes, llamadas y reportes receptados por el sistema de emergencia y seguridad, que obedecen al uso indebido, malintencionado, doloso o que implique la obstaculización y uso innecesario de los recursos materiales y humanos del sistema.
Mapa de procesos	Representación gráfica de los procesos del sistema de emergencia y seguridad, permitiendo identificar y enfocar la atención en aquellos considerados críticos para la operación del sistema.
Mapa estratégico	Herramienta que sirve para visualizar y dar seguimiento a la relación causa-efecto entre los objetivos trazados y los ejes estratégicos, planes y componentes que se hubieran establecido como resultado del proceso de planificación.
Matriz de riesgo	Herramienta que permite visualizar contingencias, eventos o incidentes negativos; la probabilidad de ocurrencia y sus posibles impactos sobre el sistema de emergencia y seguridad, la implementación de su plan estratégico, su personal, su funcionamiento (procesos y servicios) y sus instalaciones; y las estrategias de respuesta, incluyendo medidas de prevención, mitigación y respuesta. Asimismo, la matriz también facilita el monitoreo, control y la gestión de los riesgos. Está ligada al proceso de análisis de riesgo.
Mejora continua	Proceso sistemático de recolectar, analizar, utilizar y documentar información para dar seguimiento a las acciones destinadas a la elaboración de un producto o la prestación de un servicio y que tiene como finalidad identificar medidas de corrección o mejoramiento que mantengan al sistema en línea con los estándares establecidos en protocolos o instrumentos de referencia.
Mensajes pregrabados	Mensajes cortos, de voz o de texto, para comunicar e informar a la población acerca de situaciones de emergencia en curso o eventos programados. Uno de los principales motivos para la utilización de este tipo de mensajes es evitar el congestionamiento de la línea y demás canales para reportar una emergencia
Niveles de priorización	Categorización vinculada a la estimación del riesgo de las solicitudes, llamadas y reportes recibidos por el sistema de emergencia y seguridad, basada en las características y complejidad del incidente o contingencia, y que deriva en una priorización de atención.

Operador/a	Persona encargada de recibir, categorizar, indagar, apreciar y direccionar, en base a lineamientos y procedimientos establecidos, las solicitudes, llamadas o reportes que ingresan al sistema de emergencia y seguridad.
Plan de contingencia	Conjunto de procesos, pasos y acciones planificados que se activan frente a una contingencia que afecta el funcionamiento de un sistema de emergencia y seguridad para minimizar el tiempo fuera de servicio de la entidad y maximizar el tiempo de su recuperación.
Plan de continuidad de operaciones	Plan de emergencia que, a partir de la identificación y el análisis de los riesgos, y de la identificación de los procesos críticos y esenciales para el funcionamiento de un sistema de emergencia y seguridad, establece los procesos, pasos y acciones a tomar, así como también la asignación de responsabilidades, para garantizar y recuperar la operación del sistema ante cualquier contingencia.
Plan de recuperación ante desastres	Proceso planificado y testeado de recuperación, que cubre los datos, el *hardware* y *software* considerados críticos y esenciales en lo que respecta al funcionamiento de un sistema de emergencia y seguridad, para que este pueda reestablecer nuevamente sus operaciones en caso de haber sido afectado por una contingencia.
Procesos	Conjunto y secuencia de pasos y acciones a seguir en la prestación de un servicio, cumplimiento de una tarea o realización de una actividad. Hay dos tipos de procesos: los procesos críticos y los procesos de apoyo. Los procesos críticos son una serie pasos y acciones que tienen lugar en las áreas funcionales principales o misionales de un sistema de emergencia y seguridad, sin los cuales este no podría atender ni dar respuesta a las emergencias que se reportan. Los procesos de apoyo también son una serie de pasos y acciones pero estos se llevan a cabo en las áreas secundarias o de soporte, y sustentan el funcionamiento administrativo del sistema.
Protocolos	Instrumentos normativos que establecen qué se debe hacer y cómo se debe proceder y actuar frente a diferentes situaciones/contextos. Contienen una serie de reglas, instrucciones y procedimientos a seguir en la prestación de un servicio, cumplimiento de una tarea o realización de una actividad.
Reporte	Comunicación verbal o escrita que informa las características y circunstancias relacionadas con una emergencia.
Riesgo	Circunstancia o suceso que ante una vulnerabilidad tiene el potencial de causar peligro, daño o pérdida, y de amenazar el funcionamiento de un sistema de emergencia y seguridad. Se lo concibe como una combinación de la probabilidad de ocurrencia de una circunstancia o suceso y su

	impacto. Suele ser objeto de análisis, que tiende a volcarse en matrices, y ambos, (tanto el análisis como la matriz de riesgo), sirven para su gestión.
Seguridad de la información	Conjunto de medidas preventivas, proactivas y reactivas encaminadas a la preservación de la confidencialidad, integridad y disponibilidad de la información.
Sistema de Información Geográfica	Programa informático (*software*) para ingresar, integrar, analizar, compartir, visualizar, recuperar y almacenar datos e información geográficamente referenciada o con una referencia espacial. Suele ser una herramienta informática clave para la ubicación, atención y gestión de las emergencias.
Supervisor/a (o Coordinador/a)	Persona encargada de monitorear y controlar las actividades que realizan las personas operadoras y/o despachadoras del sistema de emergencia y seguridad, así como de la calidad del servicio que se brinda, basándose en los protocolos y estándares de referencia establecidos.
Unidades de respuesta (recursos o dispositivos)	Son los componentes de asistencia y concurrencia a una emergencia, compuesto por personas, vehículos y herramientas. Adicionalmente, también se utilizan las palabras recursos y dispositivos.
Usuario/a	Persona que solicita ayuda ante una emergencia, incidente o contingencia que sucedió, que está ocurriendo o que está por suceder, y que hace uso de los servicios que brinda un sistema de emergencia y seguridad.
Video operador/a	Persona encargada de monitorear y visualizar las cámaras bajo su cargo, para detectar y categorizar posibles incidentes que requieran respuesta o asistencia inmediata, y analizar, evaluar y direccionar recursos para su atención.
Vulnerabilidades	Debilidad o capacidad disminuida de un activo, sistema, proceso o herramienta que puede representar un riesgo y ser aprovechada por una o más amenazas generando un potencial efecto negativo.

Prólogo del Director General del SIS ECU-911, Ingeniero Juan Zapata Silva

El fortalecimiento de la cooperación internacional en seguridad pública, tratado durante la Séptima Reunión de Ministros en Materia de Seguridad Pública de las Américas (MISPA VII), realizada en Quito en octubre del año 2019, fue una gran oportunidad para socializar y plantear alternativas sobre un tema común: la prevención y la lucha contra la delincuencia organizada.

El proceso MISPA —que promueve la Organización de los Estados Americanos (OEA) y que cuenta con la participación de las principales autoridades y expertos de seguridad a escala nacional e internacional— permite conocer temas básicos como gestión de la seguridad integral; prevención de la delincuencia, violencia e inseguridad; gestión policial; y participación ciudadana y comunitaria sustentadas en la cooperación internacional. En la Séptima Reunión, por primera vez desde que se instalara este foro de Ministros en Materia de Seguridad Pública en 2008, se abordó el tema de la atención y respuesta a las emergencias, impulsado por el Ecuador a través del Servicio Integrado de Seguridad ECU-911 (SIS ECU-911).

Como Presidente del Grupo Técnico Subsidiario sobre los Servicios de Emergencia y Seguridad, establecido como resultado de las recomendaciones emanadas de la MISPA VII, considero oportuna la Guía que se desarrolló en el seno del mismo y que se presenta en esta publicación. La misma está orientada hacia el fortalecimiento de la cooperación internacional en materia de sistemas integrados de atención y respuesta a emergencias. La Guía sistematiza una serie de lineamientos, mecanismos y herramientas que se ponen a disposición de todos los Estados Miembros de la OEA a modo de sugerencias técnicas, basadas en la práctica y la experiencia de todos quienes participaron en su elaboración.

En un tiempo complejo, producto de la crisis sanitaria mundial por el COVID-19 y sus múltiples impactos, en donde los sistemas de atención y respuesta a emergencias han desempeñado un papel clave, esperamos que esta Guía sirva como herramienta útil y accionable para orientar procesos de creación o de fortalecimiento de este tipo de servicios en los países miembros de la Organización.

La elaboración de esta Guía es producto de la cooperación internacional. En ese sentido, valoramos el apoyo y el compromiso de países como: Costa Rica, México, Paraguay y República Dominicana. Cada uno de los países que apoyamos esta iniciativa, hemos colocado por delante las experiencias de nuestros servicios de emergencia y seguridad que permitan trascender en el tiempo en materia de seguridad integral, el diseño de un instrumento técnico-práctico que pretende sugerir acciones y establecer mecanismos orientados a la racionalización de los recursos y logística con los que cuentan los servicios de emergencia y seguridad, a fin de optimizar la atención a la población.

El contar con esta Guía y la posibilidad de compartirla con los demás Estados Miembros de la OEA, abre la oportunidad de compartir experiencias y conocimientos para enfrentar emergencias y amenazas comunes. Viabiliza también el espacio para homologar buenas prácticas en relación a las respuestas e intervenciones dirigidas a salvaguardar y proteger la vida e integridad de las personas.

De esta forma se ratifica el compromiso asumido y confiamos que a corto plazo se puedan suscribir acuerdos que permitan promover el establecimiento del número único de emergencias 9-1-1 en cada país del hemisferio, con procedimientos estandarizados para la atención y coordinación de emergencias en la región.

Se han generado acciones importantes, pero restan muchas iniciativas adicionales para consolidar un continente con altos niveles de seguridad ciudadana, convivencia pacífica y orden público.

Prólogo del Secretario General de la OEA, Luis Almagro

En la región de las Américas existen varios modelos de funcionamiento para la atención y respuesta a las emergencias. Existen también diversos niveles de avances entre los países de la región en relación con la integración de los servicios y la interoperabilidad entre estos, la cobertura territorial, la estandarización y protocolización de los procesos operativos, la infraestructura tecnológica para la información y la comunicación y el soporte informático con el que cuentan, entre otros aspectos diferenciadores. Además, no todos los países manejan un número único para recibir solicitudes de auxilio por parte de la población.

Esta asimetría y riqueza de experiencias en el hemisferio abre un espacio de trabajo interesante y necesario a nivel interamericano y desde el ámbito multilateral.

La atención y respuesta a emergencias es un tema novedoso y de reciente incorporación en el marco de la Organización de los Estados Americanos. El Ecuador, a través de su Servicio Integrado de Seguridad ECU-911 (SIS ECU-911), fue uno de los principales impulsores del posicionamiento del tema a nivel regional, en los diversos foros de la OEA y en el trabajo de la Secretaría General de la OEA a través de su Departamento de Seguridad Pública.

El evento fundacional para la inclusión del tema en la agenda hemisférica de seguridad y al interior de la Organización fue el Seminario Internacional sobre Mecanismos y Herramientas de Cooperación sobre los Servicios de Emergencia en la Región, organizado por el SIS ECU-911 en abril de 2019. Allí se presentaron una serie de propuestas de consenso, incluyendo la creación de un Grupo Técnico Subsidiario sobre los Sistemas de Emergencia y Seguridad (GTS-SES), y la elaboración de una Guía para el Establecimiento y Fortalecimiento de Sistemas Nacionales de Emergencia en los Estados Miembros de la OEA. Estas propuestas fueron luego recogidas y adoptadas por los Ministros en Materia de Seguridad Públicas de las Américas como parte del documento de recomendaciones que aprobaron en su Séptima Reunión, realizada en Quito, Ecuador en octubre de 2019.

Es a partir de esas recomendaciones y en el marco del Grupo Técnico Subsidiario sobre Sistemas de Emergencia y Seguridad (GTS-SES) que, con el liderazgo del SIS ECU-911 y el apoyo técnico ofrecido por el Departamento de Seguridad Pública, se reunieron las condiciones de base necesarias para viabilizar la redacción de esta Guía.

Esta Guía está dirigida a todos los países de la región, ya sea para la creación de sistemas nacionales integrados de emergencia y seguridad o para el fortalecimiento de los ya existentes. Es justamente en función de las asimetrías y divergencias existentes entre los países de la región en lo que respecta a los servicios de atención y respuesta a emergencias que esta Guía espera contribuir a la reducción de algunas de esas brechas, en aras de posibilitar una mayor integración entre los sistemas.

La elaboración de esta Guía es un hito que merece ser celebrado por varios motivos. En primer lugar, porque es el producto de la colaboración y coordinación de cinco instituciones: el Sistema de Emergencia 911 de Costa Rica, el Sistema Nacional de Emergencias y Seguridad 911 de República Dominicana, el Centro Nacional de Información de México, el Servicio Integrado de Información ECU-911 y el Sistema de Emergencias 911 de Paraguay, cada una de ellas aportando, desde su conocimiento y experiencia, con la redacción de entre uno hasta cuatro capítulos. Segundo, porque esa coordinación se llevó a cabo en el marco de una pandemia sin precedentes en los últimos 100 años de la historia de la humanidad. La misma colocó a todos los/as primeros/as respondientes y personal de salud en una situación de alerta, atención y servicio permanente, para intentar salvar la mayor cantidad de vidas posibles. A pesar de esa exigencia y de esa responsabilidad, estas cinco instituciones lograron producir esta Guía. Tercero, porque el resultado es una contribución concreta, valiosa y utilizable para los demás países y Sistemas de la región.

Una especie de bien público regional que se pone a disposición de todos y todas quienes trabajan en la atención y respuesta a emergencias para establecer, mejorar o fortalecer los servicios que brindan a la población.

El poder contar con esta Guía revaloriza y enaltece los espacios colectivos de trabajo existentes como parte de la estructura operativa y técnica de la OEA. Es desde estos lugares multilaterales, poblados por personas con vocación de servicio, capacidad, experiencia y conocimiento, que es posible generar productos de valor y de referencia, como lo es esta Guía, para la utilización y el beneficio de los Estados Miembros.

Con el liderazgo del Ecuador a través del SIS ECU-911 y la preparación de esta Guía, el Grupo Técnico Subsidiario sobre los Servicios de Emergencia y Seguridad ha tenido un comienzo auspicioso y productivo. Desde la Secretaría General de la OEA esperamos que este sea el primero de muchos productos que guíen a los países de la región en la maximización de las capacidades de sus sistemas de emergencia y seguridad en aras de una mayor calidad, excelencia y profesionalismo en la prestación de este tipo de servicios, y teniendo en la mira un escenario de mayor cooperación e integración entre ellos.

Presentación

La Guía para el Establecimiento y Fortalecimiento de Sistemas Nacionales de Emergencia y Seguridad en los Estados Miembros de la Organización de los Estados Americanos (OEA) nació como una propuesta del Servicio Integrado de Seguridad ECU-911 (SIS ECU-911) del Ecuador. La misma fue presentada en el marco del Seminario Internacional sobre Mecanismos y Herramientas de Cooperación sobre los Servicios de Emergencia y Seguridad de la Región, que tuvo lugar en la ciudad de Quito, Ecuador los días 25 y 26 de abril de 2019. En esa ocasión se presentó una propuesta de índice con 10 capítulo, que fue puesta a consideración de las delegaciones participantes.

El Seminario Internacional resultó en un documento de propuestas de consensos, entre las cuales se le encomendó al Grupo Técnico Subsidiario sobre Servicios de Emergencia y Seguridad (GTS-SES) el desarrollo de la Guía.

El documento de propuestas de consensos fue transmitido al proceso preparatorio de la Séptima Reunión de Ministros en Materia de Seguridad Pública de las Américas a través de la Comisión de Seguridad Hemisférica. Es así como las propuestas alcanzadas en el marco del Seminario Internacional quedaron incorporadas en las Recomendaciones de Quito para el Fortalecimiento de la Cooperación Internacional en Materia de Seguridad Pública en la Prevención y Lucha contra la Delincuencia, aprobadas el 31 de octubre de 2019. Entre las 19 recomendaciones aprobadas por los Ministros en Materia de Seguridad Pública de las Américas en aquella ocasión, se incluyó la planificación del trabajo del GTS-SES por parte del Departamento de Seguridad Pública (DSP), haciendo especial énfasis en el objetivo de finalizar la Guía para el Establecimiento y Fortalecimiento de Sistemas Nacionales de Emergencia y Seguridad en los Estados Miembros de la OEA.

De esta manera, una vez establecido el GTS-SES bajo la presidencia del SIS ECU-911, se organizó una primera reunión de planificación el 3 de marzo del 2020 en la que se acordó que el DSP elaboraría un Plan de Trabajo. El 13 de marzo, el DSP presentó una planificación de actividades para el GTS-SES con cuatro actividades, incluyendo la elaboración de la Guía. Sobre esta se decidió que se trabajaría de manera colectiva y conjunta, invitando a otros Sistemas de Emergencia y Seguridad, e instituciones relacionadas, a participar del proceso, colaborando en la redacción de uno o más capítulos.

Sin embargo, la categorización de la enfermedad por coronavirus como una pandemia por parte de la Organización Mundial de la Salud (OMS) el 11 de marzo, significó retrasar el inicio de la redacción de la Guía, y reenfocar los esfuerzos del GTS-SES en dar algún tipo de respuesta, acompañamiento y apoyo a los Sistemas de Emergencia y Seguridad de la región en el enfrentamiento del COVID-19.

Frente a ese nuevo escenario, el SIS ECU-911, en ejercicio de la presidencia del GTS-SES, y el Departamento de Seguridad Pública, en calidad de Secretaría Técnica del mismo, tomaron la iniciativa de crear una Comunidad Virtual, en el marco del Portal Educativo de las Américas, para que los/as funcionarios/as de los Sistemas de Emergencia y Seguridad de la región pudieran compartir, intercambiar y consultar materiales que pudieran ser útiles para dar respuesta a la emergencia de salud pública ocasionada por el coronavirus. La Comunidad Virtual de los Sistemas de Emergencia y Seguridad (Comunidad-SES), a su vez, vino acompañada de un ciclo de conversatorios virtuales. En el marco de dicho ciclo, en el 2020 se organizaron cuatro conversatorios dirigidos a los miembros de la Comunidad, sobre temas relacionados con la pandemia.

El desarrollo de la Guía fue retomado en junio de 2020. Es así como el 8 de junio se contactaron a las autoridades de Costa Rica, México, Paraguay y República Dominicana, vinculadas a la atención y respuesta a emergencias, para invitarlas a participar del proceso de elaboración de la Guía, solicitándoles que

eligieran uno o más capítulos sobre los cuales trabajar. A medida que dichas autoridades fueron respondiendo a las cartas enviadas, se fueron asignando los 10 capítulos que componen la Guía.

El 19 de junio se realizó una reunión de coordinación entre el SIS ECU-911 y el DSP de la OEA (DSP/OEA). Allí se presentó la asignación de los 10 capítulos entre las cinco instituciones participantes: Sistema de Emergencia 911 de Costa Rica (Capítulo 1), Sistema Nacional de Emergencias y Seguridad 911 de República Dominicana (Capítulos 2, 3, 8 y 10), Centro Nacional de Información (Capítulos 4 y 8), Servicio Integrado de Seguridad ECU-911 (Capítulos 5, 7, 8 y 9) y el Sistema de Emergencias 911 de Paraguay (Capítulo 6).

En esa reunión, el DSP hizo una serie de propuestas para consideración del SIS ECU-911, incluyendo: una planificación de 7 etapas, cubriendo los meses desde julio del 2020 hasta mayo del 2021; y lineamientos generales para la elaboración de la Guía, abarcando aspectos como el enfoque/perspectiva que se sugería adoptar, el formato, el estilo de redacción y la forma de guardado, entre otros. Adicionalmente se creó una carpeta compartida en Google Drive, dándole acceso a todos/as los/as funcionarios/as involucrados/as en el proceso de elaboración de la Guía. Allí se pusieron a disposición todos los documentos vinculados al proceso, incluyendo los lineamientos generales y de planificación de la Guía, y se fueron subiendo las sucesivas versiones de los capítulos elaborados.

Una vez obtenido el aval del SIS ECU-911 a las propuestas realizadas por el DSP/OEA, las mismas fueron presentadas a las instituciones participantes, en una reunión de planificación realizada el 1 de julio del 2021. Esa reunión puede concebirse como el punto de partida del proceso colectivo y conjunto de elaboración de la Guía, activando de esa manera la primera etapa. Como parte de esa primera etapa, se sostuvieron reuniones individuales con las cinco instituciones participantes para revisar el índice del o de los capítulo/s asignado/s, acordar los contenidos que se esperaban abarcar en cada capítulo, repasar los lineamientos generales de elaboración y evacuar cualquier duda que los equipos pudieran tener respecto a la Guía y al proceso de elaboración.

La segunda etapa de redacción de los capítulos se extendió entre agosto del 2020 y enero del 2021. Esta etapa incluyó varios flujos de ida y vuelta entre las instituciones redactoras de los capítulos y el equipo de revisión y edición del Departamento de Seguridad Pública. El mismo estuvo conformado por la Sección de Información y Conocimiento del DSP y un consultor externo con amplia y reconocida experiencia y conocimientos en el tema.

Una vez que se obtuvo un primer borrador de la Guía, se organizó un proceso de revisión interna, con las propias instituciones participantes (tercera etapa). En esta etapa, habiendo leído la Guía en su totalidad, como un producto integral, los equipos de cada país pudieron compartir y remitir sus comentarios y sugerencias al primer borrador.

La tercera etapa de revisión fue seguida por una cuarta etapa de validación, que consistió en someter el primer borrador de la Guía al escrutinio del EENA y del NENA México-Latinoamérica. Para ello, además de recibir sus comentarios por escrito, se organizaron dos reuniones de trabajo con dos representantes de las mencionadas organizaciones, para que también pudieran hacer una devolución y una retroalimentación virtual a todas las instituciones participantes. De esta manera se generó un espacio de intercambio y aprendizaje entre todos/as los/as involucrados/as.

Luego de incorporar todos los aportes resultantes de las etapas de revisión y validación, se produjo el segundo borrador de la Guía. Este segundo borrador atravesó una breve etapa de edición (quinta etapa) para ser prontamente canalizado a la sexta etapa de traducción, diagramación y diseño.

Una vez encaminadas las tareas de la sexta etapa, se procedió a presentar la Guía ante los Estados Miembros de la OEA en la Primera Reunión del Grupo Técnico Subsidiario sobre los Sistemas de Emergencia y Seguridad, presidida por el SIS ECU-911 de Ecuador. La misma tuvo lugar los días 6 y 7 de mayo del 2021, de manera virtual, a través de la Plataforma KUDO. De la misma también participaron los equipos redactores del Sistema de Emergencia 911 de Costa Rica, el Sistema Nacional a Emergencias y Seguridad 911 de República Dominicana, el Centro Nacional de Información de México y el Sistema de Emergencias 911 de Paraguay. Asimismo, estuvieron presentes los representantes del EENA y del NENA México-Latinoamérica, y el consultor externo que acompañó y brindó apoyo técnico a lo largo de todo el proceso de elaboración de la Guía.

Habiendo sido bien recibida por los Estados Miembros, quienes destacaron el hecho de que sea un producto elaborado en conjunto, basado en la coordinación, la participación, el esfuerzo y la experiencia de los propios Sistemas de Emergencia y Seguridad de la región, y agencias afines al tema, se publicó la Guía en su versión final, en formato digital.

Este es el producto que se presenta a continuación.

Introducción

La implementación de estrategias y acciones concertadas para impulsar y fortalecer capacidades necesarias para una pronta prestación de servicios de emergencia y seguridad de calidad, e incrementar la efectividad de los mismos, es un objetivo de reciente data en el hemisferio. Este surge en respuesta a una creciente demanda de protección y respuesta por parte de la población respecto a los organismos responsables de prestar auxilio, tanto en incidentes frecuentes y contingencias cotidianas como en situaciones de mayor peligro y complejidad.

Un punto de partida necesario es reconocer a la seguridad como un bien público. Se trata de un desafío singular, que se asienta en la necesidad urgente de promover condiciones, procesos y mecanismos para reducir brechas entre: seguridad e inseguridad, protección y vulnerabilidades, justicia y efectivo ejercicio de los derechos, y la impunidad e indefensión de las personas, entre otras dimensiones.

En épocas de crisis y de transformaciones profundas, el imperativo de modelar y contar con Sistemas para proteger y con servicios más efectivos para auxiliar a las personas, obliga a mover las fronteras de los paradigmas utilizados hasta ahora y, asimismo, innovar en el diseño de los servicios públicos, particularmente en lo que respecta a la interacción entre autoridades, actores institucionales y usuarios o beneficiarios. Esto representa una oportunidad para promover y coordinar la cooperación entre los Estados Miembros de la OEA.

Esta Guía nace de la necesidad de poner a disposición de los Estados Miembros de la OEA un conjunto de directrices y recomendaciones a partir de las experiencias y lecciones aprendidas en el hemisferio, ya sea para instalar o para fortalecer capacidades en la prevención y reacción ante una emergencia, incidentes asociados a la seguridad pública y ciudadana, así como también frente a situaciones de mayor magnitud y complejidad. Todas estas situaciones requieren de mayores o menores niveles de coordinación y colaboración entre distintas instituciones de respuesta inmediata y, en algunos casos, también se debe sumar el apoyo de instituciones especializadas.

El carácter público y crítico de la labor que se realiza, explica la necesidad de promover una acción mancomunada de las autoridades públicas en diferentes niveles y ámbitos, enfrentando los obstáculos y mejorando las condiciones para la atención y respuesta a emergencias, incluyendo aquellas vinculadas con la seguridad, concebida esta como vehículo para una mejor calidad de vida. Es por ello que resulta necesario la aprobación de leyes, la asignación de recursos, y el diseño e implementación de políticas públicas y de programas que apoyen este tipo servicios.

A nivel hemisférico, ese apoyo provino del Grupo Técnico Subsidiario sobre los Servicios de Emergencia y Seguridad (GTS-SES) y se materializó en esta Guía para el Establecimiento y Fortalecimiento de Sistemas Nacionales de Emergencia y Seguridad en los Estados Miembros de la OEA. En ella se presenta una sistematización de directrices y recomendaciones, organizadas en 10 capítulos, que permiten responder a una gama amplia de interrogantes. Este objetivo ha sido alcanzado en un reducido plazo de tiempo y los resultados quedan refrendados en esta Guía

Los temas de esta Guía son abordados desde una perspectiva político-estratégica, que permita echar luces y orientar en la toma de decisiones en lo que respecta al diseño y funcionamiento de un sistema de emergencia y seguridad. No es un manual que explica cómo hacer las cosas, ni una receta única con los ingredientes y pasos que se tienen que seguir de manera rígida y unilineal. Se presenta como una herramienta de consulta y referencia, con lineamientos y consideraciones generales sobre componentes, áreas, procesos y tareas que se tendrían que tener en cuenta para la creación, fortalecimiento y el funcionamiento sostenible de este tipo de servicio.

En cuanto a la creación y establecimiento de un sistema de emergencia y seguridad que se aborda en el **Capítulo I**, una constatación compartida es la pertinencia de un enfoque sistémico, integral y de corresponsabilidad en la cooperación y coordinación horizontal. La gobernanza del Sistema es un impulsor y, a la vez, el eje estratégico de un diseño institucional y orgánico adecuado.

Sin una visión y planificación estratégica de los servicios públicos como la que se presenta en el **Capítulo II**, difícilmente será posible prestar auxilio oportuno y de calidad a los requerimientos de las personas en riesgo. La configuración de un modelo efectivo, durante el diseño del sistema de emergencia y seguridad, involucra elegir entre diferentes alternativas de funcionamiento, que varían en estructura, mecanismos, niveles de integración y ámbitos de colaboración entre las entidades o instituciones articuladas (de primera respuesta) e instituciones vinculadas (complementarias), que deberían integrarlo. Estas cuestiones y decisiones intrínsecas a la etapa de diseño de un sistema de emergencia y seguridad son introducidas en el **Capítulo III**.

Esto implica enfocarse en reducir una de las principales debilidades observadas, como es -en algunos casos- la insularidad de los organismos, las asimetrías y las brechas de capacidades efectivas, y fortalecer aquellos factores determinantes que están a la base de la interoperabilidad en información y comunicación. No hay dudas de que este reto no consiste tan sólo en mejorar la coordinación, sino que también involucra esfuerzos para la integración de subsistemas existentes, la planificación de arquitecturas tecnológicas y de información interoperables, de infraestructura y recursos suficientes, de cobertura y de dispositivos en los diversos territorios, entre otros.

La gestión de calidad integral en un sistema de emergencia y seguridad que se plantea en el **Capítulo IV**, busca la mejora continua en aras de brindar a la población un servicio profesional y efectivo de manera sostenida e ininterrumpida. Involucra desde mapas de procesos, medición, monitoreo, evaluación y revisión de los estándares para la calidad hasta la introducción de las mejoras requeridas para tornar más eficiente, eficaz y satisfactorio el servicio que se brinda.

El desarrollo alcanzado en tecnologías de información y comunicación hacen más probable que los Estados Miembros de las OEA cuenten con herramientas que hagan más eficientes los procesos. No obstante, entre las áreas funcionales, la gestión de llamadas y atención de incidentes es la función esencial y la que merece especial atención, a través de la disposición de protocolos, procedimientos y estándares de actuación actualizados y validados continuamente. Es por ello que el **Capítulo V** de esta Guía está enfocado en la recepción, tratamiento y respuesta de las solicitudes, llamadas y reportes de auxilio recibidos. Es en esta área donde la inteligencia colectiva, la ingeniería organizacional y el intercambio de experiencias y lecciones se vuelven indispensables.

Como muestran las experiencias sobre modernización del Estado, la gestión del talento humano involucra un esfuerzo importante por incrementar el principal activo de toda organización pública. Es por esto que, en esta Guía, el **Capítulo VI,** pone especial interés en líneas de acción para garantizar la calidad profesional del personal, desde el reclutamiento y selección, la inducción y la capacitación continua, hasta la evaluación y salida. Asimismo, también se enfoca en el bienestar del personal por medio de una serie de criterios enfocados en promover la salud y la seguridad ocupacional, así como también en generar un ambiente laboral seguro y saludable.

La gestión de la información es considerada un proceso principal para los objetivos estratégicos del Sistema y la preparación y el direccionamiento de la prestación de los servicios. Es por esta razón que en el **Capítulo VII** se la vincula con la estrategia organizacional y con los niveles de funcionamiento de un sistema de emergencia y seguridad. Al ser la información uno de los activos principales de este tipo de

Sistemas, se sugiere también contar con un ciclo de procesos, que optimice una serie de etapas relacionadas con la obtención, organización y almacenamiento, distribución y acceso, y uso de ese recurso para el desarrollo de productos que apuntalen las decisiones en las diferentes instancias y momentos asociados a los flujos de la interoperabilidad en la atención y respuesta a solicitudes, llamadas y reportes de emergencias.

En un Sistema que atiende y responde a emergencias, la gestión de la seguridad debe abordarse desde un enfoque multidimensional, poniendo especial atención tanto en las condiciones para el funcionamiento de un centro operativo como en la continuidad de los servicios. Es por esto que el **Capítulo VIII** no sólo sugiere cursos de acción para la protección de la información, las comunicaciones, los sistemas informáticos, la seguridad física y de la infraestructura, y la seguridad del personal, sino que también aborda el análisis y la gestión de riesgos. Para ello, el Capítulo presenta lineamientos para elaborar al menos dos herramientas básicas: planes de continuidad de las operaciones y planes de recuperación ante desastres.

Un elemento central en la gestión de emergencias, así como también durante incidentes de alta intensidad o crisis de mayor magnitud, es la gestión de la comunicación, tanto institucional como operativa. Frente a estas situaciones, el **Capítulo IX** delinea los elementos mínimos que tendrían que considerarse al momento de elaborar un plan de comunicación. Esta herramienta sirve de hoja de ruta para el manejo de las comunicaciones, utilizando distintos canales y herramientas, incluyendo la vocería, el uso de las redes, los medios de comunicación tradicionales y sociales, la vinculación con la población y las comunidades, y los mensajes pregrabados. Hacia el final del Capítulo, también se postulan algunas orientaciones para guiar la planificación y preparación de la comunicación de crisis.

Finalmente, el **Capítulo X** se enfoca en la transparencia y la rendición de cuentas de un sistema de emergencia y seguridad como pilares para la gobernanza democrática, la integridad y la calidad del servicio que se le presta a la población. Se los trabaja simultáneamente como principios o valores a consagrar y fortalecer, objetivos a alcanzar y procesos a seguir. La transparencia y la rendición de cuentas no son elementos añadidos u ocurrencias tardías, sino que se las concibe como parte del proceso de planificación estratégica, así como de la comunicación organizacional. El Capítulo propone una serie de herramientas y mecanismos para brindar, de manera proactiva, información sobre el funcionamiento, la gestión y los resultados del Sistema, así como también facilitar el acceso a la información que se produce.

Nota sobre el uso del lenguaje inclusivo: La utilización de términos como “operador”, “despachador”, “video operador”, “supervisor” y otros sustantivos y artículos en masculino, no responde a estereotipos discriminatorios, sólo buscan facilitar la lectura del documento.

CAPÍTULO I: CREACIÓN Y ESTABLECIMIENTO

Introducción

En este Capítulo se presentan los elementos básicos para la creación de un sistema de emergencia y seguridad, incluyendo (a) el apoyo político e institucional al más alto nivel, (b) un instrumento legal que defina propósitos, posicionamiento en la estructura del Estado, instituciones que lo integran, responsabilidades y funciones, servicios que prestaría, recursos con los que contaría, entre otros elementos fundacionales, y (c) financiamiento.

Adicionalmente, el Capítulo presenta diferentes tipos de anclaje y posicionamiento institucional que podrían tener los sistemas de emergencia y seguridad, lo cual incidiría en su autonomía legal, administrativa, financiera y operativa.

Existirían al menos tres tipos de actores que podrían considerarse para conformar la estructura de un sistema de emergencia y seguridad. El Capítulo hace especial énfasis en la necesidad de coordinación y cooperación entre los actores, abogando por un enfoque sistémico que permita a las partes colaborar entre sí para entregar productos y servicios de calidad, y con elevado valor público. Otro elemento al que hace referencia el Capítulo es a los tres niveles con los que un Sistema podría funcionar.

La gobernanza de un sistema de emergencia y seguridad podría completarse con la creación de una Comisión o Comité Interinstitucional o Intersectorial y la designación de un Director/a Ejecutiva/a (o cargo similar). En línea con los niveles de funcionamiento de un Sistema, el primero estaría más enfocado en el direccionamiento estratégico mientras que el segundo se haría responsable de las cuestiones tácticas y operativas.

1.1 Apoyo institucional y político

Para la creación de un sistema de emergencia y seguridad, es fundamental que exista voluntad, liderazgo y apoyo político al más alto nivel, guiados por una visión sobre qué tipo de sistema crear y cómo crearlo. Esto tendría que manifestarse en consensos político-técnicos y acuerdos interinstitucionales, incluyendo acuerdos de prestación de servicios (púbicos/privados).

También sería importante contar con el involucramiento de todos los entes que se estiman necesarios por su rol directo e indirecto en la atención de emergencias y seguridad. Este involucramiento tendría que ser desde un primer momento, para generar una identidad común, un sentimiento de apropiación y el empoderamiento de quienes lo conforman. Así mismo, coadyuvaría a sentar los cimientos para la coordinación y colaboración entre las instituciones integrantes, entre otros beneficios.

La decisión de las instituciones integrantes de formar parte de este tipo de proyectos tendría que estar sustentada en una convicción compartida, como lo sería la necesidad de brindar a la población un sistema integrado de servicios para la atención de emergencias, dirigido a proteger y salvar vidas.

1.2 Base legal y marco normativo

Los instrumentos legales más frecuentes con los que se han creado sistemas de emergencia y seguridad en América Latina han sido leyes y decretos ejecutivos.

En ellos se perfilan facultades y responsabilidades, funciones y roles, así como las instancias supra e inter-institucionales para la articulación coordinada de las instituciones, órganos y cualquier otra entidad nacional y subnacional relacionados con los productos y servicios que presta un sistema de emergencia y seguridad.

Se considera que el instrumento legal idóneo para la creación de un sistema de emergencia y seguridad sería por ley, debido al respaldo Legislativo y Ejecutivo que ésta representaría, además de que se trataría de una norma de rango superior.

Adicionalmente, podría ser necesario que se establezcan convenios entre las instituciones participantes que promuevan, como mínimo, las directrices de coordinación, colaboración, coproducción y corresponsabilidad.

En todo caso, los instrumentos legales en donde se materialice la creación de un sistema de emergencia y seguridad, tendrían que dejar constancia, de manera explícita, la obligatoriedad de participación que tendrían las instituciones relacionadas con la atención de situaciones de emergencia de cada país.

1.3 Anclaje institucional

La posición del sistema de emergencia y seguridad en la estructura estatal dependerá de los grados de federalismo, regionalismo, centralización, concentración de la administración y el presupuesto fiscal.

El sistema de emergencia y seguridad podría crearse como un órgano adscrito a una entidad estatal preexistente o no. De esto dependerá la autonomía legal, administrativa, financiera y operativa del mismo.

Una posibilidad es que quede bajo la responsabilidad de una entidad del Poder Ejecutivo, en el sector de seguridad pública, al más alto nivel como, por ejemplo, un Ministerio de la Presidencia, del Interior, de Gobierno o de Seguridad. Otra posibilidad es que quede adscrito dentro de una institución del Ejecutivo, pero con autonomía jurídica, administrativa y financiera.

Una tercera posibilidad es que el sistema de emergencia y seguridad quede constituido al amparo de una institución pública descentralizada.

En cualquier esquema de anclaje, la norma tendría que establecer plenamente cuáles son las responsabilidades, competencias, atribuciones y funciones que se le adjudicarían a los componentes del Sistema, como se señaló en la Sección 1.2 del presente Capítulo, teniendo en cuenta los tipos y magnitudes de las emergencias.

Para mantener la coordinación y colaboración entre las instituciones integrantes, así como la imparcialidad y uniformidad en las acciones operativas, sería recomendable que el Sistema no quedase anclado institucionalmente en alguna entidad preexistente.

1.4 Ideación

Sobre la base de una visión estratégica, podría concebirse al Sistema como una política pública o como un instrumento de esta, un modelo de gestión o una red de entidades cooperantes para la prestación de servicios de atención a emergencias. Esta red de servicios tendría que responder a la necesidad de mejorar la interoperabilidad entre los componentes, a través de la integración y la agregación de valor. Es por ello que la conformación también requeriría adoptar un enfoque sistémico para alcanzar eficacia, integralidad y calidad de los servicios.

El sistema de emergencia y seguridad podría constituirse estratégicamente como una institución que se articula y opera en un contexto de interoperabilidad, con otras instituciones que atienden incidentes y emergencias que afectan a la población. Sus objetivos estratégicos tendrían que estar dirigidos a favorecer los intereses colectivos y lograr mayor impacto y calidad en el servicio que se le brinda a la población.

La naturaleza de la entidad que eventualmente se conforme, implicaría que las competencias asignadas a cualesquiera organismos que la conformen tendrían que formar parte de un todo orgánico. Todas

tendrían que actuar de manera integrada, aportando sus competencias y recursos para alcanzar un fin común que procure el logro ya no de objetivos individuales de cada institución sino colectivos, relacionados con la atención efectiva y de calidad de las emergencias.

1.5 Estructura

La creación de un sistema de emergencia y seguridad se tendría que traducir en una estructura que, a su vez, se presentaría como una oportunidad para procurar sinergia entre las instituciones integrantes a nivel nacional y subnacional.

La estructura de un sistema de emergencia y seguridad podría pensarse sobre la base de tres tipos de actores:

- Actores para la primera respuesta (o instituciones articuladas o instituciones del primer anillo)
- Actores de apoyo (o instituciones vinculadas o instituciones del segundo anillo)
- Actores subsidiarios (o instituciones del tercer anillo)

1.5.1 Actores para la primera respuesta (instituciones articuladas)

Los actores para la primera respuesta serían los responsables de llevar a cabo las funciones esenciales de un sistema de emergencia y seguridad. Entre esas funciones esenciales se encontrarían las siguientes:

- Recibir, tramitar y responder a las solicitudes, llamadas y reportes de auxilio, y la coordinación de respuestas en situaciones de emergencia, con cobertura en todo el país.
- Habilitar y mantener múltiples medios de comunicación entre las personas y el sistema de emergencia y seguridad, incluyendo: telefonía móvil y fija, mensajería de texto (SMS), aplicaciones, botones de auxilio (pánico) y redes sociales, entre otros.
- Servir de Centro de Coordinación, Comando, Comunicación y Control de Respuestas a Emergencias y gestionar los centros de monitoreo de video vigilancia.
- Elaborar, actualizar y validar protocolos comunes de actuación y atención.
- Desarrollar y mantener la infraestructura tecnológica y de comunicaciones de alta disponibilidad para la prestación coordinada de los servicios.
- Servir de entidad operativa para el sistema nacional de gestión de riesgo y de desastres, cuando corresponda.
- Mantener un sistema de registro de antecedentes para la trazabilidad de los casos y el análisis de los procedimientos, las auditorías de gestión y la medición de la efectividad de los servicios y, asimismo, los ejercicios de responsabilización y rendición de cuentas periódicas.

De acuerdo a los tipos y magnitud del o de lo/s evento/s, las instituciones del primer anillo son las que brindarían los servicios esenciales de respuesta. Entre los diferentes tipos de emergencias, destacarían los siguientes:

- **Tránsito y movilidad:** Las instituciones de primera respuesta estarían encargadas de la atención de las emergencias relacionadas con asuntos de tránsito vehicular o problemas de circulación en las vías del país.
- **Seguridad pública/ciudadana:** Las instituciones de primera instancia estarían encargadas de la atención de las emergencias relacionadas con la prevención y mitigación de la delincuencia, la preservación de la seguridad y el mantenimiento del orden público.
- **Atención de salud (física y mental)/sanitaria:** Las instituciones de primera instancia estarían encargadas de la atención de las emergencias, relacionadas con eventos que atentan contra la vida y la salud de las personas.

- **Gestión de incendios y siniestros:** Las instituciones de primera instancia estarían encargadas de la prevención, atención, mitigación, control, investigación y evaluación de los incendios. Asimismo, les correspondería el rescate de personas atrapadas o perdidas.
- **Atención y prevención de riesgos y desastres:** Las instituciones de primera instancia estarían encargadas de la preparación, alerta, mitigación y atención de respuesta, coordinación y gestión de emergencias provocadas por desastres de pequeña, mediana y gran escala, incluyendo terremotos, inundaciones, huracanes, ciclones, pandemias u otros.

1.5.2 Actores de apoyo (instituciones vinculadas)

De acuerdo a los tipos de emergencias y a las necesidades de grupos en situación de vulnerabilidad y/o riesgo crítico, cabría contemplar la posibilidad de que las instituciones de primera respuesta tengan que coordinarse con otros organismos estatales, así como con asociaciones de la sociedad civil. Estos actuarían como entidades de apoyo. La participación de estos resulta vital para la gestión de situaciones críticas o para el aseguramiento de la continuidad de servicios esenciales.

El espectro de entidades disponibles para prestar servicios seccionales, podría ser amplio o reducido, según la ingeniería institucional de cada país, las necesidades de coordinación y las circunstancias particulares de cada situación:

- Entidades en el nivel nacional, sub-nacional, regional y local a cargo del direccionamiento y la implementación de planes y programas: Ministerios, Secretarías Técnicas, Departamentos, Direcciones, Comisiones Especiales y municipios, entre otros.
- Entidades encargadas de segmentos específicos de la población, como aquellas relacionadas con la niñez, mujeres, personas adultas mayores, personas con alguna discapacidad y minorías, entre otros.
- Entidades encargadas de la atención de los turistas y extranjeros: aquellas que brindan atención multilingüe y guía a las personas que visitan y permanecen de forma temporal en el país y con un estatus diferente al de ciudadano o residente.
- Entidades encargadas de la prestación de los servicios básicos: agua potable, electricidad, provisión de alimentos, educación, salud, entre otras.

1.5.3 Actores subsidiarios

Hay un tercer tipo de actores que se podrían denominar entidades subsidiarias y que procurarían generar condiciones y capacidades para el funcionamiento del sistema.

Algunos ejemplos de entidades subsidiarias serían: organismos internacionales, organizaciones de la sociedad civil, sector empresarial, sector académico y sector de medios, entre otros, con quienes sería posible suscribir convenios o negociar apoyos específicos para contribuir a la mejora del servicio.

1.6 Niveles de funcionamiento

Existirían al menos tres niveles de funcionamiento que tendrían que retroalimentarse de manera continua para la atención de emergencias:

i. **Nivel estratégico:** Considerado el espacio en donde se determinan los objetivos a largo plazo y la interacción con otras entidades, y se toman decisiones proactivamente que afectan al Sistema, su organización y estructura, con una visión orientada al futuro y la sostenibilidad de los servicios.
ii. **Nivel táctico:** Relacionado con la elaboración y ejecución de planes de acción para las áreas de servicio y actividades principales; la coordinación, supervisión y evaluación (con una perspectiva cuantitativa y cualitativa) de las operaciones y metas a alcanzar. Este nivel está conformado por una serie de procesos internos que brindan apoyo para el funcionamiento del Sistema.

iii. **Nivel operativo:** Relacionado con la ejecución de los servicios, las actividades y las operaciones de rutina establecidas en los planes de acción.

En algunos casos, el nivel táctico y el operativo podrían fusionarse.

1.7 Coordinación y cooperación

Las entidades para la primera respuesta (primer anillo), las entidades de apoyo (segundo anillo) y las entidades subsidiarias (tercer anillo) tendrían que estar alineadas en torno a propósitos, objetivos y metas compartidos, en el marco de la planificación estratégica (Ver Capítulo II de esta Guía).

El adecuado funcionamiento del Sistema también requeriría de la coordinación y cooperación entre las entidades que lo integran, para generar un servicio de calidad y valor público.

Particularmente entre las entidades para la primera respuesta se sugeriría trabajar con base en una dinámica de cooperación horizontal entre pares, con canales y flujos de comunicación y mecanismos para facilitar el intercambio de recursos, información, ideas y personal.

La normativa de cada una de ellas tendría que respetarse bajo el supuesto de que todas se encuentran bajo la misma o similar condición. Adicionalmente, todas tendrían que respetar y ceñirse a la normativa del sistema de emergencia y seguridad. Esta última podría considerarse como complementaria, coadyuvando a la creación de una identidad y propósito común, y a la generación de un ambiente laboral basado en la colaboración para la prestación de un servicio público.

La coordinación y cooperación entre las entidades que conforman un Sistema podría asumir distintas modalidades:

- Redes colaborativas y redes de asuntos o temáticas
- Cooperación horizontal entre pares
- Promoción de mecanismos para el intercambio de información y conocimiento (experiencias sistematizadas y buenas prácticas)
- Colaboración en procesos de diseño y evaluación
- Creación de alternativas efectivas para el intercambio de resultados de estudios o productos de investigación
- Promoción de alianzas público-privadas, universidades y organismos internacionales
- Instancias periódicas de entrenamiento y profesionalización
- Cooperación en la formación del talento humano y la especialización profesional, entre otros.

1.8 Direccionamiento estratégico

Como parte de la gobernanza y el funcionamiento del sistema de emergencia y seguridad sería recomendable incluir en la norma que establezca su creación, la conformación de una Comisión o Comité Interinstitucional o Intersectorial.

Reuniéndose de manera periódica, y de manera extraordinaria cada vez que sea necesario, dicha Comisión o Comité podría tener algunas de las siguientes funciones:

- Definir y aprobar los procesos, políticas, procedimientos y protocolos interinstitucionales.
- Supervisar el cumplimiento de los lineamientos definidos como necesarios para que el sistema de emergencias y seguridad, así como los despachos de cada institución u organización integrante, cumplan los objetivos dispuestos por la ley.
- Establecer los parámetros y asegurar la calidad y la eficiencia en la atención de las solicitudes, llamadas y reportes de emergencia.

- Establecer los parámetros de calidad de servicio (con una perspectiva cuantitativa y cualitativa) del sistema de emergencia y seguridad desde el momento en que ingrese la solicitud, llamada o reporte de auxilio hasta el momento en que se cierre el incidente de emergencia en terreno.
- Crear las comisiones que considere necesarias para su correcto funcionamiento.

En algunos casos esta instancia podría existir transitoriamente, para liderar y acompañar el diseño e instalación. En otros podría constituirse para la supervisión del sistema de emergencias y seguridad, una vez instalado y en funcionamiento. En este segundo escenario, asumiría un carácter más permanente.

Es posible que esta Comisión, según su posición y estatus legal, esté integrada por los titulares de las entidades que conforman el Sistema, y presidida por la máxima autoridad del Ministerio que corresponda.

Las facultades y prerrogativas de la Comisión tendrían que quedar establecidas por ley, junto con la reglamentación de apoyo que la acompañe.

1.9 Director/a Ejecutiva/a (o cargo similar)

La norma que instaure el sistema de emergencia y seguridad tendría que definir el proceso de selección y el perfil para el cargo de un/a director/a ejecutivo/a, de acuerdo con el marco de contratación de funcionarios/as públicos de cada país.

El/la Director/a es quien concentra la ejecución operativa-táctica de la prestación de los servicios, por lo que se considera adecuado que el perfil del cargo incorpore las habilidades, destrezas, conocimientos y experiencias necesarias para el gerenciamiento de un sistema de emergencia y seguridad.

El proceso de selección podría llevarse a cabo en el marco de un concurso público. El mismo tendría que estar alineado con:

- Un perfil de competencias definido técnicamente en el ámbito de la seguridad y la gestión de riesgos e incidentes.
- La experiencia profesional necesaria para liderar y conducir un proceso estratégico, táctico y operativo.
- La idoneidad exigible a todo/a servidor/a público/a.

1.10 Financiamiento y sostenibilidad

El financiamiento tendría que considerar, en una primera instancia, el recurso para la creación y el establecimiento de un sistema de emergencia y seguridad, que podría provenir de un préstamo o acuerdo de cooperación internacional. Luego, en una segunda instancia, se precisaría de fondos para garantizar su funcionamiento y la continuidad de operaciones del Sistema. Estos fondos podrían proceder de al menos dos fuentes: un presupuesto nacional (anual o plurianual) y, complementariamente, un tributo o impuesto específico.

Al tratarse de recursos fiscales, el ejercicio quedaría sujeto a la aplicación y ejecución de la Ley de Presupuestos del Sector Público (o similar) de cada país. Los recursos estarían supeditados a un proceso de fiscalización, auditoría o veeduría.

Uno de los criterios rectores en lo que respecta al financiamiento de este tipo de Sistemas es que no dependan de una sola fuente, sino que se sustenten en una combinación de múltiples fuentes.

En línea con lo anterior, una fuente adicional de financiamiento podría generarse a partir de la venta de servicios del propio Sistema, sujeta a los requisitos y condiciones establecidos en la legislación que estipula su creación y funcionamiento.

CAPÍTULO II: PLANIFICACIÓN ESTRATÉGICA

Introducción

En este Capítulo se presenta la planificación estratégica como una herramienta y como un proceso. En su concepción como herramienta para la gestión, se presentan los componentes mínimos que lo tendrían que integrar. En cuanto a proceso, se procura su estandarización e institucionalización por medio de la definición de protocolos, procedimientos e instrumentos. Estos últimos se presentan en función de tres etapas inherentes al proceso de planificación: la etapa pre-planificación, durante la planificación, y post-planificación.

La planificación como herramienta, es decir, lo que resulta del proceso de planificación, sería un plan estratégico. Sobre este, el Capítulo se enfoca en explicitar los supuestos bajo los cuales se considera que el plan será implementado, identificar los factores críticos para el éxito, y analizar los riesgos que podrían dificultar e inclusive impedir el alcance de los objetivos y de las metas establecidas.

La planificación estratégica se presenta en este Capítulo como una herramienta diferente a la planificación tradicional. Esto por cuanto la primera estaría enfocada en abordar los grandes desafíos de mediano y largo plazo, incorporar el análisis prospectivo y la consideración de posibles escenarios futuros, y adaptarse a los cambios internos y externos que pudiera experimentar un sistema de emergencia y seguridad.

2.1 Planificación estratégica

El plan estratégico podría ser considerado como una herramienta para la gestión, que reúne un conjunto de objetivos, metas y actividades establecidas por una organización, con la mira puesta en alcanzarlos y realizarlos en un plazo determinado. Adicionalmente, también podría ser considerado como un producto que resulta de la culminación de un proceso de planificación, comúnmente denominado proyecto o plan. En ese proceso se tendrían que integrar todas las áreas funcionales, los más altos niveles decisivos y los actores clave de un sistema de emergencia y seguridad. A lo largo del proceso, es importante estimular el pensamiento estratégico, así como recabar información y planteamientos de valor para el establecimiento de los objetivos.

Este ejercicio podría ser llevado a cabo por el área de planificación y gestión estratégica del propio sistema de emergencia y seguridad y/o con el apoyo de una consultoría externa, con amplia y reconocida experiencia en este tipo de ejercicios.

El proceso de planificación quedaría sujeto al contexto específico de cada sistema de emergencia y seguridad. Sin embargo, como todo proceso crítico, para su funcionamiento y sustentabilidad tendría que quedar debidamente protocolizado, definido por una serie de procedimientos, pasos y herramientas para que pueda ser llevado a cabo de manera continua y sistemática.

2.2 Componentes fundamentales de un plan estratégico

Los componentes esenciales que tendrían que formar parte de un plan estratégico serían los siguientes:

- **Visión**: Es la definición a largo plazo de lo que la entidad quiere ser. Es cómo esta se visualiza a futuro. Es la referencia que guía al Sistema a alcanzar los objetivos deseados. Suele apoyarse en las emociones y servir de fuerza inspiradora.
- **Misión:** Describe el objetivo fundamental de la entidad, estableciendo su razón de ser y sus acciones para alcanzar la visión. Una declaración de misión constituye un elemento

fundamental para motivar al equipo hacia el logro de los objetivos y metas, al proveerles un claro sentido de dirección e intención estratégica.

- **Valores**: Son las creencias, virtudes o cualidades a partir de los cuales se rige la entidad. Reflejan los estándares, evocan su esencia y reflejan su identidad. Los valores de un sistema de emergencia y seguridad tendrían que reflejar y ser coherentes con su razón de ser. En esa línea, algunos de los valores que podrían inspirar el accionar de un sistema de emergencia y seguridad son: honestidad, lealtad, solidaridad, respeto, colaboración, responsabilidad, transparencia, confidencialidad y vocación de servicio, entre otros. Estos valores tendrían que verse reflejados en el Código de Ética y el Código de Conducta dirigidos al personal de la entidad (ver Capítulo VI de esta Guía).

- **Objetivos:** Resultados medibles que quiere alcanzar la entidad; podrían ser de corto, mediano y largo plazo, así como intermedios y finales.

- **Estrategias:** Hoja de ruta que combina planes y medios para alcanzar los objetivos establecidos.

2.3 Principios rectores

Los principios rectores podrían ser considerados como pautas o lineamientos esenciales que guían el desempeño de un sistema de emergencia y seguridad, los cuales tendrían que ser coherentes con los objetivos y valores de dicha entidad. Tendrían también que guardar cierto equilibrio entre el qué se hace (objetivos) y cómo se hace (funciones). Los principios podrían cimentarse en:

- Las directrices internacionales de derechos humanos
- Base legal nacional de los derechos de protección a las personas y sus bienes
- La base legal y normativa que sustenta la creación del sistema de emergencia y seguridad
- La base legal y los principios de las entidades articuladas y vinculadas

Los principios rectores actuarían como una forma de guía para que las decisiones y acciones puedan ejecutarse alineadas con la visión, misión y valores de la entidad, velando por el bienestar del personal como de los/as usuarios/as que requieren los servicios del sistema de emergencia y seguridad.

A continuación, se presentan algunos ejemplos de principios rectores:

- No discriminación por motivos de raza, color, sexo, género, idioma, religión, opiniones políticas o de cualquier otra índole, nacionalidad, posición económica o social, o cualquier otra condición social
- Imparcialidad
- Cooperación y coordinación
- Integración e interoperabilidad
- Accesibilidad a través de un número único
- Gratuidad

Estos principios rectores tendrían que verse expresados en el Código de Ética y el Código de Conducta que elabore el sistema de emergencia y seguridad (ver Capítulo VI de esta Guía).

2.4 Definición de ejes estratégicos

Los ejes estratégicos son los ámbitos o dimensiones fundamentales a partir de los cuales se funda y desarrolla todo el accionar de un sistema de emergencia y seguridad. Establecen las grandes rutas de acción y permiten mantener el enfoque en los temas que son esenciales. Algunos ejemplos de ejes estratégicos serían: excelencia operacional, fortalecimiento institucional y coordinación institucional, entre otros.

Cada eje podría venir acompañado de una breve descripción que demarque claramente de qué se trata. En ese sentido, respecto al eje de excelencia operacional, el mismo podría ser presentado de la siguiente manera: ¨Realizar mejoras continuas en procesos, sistemas, infraestructura y desarrollo del talento humano, para aumentar los niveles de calidad, eficiencia y eficacia del Sistema, y con ello la satisfacción de los usuarios¨ (Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, 2020).

Luego de establecidos los ejes estratégicos, sería necesario definir los objetivos estratégicos para cada uno de ellos. Estos, en su conjunto, tendrían que estar dirigidos a encaminar y consolidar las acciones para conseguir los resultados esperados.

Tabla 1: Ejemplo de tabla para la definición de los objetivos estratégicos

EJE	OBJETIVOS ESTRATÉGICOS	DESCRIPCIÓN
I. Excelencia Operacional Realizar la mejora continua de procesos, sistemas, infraestructura y desarrollo del talento humano, para aumentar los niveles de calidad, eficiencia y eficacia del Sistema, y con ello la satisfacción de los usuarios.	I.1 Fomentar una cultura de gestión de la calidad basada en procesos.	Establecimiento de una gestión efectiva, alineada con la visión y enfocada en procesos integrados, con el fin de crear y mantener una cultura laboral orientada a la calidad de forma sostenible y a los valores que rigen la organización.
	I.2	
	I.3	

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1 República Dominicana, 2020.

2.5 Definición de las estrategias

Para alcanzar los objetivos propuestos, se tendrían que definir las estrategias. Estas podrían concebirse como acciones o actividades encaminadas a la consecución de los objetivos establecidos.

Tabla 2: Ejemplo de tabla para la definición de estrategias

EJE	OBJETIVO	ESTRATEGIAS
I. Excelencia Operacional Realizar la mejora continua de procesos, sistemas, infraestructura y desarrollo del talento humano, para aumentar los niveles de calidad, eficiencia y eficacia del sistema, y con ello la satisfacción de los usuarios.	I.1 Fomentar una cultura de gestión de la calidad basada en procesos.	I.1.1. Estandarizar los procesos, definiendo normas y procedimientos técnicos para: • Modelo operativo de radiocomunicación • Norma técnica eléctrica I.1.2. Integración de Calidad y Seguridad, estableciendo Acuerdo de Niveles

		de Servicio (ANS) con las agencias de respuesta
	I.2	I.2.1 I.2.2 I.2.3

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1 República Dominicana 2020.

2.6 Planes de acción

Los planes de acción u operativos podrían definirse como productos de la planificación y/o programas enmarcados dentro del contexto de una estrategia, orientados hacia la consecución de los objetivos, trazando la hoja de ruta. Serían también herramientas de gestión que permitirían organizar, implementar y controlar el conjunto de tareas necesarias para alcanzar las metas. Una estrategia podría ser parte de uno o varios planes de acción.

2.7 Sistema de indicadores y metas

Un elemento esencial de la planificación estratégica sería la medición del grado de consecución de los objetivos institucionales. De forma que, vinculado a cualquier plan estratégico, también tendría que definirse un conjunto de indicadores de monitoreo y de resultado de las metas parametrizadas. La definición de un indicador incluiría una descripción, la unidad de medición y la fórmula de cálculo.

Tabla 3: Ejemplo de un Sistema de Indicadores y Metas

					Línea Base	Metas			
Indicador	**Descripción**	**Unidad**	**Método de cálculo**	**Alineación Objetivos Estratégicos**	**Año Base**	**Año 1**	**Año 2**	**Año 3**	**Año 4**

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1 República Dominicana, 2020.

Para saber si se ha cumplido o no con las metas establecidas, primero sería necesario establecer una línea de base contra la cual comparar. Tabla 4: Ejemplo de un Sistema de Indicadores y Metas

Adicionalmente, se tendría que fijar la periodicidad con la cual los indicadores serían calculados y, de ser posible, incorporar la medición de estos indicadores en el área funcional de control de la gestión de la calidad y convertirse en parte sustantiva de la arquitectura de la información y tecnológica del sistema de emergencia y seguridad (ver Capítulo III de esta Guía.) El contar con esta información de manera continua, constante y, de ser posible, automática, permitiría saber si se está cumpliendo o no con los objetivos estratégicos del Plan, y hacer los ajustes que fueran necesarios a lo largo del camino.

Cada objetivo estratégico también tendría que tener una asignación de responsabilidad. Esta asignación podría recaer en un departamento, unidad, equipo o individuo.

2.8 Presupuesto

Las actividades asociadas con la consecución de la misión y los objetivos, tendrían que venir acompañadas de los recursos asignados a partir de la planificación presupuestaria. Es importante diferenciar entre dos

tipos de recursos. Primero, los recursos anuales, destinados a la prestación de los servicios de atención y respuesta a emergencias dirigidos a los/as usuarios/as y los costos de operación. Segundo, los recursos destinados a gestionar el talento humano, desarrollar la infraestructura para aumentar en el mediano plazo la cobertura o bien fortalecer el sistema de control de gestión de la calidad. Sin este segundo tipo de recursos es casi imposible ejecutar el plan estratégico. La ejecución presupuestaria tendría que ser consistente con los programas y los planes de acción para la obtención de las metas.

Los criterios de priorización y focalización de recursos resultarían claves en la asignación del presupuesto para el desarrollo de capacidades del personal y el fortalecimiento tecnológico, operativo y administrativo de las áreas funcionales (ver Capítulo III, Sección 3.2). Asimismo, con estos criterios también se podría dar preferencia a los proyectos y programas con mayor impacto social y valor institucional, y menor costo.

2.9 Algunas herramientas para la planificación estratégica y su ejecución

La planificación estratégica resultaría más recomendable que la planificación tradicional, puesto que esta última no está diseñada para la formulación de respuestas a los grandes desafíos de largo plazo.

La planificación estratégica consistiría en la construcción, desarrollo y puesta en marcha de los diferentes planes de acción u operativos que tendrían que ser formulados por la entidad con el propósito de alcanzar su visión, misión, objetivos y metas.

El proceso de planificación estratégica podría servirse de una serie de herramientas a lo largo de su ciclo de elaboración, teniendo en cuenta al menos tres etapas: la etapa de pre-planificación, la etapa de planificación y la etapa de post-planificación.

2.9.1 Pre-planificación: Análisis FODA

Como parte de esta etapa, resultaría útil que, en el marco de un diagnóstico, se identificasen fortalezas y debilidades del sistema de emergencia y seguridad, y oportunidades y amenazas para los servicios que el Sistema presta. Este ejercicio se podría llevar a cabo con la herramienta de análisis FODA.

Figura 5: Ejemplo FODA

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1 República Dominicana, 2020.

2.9.2 Durante la planificación: Mapa estratégico

Un mapa estratégico permitiría representar visualmente la relación causa-efecto que existiría entre los objetivos trazados y los ejes estratégicos, planes y componentes que hubieran resultado de la planificación. En una sola imagen sería posible visualizar cómo se podría agregar valor público al servicio que entrega el sistema de atención de emergencia y seguridad.

Existirían varias formas de diagramar los mapas estratégicos. A continuación, se presentan dos ejemplos:

Figura 6: Ejemplo 1 de Mapa Estratégico

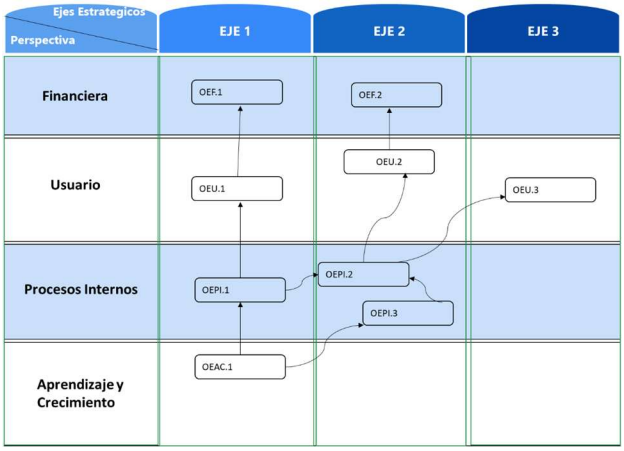


Figura 7: Ejemplo 1 de Mapa Estratégico

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1 República Dominicana, 2020.

En el ejemplo 1, es posible ver gráficamente cómo se interrelacionan los objetivos estratégicos de manera transversal, entre los diferentes ejes.

En ambos casos, el mapa estratégico permitiría hacer un seguimiento entre los objetivos de las cuatro perspectivas del Cuadro de Mando Integral: financiera, del usuario, de los procesos y, por último, de aprendizaje y crecimiento. Resultaría recomendable utilizar el mapa estratégico como herramienta porque, entre otras ventajas, ayudaría a detectar posibles inconsistencias entre los objetivos, así como también identificar rápidamente las estrategias que carecen de objetivos y de esta manera proceder a su eliminación.

2.9.3 Post-planificación: Cuadro de Mando Integral (CMI)

La metodología de *Balanced Score Card* (BSC) o Cuadro de Mando Integral (CMI) resultaría útil para la dirección y gestión estratégica operacional. Es una herramienta que permitiría monitorear y gestionar la implementación de la estrategia, el alcance de los objetivos, la obtención de los resultados y la medición de los indicadores.

La información que genera suele ser de fácil comprensión, comunicable y accionable. Es a partir de esa información que el sistema de emergencia y seguridad podría reformular y ajustar su estrategia, mejorar la capacidad de análisis y revisar su desempeño.

El Cuadro de Mando Integral (CMI) permitiría analizar la entidad desde varias perspectivas o puntos de vista.

El CMI tradicional incluye cuatro perspectivas:

- **Usuario:** la atención tendría que estar dirigida a cómo posicionar estratégicamente los productos y servicios de la entidad para satisfacer las necesidades de los/as usuarios/as y alcanzar sus expectativas.

- **Procesos internos:** buscaría identificar y mejorar los procesos claves dentro de la entidad. Los procesos claves tendrían que estar alineados con los objetivos estratégicos. La atención tendría que centrarse en la efectividad de esos
procesos internos claves.

- **Financiera:** desde esta perspectiva, la atención tendría que estar centrada en la asignación adecuada y oportuna de recursos, y la minimización de costos.
- **Aprendizaje y crecimiento:** el foco estaría puesto en el desarrollo del talento humano y el fortalecimiento de las competencias del personal.

El CMI podría utilizarse para dar seguimiento al plan estratégico, estableciendo alguna periodicidad que permita detectar a tiempo cualquier desviación y tomar las decisiones correctivas correspondientes. Desde esta perspectiva tendría que dialogar con el área funcional encargada del control y gestión de la calidad del sistema de emergencia y seguridad.

Figura 8: Ventajas del Cuadro de Mando Integral

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

El empleo de un CMI contribuiría con información relevante en la elaboración de un informe anual de avances y logros del plan estratégico, con recomendaciones de replanteamiento de algunas estrategias (si fuera necesario). De ser así, estos informes anuales tendrían que incluirse dentro del sistema de reportería que, a su vez, tendrían que formar parte de la arquitectura de la información del sistema de emergencia y seguridad (ver Capítulo III de esta Guía).

2.10 Premisas del Plan

Es importante diferenciar entre condiciones y riesgos para el funcionamiento del sistema de emergencia y seguridad, y aquellas condiciones y riesgos para la ejecución de la planificación estratégica. En el primer caso el foco estaría puesto en el sistema de atención a emergencias, en el centro de operaciones o bien en la prestación de los servicios (riesgos sistemáticos y no sistemáticos). (Este tema se desarrolla en el Capítulo VIII de la presente Guía).

En esta sección se abordan las condiciones y riesgos para la ejecución de la planificación estratégica. Estos también tendrían que ser objeto de un análisis y seguimiento constante. Para ello, la atención tendría que centrarse en las premisas de partida y las condiciones o circunstancias, internas y externas, bajo las cuales se espera que esa planificación y el plan estratégico resultante, tengan lugar.

Las premisas y condiciones para un adecuado proceso de planificación y de gestión estratégica, que persigue el fortalecimiento del sistema de emergencia y seguridad en su conjunto, podrían ordenarse según tipo u origen. En general se trataría de premisas sistémicas, que refieren a aquellas condiciones básicas, y que, a modo de ejemplo, podrían distinguirse entre las siguientes:

- **Supuestos políticos:** Respaldo, voluntad y liderazgo requerido para alinear esfuerzos de los actores involucrados (internos) y concitar el apoyo de los grupos de interés (externos).
- **Supuestos legales:** Bases legales y normativas que facultan la conducción y ejecución de la planificación, la supervisión externa y administrativa.
- **Supuestos técnicos:** Las metodologías de gestión para el diseño, ejecución, seguimiento y evaluación de la planificación; y para la gestión adecuada de los riesgos.

- **Supuestos económico-financieros:** Provisión de recursos específicos adecuados y continuos, sujetos a una estimación y planificación validada por las autoridades y la supervisión en el uso de los recursos asignados.

Tabla 9: Ejemplo tabla para definir y explicitar los supuestos

Premisas	Supuestos
Supuestos políticos	• Respaldo de autoridad gubernamental • Interés de autoridades internas y externas • Liderazgo requerido para la conducción • Apoyo de grupos de interés (externos)
Supuestos legales	• Cumplimiento adecuado de las leyes y normas que sean aplicables • Marco legal general del Sistema • Normativas asociadas a la institucionalidad y coordinación de las entidades componentes del Sistema • Facultades y responsabilidades en la ejecución de la planificación, la supervisión externa y administrativa • Asuntos inter-agenciales • Conformación de comité directivo
Supuestos técnicos	• Conformación de equipos de trabajo multidisciplinarios • Metodologías de gestión en el diseño, ejecución, seguimiento y evaluación de los procesos asociados a la planeación estratégica • Planificación para la continuidad de las operaciones del Sistema • Gestión adecuada de los riesgos • Disponibilidad de información adecuada • Equipos humanos capacitados • Metodologías de seguimiento y cuantificación-cualificación (Cuadro de Mando Integral)
Supuestos económico-financieros	• Situación económica estable • Política de financiamiento asegurada para el funcionamiento en tiempos “normales” y en tiempos de “catástrofes” • Presupuesto delineado y asignado • Metodología de evaluación presupuestaria • Análisis de impacto social de los objetivos estratégicos

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

La planificación estratégica supone prever cambios en las condiciones (y sus impactos, en función de riesgos y probabilidad de afectación), bajo las cuales se pensaba que tendría lugar la implementación de los planes estratégicos y operativos. El análisis de cómo podrían afectar el curso y, consecuentemente, la posibilidad de alcanzar las metas y objetivos establecidos, y el funcionamiento del sistema de emergencia y seguridad tendría que ser una tarea permanente.

Es por ello que sería recomendable realizar ejercicios de análisis de escenarios posibles y también prospectivos para identificar condiciones presentes, emergentes y futuras bajo las cuales se considera que se pondrá en marcha y funcionará el plan estratégico.

La visualización y proyección de estas condiciones, permitiría a quienes conducen el proceso de planificación estar debidamente preparados ante posibles cambios. Más aún, facilitaría las posibilidades de distinguir si los cambios o distorsiones advertidas en el desempeño del sistema de emergencia y seguridad, se deben a la puesta en marcha de los planes operativos contenidos en el plan estratégico en

sí mismo, o bien al cambio de las circunstancias y condiciones internas y/o exógenas de funcionamiento (entorno).

2.11 Factores críticos para el éxito

Los Factores Claves para el Éxito (FCE), en ciertos contextos también llamados Factores Críticos para el Éxito, son aquellas condiciones o metas que ineludiblemente tendrían que ser alcanzadas para lograr los objetivos estratégicos.

Aunque la planificación estratégica produce una cantidad de objetivos y metas, no todos pueden ser considerados Factores Críticos para el Éxito. A continuación, se presentan algunos de los criterios para que objetivos y metas puedan ser considerados FCE:

- Son vitales o indispensables para la entidad
- Aportan beneficios a la entidad
- Pueden ser considerados metas de alto nivel
- Están relacionados con el plan estratégico

2.12 Identificación y análisis de riesgos

Toda actividad lleva implícito riesgos. La planificación estratégica también implicaría la identificación de riesgos o eventualidades que pudiesen afectar su implementación. Es por ello que no sólo es necesario identificarlos, sino también evaluar la probabilidad de que ocurran y el impacto que pudieran acarrear.

Existen distintas metodologías para la identificación y estimación de riesgos, incluyendo:

- Estándar ISO 21500:2012 Orientación sobre la gestión de proyectos
- Estándar ISO 31000:2018 Gestión de Riesgos
- Conjunto de Conocimientos sobre la Gestión de Proyectos (PMBOK, por sus siglas en inglés) del Instituto para la Gestión de Proyectos (PMI, por sus siglas en inglés),
- Guía PRAM de la Asociación para la Gestión de Proyectos (APM, por sus siglas en inglés), entre otras.

A pesar de la variedad de metodologías existentes, la mayoría converge en cuatro fases:

i. **Fase Identificación de Riesgos.** Esta fase constaría de los siguientes campos:

   a. **Prioridad:** Es la prioridad asignada al riesgo (Alta, Media o Baja).

   b. **Estatus del Riesgo:** Identifica si el riesgo está Activo (es decir, si el Riesgo está siendo Monitoreado y Controlado activamente) o Inactivo (No afecta en este momento, pero podría activarse en el futuro).

   c. **Evento del Riesgo/Oportunidad:** Explicación del Riesgo.

   d. **Síntoma o Disparador:** Situación que indica que el evento de riesgo está por ocurrir o ya se ha presentado.

   e. **Proyecto(s) Relacionado(s):** Describe los proyectos que se relacionan con el riesgo.

f. **Categoría o Aspecto Funcional:** Categoría del riesgo (ejemplo: Técnico, Administración del Proyecto, Funcional) o Aspecto Funcional (ejemplo: Legal, Seguridad).

g. **Fecha Identificación:** Fecha en la que se identificó el riesgo.

h. **Fase del Proyecto:** Fase del proyecto en la que se espera la ocurrencia del riesgo.

Tabla 10: Ejemplo de Tabla para la Identificación y clasificación de Riesgos

Prioridad	Estatus	Evento de Riesgo/Oportunidad	Descripción del Evento	Síntoma o Disparador	Proyecto Relacionado	Fecha y/o Fase	Categoría o Aspecto Funcional
	Activo	Contratación del personal.	Contratación del personal requerido para la expansión Norte.	El personal requerido para la ampliación Norte debe estar contratado al 27 Jun. 16. Personal administrativo contratado al 27 de Jun. 16 Personal técnico contratado al 25 de Abr. 16 Personal operativo contratado al 27 Jun. 16 Personal de las agencias seleccionado al 27 Jun. 16	- obra civil. - Mobiliario. - Implementar las licitaciones o donaciones tecnológicas	27 Jun. 16 Ejecución	Funcional

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

ii. **Fase Análisis de Riesgos**

- Análisis Cualitativo

  a. **Tipo:** Área/s impactada/s por el riesgo.

  b. **Probabilidad:** Evaluación cualitativa de la probabilidad de ocurrencia del evento de riesgo. Los valores válidos podrían ser: Muy Baja, Baja, Media, Alta y Muy Alta.

  c. **Impacto:** Severidad del efecto del riesgo en los objetivos del plan. Los valores válidos podrían ser: Muy Bajo, Bajo, Medio, Alto y Muy Alta.

  d. **Efectos:** Consecuencias estimadas a enfrentar post-riesgo.

- Análisis Cuantitativo

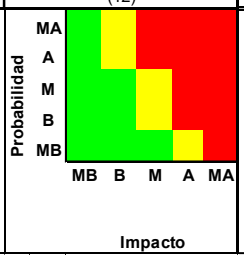
  a. **Probabilidad:** Esta celda se registraría automáticamente con base en la evaluación cualitativa de probabilidad. Muy baja = 10%, Baja = 30%, Media = 50%, Alta = 70% y Muy Alta = 90%.

  b. **Impacto:** Evaluación del impacto del riesgo especificado en valor monetario o días.

  c. **Efecto:** El efecto es el producto de la probabilidad por el impacto.

  d. **Costos:** Estimación de pérdidas económicas.

Tabla 11: Ejemplo de Tabla par el Análisis de Riesgo

Análisis Cualitativo				Análisis Cuantitativo		
Tipo	Probabilidad	Impacto	Matriz Riesgo	Probabilidad (%)	Impacto ($ o días)	Efecto ($ or días)
(9)	(10)	(11)	(12)	(13)	(14)	(15) =(13)x(14)
						

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

iii. **Fase Tratamiento de Riesgos** (Tabla 12: Ejemplo de Tabla para el Tratamiento de Riesgos)

Estrategia de Respuesta	
Estrategia	Respuesta Ventajas/Desventajas
Mitigar	Seguimiento a la contratación del personal.

a. **Estrategia:** Estrategia a utilizar para dar respuesta al riesgo.

   Los valores posibles podrían ser:

   - Para Riesgos Negativos (Amenazas): Mitigar oTransferir.
   - Para Riesgos Positivos (Oportunidades): Explotar, Compartir o Mejorar.

b. **Acción de Respuesta:** Acción de respuesta detallada a ser realizada.

c. **Elemento/s o Componente/s del plan estratégico afectado/s:** Diseño de cursos de acción alternativos como parte de la estrategia de respuesta.

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

iv. **Fase Monitoreo y Revisión** (Tabla 13: Ejemplo de Tabla para el Monitoreo y Revisión de los Riesgos)

Monitoreo y Control		
Responsable (Admin. Tarea)	Periodicidad del Estatus o Hito de Verificación	Fecha, Estatus y Comentarios de Revisión
RR.HH.	Semanalmente	15/1/2016 En Progreso de Revisión

a. **Responsabilidad:** Nombre del área, equipo, funcionario/a responsable por la gestión de cada uno de los riesgos.

b. **Periodicidad:** Cada cuánto tiempo o en qué momento específico se verificará el estatus del riesgo.

c. **Fecha, Estatus y Comentarios de Revisión:** Es la fecha de la última revisión, el estatus al momento de la revisión del riesgo y algún comentario derivado a partir de la revisión realizada.

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

La mayoría de las fases involucraría la realización de talleres, entrevistas, análisis de escenarios, encuestas y análisis de causa-raíz, entre otras herramientas para la recolección de información e insumos.

Una herramienta básica para la identificación y análisis de riesgos en la planificación estratégica es la matriz de riesgo. Los diferentes tipos de riesgo se posicionarían en una matriz de visualización a partir de una estimación alcanzada a través de la comparación de distintas fuentes de apreciación (talleres, entrevistas, encuestas, consultas, entre otras). La matriz ayudaría a identificar cuáles serían las prioridades, y hacia dónde tendrían que estar dirigidos los esfuerzos.

El foco tendría que estar puesto en el cuadrante de alto impacto y alta probabilidad de ocurrencia. La identificación tendría que dar lugar a un plan de mitigación, que incluiría responsables y cursos de acción alternativos.

A continuación, se presentan dos ejemplos de matrices de riesgo:

Tabla 14: Ejemplo 1 de Matriz de Riesgo

Plan Administración del Riesgo																							
Identificación									Análisis Cualitativo				Análisis Cuantitativo			Estrategia de Respuesta			Monitoreo y Control		
Prioridad	Estatus	ID #	Fecha y/o Fase	Categoría o Aspecto Funcional	Evento de Riesgo/Oportunidad	Descripción del Evento	Síntoma o Disparador	Proyecto Relacionado	Tipo	Probabilidad	Impacto	Matriz Riesgo	Probabilidad (%)	Impacto ($ o días)	Efecto ($ or días)	Estrategia	Respuesta Ventajas/Desventajas	Elemento del WBS afectado	Responsable (Admin. Tarea)	Periodicidad del Estatus o Hito de Verificación	Fecha, Estatus y Comentarios de Revisión
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)		(9)	(10)	(11)	(12)	(13)	(14)	15) =(13)x(14)	(16)	(17)	(18)	(19)	(20)	(21)
1	Activo	1	2/17/2020 Ejecución	Tecnico	Interrupción del sistema eléctrico/de respaldo de la información entre los distintos centros de atención	Interrupción del sistema eléctrico/de respaldo de la información entre los distintos centros de atención a Emergencia (PSAP Norte y PSAP Metro)	Falla o alarma crítica de los diferentes sistema de respaldo eletico de los distintos centros de atencion. Falla o alarma crítica de los diferentes sistemas de respaldo de la informacion de los distintos centros de atencion.	N/A	Calidad Tiempo	Alta	Alto	Probabilidad: MA, A, M, B, MB; Impacto: MB B M A MA; X				Mitigar	Aquirir e instalar equipos de respaldo Electricos y de los diferentes sistemas de informacion		Departamento de planificación, de logística y presupuesto	Semanal	

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

Tabla 15: Ejemplo 2 de Matriz de Riesgo

Identificación de Riesgo	Probabilidad	Impacto	Mitigación	Responsable(s)
Interrupción del financiamiento para el programa de mejora del sistema de control de gestión de los servicios	Media	Reducción del personal destinado a la detección de buenas prácticas e innovación	Plan de contención para alinear esfuerzos internos del área funcional para el talento humano	Departamento de planificación, de logística y presupuesto del servicio

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

2.13 Plan de continuidad en la planificación estratégica

Garantizar la continuidad operativa del sistema de atención a emergencias y seguridad tendría que ser uno de los objetivos principales del plan estratégico institucional. En línea con lo anterior, resultaría de vital importancia que el desarrollo del plan de continuidad sea incluido en la creación y posteriores actualizaciones del plan estratégico.

La elaboración del plan de continuidad tendría que partir con la identificación de los procesos y sistemas esenciales para la atención y respuesta a emergencias, en caso de desastre o evento no planificado. Tendría que venir acompañado de planes de contingencia que garanticen la continuidad operativa del Sistema.

Algunos puntos importantes a considerar para la creación del plan de continuidad serían:

- Identificar los procesos y sistemas críticos para el funcionamiento del Sistema, otorgando prioridad a aquellos esenciales.

- Definir los indicadores y niveles de servicio que estarán en efecto durante la contingencia.
- Definir el plan de retorno a la "nueva" normalidad post-evento de riesgo, una vez superada la contingencia, garantizando la integridad de los datos o informaciones.

Al momento de implementar los planes de continuidad, sería importante tener en cuenta las siguientes consideraciones:

- Determinar el alcance de un plan de continuidad a partir de la apreciación de los equipos involucrados en la ejecución de las actividades/servicios esenciales del sistema de emergencia y seguridad.
- Identificar mecanismos alternativos para acompañar a los niveles administrativos altos y medios, así como los equipos de las áreas funcionales.
- Definir el plan de manejo y comunicación ante crisis.
- Organizar sesiones de socialización y capacitación dirigidas al personal para asegurar su apoyo e involucramiento.
- Definir un plan para el seguimiento de condiciones internas y externas en la ejecución de la planificación estratégica, testeo de indicadores e índices alternativos en el Cuadro de Mando Integral (CMI).
- Propender a la retroalimentación para redefinir programas y procesos según los impactos experimentados y los efectos evaluados.

2.14 Prospectiva y adaptación

La planificación estratégica y la prospectiva estratégica van de la mano. Una vez diseñado el plan estratégico y puestos en ejecución los diferentes planes operativos que lo componen, es importante tomar en cuenta que el mismo no es una entidad estática. El plan estratégico tendría que entenderse como una herramienta en constante revisión y actualización (a realizarse cada 3-5 años), en función de una serie de factores, incluyendo:

- Las realidades cambiantes del entorno (por ejemplo, nuevas tecnologías)
- Las novedades institucionales (incorporación de nuevos servicios)
- Los resultados del CMI
- Los análisis de riesgo que se hubieran llevado a cabo

A su vez, la construcción de posibles escenarios futuros facilita al cuerpo directivo tomar decisiones más adecuadas en el presente y estar mejor preparados para lo que se podría avecinar en el futuro.

La prospectiva estratégica se basa en el análisis de la situación presente, la identificación de fuerzas impulsoras de cambio, la determinación de los principales problemas, desafíos y tendencias, la exploración de posibles acciones y decisiones, y la conformación de alianzas con el fin de construir el futuro deseado y evitar el futuro no deseado.

CAPÍTULO III: DISEÑO DEL SISTEMA

Introducción

El desarrollo de un sistema integrado supone un diseño y estructura de trabajo de los servicios públicos, a partir de facilitar el flujo de información, la centralización eficiente de comunicaciones, la coordinación de respuestas entre organismos pertinentes, según la naturaleza de los servicios requeridos, y la evaluación de procesos, operaciones y actividades (con una perspectiva cuantitativa y cualitativa).

En este Capítulo se abordan tres aspectos fundamentales: el modelo de funcionamiento, la estructura y organización (arquitectura institucional) y los requerimientos funcionales. En este último, se revisan la infraestructura/arquitectura tecnológica (*hardware* y *software*), la arquitectura de la información, y la infraestructura física y el equipamiento mínimo necesario para el funcionamiento de un sistema de emergencia y seguridad.

3.1. Modelos de funcionamiento

La prestación de servicios de emergencia y seguridad podría organizarse con base en diferentes modelos de funcionamiento, que varían en cuanto a estructura, mecanismos, niveles de integración y ámbitos de colaboración entre las distintas entidades que lo integran.

Con independencia de la denominación, generalmente la estructura del Sistema refleja un modelo de funcionamiento con base en una red de nodos, centros o puntos de atención de emergencias (PSAP, por su acrónimo en inglés).

La atención de una emergencia suele contemplar dos etapas: la etapa de procesamiento y la etapa operativa, cada una de ellas compuesta por las siguientes seis actividades principales:

- Etapa 1 Procesamiento:
    a) Geolocalización e identificación de la situación
    b) Levantamiento de la información y tipificación
    c) Creación y documentación del evento
    d) Asignación de la unidad

- Etapa 2 Operativa:
    e) Asistencia de la unidad o dispositivo
    f) Documentación y cierre operativo del evento

a) **Geolocalización e identificación de la situación:** Se recibe la solicitud de la persona usuaria y de manera automática, vía sistemas de información geográfica, y/o por medio de una serie de preguntas, se establecería el lugar desde donde se está reportando la emergencia, con la mayor precisión posible. Se seguirían los protocolos establecidos, incluyendo guión con una serie de preguntas estandarizadas, dirigidas a determinar el tipo de emergencia y de riesgo, el grado de urgencia y priorización, y el tipo de servicio a despachar. (Etapa 1)

b) **Levantamiento de la información y tipificación:** Búsqueda y verificación de antecedentes**.** Se identifica la dirección del lugar en que está ocurriendo el evento, lo que está aconteciendo y los datos del usuario. Se tipifica el incidente con base a una preevaluación, clasificación y priorización, de acuerdo a la tipología de incidentes parametrizados en el sistema computarizado. (Etapa 1)

c) **Creación y documentación del evento:** Reporte para notificar a las unidades de respuesta que tendrían que asistir al lugar de los hechos, de acuerdo a la parametrización del incidente. Una vez

creado, sería conveniente que se recolectasen otros datos para completar y complementar la información sobre el incidente y la escena. (Etapa 1)

d) **Asignación de la unidad:** Notificación y despacho de la unidad más próxima al evento por los medios establecidos (radio, flota, plataforma u otro canal), y asignación del evento. Posibilidad de solicitar apoyo de otras entidades de primera respuesta o de apoyo, y asignar unidades adicionales. (Etapa 1)

e) **Asistencia de la unidad:** Seguimiento y contacto con las unidades de respuesta desde la llegada al lugar del incidente hasta su retiro, reportando lo que está aconteciendo en el lugar. (Etapa 2)

f) **Documentación y cierre operativo del evento:** Documentar el evento con toda la información recolectada, incluyendo durante el despacho y la asistencia. Cerrar el evento cumpliendo con los protocolos establecidos. (Etapa 2)

Figura 16: Seis tareas operativas básicas

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

No existe una única manera de llevar a cabo ni de combinar las seis tareas operativas básicas. De hecho, se habrían identificado al menos seis modelos de funcionamiento que se diferencian entre sí con base en la asignación de responsabilidades, los grados de concentración y la ubicación institucional de esas seis tareas operativas. Esos modelos de funcionamiento son:

Modelo A: Las entidades operativas de emergencia reciben, administran llamadas de manera independiente y responden a las solicitudes de manera independiente. Se trata de un modelo esencialmente autónomo comprendiendo los Etapas 1 y 2.

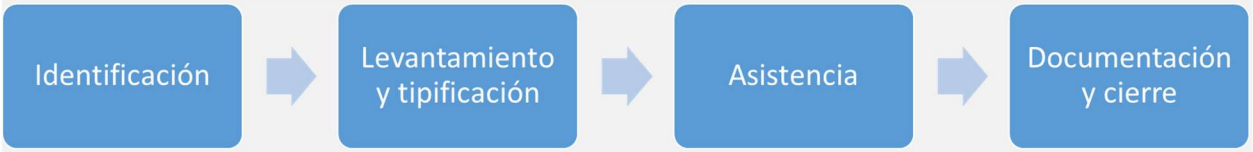
Modelo B: Existe una central de recepción de solicitudes, llamadas y reportes de emergencia que las canaliza a la/s institución/es de respuesta (Etapa 1). El despacho cae bajo la responsabilidad de cada institución y es independiente (Etapa 2).

Figura 17: Modelo B

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

Modelo C: Existe un punto único o central de recepción de solicitudes, llamadas y reportes en una sala de coordinación (Etapa 1), que enruta la comunicación a una unidad operativa, dando seguimiento al servicio hasta el cierre operativo del caso, pero el despacho de las unidades se realiza desde otro lugar (Etapa 2).

Figura 18: Modelo C



Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

Modelo D: Existe una central integrada por las instituciones de respuesta, que funciona desde una sala de recepción de solicitudes, llamadas y reporte, y de coordinación, comando y control, concentrando en un mismo lugar, las 6 tareas operativas básicas (Etapas 1 y 2).

Modelo E: Existe una entidad independiente de las instituciones de respuesta, que administra el Sistema y los recursos de las entidades operativas, a través de una central integrada de recepción/respuesta o sala de coordinación, comando y control (PSAP).

Modelo F: Existe una red de centros de atención o puntos de respuesta de emergencia y seguridad (PSAP) interconectados por un sistema tecnológico integrado. Esta prestaría servicios remotos: recibiría, daría asistencia remota y seguimiento al servicio hasta el cierre, sin involucrarse directamente en el despacho de unidades.

3.2. Estructura y organización (arquitectura institucional)

El modelo de funcionamiento que se adopte, precisaría de una estructura organizacional que esté alineada con la misión, visión y lineamientos estratégicos establecidos (ver Capítulo II de esta Guía).

La estructura organizacional podría plantearse con base en áreas funcionales, que podrían agruparse según dos tipos: principales o misionales y de apoyo o de soporte.

Ejemplos de áreas funcionales que podrían ser consideradas principales o misionales:

- **Gestión de Operaciones:** Su función principal sería coordinar y encargarse de las operaciones necesarias para garantizar la oportuna, eficiente y eficaz prestación del servicio al usuario, así como la coordinación institucional e interinstitucional para el aseguramiento de la interoperabilidad del Sistema.
- **Gestión de Procesos y Protocolos:** Su función principal sería asegurar el diseño de cada uno de los procesos y sus respectivos protocolos de actuación e interacción para la atención, teniendo en cuenta leyes, reglamentos y normas o estándares que permitan el cumplimiento de los objetivos.
- **Gestión de Calidad:** Su función principal sería implementar y promover el sistema y los mecanismos de aseguramiento de la calidad, y las herramientas que direccionen hacia el mejoramiento continuo, así como la medición y monitoreo de la calidad de la prestación del servicio, teniendo en cuenta la retroalimentación de las personas usuarias y de las entidades de apoyo o articuladas (ver Capítulo IV de esta Guía).
- **Tecnologías de la Información y la Comunicación**: Su función principal sería definir la plataforma tecnológica base, así como garantizar la disponibilidad y funcionamiento de la infraestructura tecnológica que soportan las operaciones del Sistema, tomando en cuenta la gestión de la seguridad de la información, la planificación del crecimiento de la capacidad, planes de contingencias como constituyentes de la continuidad de las operaciones.

- **Gestión de Seguridad:** Su función principal sería velar por la seguridad de las instalaciones, del personal, los equipos, propiedades y visitantes del Sistema, identificando las vulnerabilidades, amenazas y las medidas que pueden ejecutarse para proteger física y digitalmente los recursos y la información de la institución (ver Capítulo VIII de esta Guía).

- **Gestión de Información y Análisis:** Su función principal sería el procesamiento de los indicadores operativos e insumos para la gestión administrativa, generando información oportuna y confiable que sirva de base para la toma de decisiones y el mejoramiento del servicio (ver Capítulo VII de esta Guía).

Ejemplos de áreas funcionales que podrían ser consideradas de apoyo o de soporte:

- **Talento Humano:** Su función principal sería crear políticas, administrar y gestionar de manera oportuna el talento humano que apoye de manera eficiente la gestión del servicio, por medio de procesos de selección, reclutamiento, capacitación y evaluación continua, gestión del clima laboral y gestión de la compensación entre otros. (Ver Capítulo VI de esta Guía).

- **Administración y Finanzas:** Su función principal sería gestionar, coordinar y optimizar el uso de los recursos financieros y materiales que permita apoyar de manera eficiente la gestión y continuidad del servicio.

- **Jurídica:** Su función principal sería brindar asesoría jurídica especializada y oportuna, así como gestionar respuestas oportunas a las actividades de índole legal del Sistema.

- **Comunicación:** Su función principal sería diseñar estrategias de relacionamiento con el entorno (incluyendo las entidades del tercer anillo), el establecimiento de canales de comunicación con la población y el fortalecimiento de la imagen institucional, mediante el lanzamiento de campañas y difusión de actividades, entre otras acciones comunicaciones. (Ver Capítulo IX de esta Guía).

- **Planificación Estratégica y Operativa:** Su función principal sería diseñar y dar seguimiento a la ejecución de planes de desarrollo que permitan alcanzar los objetivos de fortalecimiento, crecimiento y aseguramiento de la continuidad del servicio. (Ver Capítulo II de esta Guía).

- **Gestión de Proyectos:** Su función principal sería diseñar, ejecutar y supervisar los planes, programas y proyectos que apoyen al logro de las estrategias descritas en la planificación institucional.

La estructura organizacional tendría que quedar plasmada en un organigrama, teniendo en cuenta lo establecido en el marco normativo y el mapa de procesos (estratégicos, misionales y de apoyo, entre otros).

En línea con el mapa de procesos, el trabajo de cada área funcional tendría que estar sustentado en la identificación y protocolización de procesos que, a su vez, podrían clasificarse como críticos o de apoyo.

Asimismo, al establecer las áreas funcionales resultaría pertinente definir también las competencias técnicas que cada una de ellas precisaría. A su vez, esa definición facilitaría la identificación de los perfiles profesionales necesarios para cada posición. (Ver Capítulo VI de esta Guía).

3.3. Requerimientos funcionales

Entre los requerimientos funcionales de un sistema de emergencia y seguridad, se podrían mencionar al menos tres:

- Infraestructura/arquitectura tecnológica
- Arquitectura de la información
- Infraestructura física y equipamiento

3.3.1. Infraestructura/arquitectura tecnológica

En el diseño de un sistema de emergencia y seguridad se tendría que considerar las normas técnicas asociadas al empleo intensivo de las tecnologías de información y comunicación disponibles.

Hay al menos cuatro organizaciones con influencia internacional que establecen directrices y normas técnicas en relación a las tecnologías para el tratamiento de emergencias:

- Unión Internacional de Telecomunicaciones (UIT)
- *European Telecommunications Standards Institute* (ETSI)
- *European Emergency Number Association* (EENA)
- *National Emergency Number Association Estados Unidos* (NENA)

Los estándares de estas organizaciones son complementarios. La elección dependerá de los diseños asociados al Sistema y de las expectativas, por ejemplo, en torno a telefonía fija, móvil, radio, sistemas convergentes, tecnologías de transmisión e internet.

El ecosistema tecnológico de un centro de atención de emergencias y seguridad tendría que incluir todos los componentes de *hardware* y *software* necesarios para gestionar efectivamente los procesos operativos y administrativos vinculados a las áreas funcionales.

A partir de las normas técnicas existentes, el diseño del sistema operativo tendría que contemplar los siguientes componentes tecnológicos de información y comunicación:

a. Infraestructura de *hardware* y servicios web, servicios de correo, servicios de archivos, servicios de red, servicios de base de datos y servicios de aplicaciones, entre otros.

   Adicionalmente, respecto a los servidores de base de datos, se recomendaría que posean las siguientes características técnicas:

   - Alta disponibilidad (CLUSTER)
   - Replicación de base de datos
   - Almacenamiento conforme a los sistemas operacionales
   - Herramienta para la minería, análisis y visualización de datos
   - Herramienta de búsqueda y reportería
   - Herramienta de *on-line analytical processing* (OLAP)
   - Herramienta de Información de Gestión (*Executive Information System*, EIS)
   - Herramienta de *Decision Support Systems* (DSS)

b. Infraestructura de alta disponibilidad, a partir de la existencia de sistemas, matrices, red y fuentes de poder redundantes; interruptor de transferencia automática; equipos de redes y conectividad, entre otros.

c. Sistema de radio comunicación entre las áreas y entidades vinculadas a la respuesta. La red de radiocomunicación tendría que ser digital y contar con ciertas características como el cifrado de datos. La escalabilidad de la red y la interoperabilidad con otros sistemas de comunicación existentes permitirían ofrecer mayor cobertura geográfica, en menor tiempo y a menor costo.

d. La compatibilidad tecnológica e integración de sistemas del siguiente tipo:

    - Sistema de Recepción de Llamadas de Emergencias (CTI)
    - Sistema de generación de ficha, código y número de registro
    - Sistema de identificación de número teléfono (identificación de IP)
    - Sistema de Información Geográfica (GIS)
    - Sistema de monitoreo y geolocalización de unidades de respuesta (AVL)
    - Cámaras de uso personal o videovigilancia personal para monitorear lo que está ocurriendo en terreno
    - Sistema de despacho asistido computarizado (CAD)
    - Protocolo de derivación según preevaluación (PDS, *Priority Dispatch System* M*P*F)
    - PABX (*Private Automatic Branch Exchange*) o central privada automática (enrutamiento, derivación, en cola - erlang, llamadas perdidas)
    - *Computer aided call handling* (CACH)
    - *Mobile data terminals* (MDTs)
    - *Mobile data computers* (MDCs)
    - Sistema de radiocomunicaciones móviles (*trunking*)
    - Comunicaciones radiales entre Centro de Atención de Emergencia y Seguridad (CAES) y vehículos y dispositivos de primera respuesta (PRV o *Primary Response Vehicle*; *Ambulance y Advanced Life Support*).
    - Reporte de estado de unidades/vehículos disponibles (PRVs)
    - Reporte de decisiones adoptadas (ATR)
    - Sistema de monitoreo y análisis de imágenes por video vigilancia
    - Sistema de alertas
    - Solución de video *wall*

e. Acceso a Internet, sitio web, servicios web

3.3.2. Arquitectura de la información

Uno de los elementos de mayor relevancia para disponer de una arquitectura de información adecuada a las necesidades del centro de atención de emergencias y seguridad, es que su diseño responda a las necesidades de información tanto operativas, estratégicas, de política pública como de gestión de la calidad de los servicios.

Los aspectos que componen esa arquitectura tendrían que estar ligados a los procesos y etapas directamente relacionados con la atención de las emergencias, así como con los controles e indicadores establecidos para monitorear y evaluar el servicio que se brinda, el funcionamiento y el desempeño en las seis tareas operativas básicas (Etapas 1 y 2), y las metas y objetivos establecidos en el plan estratégico.

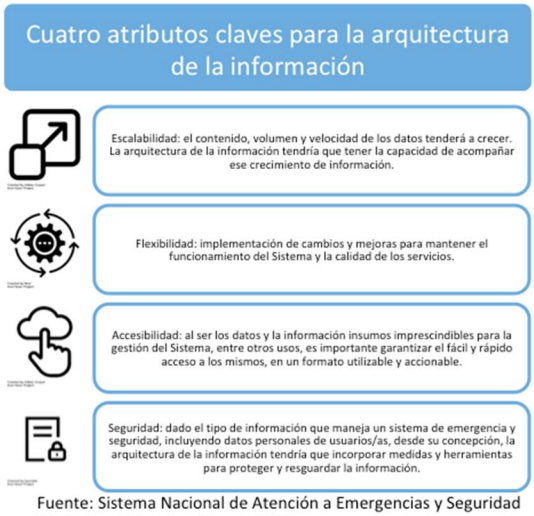
Dependiendo del modelo de funcionamiento del sistema de emergencia y seguridad, la arquitectura de la información tendría que estar alineada con y brindar soporte a las seis tareas operativas básicas, facilitando el registro de datos e informaciones y la comunicación desde el inicio hasta el cierre del evento.

En general, al momento de diseñar la arquitectura de la información, resultaría necesario considerar los siguientes aspectos:

- Los usos que se le dará a la información (para qué), qué tipo de información se requiere, en qué formato, para quiénes y en qué momento (se recolecta y entrega).
- La definición de tipologías, clasificaciones, categorías, etiquetas y palabras claves para estructurar, organizar, relacionar la información, y facilitar su búsqueda y recuperación.
- La generación de un vocabulario común y estandarizado.
- Las vías, canales o medios a través de las cuales el centro de atención recibirá las alertas de emergencia: llamada, video vigilancia, botón de auxilio, aplicación móvil, mensajería de texto, entre otras. Si en la recepción de la emergencia interactúan una o más plataformas, la decisión sobre el almacenamiento, organización y estructura de la información será diferente.
- El mecanismo de registro de las alertas de emergencia.
- El mecanismo de retroalimentación entre las unidades en campo y el centro de atención.
- Los formularios para la captura de la información intentando buscar un equilibrio entre el tiempo de captura y los requerimientos de información.
- Los reportes y herramientas de visualización de datos que serán generados para retroalimentar las operaciones del centro.
- Espacio suficiente para almacenar y acceder a los datos y la información capturada.

Existirían al menos cuatro atributos recomendables al momento de concebir la arquitectura de los datos: escalabilidad, flexibilidad, accesibilidad y seguridad.

Figura 19: Algunos atributos recomendables para la arquitectura de la información



Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

3.3.2.1. Tipología de incidentes

Para garantizar una adecuada atención y respuesta ante los eventos de emergencia, resultaría necesario establecer en la arquitectura de la información una tipología de incidentes, con categorías exclusivas y mutuamente excluyentes, claramente definidas, abarcando todos los ámbitos posibles, y siendo consistentes con tipologías existentes.

Adicionalmente, también sería necesario establecer qué se concebirá como "incidente" para fines operativos y su relación con una tipología de emergencias. Esta relación podría definirse de uno a uno, en la que para un tipo de emergencia se tendría un tipo de incidente identificado, que es el que generaría la alerta. Otra posible relación es de uno a muchos, en la que a una emergencia se le podrían asociar diversos incidentes, a partir de las especificaciones y asociaciones que se definan.

En la creación de esta tipología, dependiendo del modelo de funcionamiento, también habría que vincular cada incidente con un tipo de respuesta. La clasificación y/o el reagrupamiento de uno o varios incidentes, según las especificaciones y reglas de asociaciones, se vería reflejado en el enrutamiento y tipo de despacho, con la posibilidad de sumar a otras entidades en la respuesta.

A medida que se expanda y fortalezca el sistema de atención de emergencia y seguridad, sería posible incorporar nuevos tipos de incidentes, así como cambios o ajustes en las definiciones. Un requisito esencial sería documentar estos cambios, tanto si son de estándares y conceptos, como de codificación.

La tipología de incidentes contendría categorías y subtipos o subgrupos, y las reglas de clasificación. La tipología y las reglas tendrían que ser comunes a todas las entidades participantes del Sistema en las Etapas 1 y 2. A modo de ejemplo, a continuación, se presentan algunas de estas posibles categorías generales:

- **Delitos, violencias e incidentes de seguridad pública/ciudadana:** Son eventos que ponen en riesgo la vida y/o los bienes de las personas. Por ejemplo, robos a propiedades, riñas, violencia doméstica o intrafamiliar, violencia de género, abusos a menores, daños a bienes y propiedades, entre otros.
- **Incidentes de atención a la salud:** Son eventos que ponen en peligro inmediato la vida y la integridad física de las personas. Por ejemplo, hemorragias, heridas de armas blancas

y armas de fuego, fracturas, intoxicaciones, envenenamientos, infartos y dificultad respiratoria, entre otros.

- **Incidentes de atención a la salud mental:** Son eventos en donde la persona evidencia comportamientos de riesgo, incluyendo intentos suicidas, alteración del comportamiento por abusos de sustancias, depresión, trastornos y enfermedades mentales, entre otros.
- **Desastres:** Son eventos de magnitud que afectan grandes áreas territoriales, además intervienen varias instituciones de respuesta durante periodos prolongados de atención. Por ejemplo, inundaciones, incendios forestales, derramamientos de combustible, tsunamis, huracanes, terremotos, y derrumbes, entre otros.
- **Siniestros y crisis:** Son eventos focalizados en los que intervienen una o varias agencias de respuesta durante períodos prolongados de atención. Por ejemplo, explosiones, incendios y rescate de personas, entre otros.
- **Afectaciones a la seguridad nacional y/o de Estado:** Son eventos vinculados a la alteración del orden público, que podrían amenazar la integridad de la nación, poniendo en riesgo la vigencia de sus intereses y objetivos nacionales. Por ejemplo, ataques terroristas.
- **Eventos programados:** Son eventos que ya se conoce con antelación que ocurrirán (a modo de ejemplo, la voladura de un edificio) y para los que el sistema de emergencia y seguridad espera recibir un alto volumen de llamadas.

3.3.2.2. Tipología de canales de acceso

En lo que respecta a la arquitectura de la información para la gestión de emergencias, resultaría fundamental la categorización de los canales para recibir solicitudes, llamadas y reportes de los/as usuarios/as, generar alertas y establecer mecanismos de comunicación con la población.

En ese sentido, uno de los principales canales sería contar con un número telefónico único. Su funcionamiento no descartaría la activación de otros mecanismos de contacto o reporte, incluyendo: mensajería de texto (SMS), video vigilancia, aplicación móvil, entre otras.

En el diseño se tendrían que aprovechar los recientes desarrollos de las tecnologías de la información y la comunicación (TICs) y los estándares técnicos ya desarrollados. También se tendrían que tomar en consideración las distintas características y necesidades de la población usuaria, incluyendo el acceso a personas con discapacidades y a grupos y subgrupos en situación de vulnerabilidad. Para ello se podría incorporar dispositivos TTY, botones de pánico y RTT (*real time text*), entre otros.

3.3.2.3. Tipología de llamadas

Teniendo en cuenta la masividad de contactos por vía telefónica que suelen recibir los centros de atención de emergencias y seguridad, la arquitectura de la información tendría que incorporar una tipificación de las llamadas, cada una con sus respectivas definiciones, así como criterios para su tratamiento. Asimismo, también tendría que contar con un mecanismo de priorización y un conjunto de cursos de acción o protocolos de actuación predefinidos para reaccionar y responder frente a ellas.

La clasificación podría incorporar tres criterios para diferenciar entre las llamadas que, a su vez, tendrían que venir acompañadas de protocolos específicos para su tratamiento:

- Llamadas con o sin audio
- Llamadas procedentes e improcedentes

- Llamadas con o sin movilización de unidades o dispositivos

En el caso específico de las llamadas procedentes, estas podrían organizarse con base en las siguientes categorías, u otras que pudieran surgir de acuerdo al contexto de cada país:

Tabla 20: Clasificación llamadas procedentes

Clasificación	Descripciones
Emergencia	Evento que puede poner en riesgo la vida, la salud mental y emocional, la seguridad o integridad de las personas físicas o jurídicas, o de los bienes, y que exige un auxilio inmediato.
Urgencia	Circunstancia o evento que precisa atención inmediata, pero que no es de emergencia, y no representa peligro inmediato ni inminente.
Denuncia	Notificación de que se está cometiendo un delito o una infracción.
Servicios y asistencia	Llamadas para solicitar asistencia que requiere el acompañamiento de una unidad de respuesta.
Consulta	Llamadas para solicitar información sobre los servicios ofrecidos o consultas sobre temas específicos que maneja el sistema de emergencia y seguridad.

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

Adicionalmente, las llamadas procedentes de emergencia podrían ser de diferentes tipos, en función de la tipología de incidentes ya presentada:

- Delitos, violencias y seguridad pública/ciudadana
- Salud
- Salud mental
- Desastres
- Siniestros/crisis
- Seguridad nacional
- Eventos programados

3.3.2.4. Tipología de niveles de priorización

Otra herramienta fundamental sería contar con un esquema para establecer la priorización de las solicitudes, llamadas y reportes recibidos. Siguiendo con el ejemplo de la Tabla 1, un esquema de priorización podría ser el siguiente:

Tabla 21: Esquema de priorización

Clasificación	Priorización
Emergencia	**1**
Urgencia	**2**
Denuncias	**3**
Servicios y asistencia	**4**
Consultas	**5**

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

- **Nivel o Priorización 1:** Es todo tipo de situación o evento en el cual existe un riesgo inminente contra la integridad de las personas o sus bienes y/o de afectación a la población o industria, y que por lo tanto precisan de una atención inmediata.

  Las solicitudes, reportes y llamadas que alertan este tipo de situación son clasificadas como de emergencia y tendrían que ser gestionadas sin retraso, activando de forma inmediata el recurso de respuesta más adecuado. Suelen clasificarse como de "prioridad alta" o de "atención inmediata" y, en ocasiones, se las visualiza con el color rojo.

  Ejemplos de situaciones de emergencia serían: situaciones en las que peligra la vida, delitos graves, como violencia contra mujeres, niñas, niños y adolescentes, situaciones en las que peligra la propiedad de las personas, y eventos hidrometeorológicos.

- **Nivel o Priorización 2:** Es todo tipo de situación o evento sin riesgo inminente pero que podrían afectar la integridad de las personas o sus bienes, a la población o la industria pero que, no obstante, precisa de una respuesta o atención lo antes posible.

  Este tipo de situaciones o eventos tendrían que ser atendidos luego de haberse despachado los recursos para emergencias del Nivel o Prioridad 1. Suelen clasificarse como de "prioridad intermedia" o de "atención prioritaria, y se las suele visualizar con el color naranja.

  Ejemplos de situaciones de Nivel 2 serían: accidente en el hogar, en el que no peligra la vida de ninguna persona.

- **Nivel o Prioridad 3:** Es todo tipo de situación o evento en el que existe una urgencia de "prioridad baja" ya que no se identifica riesgo para las personas o sus bienes, ni afectación de la población o industria. Por lo tanto, no requieren de atención inmediata. Se tendrían que atender una vez cerrados los casos de Nivel o Prioridad 1 y Nivel o Prioridad 2, cuando se tengan unidades de respuesta disponibles.

  Suelen ser rotuladas como de "prioridad baja" o de "atención sin urgencia" y visualizadas con el color amarillo.

  Ejemplo de este tipo de situaciones de Nivel 3 serían: caída de árboles y caída de bardas, entre otros.

- **Nivel o Prioridad 4:** Es todo tipo de situación o evento que no presenta una urgencia, pero podría o no precisar de algún recurso para su solución; o bien podría registrarse como recepción de información útil.

  Serían atendidas luego de haber sido solucionadas las prioridades anteriores, de manera presencial, por vía telefónica o en forma remota.

- **Nivel o Prioridad 5:** Llamadas para solicitar información sobre los servicios ofrecidos o consultas sobre temas específicos que maneja el sistema de emergencia y seguridad.
  Su atención quedaría relegada a último lugar, luego de canalizadas las anteriores.

Además de una numeración para indicar el orden de priorización y de indicadores cualitativos, la categorización también podría venir acompañada de una semaforización.

Cada uno de estos niveles o prioridades podría ser objeto de una subescala interna.

3.3.2.5. Llamadas improcedentes

Las llamadas improcedentes llevan a un mal uso de los recursos del Sistema. Aún cuando no den origen a una respuesta de emergencia, urgencia, denuncia, servicios y asistencia ni consulta, sería aconsejable incorporar una tipología y cursos de acción predefinidos, como parte de la arquitectura de la información. Este tratamiento estandarizado de las llamadas improcedentes facilitaría su análisis posterior, la identificación de patrones de mal uso del servicio, y el diseño de eventuales posibles soluciones.

A continuación, se ofrece un ejemplo de tipología de llamadas improcedentes con posibles categorías a considerar:

- **Llamada de falsas emergencias:** Llamadas para reportar situaciones ficticias de emergencias, que provocan el desplazamiento de las unidades de respuesta.
- **Llamada abandonada:** Cuando alguien llama al centro de atención y cuelga antes de ser atendido.
- **Llamada colgada:** Cuando alguien llama al centro de atención de forma maliciosa o accidental, y la llamada se interrumpe luego de haber sido contestada por la operadora.
- **Llamada equivocada:** Llamada que se realiza al centro de atención de forma errónea, sin intención.
- **Llamada molestosa:** Llamadas obscenas, morbosas o insultantes, que se realizan por entretenimiento o diversión.

Inicialmente, las siguientes llamadas podrían ser consideradas como improcedentes:

- **Llamada cancelada:** Llamada que se termina porque la operadora o quien llamó cuelga, o por alguna falla del sistema.
- **Llamada de no emergencia:** Llamada en la que no se describe una situación tipificada como emergencia, que puede ser importante o urgente, pero debe ser atendida a través de otras vías de respuesta.
- **Llamada redundante:** Llamada que ya ha sido reportada y está siendo atendida por las unidades de respuesta.
- **Llamada silenciosa:** Llamada contestada por la operadora en las que no se escucha ninguna voz o a nadie hablando de forma directa.

Sin embargo, habría que darles un tratamiento especial para descartar que, efectivamente, se trata de llamadas improcedentes. Para ello, los protocolos de actuación que se elaboren al respecto, resultarán fundamentales.

3.3.2.6. Captura de información de los incidentes

Como parte de la arquitectura de la información sería necesario definir los datos a capturar en cada solicitud, llamada o reporte de incidente, desde la recepción hasta el cierre del caso. La determinación de qué insumos recolectar tendría que responder a las necesidades de información para una adecuada prestación del servicio. Adicionalmente, también podría responder a la necesidad de generar más datos agregados para evaluar el funcionamiento y la calidad del servicio que brinda el Sistema.

Hay al menos cuatro preguntas que podrían guiar este importante paso del diseño de la arquitectura de la información:

- Qué datos/información capturar, qué datos/información se podrían extraer/exportar de otras bases de datos.
- En qué momento/s realizar la captura, extracción/exportación, consolidación y combinación de los datos.
- Cómo capturar, empleando protocolos y plantillas predeterminadas para estandarizar tanto los datos que se recolectan como la metodología que se utiliza para hacerlo.
- Dónde almacenar, cómo respaldar y proteger datos e informaciones. Para una gestión eficiente de información sería recomendable una arquitectura informática que contemple un repositorio exclusivo y centralizado, y con un único motor de bases de datos.

3.3.2.7. Bases de datos interoperables y relacionadas

La interoperabilidad se refiere a la funcionalidad de los sistemas de información para intercambiar datos o antecedentes de distinta naturaleza y facilitar su uso. La integración que permite la interoperabilidad de las bases de datos resulta clave para un uso más eficaz, eficiente, oportuno de la información, repercutiendo positivamente en el funcionamiento y la calidad del servicio que se brinda.

En un sistema de emergencia y seguridad se tendrían que crear varias bases de datos vinculadas a las solicitudes, llamadas y reportes de emergencias, al despacho de unidades y a la asistencia que brindan, a la videovigilancia, y a otros potenciales servicios que se pudieran estar brindando. Estas bases de datos contendrían información sobre atributos de las emergencias y las personas, ya sea que se disponga de una plataforma integrada para la atención de las emergencias o de múltiples plataformas, tendría que identificarse dónde y cómo estos sistemas podrían comunicarse entre sí e intercambiar, almacenar y resguardar la información.

La interoperabilidad de las bases de datos y la integración de la información tendría que regirse por los principios de protección de datos.

3.3.2.8. Procesamiento, análisis y visualización de datos

Además de los datos e indicadores resultantes de la estructura que se diseñe y de las bases de datos que se desarrollen para su captura, uso e integración, resultaría necesario contar con una herramienta para el procesamiento, análisis y visualización de los datos, en los diferentes niveles de funcionamiento del Sistema (operativo, táctico y estratégico).

A continuación, se especifican al menos cuatro dimensiones que se tendrían que definir para configurar un sistema de procesamiento, análisis y visualización de datos y estadística:

- **Tipo de datos:** estructurados, no estructurados
- **Foco de análisis:** reportes, informes, indicadores claves de gestión (KPI, por su acrónimo en inglés), análisis de tendencias, patrones, correlaciones, modelos
- **Tipo de análisis:** retrospectivo, descriptivo, predictivo, prescriptivo
- **Proceso de análisis:** estático, comparativo, explorativo, experimental

3.3.2.9. Generación y uso de la información

El tipo de información que estaría disponible dentro del centro de atención de emergencias y seguridad dependería, sustantivamente, de la manera cómo se configure la arquitectura de la información, incluyendo las diferentes tipologías de incidentes, solicitudes, llamadas y reportes, las categorizaciones y clasificaciones, la captura y almacenamiento de la información, las normas técnicas para la integración de

las bases de datos y la interoperabilidad. Es por ello que la arquitectura de la información tendría que idearse en función de los tipos de información que se precisarán y los usos que se le dará a la misma.

Uno de los usos más frecuentes de la información tendría lugar en lo inmediato, en el campo operativo, para guiar en tiempo real la respuesta y el servicio que se brinda en una emergencia.

Posteriormente también podría servir como insumo para monitorear y evaluar el funcionamiento del sistema de emergencia y seguridad, y la calidad de los servicios prestados. A partir de desviaciones o deficiencias identificadas, serviría para priorizar áreas de intervención e informar el diseño de medidas en aras de la mejora continua del Sistema.

Asimismo, resultaría útil, en su forma más agregada, para alimentar y dar soporte al proceso de planificación estratégica, así como para dar cuenta de los avances alcanzados en relación a los objetivos y las metas establecidos.

Adicionalmente, también podría ser utilizada más allá del propio sistema de emergencia y seguridad, en al menos dos contextos o situaciones externos:

- Para instancias prejudiciales, investigaciones criminales y procesos penales (ver Capítulo VII de esta Guía); y,
- Para el diseño, monitoreo y evaluación de programas y políticas públicas (ver Capítulo VII de esta Guía).

3.3.2.10. Sistema de reportería

Para definir los tipos de reportes que producirá el sistema de emergencia y seguridad, se podría comenzar identificando a los potenciales usuarios y al tipo de información que precisarían. Luego, para cada tipo de reporte tendrían que definirse algunas características, incluyendo: objetivo, formato, periodicidad, distribución, área responsable y lugar de almacenamiento y acceso, entre otros elementos.

Los reportes podrían brindar información sobre el funcionamiento del Sistema en lo que respecta a la atención y respuesta a las emergencias, a partir de una matriz de indicadores predefinidos. Esta matriz tendría que ser parte del sistema de gestión de la calidad y podría incluir indicadores de actividad, de gestión o administración, de procesos y de resultados, entre otros.

En función de la información que el Sistema genere, a las herramientas de procesamiento, análisis y visualización de datos disponibles, a las competencias técnicas del personal, y a los usos que se le dará a la información, se podrían definir diferentes tipos de reportes. A modo de ejemplo, se podrían considerar al menos cinco tipos de reportes:

- Reportería sobre el desempeño y el desarrollo del talento humano
- Reportería de gestión (resultado y productividad)
- Reportería de atención (ligada los servicios brindados)
- Reportería financiera-administrativa
- Reportería de proyectos

En función de las posibilidades tecnológicas, se tendría que contar con plataformas que permitan la generación y el envío de reportes de forma automatizada. Otras funcionalidades útiles a considerar el momento de diseñar un sistema de reportería serían:

- Repositorio común

- Parámetros y motor de búsqueda: a través de la especificación de palabras claves o combinaciones, para encontrar reportes rápidamente
- Estandarización de los formatos de tablas, gráficos y demás instrumentos para la presentación y visualización de los datos
- Opción de envío o descarga en diferentes formatos
- Actualizaciones en tiempo real
- Visualización de los datos tipo *dashboard* o tablero de control

3.3.2.11. Sistema de gestión de documentos

Como resultado de la arquitectura de la información y del sistema de reportería que esta posibilite, el centro de atención de emergencias y seguridad tendría a su disposición una serie de documentos, tanto físicos como digitales.

Para poder gestionar efectiva y eficientemente esos documentos, sería necesario definir una tipología, así como también una clasificación basada en la confidencialidad de la misma (a modo de ejemplo: confidencial, reservada, clasificada y pública), en línea con la legislación de cada país, incluyendo las de transparencia y acceso a la información pública, y las necesidades del sistema de emergencia y seguridad.

El área funcional a cargo del tratamiento de los documentos podría también ser la encargada de estandarizar los procesos de creación, aprobación, almacenamiento y destrucción del material físico y digital, y velar por su cumplimiento.

A continuación, se indican algunas actividades asociadas a cada uno de los cuatro procesos señalados:

- **Creación**: establecer los lineamientos para la elaboración de documentos internos, incluyendo formato, identificación (numeración/codificación), metadata correspondiente y el nivel de confidencialidad, entre otros elementos. La creación también podría venir acompañada de una propuesta sobre los usos que se le darán al documento.
- **Aprobación:** definir los pasos en la revisión y validación de los documentos, por ejemplo, quiénes participan, cuáles son los plazos, quiénes autorizan la versión final del documento, quiénes están a cargo de darle el tratamiento autorizado. Toda la documentación autorizada para uso interno, tendría que ser puesta a disposición del personal y, según el tipo de material, socializada.
- **Almacenamiento:** Establecer formato para el guardado de los documentos y metodología para el archivo. Definir también el tratamiento de las versiones anteriores de los documentos y plazos.
- **Destrucción:** definir la vigencia de la documentación, los plazos de archivo y destrucción de documentos, incluyendo en las normas de procedimiento pasos, autorizaciones y tratamiento según nivel de confidencialidad, entre otros aspectos.

3.3.2.12. Área funcional para la gestión de la información

Como toda área funcional, además de definir sus funciones, sería necesario establecer su alcance y su posicionamiento dentro de la entidad.

Respecto al alcance, se podrían considerar al menos tres opciones:

- **Alcance limitado**, podría estar vinculado a lo meramente operativo.
- **Alcance estratégico**, abarcaría el soporte para la toma de decisiones a todo nivel, y el desarrollo de inteligencia corporativa.
- **Alcance extensivo**, involucraría también la gestión comunicacional de relacionamiento con el entorno, contemplando rendición de cuentas y la transparencia.

Estos alcances no son mutuamente excluyentes.

En cuanto al posicionamiento dentro de la estructura y el organigrama de un sistema de emergencia y seguridad, podría pensarse como un área independiente o como parte de otra área funcional que la englobase.

3.3.3. Infraestructura física y equipamiento

La construcción y el diseño de los espacios físicos que conforman un centro de atención de emergencias y seguridad tendrían que tomar como eje rector la seguridad humana. Existen algunos documentos de referencia en la materia, incluyendo: NFPA 101®, norma ISO 45001-Sistema de gestión de la seguridad y salud en el trabajo; OSHA 18001-Sistema de Gestión en Seguridad y Salud Ocupacional. En este contexto, son también relevantes la supervisión y la cooperación de los organismos correspondientes en cada país.

Las áreas físicas también podrían ceñirse a normas de diseño ergonométrico y de iluminación, establecidas específicamente para entornos de trabajo, que aporten a la productividad y a la salud del personal. En pos de generar un ámbito saludable y cómodo de trabajo, también sería importante pensar en formas para absorber y reducir los niveles de ruido, y establecer sistema de climatización.

El espacio físico podría concebirse a partir de dos grandes áreas: el área operativa y el área administrativa. A su vez, el área operativa de un centro de atención de emergencias y seguridad podría disponer de las siguientes facilidades: sala de recepción de llamadas, sala de despacho, sala de video vigilancia (si aplica). Adicionalmente, sería necesario pensar en una serie de áreas de apoyo como, por ejemplo: área de alimentación, área de descanso, área de mantenimiento, salas de reuniones y salas de contingencia o de crisis.

El espacio físico tendría que estar debidamente señalizado y equipado para enfrentar situaciones de emergencia. Asimismo, también se tendría que contemplar espacios alternativos de trabajo en caso de que las instalaciones no se pudieran utilizar.

Otros elementos importantes, a tener en cuenta en relación al espacio físico y al equipamiento, serían:

- La ubicación y tamaño de los puestos o estaciones de trabajo.
- El equipamiento de las estaciones de trabajo, incluyendo la cantidad de monitores, aparatos de comunicación de radio o telefónica, diademas, computadoras.
- Pantallas (monitores o TV) para visualizar la concurrencia de unidades, según tipo de respuesta, entidad a cargo del servicio, área geográfica, entre otras características definidas en el modelo de funcionamiento sobre la recepción, administración, coordinación de la respuesta y despacho-cierre.

CAPÍTULO IV: GESTIÓN DE CALIDAD INTEGRAL

Introducción

Luego de la planificación y el diseño, el sistema de emergencia y seguridad tendría que entrar en funcionamiento. Este capítulo se enfoca en cómo gestionar el funcionamiento de un sistema de emergencia y seguridad desde un modelo de gestión de la calidad. Este modelo de gestión basado en la calidad busca la mejora continua en aras de brindar a la población un servicio profesional y efectivo de manera sostenida e ininterrumpida.

El modelo de gestión de calidad contempla cuatro insumos que se describen en el presente Capítulo: (i) el monitoreo y la medición de procesos y actividades en cada uno de los puntos de la cadena de prestación del servicio, (ii) la retroalimentación por parte de los/as usuarios/as, (iii) la retroalimentación por parte de las instituciones articuladas y vinculadas, y (iv) la gestión de riesgos.

Adicionalmente, en este Capítulo, también se presentan dos herramientas claves para llevar a cabo una gestión de la calidad de los procesos, servicios y actividades que realiza un sistema de emergencia y seguridad. La primera implicaría identificar y mapear procesos y protocolizar aquellos considerados críticos para el funcionamiento y la continuidad de operaciones del Sistema. El cumplimiento de esos protocolos por parte del personal permitiría mantener los niveles de calidad deseados. Adicionalmente, el contraste entre esos protocolos con las actuaciones llevadas a cabo, permitiría identificar oportunidades de mejoras.

La segunda herramienta estaría relacionada con la definición y el cálculo de una serie de indicadores para monitorear y medir el funcionamiento del Sistema en general, así como también por cada una de sus áreas funcionales y de las actuaciones realizadas, particularmente en lo que respecta a la atención y respuesta a las emergencias.

Ambas herramientas contribuirían a disminuir los márgenes de discrecionalidad y subjetividad en el funcionamiento y la gestión del sistema de emergencia y seguridad. Adicionalmente, abonarían al profesionalismo y a la imparcialidad con la que se tendrían que llevar a cabo las funciones y actividades operativas y administrativas de este tipo de Sistemas. Más aún, ambas herramientas brindarían parámetros y referencias claras, comunes y uniformes para todo el personal.

4.1. Modelo de gestión de la calidad

Un modelo de gestión de la calidad está estrechamente vinculado con la gobernanza del Sistema, en tanto involucra desde la medición, monitoreo, evaluación y revisión de la calidad de la prestación del servicio hasta la introducción de las mejoras requeridas para tornar más eficiente, eficaz y satisfactorio el servicio que se brinda. Este ciclo tendría que ser permanente y repetirse de manera constante, como parte integral del funcionamiento del Sistema, con miras al mejoramiento continuo del servicio que se le ofrece a la población.

Un modelo de gestión de la calidad atraviesa todas las áreas funcionales (principales o misionales y de apoyo o de soporte). Además, incluye los niveles de funcionamiento de un Sistema (estratégico, táctico y operativo), con especial énfasis puesto en la prestación de los servicios de emergencia y seguridad.

A partir del marco legal vigente y el establecimiento de estándares, protocolos y lineamientos, el modelo de gestión de calidad podría tener por objeto:

- La mejora continua e innovación de procesos y servicios.
- La satisfacción de las necesidades, requerimientos y expectativas de las personas usuarias, incluyendo aquellas de los grupos en situación de vulnerabilidad.

- El perfeccionamiento de la eficiencia para lograr mayor eficacia.
- La medición y evaluación del desempeño.

Existen distintos modelos de gestión de la calidad. El modelo que finalmente se adopte tendría que basarse en el modelo operativo del sistema de emergencia y seguridad, tomando en cuenta cada punto crítico de la cadena de prestación del servicio. Adicionalmente, sería conveniente que el modelo de gestión de la calidad estuviera alineado con las normas y estándares internacionales más influyentes en la materia, como las normas ISO 9000[3] o el Modelo de Excelencia EFQM (*European Foundation Quality Management*)[4].

A pesar de la diversidad de modelos de gestión de la calidad disponibles, a continuación se presentan cuatro enfoques mínimos:

i. Monitoreo en cada punto de la cadena de prestación del servicio

Un primer enfoque se basa en la medición y control de la calidad en cada fase, proceso o área de actividad de la prestación del servicio, por ejemplo: la recepción de la solicitud de servicio, el despacho o asignación de unidades, entre otras.

El monitoreo tendría que realizarse comparando el funcionamiento general y las actuaciones específicas llevadas a cabo con lo establecido en reglamentos, protocolos, estándares y lineamientos. Adicionalmente, el monitoreo podría sustentarse a partir de la definición y el cálculo de indicadores, así como el seguimiento y medición de los resultados obtenidos, teniendo como punto de referencia los objetivos y metas trazados.

Al llevar a cabo este primer tipo de monitoreo, sería recomendable que se tomen muestras de todas las áreas, todos los tipos de eventos, todas las personas y todas las entidades prestadoras del servicio en los diferentes niveles. Este muestreo tendría que ser aleatorio y representativo, en virtud del volumen de los eventos que atiende un sistema de emergencia y seguridad**.** Esto abonaría a la objetividad del ejercicio y respondería también a la integralidad del servicio.

El monitoreo también podría llevarse a cabo a través de auditorías internas o herramientas de control de gestión, que requieren objetivos, metas e indicadores bien definidos. Estos podrían considerarse como mecanismos complementarios de supervisión.

A partir de la aplicación de estos instrumentos de monitoreo, en caso de existir divergencias, brechas o desviaciones entre la práctica y los reglamentos, protocolos, estándares y lineamientos establecidos, así como también en relación con las metas y objetivos trazados, se tendría que proceder a la elaboración e implementación de planes de acción. Estos presentarían un conjunto de recomendaciones para superar las divergencias, brechas o desviaciones identificadas.

[3] ISO 9000: Sistemas de Gestión de la Calidad. Fundamentos y Vocabulario; ISO 9001: Sistemas de Gestión de la Calidad. Requisitos; ISO 9004: Gestión de la Calidad. Calidad de una Organización. Orientación para lograr el éxito sostenido. La familia ISO 9000-2015 promueve "principios de gestión de la calidad", como los siguientes: (1) Enfoque al cliente; (2) Liderazgo; (3) Compromiso de las personas; (4) Enfoque a procesos; (5) Mejora; (6) Toma de decisiones basada en la evidencia; y (7) Gestión de las relaciones.

[4] El Modelo EFQM consta de 7 criterios alineados con un eje estratégico. Los tres ejes de la estructura del modelo son la base de la conexión entre el propósito y la estrategia de una organización y, a su vez, orienta las acciones de la creación de valor sostenible para sus grupos de interés clave y la generación de resultados sobresalientes. Estos son: Dirección: (1) Propósito, visión y estrategia; (2) Cultura de la organización y liderazgo; Ejecución: (3) Implicar a los grupos de interés; (4) Crear valor sostenible; (5) Gestionar el funcionamiento y la transformación; Resultados: (6) Percepción de los grupos de interés; (7) Rendimiento estratégico y operativo.

En aras de la transparencia y la rendición de cuentas, los resultados de las auditorías internas, así como los planes de acción diseñados para subsanar las divergencias, brechas o desviaciones identificadas, podrían ser publicados en el sitio web del sistema de emergencia y seguridad (ver Capítulo X de esta Guía).

ii. Retroalimentación de usuarios

Este segundo enfoque consistiría en el establecimiento de mecanismos de consulta con los usuarios, que permitirían medir su satisfacción con el servicio brindado, detectar oportunidades de mejora y tomar medidas para rectificar las desviaciones detectadas. Algunos de esos mecanismos de consulta que se podrían aplicar son: encuestas de satisfacción, llamadas de seguimiento, grupos focales, y buzones de quejas y sugerencias (presenciales o virtuales), entre otros.

iii. Retroalimentación y seguimiento a las instituciones articuladas

El tercer enfoque implicaría la creación de instancias de coordinación intra e interinstitucionales, incluyendo: reuniones de seguimiento, mesas técnicas y de intercambio, entre otras; y la incorporación de herramientas o técnicas como, por ejemplo, el análisis después de la acción o ex-post emergencias atendidas, para:

- Retroalimentar a las entidades articuladas con los resultados de las operaciones a partir de los mecanismos de monitoreo y consulta establecidos, reportes estadísticos y el cálculo de indicadores, análisis de tendencias, reportes después de la acción, entre otras informaciones.
- Identificar situaciones que pudieran estar afectando negativa o positivamente la operación.
- Respecto a las primeras, tomar acciones correctivas de manera oportuna y considerar qué se podría documentar como una lección aprendida para compartir con el resto del personal y evitar la repetición de errores.
- En relación con las segundas, considerar qué se podría documentar como una práctica prometedora o buena práctica para compartir con el resto del personal y promover su propagación y adopción de manera transversal al interior del Sistema.

Estos tres enfoques estarían compuestos por los siguientes 5 pasos:

a. Recolección de datos e información.
b. Análisis de esos datos e información para la identificación de posibles puntos de mejora.
c. Elaboración de planes para atender las áreas de oportunidad identificadas. Estos planes tendrían que estar priorizados y alineados con las metas y objetivos estratégicos.
d. Establecimiento de un marco de trabajo para la ejecución de los proyectos de mejora.
    - Definir los mecanismos de medición y seguimiento del avance de estos planes.
    - Analizar la factibilidad y viabilidad presupuestaria de los planes de mejora.
e. Ejecución de las actividades definidas en los planes de mejora, e implementación de los mecanismos de medición y seguimiento.

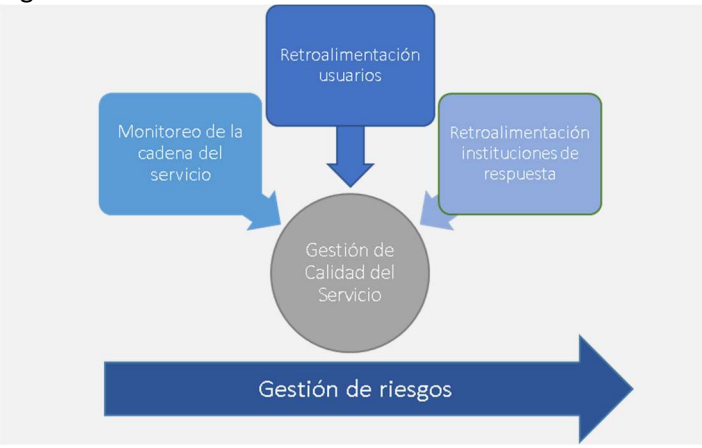
iv. Gestión de riesgos

Un cuarto enfoque se concentra en la gestión de riesgos. Su despliegue parte de la identificación y relevamiento de situaciones inesperadas y previsibles que podrían perjudicar el funcionamiento del

Sistema, buscando identificar la probabilidad de ocurrencia, el nivel de impacto y las vulnerabilidades existentes.

A partir de ese diagnóstico, se tendrían que establecer acciones de prevención y mitigación como parte de un plan de tratamiento de riesgos. Dicho documento tendría que actualizarse de manera periódica (ver Capítulo VIII de esta Guía).

Figura 22: Gestión de Calidad del Servicio



Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

4.2. Estandarización de procesos y aplicación de protocolos

Esta sección se centra en la primera herramienta del modelo de gestión de calidad. El punto de partida sería realizar un mapeo o esquema del proceso general de atención y respuesta a las emergencias, así como también de los procesos y actividades específicos, asociados a cada uno de los productos y servicios que se ofrecen.

A los efectos de poder elaborar ese mapa o esquema de procesos, se tendrían que llevar a cabo al menos cinco pasos, teniendo en cuenta: a) los requisitos funcionales y de desempeño, y b) los requisitos legales y reglamentarios aplicables:

i. Describir y caracterizar los procesos, e identificar cuáles son los procesos críticos

ii. Estandarizar y protocolizar los procesos, particularmente aquellos que fueron identificados como críticos

iii. Elaborar manuales/guías de procedimiento y protocolos de acción

iv. Definir indicadores de seguimiento de los procesos

v. Establecer parámetros de calidad y estándares

Estos cinco pasos, a su vez:

- Servirían como guía y referencia para la ejecución de los procesos
- Facilitarían el entrenamiento del personal (ver Capítulo VI de esta Guía)
- Ayudarían a comprobar o verificar la conformidad de las actividades realizadas por el personal, brindando parámetros objetivos para la evaluación de desempeño de los/as funcionarios/as (ver Capítulo VI de esta Guía).

- Permitirían el monitoreo y la evaluación de manera objetiva del funcionamiento del Sistema y de sus procesos, en aras de la mejora continua del mismo.

Entre los procesos más importantes para el funcionamiento de un sistema de emergencia y seguridad, podrían identificarse siete:

i. Recepción de solicitudes de asistencia e identificación de la situación

ii. Recolección de información, clasificación y priorización

iii. Creación de incidente y derivación/comunicación de información

iv. Despacho/asignación a unidad/es de respuesta

v. Coordinación, supervisión de comunicaciones y seguimiento de la/s unidad/es de respuesta en el lugar o sitio del suceso o evento

vi. Cierre operativo del caso

vii. Evaluación retrospectiva o post-mortem de todos los anteriores

Cada una de estos procesos o etapas de la prestación de los servicios ameritaría la estandarización y protocolización para asegurar el funcionamiento eficiente, oportuno y de calidad del Sistema.

4.3. Establecimiento y medición de indicadores

Esta sección aborda la segunda herramienta de un modelo de gestión de calidad, relativa al establecimiento y medición de una serie de indicadores para monitorear y evaluar el funcionamiento del Sistema en general, de sus áreas funcionales y de las actuaciones realizadas, particularmente en lo que respecta a la atención y respuesta a las emergencias. A continuación, se presentan algunos de los indicadores que podrían considerarse como parte de un modelo de gestión de la calidad:

- Indicadores de actividad
- Indicadores de procesos
- Indicadores de evaluación
- Indicadores de gestión/administración

Cada indicador tendría que reunir todas las características de diseño, incluyendo una ficha técnica. Los indicadores tendrían que ser cuantificables, cualificables y expresarse en alguna unidad de medida, incluyendo porcentajes, índices o tasas, entre otros.

La ficha técnica de cada indicador podría incluir los siguientes campos:

- Nombre del indicador
- Descripción/propósito del indicador
- Meta, objetivo y eje estratégico asociado el indicador
- Tipo de indicador
- Fórmula para calcular el indicador
- Los datos que se necesitarían para calcularlo, las fuentes donde esos datos estarían disponibles y de quién depende esa fuente de datos

- Unidad de medida y categorías asignadas
- Rangos y escala
- Frecuencia de medición
- Línea de base
- Responsable de la medición y seguimiento (o si el cálculo está automatizado)
- Dónde estaría disponible ese indicador, en qué reporte tendría que incluirse
- Quién tendría acceso al indicador

Estos indicadores tendrían que ser consistentes con el Cuadro de Mando Integral (CMI) (ver Capítulo II de esta Guía) y podrían agruparse, organizarse y visualizarse a través de un tablero de control. Su definición tendría que haberse realizado, preferentemente, al momento de diseñar la arquitectura de la información del Sistema (ver Capítulo III de esta Guía). Asimismo, su cálculo, resguardo y almacenamiento tendría que estar soportado por la arquitectura tecnológica configurada para el funcionamiento del servicio de emergencia y seguridad.

4.3.1. Indicadores de actividad

Son aquellos que miden la cantidad de solicitudes, llamadas o reportes de auxilio recibidas por el servicio de emergencia y seguridad. Tendrían un valor informativo para evaluar el uso de recursos y su asignación, además permitirían realizar comparaciones con otros centros, otros servicios u otros períodos de tiempo. A modo de ejemplo:

1) Número total de solicitudes, llamadas o reportes de auxilio recibidos
2) Número de solicitudes, llamadas o reportes de auxilios recibidos por canal de atención
3) Número de solicitudes, llamadas o reportes de auxilio por tipo de incidente
4) Número de solicitudes, llamadas o reportes de auxilio por localidad
5) Número de casos atendidos (nivel de servicio)
6) Número de operadores disponibles sobre solicitudes, llamadas o reportes de auxilio recibidos
7) Número de despachos realizados sobre solicitudes, llamadas o reportes de auxilio recibidos
8) Precisión de los servicios de geolocalización de las solicitudes, llamadas y reportes de emergencia[5]

4.3.2. Indicadores de procesos

Estos indicadores servirían para verificar la disponibilidad del servicio, particularmente ligado a la atención y respuesta a las emergencias, y podrían agruparse por tipo de proceso. A modo de ejemplo:

1) Promedio de tiempo de atención de la solicitud, llamada o reporte de emergencia

[5] En México, la medición de la precisión de la geolocalización que entregan los operadores telefónicos al CALLE, se realiza a partir de los lineamientos de colaboración en materia de seguridad y justicia emitidos por el Instituto Federal de Telecomunicaciones (IFT). Con base a parámetros y regiones claramente establecidos, dicha entidad es quien realiza las mediciones de forma anual. En caso de no cumplir con los parámetros mínimos requeridos, los operadores podrían ser sancionados.

2) Porcentaje de llamadas fuera del tiempo establecido, según tipo y características de la solicitud, llamada o reporte de emergencia

3) Tiempo de procesamiento y envío de reporte a despacho

4) Promedio de tiempo de despacho de la unidad de asistencia

5) Porcentaje de llamadas abandonadas

6) Porcentaje de llamadas en espera

7) Porcentaje de incidentes despachados que no son emergencias

8) Porcentaje de incidentes no cerrados

4.3.3. Indicadores de evaluación

Se podrían utilizar para evaluar de forma mensual, trimestral/cuatrimestral, semestral o anual, el servicio brindado e identificar áreas de oportunidad a partir de las respuestas a las solicitudes, llamadas o reportes de auxilio recibidos por el Sistema. A modo de ejemplo:

1) Porcentaje de incidentes clasificados correctamente

2) Porcentaje de incidentes despachados

3) Porcentaje de incidentes atendidos

4) Tiempo promedio para el procesamiento de la llamada, según tipo y características

5) Tiempo promedio para el despacho de las unidades (desde que el llamado entra hasta que la unidad es despachada)

6) Tiempo promedio de despliegue (desde que el despachador informa al servicio articulado y la unidad deja la instalación para dirigirse al sitio de la emergencia)

7) Tiempo promedio de la respuesta (desde la recepción de la solicitud, llamado o reporte de auxilio y la llegada de la unidad al sitio de la emergencia)

8) Porcentaje de incidentes atendidos en el tiempo establecido como parámetro

9) Porcentaje de solicitudes, llamadas y reportes que cumplieron con los protocolos

4.3.4. Indicadores de gestión/administración

Estos indicadores medirían el funcionamiento del servicio desde el punto de vista de la planificación y la administración del Sistema, y podrían agruparse por área funcional. Algunos ejemplos se presentan a continuación:

4.3.4.1. Recursos Humanos

1) Número de operadores certificados

2) Edad promedio del personal operativo

3) Número de plazas disponibles

4) Número de personal en proceso de entrenamiento

5) Número de personal operativo por retirarse y previsión del número de personas que tendrían que ser reemplazadas

6) Porcentaje de ausentismo o puntualidad

7) Indicadores de clima laboral, podrían construirse a partir de la percepción del personal sobre:

    - Relaciones entre compañeros
    - Condiciones físicas del trabajo
    - Compensación y reconocimiento
    - Oportunidades de desarrollo profesional
    - Igualdad de oportunidades
    - Integración de personas con discapacidades, de acuerdo al área a desempeñarse

4.3.4.2. Operaciones

1) Rotación (voluntaria e involuntaria) de operadores

2) Capacidad operativa (disponibilidad de recursos), por turno y por operador

3) Promedio o tasa de solicitudes, llamadas y reportes de auxilio que atiende cada operador del Sistema

4) Número de cámaras disponibles o en funcionamiento

5) Número de cámaras que monitorea cada persona (en los casos en que corresponda)

4.3.4.3. Calidad

1) Porcentaje de proyectos ejecutados de mejora continua

2) Porcentaje de usuarios/as satisfechos con el servicio brindado por el sistema de emergencia y seguridad

4.3.4.4. Administración y finanzas

1) Porcentaje del presupuesto ejecutado

2) Porcentaje del presupuesto asignado por área funcional

3) Nivel de endeudamiento como porcentaje promedio de los recursos asignados

CAPÍTULO V: GESTIÓN DE LLAMADAS E INCIDENTES

Introducción

Este Capítulo brinda algunos lineamientos generales para abordar las seis tareas operativas claves presentadas en el Capítulo III, que hacen al núcleo del funcionamiento de un sistema de emergencia y seguridad:

i. Recepción de solicitudes, reportes y llamadas de asistencia e identificación de la situación

ii. Levantamiento de la información y tipificación según incidente, riesgo y priorización

iii. Creación y documentación del evento (ficha de asistencia)

iv. Derivación/comunicación de información y asignación de la unidad

v. Asistencia de la unidad

vi. Documentación y cierre operativo del evento

El abordaje se realiza desde la necesidad de protocolizar estas seis tareas operativas en una serie de pasos y procedimientos claramente definidos para guiar de manera objetiva, homogénea e institucionalizada las actuaciones del personal operativo. Es por ello que, a lo largo de este Capítulo, se identifican fases y se presentan consideraciones y criterios a tener en cuenta para estandarizar el desarrollo de esas seis tareas operativas.

El Capítulo también destaca la importancia de estandarizar la atención y respuesta a las emergencias en una serie de protocolos, desde tres perspectivas:

i. Personal: como material para entrenar al personal operativo, orientar su accionar y evaluar su desempeño

ii. Gestión: como parámetro para comparar entre lo actuado y lo esperado

iii. Calidad: como herramienta para identificar desviaciones de lo pautado e introducir mejoras

5.1. Recepción de solicitudes, llamadas y reportes

La gestión de solicitudes, llamadas y reportes de auxilio tendría que estar apoyada en tecnologías para facilitar el registro y la consulta de datos, y otras funcionalidades tales como:

- La visualización de las pautas para guiar la llamada
- La activación de un formulario en línea con las reglas de clasificación y priorización, y la tipología de incidentes desde los cuales poder seleccionarlos
- Geolocalización, direcciones, accesos y puntos geográficos de referencia
- Identificación del número de teléfono o IP de la persona usuaria, entre otros

El diseño de la arquitectura de la información y el soporte tecnológico tendrían que estar dirigidos a reducir al máximo las oportunidades para introducir sesgos y errores durante el proceso de registro de información de la persona y del incidente en la ficha de atención.

La estandarización y protocolización de procesos, particularmente de aquellos identificados como críticos para la misión del sistema de emergencia y seguridad, también resultarían claves para tornar más objetiva y consistente la tarea de atención, respuesta y cierre de las emergencias.

El operador o receptor de una solicitud de auxilio, llamada telefónica o reporte tendría que contar con un sistema automatizado que genere un código de registro, y que brinde indicaciones para el llenado de la ficha de atención con campos y opciones de selección preestablecidos.

Adicionalmente, el sistema tendría que reconocer y visualizar en pantalla, información básica de la persona usuaria como, por ejemplo, los campos que se enumeran a continuación:

- Número telefónico o dirección de la llamada (IP) (en caso de tener que devolver la llamada)
- Dirección o ubicación de la persona (que no necesariamente coincidirá con la localización de la emergencia)
- Nombre de la persona

La disponibilidad de los datos de localización de la llamada dependerá, entre otros factores, del marco normativo que cada Estado hubiera establecido en el ámbito de las telecomunicaciones, incluyendo con las empresas de telefonía fija y móvil.

Si el sistema no puede reconocer los tres campos anteriormente enumerados, el operador tendría que hacer las preguntas correspondientes para capturar la información básica de la persona y su ubicación. Asimismo, también tendría que completar la información en función de los campos preestablecidos en el Despacho Asistido por Computadora (CAD, por sus siglas en inglés).

Otro paso importante sería el de verificar y completar la información de la ficha de atención, a partir de los registros guardados en las bases de datos del sistema. Es a partir de este soporte informático que se tendría que complementar el reporte con información disponible en sus bases de datos, incluyendo: la cantidad de llamadas recibidas desde ese número telefónico o IP y los tipos de llamadas (procedentes y no procedentes) realizadas, entre otros.

Cada Centro tendría que definir protocolos para la atención según tipo de canal de acceso, tipo de llamada (procedente y no procedente) y tipo de incidente. Esos protocolos tendrían que incluir un guión, con una serie de preguntas predefinidas, que permitan conducir la comunicación con el usuario de manera estandarizada, recolectar información que pudiera ser necesaria para la atención de la emergencia y responder ante los diferentes tipos de emergencia de manera oportuna y con las unidades y recursos adecuados, en función de su complejidad y priorización.

Todo centro de recepción de llamadas tendría que contar con la capacidad de procesar un volumen atípico de llamadas que sobrepasen la capacidad operativa, y que pudieran afectar significativamente la atención de las emergencias. Para ello se recomienda considerar las siguientes medidas de mitigación, sujetas a la disponibilidad de un presupuesto para contingencias que permita cubrir costos adicionales en tiempos extraordinarios:

- Contar con personal de contingencia capacitado (operadores de video vigilancia y personal administrativo).
- Contar con consolas de contingencia y el soporte tecnológico respectivo.
- Habilitar espacios adicionales de soporte.
- Redirigir las llamadas a otros centros de atención a emergencias.

Las cámaras de video vigilancia podrían ser otro de los canales a través de los cuales el sistema podría capturar incidentes catalogados como de emergencia (prioridad o nivel 1). Hay al menos dos modalidades para llevar a cabo esta tarea: manual o automatizada. La primera implicaría apoyarse en video operadores, capacitados especialmente para llevar a cabo el monitoreo y detección de situaciones de emergencia. La

segunda dependería de la disponibilidad de cámaras “inteligentes” con la capacidad integrada de identificación de incidentes críticos. Ambos casos también tendrían que regirse por protocolos.

5.2. Clasificación según riesgo y priorización

En el Capítulo III, en la sección sobre la arquitectura de la información del sistema de emergencia y seguridad, se hizo referencia a la necesidad de definir una tipología de incidentes, con categorías exclusivas y mutuamente excluyentes, claramente definidas, y abarcando todos los ámbitos posibles de emergencias.

Esa tipología podría visualizarse en la pantalla del operador como un listado de incidentes del cual seleccionar.

Asimismo, también tendría que contar con una tipología de niveles de riesgo para establecer la priorización de la atención. En el Capítulo III se introdujo también un ejemplo de posibles niveles de priorización.

5.3. Lineamientos generales para la protocolización

Dada la centralidad de la recepción y el tratamiento de las llamadas, solicitudes y reportes de emergencia, y desde un enfoque de calidad, resultaría necesario estandarizar el procedimiento en un protocolo de actuación que permita darle consistencia, continuidad y eficiencia al servicio brindado.

Esta protocolización, operando en el marco de una serie de indicadores, controles y herramientas para medir la calidad del servicio brindado, permitiría identificar deficiencias y debilidades, introducir los cambios y actualizaciones necesarios y sustentar la mejora continua del Sistema. Adicionalmente, podría facilitar la identificación de aspectos en donde sería necesario fortalecer la capacitación y especialización del personal.

A continuación, se presentan algunos lineamientos básicos que tendrían que considerarse para el protocolo de recepción de llamadas que ingresan al sistema de emergencia y seguridad, organizados en cuatro fases:

Fase I. Recepción de la llamada

- Especificar la cantidad de veces que se tendría que dejar sonar el teléfono.
- Saludo estandarizado, expresarlo de forma clara, cordial y pausada. Especificar la cantidad de veces que dicho saludo tendría que ser repetido.
- Establecer si la llamada es en otro idioma e identificar el idioma. Si lo es, indicar con algún código preestablecido y aplicar el protocolo de actuación específico para estos casos (ver más abajo).
- Identificar/evaluar si la llamada es procedente/efectiva o no procedente/no efectiva a partir de una serie de criterios/preguntas preestablecidos.
- Si lo es, preguntar dirección e indagar respecto a la ubicación del incidente, incluyendo alguna referencia geográfica, apoyándose en la geolocalización y haciendo uso de las preguntas-guía para facilitar su ubicación. Preguntar el nombre del usuario, y en caso de que no lo indique, utilizar algún código o sigla para registrar la falta de ese dato. A modo de ejemplo, se podría utilizar: “NN”. La operadora podría brevemente explicarle a la persona usuaria, la importancia de contar con la información que se le está solicitando.

- En caso de ser una llamada procedente/efectiva pero el interlocutor no responde, brindarle todas las facilidades, a través de preguntas cerradas, para que pueda hacerlo. Valorar la situación de fondo o de contexto.
- Realizar una indagación previa sobre el incidente y completar la ficha que genera el sistema de atención de emergencias.
- Verificar cámara(s) cercana(s) para completar y complementar el entendimiento de la situación que se está reportando, si las hay o estuvieran disponibles.
- En caso de ser una llamada improcedente, se tendría que aplicar el protocolo correspondiente, en función del tipo de llamada improcedente que se hubiera identificado. Un ejemplo de tipología de llamadas improcedentes, con posibles categorías a considerar, fue presentada en el Capítulo III de esta Guía.

Este protocolo tendría que tener en cuenta diferentes situaciones en las que podría encontrarse la persona que llama o reporta una emergencia, incluyendo:

- Incapacidad de hablar
- Situación de peligro o de alto riesgo
- Algún tipo de discapacidad por parte de la persona usuaria

Fase II: Atención de la llamada

El protocolo en esta fase tendría que cubrir al menos dos aspectos:

- Clasificación del incidente con base en categorías predefinidas en el sistema, y determinación del nivel de riesgo y la priorización que amerita. El sistema tendría que brindar la posibilidad de re-priorizar el incidente y, de esta manera, cambiar el nivel de riesgo.
- Validación de enrutamiento y captura de datos adicionales según el tipo de incidente que pudiesen ser de utilidad para el personal que estará atendiendo la emergencia en terreno.

Fase III: Atención del incidente

A partir del modelo de funcionamiento del Sistema, la información sobre el incidente y el usuario tendría que ser enviada al área de despacho o a las instituciones articuladas y, de ser el caso, correspondería establecer los pasos a cumplir para su posterior coordinación con las instituciones vinculadas.

La protocolización en esta fase tendría que establecer parámetros para un esquema diferenciado de atención, según el tipo de incidente y las necesidades especiales que pudiera tener la persona que reporta la emergencia, entre otros elementos.

En casos de situaciones que pudiesen derivar o escalar en un **homicidio (intencional/doloso),** incluyendo secuestros, tomas de rehenes, intimidación o amenaza de muerte, entre otros, el protocolo de actuación específico podría considerar:

- Activar la ficha multidespacho en el CAD para la articulación de varias instituciones de respuesta. Al ser un evento en proceso se necesitaría capturar datos básicos y pasar la comunicación a las instituciones de respuesta para el soporte telefónico en línea y, de manera paralela, activar el despacho.
- En caso de evidenciar este tipo de incidente por cámaras de video vigilancia, además de activar el protocolo específico, estas podrían dar acompañamiento al despacho y monitorear el lugar de la emergencia y sus alrededores. Adicionalmente, y según el código procesal penal de cada país,

las imágenes captadas podrían ser remitidas a la entidad judicial a cargo de la investigación para su eventual procesamiento y juzgamiento.

En casos de **violencia de género, incluyendo riesgo de femicidio, violencia doméstica o intrafamiliar:** El protocolo de actuación específico podría considerar:

- Activar la ficha multidespacho en el CAD para la articulación de varias instituciones de primera respuesta. Al ser un evento en desarrollo o en proceso, correspondería la articulación inmediata de la policía y, de ser necesario, de unidades de salud. A nivel del CAD, ya se podría programar las instituciones articuladas y vinculadas que tendrían que ser activadas en ese tipo de situaciones.

- De ser posible y necesario, se tendría que brindar ayuda psicológica a la persona afectada por teléfono o por otro medio disponible, hasta el arribo de las unidades al lugar de los acontecimientos.

- En caso de existir cámaras de video vigilancia, y de acuerdo con el código penal procesal de cada país, las imágenes del acto flagrante que se hubieran capturado podrían ser remitidas a la entidad judicial a cargo de la investigación para su eventual procesamiento y juzgamiento.

En casos de personas con **problemas de salud mental**: El protocolo de actuación específico podría considerar los siguientes pasos:

i. Durante el diseño de la arquitectura de la información
    - Determinar los trastornos de salud mental que podrían activar o desatarse en una situación de emergencia, incluyendo: intentos autolíticos, alteraciones del comportamiento producto del consumo de sustancias estupefacientes y psicotrópicas, shock por un incidente crítico o evento peligroso, entre otros.
ii. Durante la indagación de la llamada de emergencia
    - Realizar una serie de preguntas pre-definidas para determinar el tipo de situación con la que se estaría lidiando.
    - Si fuera el caso, aplicar pautas generales para sosegar a la persona.
    - Activar la ficha ordinaria o multidespacho, según corresponda.
iii. Durante el despacho
    - Despachar las unidades o dispositivos adecuados.
    - Derivar el soporte telefónico y de primeros auxilios psicológicos a la institución que corresponda.
iv. Durante el post-cierre
    - Desplegar acciones complementarias de atención y de seguimiento post emergencias con las instituciones de apoyo psicológico.

En casos de **personas con discapacidades:** El protocolo de actuación específico podría considerar:

- Identificar el tipo y grado de discapacidad.

- Atender a la persona de acuerdo con la discapacidad identificada.

- Activar la ficha ordinaria o multidespacho, según corresponda.

- Despachar el recurso o dispositivo, y brindar el soporte telefónico, según sea el caso.

- Activar acciones complementarias de atención post emergencia con instituciones de apoyo y también con actores subsidiarios, si correspondiera.

El desarrollo de protocolos de actuación para tipos específicos de incidentes, incluyendo los cuatro anteriormente presentados, tendrían que elaborarse con la participación y los aportes de agencias públicas y de asociaciones de la sociedad civil especializadas. La metodología y la dinámica con la cual se confeccionen dependerá de cada país y de su sistema de emergencia y seguridad.

En casos de empleo de otro idioma: El protocolo de actuación específico podría considerar:

- Especificar preguntas para identificar el idioma que el/a usuario/a está utilizando.
- Contactar a quien responsablemente pudiera actuar como intérprete en la atención de la emergencia, ya sea a partir de un listado predefinido de operadores indicando sus respectivos conocimientos de idiomas, o enlazando con un servicio externo de interpretación.
- Solicitar el apoyo para la interpretación, siguiendo el guión establecido.
- En la ficha o reporte del incidente se tendría que poder registrar el hecho de que el usuario hablaba otro idioma. Esto podría hacerse, por ejemplo, con el uso de un prefijo o siglas preestablecidos.

Fase IV: Cierre de la llamada

En esta fase se tendría que elaborar un guión específico para el cierre y fin de la llamada. El mismo podría contener algunos de los siguientes elementos:

- Confirmar los datos de ubicación proporcionados para la atención de la emergencia.
- Brindar el número de reporte generado a partir del pedido de ayuda.
- Preguntar si la persona necesita algo más.
- Incorporar una frase de despedida.
- Brindar el nombre (código o clave) del/a operador/a y su número o código, si aplica.
- Esperar a que la persona usuaria cuelgue primero.
- Fin de la llamada.

En función de la tipología de incidentes, las necesidades especiales que pudieran tener las personas que reportan una emergencia y los diferentes canales de acceso disponibles, incluyendo aplicaciones web, aplicaciones móviles, servicio de SMS, mensajes de voz, dispositivos TTY y botones de auxilio, entre otros, se tendrían que elaborar protocolos específicos para atender cada una de las combinaciones posibles.

5.4. Transferencia de la información a los servicios de despacho

De acuerdo con el modelo de funcionamiento adoptado por el Sistema, el operador tendría que transferir o enrutar la información capturada.

Existirían distintos tipos de transferencias posibles:

i. **Emergencia estándar (normal):** El operador tendría que direccionar el reporte o ficha de atención al despachador de la institución indicada según el tipo de incidente. Este direccionamiento también lo podría hacer el CAD de manera automática a partir de la clasificación de la situación de emergencia que hubiera realizado el operador.

ii. **Emergencia que requiere coordinación entre dos o más instituciones articuladas**: En caso de ser necesario, según la complejidad del incidente, y si el CAD no lo contempla, el operador

tendría que direccionar la información de forma simultánea a dos o más instituciones de primera respuesta o de apoyo, para la atención coordinada de la emergencia en terreno.

iii. **Emergencia en proceso:** En este caso, el operador transferiría la información "básica" para que la institución de primera respuesta pueda brindar un soporte telefónico a quien realizó la llamada, hasta que la unidad o dispositivo llegue al sitio de la emergencia.

iv. **Despacho por mano:** Son emergencias asignadas y comunicadas de forma directa por medio de un formulario, ficha o registro físico que se le entrega, en mano, a un responsable de los servicios de despacho. Este tipo de despacho sería posible cuando operadores y despachadores se encuentran en un mismo centro.

Tanto para la información que se captura en la ficha de atención como para su transferencia a los servicios de despacho, el Sistema tendría que contemplar mecanismos de resguardo ante posibles contingencias y así evitar la pérdida de la información. En ese sentido, se podría recurrir al registro de forma manual, o a la funcionalidad de reenvío de la información capturada de manera digital una vez superada la contingencia.

5.5. Despacho y monitoreo de unidades

De acuerdo con el modelo de funcionamiento, la arquitectura de la información prevista en el Sistema y las características del sistema de despacho (CAD), el operador o despachador podría contar con diferentes funcionalidades para facilitar la articulación operativa de las instituciones que se requieran para la atención de la emergencia. Algunas de las funcionalidades básicas que se podrían considerar son:

Posibilidad de administrar/asignar. El sistema tendría que permitir asignar unidades o recursos en función de la disponibilidad operativa de las instituciones de primera respuesta e instituciones vinculadas de ser el caso.

Posibilidad de anular/modificar. El sistema tendría que tener la opción de anular o modificar el envío de unidades, en los casos en que el personal operativo de respuesta determine que no es necesario o que es necesario ajustarlo.

Posibilidad de escalamiento. El sistema tendría que permitir escalar la atención de la emergencia, sumando a otras instituciones necesarias, una vez constatados los riesgos y la complejidad de la emergencia en terreno.

Otras funcionalidades adicionales para considerar serían:

Ubicación del incidente y la gestión del despliegue de las unidades despachadas. El sistema tendría que permitir que el despachador tenga acceso a la información capturada por el operador y despachar la unidad o recurso más cercano, que pueda acceder al lugar del incidente en el menor tiempo posible.

Manejo simultáneo de múltiples servicios. El sistema tendría que permitir que el despachador pueda:

- Evaluar la información de la emergencia.
- Validar la información del incidente, en caso de requerirse.
- Brindar soporte telefónico, según los protocolos establecidos.
- Identificar si se requiere del despacho de recursos.
- Asignar el/los recurso/s disponible/s.

- Registrar el estatus del recurso (a modo de ejemplo: asignado, en camino, en sitio, procesando, retorno, finalizado).
- Verificar el arribo del/los recurso/s.
- Retroalimentar el incidente en el sistema de atención de emergencias.
- Actualizar la información del incidente.

Capacidad de modificar el incidente inicial (re-categorizar). El despachador/supervisor tendría que tener la capacidad de cambiar o re-categorizar la ficha inicial, en función de la información que fuera reportada por las unidades que acuden al sitio de la emergencia, a través de la llamada o los video operadores.

Comunicación permanente, soporte y seguimiento de las unidades o dispositivos en terreno. Los despachadores tendrían que poder interactuar con el personal operativo asignado a la respuesta de la emergencia reportada y brindarles toda la información necesaria para la adecuada atención de la misma.

Soporte de las cámaras de video vigilancia.[6] El sistema tendría que poder aprovechar la plataforma de cámaras de video vigilancia para brindar el apoyo necesario y monitorear las unidades desplegadas en terreno.

Dependiendo del tipo de cámaras con el que cuente el sistema de emergencia y seguridad, el video operador tendría que contar con la posibilidad de:

- Verificar la operatividad de las cámaras y poder operarlas.
- Monitorear cámaras asignadas.
- Corroborar si la cámara cuenta con elementos tecnológicos de soporte (megafonía IP, *software* específico y sirenas, entre otros).
- Identificar la ocurrencia de incidentes con base en los protocolos establecidos para el monitoreo y análisis de las imágenes.
- Registrar el incidente (normal o multidespacho), según sea el caso, identificar la/s institución/es de respuesta que tendrían que atender la emergencia y enviar ficha de atención del incidente al despachador, con base en los protocolos establecidos. Este flujo dependería del modelo de funcionamiento adoptado por el Sistema, así como también, entre otros elementos, del tipo de cámaras con el que se cuente.
- Una vez reportada una emergencia y asignada y despachada una unidad o dispositivo, el sistema de cámaras podría utilizarse para brindar soporte visual, acompañar, dar seguimiento y coordinar la atención de la emergencia en terreno, y monitorear y proteger al personal desplegado.

[6] Las redes de cámaras de video vigilancia también podrían desempeñar un papel disuasivo, enfocado en prevenir la ocurrencia de contravenciones, conductas anti-sociales y delitos. Adicionalmente, también podrían ser un elemento integral del sistema de alerta. Habiendo predefinido una tipología de incidentes, y dependiendo de la sofisticación tecnológica de las cámaras a disposición del sistema de emergencia y seguridad, estas podrían ayudar a detectar la ocurrencia de ciertos incidentes, incluyendo siniestros y desastres, y alertar a las instituciones correspondientes, de acuerdo al modelo de funcionamiento adoptado.

5.6. Captura, visualización y almacenamiento de datos

5.6.1 Para la operación

En cada solicitud, llamada o reporte recibido, sin importar el canal o medio utilizado, la captura e ingreso de los datos tendría que realizarse de manera estandarizada, según la arquitectura de la información, el soporte tecnológico disponible y los protocolos elaborados, cubriendo desde la recepción, el despacho, la atención, hasta el cierre del incidente.

La arquitectura de la información y tecnológica desempeñarían un papel clave en lo que respecta a la facilidad de acceso y uso de los formularios a completar, y de las herramientas de apoyo disponibles para acompañar ese proceso, así como en lo relativo a la visualización de la información. Los datos capturados a lo largo de todo el proceso tendrían que quedar almacenados en las bases de datos y servidores del sistema.

Algunos de los campos mínimos que tendrían que ser capturados son:

- Nombre del usuario
- Dirección o ubicación
- Referencia geográfica del lugar del incidente
- Número de teléfono o IP
- Tipo de incidente o emergencia
- Descripción del incidente
- Asignación y despacho del recurso que acude a la emergencia

5.6.2 Para la evaluación y la mejora continua

El ingreso oportuno y completo de los datos desde la recepción de la solicitud, llamada o registro de auxilio hasta el cierre del incidente, resultaría esencial para la gestión de calidad del servicio y la mejora continua.

Es por ello que, con base en la arquitectura de la información ideada y al soporte tecnológico del Sistema, se tendría que poder calcular y registrar, de manera automática, una serie de indicadores durante y posterior a la emergencia atendida, con base en controles de calidad preestablecidos.

Los controles de calidad tendrían que atravesar las seis tareas críticas que integran el proceso neurálgico de todo sistema de atención y respuesta a emergencias. Podrían llevarse a cabo a partir de la aplicación de plantillas o matrices de control de calidad, que contemplan una serie de categorías, criterios e indicadores predefinidos. Estas matrices podrían aplicarse a las fichas de atención, los audios grabados y los registros de la actividad operativa.

Si el control de calidad no puede realizarse sobre el universo de solicitudes, llamadas y reportes recibidos o despachos desplegados por el sistema de emergencia y seguridad, se podría calcular una muestra representativa. La representatividad de la muestra tendría que contemplar el peso o incidencia de cada tipo de solicitud, llamada y reporte recibido, incluyendo los procedentes y no procedentes. En lo que respecta al control de calidad de los despachos, la muestra tendría que ser representativa de cada tipo de incidente de emergencia respondido, así como de las instituciones articuladas (o de primera respuesta) y vinculadas, involucradas en la atención.

Como se mencionó en el Capítulo IV, los indicadores de evaluación o control tendrían que permitir medir la calidad del servicio brindado, determinar el nivel de cumplimiento de protocolos y criterios

estandarizados, y dar seguimiento a las metas y objetivos establecidos como parte del plan estratégico y operativo. Otras herramientas mencionadas en dicho Capítulo fueron, en lo que respecta a la retroalimentación de los usuarios: encuestas de satisfacción, llamadas de seguimiento, grupos focales, y buzones de quejas y sugerencias (presenciales o virtuales), entre otros. Adicionalmente, con relación a las instituciones articuladas y vinculadas, entre las herramientas de retroalimentación, se mencionaron: metodologías o técnicas para el análisis después de la acción, reuniones de seguimiento post emergencias atendidas y mesas técnicas.

Toda esta información cuantitativa y cualitativa tendría que facilitar la identificación de deficiencias y debilidades, a partir de la cual proponer mejoras en ciertos procesos y protocolos, introducir nuevas normas y estándares, y fortalecer la capacitación en determinados aspectos relacionados con las brechas evidenciadas.

A partir del cálculo de estos indicadores, de los controles de calidad llevados a cabo y de la retroalimentación recibida tanto por usuarios como por las instituciones articuladas y vinculadas, el Sistema también podría generar una serie de reportes para guiar la gestión (desde los niveles operativos, tácticos y estratégicos) y el proceso de mejora continua. En el Capítulo III se hizo referencia a algunos de los requisitos generales de reportería que un sistema de emergencia y seguridad podría contemplar.

CAPÍTULO VI. GESTIÓN DEL TALENTO HUMANO

Introducción

La estrategia para gestionar el talento humano en los sistemas de emergencia y seguridad tendría que estar direccionada hacia el desarrollo de competencias. Adicionalmente, tendría que garantizar suficiente personal con la capacidad para responder de manera oportuna y adecuada a las demandas propias de la entidad, sostener la continuidad de las operaciones, y contribuir al cumplimiento de los objetivos y metas establecidos en en el plan estratégico.

Las personas son el recurso más importante de toda organización, particularmente en un centro de atención de emergencias. Su trabajo estaría dirigido a preservar la vida de las personas en situaciones apremiantes y de alta tensión. No todas las personas estarían preparadas para llevar a cabo las tareas críticas, inherentes a un centro de atención, particularmente aquellas seis tareas operativas básicas que se presentaron en el Capítulo III de esta Guía. Serían necesarias una serie de competencias, habilidades, conocimientos y aptitudes específicos para un desempeño adecuado en un centro de atención de emergencias. Es por ello que resulta vital la planificación y gestión del talento humano que abarque la atracción, inducción, evaluación, capacitación y fidelización del mismo.

En las siguientes secciones de este Capítulo, se brindará una serie de lineamientos sobre las cinco etapas conducentes a una buena gestión del talento humano, desde la perspectiva de un centro de atención de emergencias.

6.1. Planificación y gestión del talento humano

Habiendo caracterizado al personal como uno de los principales recursos en todo centro de atención de emergencias, resultaría necesario adoptar un proceso de planificación que resulte en una estrategia institucional para guiar la gestión de este activo.

Para la planificación y promoción del talento humano, se tendría que tomar como base el plan estratégico institucional (ver Capítulo II de esta Guía) y los objetivos planteados a corto, mediano y largo plazo. En función de esos objetivos, se tendrían que identificar los recursos humanos necesarios para alcanzarlos y, adicionalmente, establecer los modelos de trabajo y definir los procesos principales de la gestión del talento humano. (En la Sección 6.2 de este Capítulo se presentan seis posibles procesos principales que caracterizan el funcionamiento de esta área funcional).

De igual forma, la planificación tendría que contemplar la formación y las expectativas sobre la trayectoria laboral o carrera del personal, para reforzar sus competencias técnicas y destrezas de cara a los cambios, innovaciones y nuevos retos que se pudieran avecinan y/o proyectan. Asimismo, invertir en el personal en materia de su crecimiento profesional, serviría como mecanismo de fidelización, elemento de motivación, e incentivo para fortalecer el sentido de compromiso con la entidad.

Adicionalmente, como parte del proceso de planificación, se tendrían que definir los objetivos específicos que se intentarían alcanzar por medio de la implementación de la estrategia de gestión del talento humano que resulte de dicho proceso. Algunos de esos objetivos podrían ser los siguientes:

- Atraer y retener el mejor talento humano con las competencias requeridas para los diferentes puestos de trabajo.
- Garantizar la calidad profesional y humana del personal que se desenvuelve en las distintas áreas o procesos del servicio de emergencia y seguridad.
- Fortalecer capacidades del personal para brindar un servicio eficiente y eficaz a la población.

- Identificar oportunidades de cada puesto y definir limitaciones.
- Mantener un adecuado clima laboral.
- Fomentar el espíritu de equipo, lazos de confianza y sentimiento de pertenencia.
- Prevenir y preparar al personal ante riesgos y posibles contratiempos que pudieran afectar la gestión institucional y asegurar el mantenimiento y la continuidad del servicio.

La planificación del talento humano tendría que cuantificar y cualificar al personal requerido, según el área funcional, proyectando la cantidad y el tipo de recursos que se necesitarán para cubrir los requerimientos de personal.

La cualificación implicaría definir funciones, responsabilidades y perfiles de cada puesto, por área, dentro de la entidad. Este sería uno de los procesos más complejos y, a la vez, más necesarios de llevar a cabo. Tendría que ser compatible con el diagnóstico de capacidades institucionales y la proyección de demanda de servicios. Es a partir de esa definición que se podría modelar y saber qué tipo de talento sería necesario atraer y, a la vez, prever qué aspectos formativos serían necesarios desarrollar o fortalecer internamente.

Este proceso podría desagregarse en dos fases:

a) Análisis del puesto: es el levantamiento de información relacionada con el puesto de trabajo a través de diversas técnicas.

b) Descripción del puesto: es el proceso de plasmar por escrito los objetivos, funciones principales y perfil del puesto de trabajo, producto del análisis previamente realizado en la fase anterior.

6.1.1. Análisis de los puestos de trabajo

El análisis de los puestos de trabajo o perfil de los cargos buscaría identificar las funciones con las competencias esenciales requeridas y podría llevarse a cabo a partir de la implementación de diversas técnicas:

- Entrevistas:
  - Con el ocupante del puesto
  - Con la persona responsable de supervisar el puesto
- Observación directa de la ejecución de las funciones del puesto de trabajo
- Cuestionarios estructurados para ser completados por el ocupante del cargo
- Evaluaciones
- Bitácoras
- Grupos de expertos

Es importante tomar en cuenta que cuando existen varios puestos con las mismas funciones y responsabilidades, no sería necesario entrevistar o aplicar un cuestionario a todo el universo de quienes ocupan un mismo puesto. En estos casos, se podría armar una muestra.

Cuando este análisis se realiza por primera vez y no se cuenta con experiencia en la entidad para el modelamiento de las tareas en cada puesto de trabajo, sería posible recurrir a grupos de expertos o consultar con otros centros de emergencias, examinando perfiles, procesos y funciones.

6.1.2. Descripción de los puestos de trabajo

La descripción del puesto de trabajo es la síntesis del modelamiento de las funciones a partir de la información recolectada durante el análisis anterior.

El resultado se tendría que plasmar en un documento en donde se identifiquen claramente todas y cada una de las responsabilidades, obligaciones y tareas asignadas.

Existiendo diversos modelos de funcionamiento, que se abordaron en el Capítulo III de esta Guía, tendrían que considerarse perfiles específicos congruentes con cuatro funciones operativas esenciales de un sistema de emergencia y seguridad: recepción, administración, coordinación de la respuesta y despacho, que usualmente se traducen en roles esenciales como los siguientes:

- Receptor de llamadas (operador o *call taker*)
- Operador de videovigilancia (video operador u operador de video)
- Despachador (*dispatcher*)
- Supervisor/coordinador

Asimismo, para la configuración o perfilamiento de los puestos de trabajo, podrían seguirse los lineamientos presentados en el Capítulo IV, relativos a las tareas asociadas a las seis tareas operativas más importantes para el funcionamiento de un sistema de emergencia y seguridad:

- Recepción de solicitudes de asistencia e identificación de la situación
- Recolección de información, clasificación y priorización
- Creación de incidente y derivación/comunicación de información
- Despacho/asignación de unidad/es de respuesta
- Coordinación, supervisión de comunicaciones y seguimiento de la/s unidad/es de respuesta en el lugar o sitio del suceso o evento
- Cierre operativo del caso

Específicamente, la descripción de los puestos de trabajo podría estructurarse sobre la base de las siguientes dimensiones:

- **Información identificatoria.** Situada habitualmente en la parte superior del documento. Presenta datos generales del puesto, incluido el lugar y dónde se ubicaría en la jerarquía de la entidad. En ella se podría indicar la siguiente información:
    - Código
    - Nombre del puesto
    - Lugar del mismo dentro de la entidad
    - Unidad administrativa u operativa
    - Rol
    - Grupo ocupacional
    - Grado

- Ámbito
- Fuente de la información con la que se elaboró el análisis del puesto y autor del mismo
- Fechas de elaboración y verificación del análisis
- Consideraciones económicas, tales como si el puesto está exento o sujeto al pago de horas extraordinarias

- **Resumen del puesto.** Es una pequeña síntesis introductoria relativa a las obligaciones, responsabilidades o tareas asociadas al puesto, y a las capacidades necesarias para su desempeño, incluidas las emocionales. También se indicaría el lugar que ocuparía dentro de la jerarquía organizativa.
- **Interfaz del puesto**. Explicaría la relación de las actividades esenciales del puesto de trabajo en relación con los usuarios internos y externos.
- **Obligaciones y responsabilidades.** En esta dimensión se tendría que dar respuesta a las siguientes preguntas:
  - ¿Qué es lo que se ha de hacer en el puesto?
  - ¿Para qué se lleva a cabo?
  - ¿Cómo y con qué herramientas se realiza el trabajo?
  - ¿Dónde se ejecuta el trabajo?

Las respuestas a estas preguntas tendrían que quedar capturadas en protocolos que guían a los/as ocupantes de los puestos respecto a las obligaciones, responsabilidades o tareas que deben llevar a cabo, y cómo hacerlas. Estos a su vez servirían como parámetro al momento de evaluar y calificar el desempeño.

- **Especificaciones y cualificaciones exigidas para el puesto.** En esta parte se expondrían claramente las competencias, experiencias y formación necesarias que se le han de exigir a la persona para llevar a cabo las tareas asociadas al puesto.
- **Área de conocimiento.** Es la carrera técnica de instrucción formal que se exigiría a la persona para ocupar el puesto.
- **Experiencia laboral requerida.** Es el nivel y tipo de experiencia que se requeriría para llevar a cabo las tareas asociadas al puesto de trabajo.
- **Capacitación requerida para el puesto.** Define las temáticas de las capacitaciones y las certificaciones vinculadas al puesto de trabajo que la persona interesada tendría que poseer.
- **Competencias técnicas.** Son aquellas que harían referencia a los estándares específicos, vinculados al correcto desempeño de puestos en un área técnica o función específica.
- **Competencias organizacionales.** Son habilidades básicas que tendrían que poseer las personas que aspiren a ingresar a la entidad. Están compuestas por competencias conductuales como la orientación a la calidad, al trabajo en equipo, el interés en la innovación, el compromiso con los valores y principios éticos de la entidad, entre otros.
- **Competencias emocionales.** Rasgos de personalidad y conjunto de capacidades, habilidades y actitudes para procesar, comprender, regular y expresar de forma apropiada los fenómenos emocionales y los niveles de estrés relacionados al puesto.

- **Condiciones de salud requeridas para el puesto.** Especificar si algunas enfermedades (como la epilepsia) o afecciones pre-existentes (como la hipertensión o la diabetes, entre otras) serían incompatibles con el puesto de trabajo por los niveles de estrés y la alta carga emocional que el puesto acarrea.

Por competencias se podría entender un conjunto de conocimientos, habilidades y destrezas, que permiten desempeñar de manera eficaz un determinado puesto de trabajo en la cadena de servicios de un Centro y, de esta manera, contribuir al logro de los objetivos y metas de la entidad. Sirven tanto para definir los perfiles del puesto así como para establecer los parámetros sobre los cuales evaluar el desempeño del personal.

Las competencias podrían ser consideradas como dinámicas. Se pueden ir adquiriendo y desarrollando a lo largo de la carrera profesional de una persona. Además de las competencias técnicas y organizacionales ya mencionadas, también se podrían considerar las competencias de gestión, entre otras.

La estructura y características de los puestos de trabajo y, asimismo, las competencias que se necesitarían en cada uno de ellos, estarían sujetas a la organización interna y al modelo de gestión del talento humano adoptado por cada entidad.

6.2. Área funcional para la gestión del talento humano

La planificación y gestión del talento humano tendrían que recaer en un área funcional específica. Esta estaría a cargo de implementar y operacionalizar las directrices de la política institucional con tales fines, consagradas en un plan, producto de un proceso de planificación.

El área funcional tendría la misión de abastecer a la entidad del mejor recurso posible para cada puesto de trabajo, abarcando todo el ciclo de vida laboral de la participación de un individuo en la misma, desde que surge un requerimiento para un determinado puesto hasta que concluye la relación laboral entre el individuo y la entidad.

El aprovisionamiento oportuno de los talentos que necesita un centro de atención de emergencias es crítico para el buen funcionamiento de sus operaciones, para mantener la eficiencia y calidad de sus servicios, y para el logro de sus objetivos y metas.

El área funcional tendría que estructurarse y organizarse para definir y gestionar los siguientes procesos fundamentales, entre otros:

- Reclutamiento y selección
- Inducción
- Desarrollo (programa de capacitación continua)
- Evaluación
- Fidelización
- Salida

Todos estos procesos tendrían que quedar protocolizados. Asimismo, tendrían que estar guiados por el principio de la no discriminación[7] y un enfoque de género, y en línea con el marco normativo y las políticas labores y sindicales/gremiales de cada país.

[7] La no discriminación por motivo de raza, origen, religión, discapacidad, género, orientación sexual y/o afiliación política.

6.3. Reclutamiento y selección del talento humano

Luego de haber concluido el diagnóstico, el análisis y la definición del perfil de los puestos de trabajo, se llevaría a cabo el proceso de reclutamiento y selección del personal idóneo.

El reclutamiento y selección de personal podría estructurarse basándose en cinco fases, dentro las normativas legales vigentes de cada país:

a) **Necesidad:** como primera acción, sería necesario identificar el área en la cual se requiere incorporar o reforzar personal, así como también definir el perfil de competencias para cubrir los exigencias del área en cuestión. En esta fase se tendría que analizar la disponibilidad de recursos económicos y la proyección de la demanda de los servicios.

b) **Reclutamiento:** es la fase donde se iniciaría la captación de los/as candidatos/as a través de distintas fuentes y canales, de acuerdo con el perfil definido. Este indicaría las capacidades técnicas, competencias, formación y experiencia deseadas para el puesto de trabajo. Adicionalmente, también especificaría los beneficios y la compensación que podría esperar la persona interesada en el puesto.

   Resultaría útil considerar criterios de selectividad y de priorización para establecer qué aspectos del perfil son vitales e imprescindibles, y cuáles son importantes, pero no decisivos para el puesto de trabajo.

   La convocatoria, dependiendo de las plazas o puestos de trabajo por cubrir, podría ser tanto interna como externa. Estos dos frentes no son mutuamente excluyentes. Los medios para realizar la convocatoria son múltiples, incluyendo medios de comunicación y redes sociales, el sitio web de la propia entidad, las plataformas de búsqueda de empleos, universidades con servicio de colocación laboral para sus graduados/as, entre otras.

c) **Depuración y Evaluación:** fase en la que se verificarían las cualificaciones de los/as candidatos/as, mediante aplicación de pruebas, entrevistas y validación de las referencias. Para esta fase resultaría útil contar con criterios predefinidos de admisibilidad técnica.

   En esta fase, iniciaría el proceso de evaluación de los/as candidatos/as con base en la hoja de vida de los/as postulantes, cualquier otro material de soporte que se hubiera solicitado, y en función de los requisitos establecidos para el puesto.

   Para asegurar la transparencia del proceso, sería preciso constatar el cumplimiento de los requisitos técnicos y administrativos para la postulación y validar los antecedentes acreditados por entidades ajenas, incluyendo los cuerpos de seguridad y policías, centros de formación profesional o de educación superior, entre otras.

   Luego de haber identificado a los/as candidatos/as que cumplen con el perfil, se podrían llevar a cabo una serie de pruebas para confirmar y evaluar las competencias señaladas. Para ello se recomendaría la realización de al menos tres tipos de pruebas:

   - **Pruebas técnicas:** son aquellas que buscan validar la capacidad del candidato en competencias de habilidad enfocadas al puesto. Por ejemplo, una prueba de digitación, de programación o de idiomas.
   - **Pruebas de competencias:** dirigidas a evaluar las habilidades asociadas al desempeño eficiente y eficaz en un puesto de trabajo.

- **Pruebas psicométricas de personalidad:** se aplican para desvelar rasgos de personalidad acordes con las obligaciones, responsabilidades y funciones del puesto de trabajo, y los niveles de estrés y carga emocional que deberá enfrentar la persona.

También se podrían realizar evaluaciones de conocimiento básicos y/o especializado, y pruebas psicométricas. Es en esta fase en donde, además, se podría conducir una serie de entrevistas con los/as candidatos/as preseleccionados/as, ya sea por parte de uno o varios entrevistadores.

Además de medir y determinar las cualificaciones, competencias, conocimiento, formación anterior y experiencia específicas para cada puesto de trabajo, resultaría fundamental poder identificar tempranamente entre los/as candidatos/as la orientación y actitud para el servicio público.

d) **Selección:** es la fase final del proceso en donde a partir del grupo de candidatos/as preseleccionados/as, se tendría que seleccionar al/a candidato/a que mejor se ajuste a los requisitos solicitados y presente las mejores aptitudes para desempeñar las funciones inherentes a la posición.

e) **Contratación:** de ser aceptada, se publicaría la declaratoria de selección del/a postulante, y se concretaría la contratación de acuerdo con las normas legales vigentes de cada país.

Adicionalmente, es posible que la contratación venga precedida de la realización de exámenes médicos, tanto físicos como mentales, y la consulta acerca de antecedentes penales. Más aún, en el marco de la política de seguridad y salud ocupacional que establezca la entidad, es posible que estos exámenes se repitan con cierta frecuencia, en función de las obligaciones, responsabilidades y carga laboral, emocional y de estrés de los/as funcionarios/as de un centro de atención y respuesta a emergencias.

6.4. Inducción del talento humano

Todo/a funcionario/a que se incorpore a la entidad, tendría que pasar por un proceso de inducción. La inducción permitiría a la persona que se integra a la entidad, familiarizarse con la misma, con su declaración de misión y visión, con los valores y principios que guían sus decisiones y actuaciones, y los objetivos que intenta alcanzar, entre otras cuestiones.

La inducción es también un momento propicio para familiarizar a los/as nuevos/as funcionarios/as con los estándares, procesos, mecanismos y funcionamiento, entre otros aspectos, de la entidad. Aquí es cuando se podría comenzar a construir un sentimiento de pertenencia y compromiso con la entidad, y dar inicio a la carrera profesional de cada persona que ingresa.

En un centro de atención de emergencias se podría diferenciar entre personal administrativo y técnico por un lado, y personal operativo por el otro. Este último es quien labora directamente con la recepción de llamadas, despacho y atención a emergencias. La organización, distribución, grado de centralización de estas funciones dependerá del modelo de funcionamiento adoptado, como ya se mencionó en el Capítulo III de esta Guía.

En función de lo anterior, se podría considerar al menos dos tipos de procesos de inducción: la induccíon general y la operativa.

- **Inducción general:** aplicaría a todo el personal de nuevo ingreso, contendría información general de la institución sobre su misión, visión, valores, mapa de procesos, políticas y normativas generales y condiciones de trabajo, entre otros aspectos de orientación general que se quiera agregar.

- **Inducción operativa:** esta estaría dirigida al personal de las áreas vinculadas a la recepción de solicitudes, llamadas y reportes, despacho y atención de emergencias en terreno, en la cual se brindaría orientación sobre los protocolos y procesos, el uso de las herramientas y las plataformas tecnológicas y de comunicación, entre otros aspectos. Sería recomendable incluir una sección enfocada en el cuidado de la salud física y emocional, y el manejo del estrés laboral, indicando los servicios y mecanismos disponibles para su tratamiento.

Si, en cambio, el modelo de funcionamiento es tal que el centro de atención es el ente coordinador entre instituciones de respuesta, donde cada una de ellas sería responsable de la contratación y formación de su personal, se recomendaría preparar una inducción para el personal que estará brindando atención a situaciones de emergencias en terreno. Esa inducción podría enfocarse en los protocolos y procedimientos que se estarían utilizando de manera transversal, en aras de promover la integración del servicio y mitigar el choque de diferentes culturas institucionales y modalidades de trabajo.

A continuación se presentan algunos contenidos mínimos recomendables para este tipo de inducción operativa:

- Componentes y etapas de la cadena de servicios, procedimientos de clasificación, esquemas de despacho, uso de equipo técnico, actuaciones específicas en emergencias a gran escala y otros.
- Marco legal, código de ética y código de conducta, y protocolos para la prestación de servicios y manejo de emergencias específicas, incluyendo los casos presentados en la Fase III: Atención del incidente del Capítulo V.
- Comunicación eficaz con las personas que llaman, procesamiento de llamadas de emergencia, aspectos éticos y psicosociales de la recepción de llamadas, métodos de manejo del estrés, entre otros.
- Análisis de riesgos y manejo de incidentes, coordinación de las intervenciones de los servicios de rescate, entre otros.
- Trabajo en equipo y roles de coordinación.
- Utilización de tecnologías de la información y la comunicación.
- Dominio de glosario técnico y códigos de comunicación con usuarios internos.

De ser posible, la inducción operativa, también tendría que venir enlazada a un acompañamiento del proceso socioafectivo de integración del/a nuevo/a funcionario/a al equipo o turno de trabajo.

En adición a la inducción general y operativa, el nuevo/a funcionario/a también tendría que recibir una **inducción específica** al puesto de trabajo para el cual fue contratado/a, en línea con el programa de inducción y entrenamiento establecido por la entidad.

También se podría considerar tener representantes por área, encargados de dar un acompañamiento a los/as nuevos/as funcionarios/as durante sus primeros días (que podría ser de entre 7 a 15 días). Este tipo de soporte podría facilitar su período de adaptación y acelerar la curva de aprendizaje. Para ello sería recomendable involucrar a personal con experiencia y alto sentido de pertenencia y compromiso institucional, para que actúen como tutores o mentores.

Luego de haber concluido la inducción, podría activarse un período de prueba, en el que la persona tendría que demostrar que tiene la capacidad para desempeñarse en el puesto para el cual fue contratado/a. Transcurrido ese período de prueba (que podría ser de entre 3 a 6 meses), se tendría que llevar a cabo una evaluación en donde se determine si la persona se ha podido adaptar al puesto. Si el resultado no es

favorable, la entidad tendría la posibilidad de no extender el contrato y reiniciaría el proceso de reclutamiento y selección.

Debido a la naturaleza del trabajo que se lleva a cabo en los centros de atención de emergencias, estos períodos de prueba permitían a ambas partes determinar si el puesto de trabajo, las obligaciones y responsabilidades asociadas al mismo, y la persona inicialmente contratada para asumirlos, resultan compatibles o no.

6.5. Capacitación continua para el fortalecimiento de funciones y capacidades

En todo sistema de emergencia y seguridad, la calidad y eficiencia del servicio brindado dependen, entre otros elementos, del nivel de preparación y experiencia del personal. Es por ello que la capacitación es uno de los pilares de la mejora continua y del desarrollo del talento humano.

La capacitación continua tendría que obedecer a un programa de aprendizaje y especialización. Existen directrices para el desarrollo de este tipo de programas que podrían servir de guía y como referencia, incluyendo aquellas brindadas por NENA, EENA, IAED y APCO, por mencionar algunas.[8] La capacitación tendría que ejecutarse como un proceso, en relación a los objetivos y metas definidos en el plan estratégico, y sobre la base de un programa de aprendizaje y especialización definido por la propia entidad, conforme a las demandas de servicio y a las necesidades de fortalecimiento de las competencias del personal.

Dicho programa de capacitación continua tendría que haber partido de una línea de base y de una oportuna identificación de las brechas y necesidades de mejora. La línea de base podría construirse a partir de las evaluaciones al momento del ingreso, las evaluaciones de adaptación al puesto, y las evaluaciones de desempeño, entre otras fuentes. El programa tendría que incorporar entrenamientos, capacitaciones y cursos certificados, estos últimos brindados por agencias acreditadoras.

Se podría hacer uso de plataformas tecnológicas como soporte para impartir las capacitaciones y entrenamientos, así como incorporar diferentes experiencias prácticas, casos de estudio y, si fuera posible, de simulación. Ante la posibilidad de que no todos/as puedan participar de las capacitaciones y entrenamientos, sería importante desarrollar estrategias y herramientas para compartir y transferir los conocimientos adquiridos internamente, al resto del personal que corresponda.

Las capacitaciones y entrenamientos tendrían que contar con instructores calificados o certificados, materiales de capacitación actualizados, insumos logísticos, el espacio y el equipamiento necesarios para su desarrollo.

Al finalizar cada capacitación y entrenamiento, sería conveniente aplicar evaluaciones para medir conocimientos y logros alcanzados, según los objetivos de aprendizaje establecidos. Asimismo, las evaluaciones también facilitarían la detección de nuevos temas y ayudarían a dar seguimiento y retroalimentación al personal.

A modo de soporte del programa de capacitación continua, sería óptimo considerar el uso de otras herramientas de apoyo, tales como:

- Registro de las capacitaciones brindadas, con una serie de datos sistematizados sobre su realización y participación, entre otros aspectos, y sus respectivas evaluaciones.

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

- Directorio de instructores, en donde también conste, entre otras informaciones sistematizadas, las capacitaciones y entrenamientos brindados, y las evaluaciones recibidas.
- Indicadores que permitan medir el impacto y la aplicación de lo aprendido en las respectivas áreas de trabajo.
- Sistema de legajos por persona, donde además de las capacitaciones realizadas y certificaciones recibidas, consten los indicadores post capacitación, las horas y cantidad de jornadas de formación, las habilidades, competencias y experiencias adquiridas, entre otros aspectos.

Adicionalmente, se recomendaría que el programa de capacitación continua también fuera objeto de una evaluación. La determinación de la efectividad de las capacitaciones y entrenamientos brindados, tendría que intentar establecerse a partir de mejoras en procesos, productos y servicios, y la satisfacción de los/as usuarios/as con la atención y los servicios recibidos.

6.6. Evaluación de desempeño

La evaluación del desempeño es un instrumento fundamental a nivel individual y organizacional.

A nivel individual permitiría:

- Brindar retroalimentación respecto al trabajo realizado.
- Resaltar logros y actuaciones.
- Identificar fortalezas y debilidades y proponer medidas o acciones para superarlas.
- Sugerir o actualizar planes de carrera y de desarrollo.
- Establecer metas y comunicar las expectativas que la entidad tiene respecto a la persona.
- Guiar las decisiones de promoción y ascenso, así como las de desvinculación del personal.

A nivel organizacional, el análisis de las evaluaciones de desempeño permitirían planificar estrategias para guiar el crecimiento profesional del personal y servir de insumo para informar el programa de capacitación continua, entre otros usos.

La realización de este tipo de evaluaciones tendría que verse reflejada en la calidad del servicio que se brinda y en la satisfacción de las personas usuarias. Es por esta razón que tendría que considerarse como una actividad estrechamente vinculada con la gestión para la calidad integral y la mejora continua de la entidad (ver Capítulo IV de esta Guía).

La evaluación del desempeño tendría que llevarse a cabo de manera cíclica, continua y objetiva, con los instrumentos necesarios. Es un proceso que tendría que estar guiado por criterios e indicadores específicos para calificar al personal respecto a su trabajo, desempeño y conductas.

Algunas dimensiones mínimas a tener presente para evaluar el desempeño del personal podrían ser:

- Rendimiento
    - Cumplimiento de los objetivos/metas establecidos en torno a las funciones, obligaciones y responsabilidades asociadas al puesto de trabajo
    - Calidad de la labor realizada
- Condiciones personales

- Interés por el trabajo que realiza
- Capacidad para realizar trabajos en equipo

- Comportamiento
  - Cumplimiento de normas, protocolos e instrucciones
  - Asistencia y puntualidad

6.7. Fidelización del talento humano

La curva de aprendizaje y el alto nivel de especialización que se requiere para el personal de un centro de atención de emergencias tornan necesario que se establezcan estrategias y mecanismos internos para retener el talento humano y evitar su fuga.

Para ello, la entidad tendría que crear las condiciones para que las personas puedan desarrollar una carrera técnica o profesional con perspectivas de promoción, crecimiento profesional y oportunidades laborales. Una de esas condiciones es el salario que los/as funcionarios/as perciben. El monto salarial tendría que estar en línea con las responsabilidades y funciones que la persona desempeña, y ser lo más competitivo posible, en función de lo que el mercado laboral ofrece. También se podrían establecer incentivos y beneficios para retener a los/as funcionarios/as calificados/as. En línea con lo anterior podría, a modo de ejemplo, reconocer y premiar el desempeño sobresaliente del personal. En esa línea, sería necesario:

- Establecer criterios, indicadores y mecanismos para identificar a quienes se destacan por su desempeño.
- Definir un esquema de reconocimiento e incentivos conforme a áreas de desempeño tanto individual como grupal.
- Sistematizar el desempeño sobresaliente del personal; comunicar y compartir esas buenas prácticas al interior de la entidad.

6.8. Proceso de salida

Con independencia de las razones, el proceso de salida o desvinculación de un/a funcionario/a tendría que ajustarse a las normativas legales y a los procedimientos internos definidos por la entidad para este tipo de situaciones.

La desvinculación de un funcionario/a, particularmente cuando este/a se retira o es profesionalmente apreciado/a por la entidad, no tendría que significar perder la posibilidad de aprovechar su talento. Hay varias maneras en las que la entidad podría quedar vinculada a ciertas personas consideradas de alto valor debido al conocimiento y la experiencia acumulados. El conocimiento tácito de esas personas podría retenerse a través de entrevistas filmadas o podcasts disponibles para todo el personal. También podrían quedar vinculadas a la entidad como instructores/as, formando parte de su directorio de capacitadores. Adicionalmente, podrían quedar disponibles como expertos, a quien consultar en instancias o antes situaciones específicas, o como tutores/as o mentores/as para guiar a los/as funcionarios/as de nivel de entrada y de mando medio.

6.9. Salud y seguridad ocupacional

El talento humano de la entidad podrá ser aprovechado en la medida en que se proteja y promueva la salud de los/as funcionarios/as y se establezca y conserve un ambiente laboral seguro y saludable. Para

ello sería necesario contar e implementar una política de salud y seguridad ocupacional apropiada, dada la naturaleza, dinámica y condiciones de trabajo de un centro de atención de emergencias.

Una de las características del trabajo en un centro de atención a emergencias, es que los/as funcionarios/as conviven de manera cotidiana y continua con solicitudes, llamadas, reportes, videos e incidentes traumáticos y de alta tensión, generando elevados niveles de estrés y afectaciones a la salud. Frente a ello, sería necesario establecer un servicio de acompañamiento, que brinde soporte médico, así como también contención, tratamiento y seguimiento psicológico especializado al personal.

Sería importante también, establecer mecanismos y herramientas para detectar de manera temprana síntomas y señales de depresión, estrés, agotamiento, tensión y otros cuadros similares derivados de las situaciones traumáticas que experimenta el personal. La detección temprana permitiría canalizar los casos oportunamente a la unidad especializada de soporte y, de esta manera, evitar que escalen a situaciones más complejas.

Además de lidiar con algunas de las características del trabajo que pueden afectar la salud física y mental de los/as funcionarias, la política de seguridad y salud ocupacional de un centro de atención de emergencias también tendría que abordar los siguientes aspectos (algunos de ellos se abordan en el Capítulo VIII de esta Guía):

- Factores de riesgo
- Condiciones de trabajo
- Accidentes de trabajo
- Enfermedades
- Ausentismo
- Sistemas de prevención y vigilancia epidemiológica

6.10. Código de Ética y Código de Conducta

Un Código de Ética tendría que establecer el conjunto de principios y valores que guían las actuaciones de la entidad y del personal. Por su parte, un Código de Conducta identifica, prescribe y prohíbe comportamientos específicos individuales y en las relaciones interpersonales. Es decir que un Código de Ética se tendría que operacionalizar o traducir, en términos prácticos, en un conjunto de conductas a evitar/rechazar y/o a seguir, que quedarían plasmadas en un Código de Conducta. Ambos tendrían que estar alineados con la misión y los objetivos institucionales del sistema de emergencia y seguridad.

Los principios y valores que orientan las actuaciones consideradas altamente deseables tendrían que ser consistentes tanto con la dignidad humana y los derechos humanos así como con el valor público de los servicios que se entregan a la población.

Algunos principios éticos que podrían considerarse son:

- El servicio de emergencia y seguridad constituye un bien de uso público.
- Los bienes y recursos públicos se destinan exclusivamente a las funciones propias de la entidad.
- La razón de ser del/a funcionario/a público/a es prestar un servicio de calidad a la población.
- El interés público prevalece sobre el interés particular.

- El sistema de emergencia y seguridad rinde cuentas a la ciudadanía sobre la utilización de los recursos públicos que le fueron encomendados y sobre los resultados de la gestión.

Algunos valores éticos que se podrían tener en cuenta al momento de crear el Código de Ética son:

- Honestidad. Proceder con rectitud, disciplina y honradez en el cumplimiento de las obligaciones y responsabilidades, y en la prestación de los servicios institucionales.
- Lealtad. Actuar con fidelidad, compañerismo y respeto a las convicciones personales y a la visión, misión y objetivos institucionales.
- Solidaridad. Actuar de manera desinteresada ante las necesidades de los demás.
- Respeto. Reconocer a cada persona como un ser único, con intereses y necesidades particulares.
- Colaboración. Demostrar actitud de cooperación que permita la sinergia entre conocimientos y experiencias para alcanzar objetivos comunes.
- Responsabilidad. Ejecutar funciones con alto nivel de compromiso, eficiencia y eficacia, a fin de cumplir con los objetivos institucionales y contribuir al buen uso de los recursos públicos.
- Confidencialidad. No brindar información que por ley tenga carácter reservado, de la cual se podría derivar un interés indebido, podría causar daño grave a terceras personas, o podría usarse para poner en riesgo la finalidad de la función pública o el patrimonio del Estado.

Algunos comportamientos deseables que podrían tenerse en cuenta al momento de elaborar el Código de Conducta son:

- Respetar las políticas, normas, protocolos y procedimientos de la entidad.
- No participar ni respaldar públicamente a ningún grupo u organización que degrade la visión, misión, objetivos, metas, credibilidad, reputación de la entidad.
- No proporcionar información que sea falsa, engañosa o que cree expectativas erradas.
- Notificar a la entidad de los sucesos que pudieran poner en duda la capacidad de una persona para cumplir con su deber como funcionario/a del centro de atención de emergencias.
- Notificar de inmediato si un/a funcionario/a es declarado/a culpable de un delito.
- No usar la/s certificación/es y conocimientos para beneficio privado o comercial.
- Respetar las leyes y los derechos de privacidad de los/as usuarios/as.
- Evitar el consumo de alcohol, drogas ilícitas o cualquier otra sustancia que pudiera afectar la capacidad del/a funcionario/a y/o el entorno de trabajo.
- Prevenir, evitar y erradicar prácticas discriminatorias.

CAPÍTULO VII. GESTIÓN DE LA INFORMACIÓN

Introducción

La información es uno de los activos principales de un sistema de emergencia y seguridad; un recurso que podría considerarse estratégico. Por esta razón se vuelve indispensable establecer y gestionar una serie de procesos que guíen el ciclo de vida de la información, y propicien la toma proactiva de decisiones, para alcanzar el cumplimiento de las metas y de los objetivos trazados en el plan estratégico y operativo de un sistema de emergencia y seguridad.

A su vez, ese ciclo de la información tendría que darse en un ambiente seguro, con protocolos y medidas para resguardar la información y evitar su filtración y mal uso (ver Capítulo VIII sobre Gestión de la Seguridad).

La información que emana o que esté en poder de las instituciones, organismos, entidades públicas, incluyendo los sistemas de emergencia y seguridad, tendrían que regirse por las normas que regulan el uso y la difusión de información. El principal resguardo que habría que tener al hacerlo es el de proteger la información personal de los/as usuarios/as, así como también no vulnerar la seguridad nacional, pública ni del Sistema.

En este Capítulo se ofrecen lineamientos sobre cómo gestionar la información de un sistema de emergencia y seguridad, proponiendo para ello un ciclo de información que funcionaría a partir de la iteración de al menos seis actividades principales. El punto de partida de dicho ciclo sería la elaboración de un diagnóstico informacional, para lo cual se sugiere la construcción de algunas herramientas, incluyendo un inventario de recursos, un mapeo de flujos, entre otras. Hasta llegar al punto final del ciclo, que significaría evaluar la gestión, concebida y llevada a cabo como un proceso institucionalizado en aras de la calidad y mejora continua del servicio.

7.1. Diagnóstico informacional

Un posible punto de partida para la gestión de la información sería elaborar un diagnóstico informacional.

Realizar este tipo de diagnósticos resultaría recomendable, porque permitiría identificar las fuentes, los flujos, los recursos, y los productos o servicios informativos que requiere y genera un sistema de emergencia y seguridad. Esta identificación, a su vez, sería el punto de partida para entender y orientar mejor qué es lo que se tiene que gestionar en materia de información.

Adicionalmente, el ejercicio tendría que estar dirigido a identificar las condiciones normativas, organizacionales, procedimentales, materiales y humanas, entre otras, que inciden positiva o negativamente en la gestión de la información.

Posibilitaría también el reconocimiento de las fortalezas y debilidades de la información disponible en la entidad, e introducir planes de acción para superar los puntos débiles identificados en aras de la mejora continua.

7.1.1. Fuentes

Respecto a las fuentes de información, estas se podrían clasificar en dos grandes categorías: fuentes internas y externas.

- **Fuentes internas:** Son las fuentes que se encuentran dentro del propio sistema de emergencia y seguridad, por ejemplo: las bases de datos internas con antecedentes sobre las atenciones brindadas, los usuarios atendidos, el personal operativo y administrativo, el equipamiento y la

ejecución presupuestaria. Las evaluaciones de desempeño que se realizan de manera sistemática al personal y las encuestas de satisfacción que responden los usuarios del Sistema.

- **Fuentes externas:** Son las fuentes que se encuentran fuera del sistema de emergencia y seguridad y sobre las cuales no tiene ningún control o responsabilidad, pero que contienen información de utilidad para su funcionamiento. Entre esas fuentes externas se podrían mencionar las bases de datos de otras instituciones públicas, sitios web de organismos estatales, guías y protocolos para eventos de magnitud, publicaciones, encuestas de opinión pública, entre otras.

7.1.2. Flujos de la información

En el Capítulo I de esta Guía se mencionó que un sistema de emergencia y seguridad podría funcionar teniendo en cuenta tres niveles: el nivel estratégico, el nivel táctico y el nivel operativo.

La información tendría que fluir en cada nivel, así como también entre los niveles. Estos flujos supondrían la existencia de procesos que habrían sido analizados, planificados, modelados y, si fuera posible, automatizados.

Adicionalmente a los flujos internos de información también podrían establecerse flujos desde el sistema de emergencia y seguridad hacia afuera, así como desde el exterior hacia el Sistema. En ese sentido se podría hablar de tres tipos de flujos informativos:

- **Flujos externos:** Conformados por la información proveniente del ambiente externo y que ingresa a la entidad.

- **Flujos internos:** Conformados por la información que, una vez que se convierte en un recurso organizacional, transitaría y se distribuiría dentro del Sistema, para ser utilizada y reutilizada internamente.

- **Flujos institucionales:** Conformados por la información que la organización comparte con otras entidades y públicos en su entorno, materializada en productos y servicios informativos y/o comunicacionales.

En todo caso, la identificación de estos flujos permitiría no sólo establecer el alcance informativo de un sistema de emergencia y seguridad, sino también tener mayor claridad de qué tipo y la cantidad de flujos que se tendrían que gestionar.

Algunos de los flujos de información externos e institucionales implicarían también establecer una red de interrelaciones con actores externos, incluyendo: proveedores, usuarios, organismos públicos y medios de comunicación.

Para una adecuada gestión, el diagnóstico podría resultar en un mapeo de los flujos de información considerados clave, para apuntalar los procesos y las áreas funcionales críticos de un sistema de emergencia y seguridad en tiempos de normalidad y también durante eventos críticos.

7.1.3. Recursos de información

Se sugeriría definir y registrar los recursos de información con los que cuenta un sistema de emergencia y seguridad. A partir del registro, se podrían generar inventarios, organizados por tipo, nombre, nivel de funcionamiento, uso, responsable, entre otras categorías.

Existirían al menos dos tipos de recursos de información que se tendrían que registrar:

- **Activos de información tangible:** Son recursos físicos y digitales a través de los cuales los datos, la información y el conocimiento de un sistema de emergencia y seguridad se materializan,

explicitan y se tornan disponibles para una variedad de audiencias internas y externas, y de propósito, desde la prestación de los servicios de atención y respuesta a emergencias hasta la rendición de cuentas, entre otros.

- **Activos de información intangible:** Son los recursos tácitos, integrados por la información estratégica y táctica, y el conocimiento (derivado de la experiencia, la lecciones aprendidas, las buenas prácticas, la retroalimentación recibida, entre otros), que permiten apuntalar el alcance de los objetivos y el cumplimiento de las metas establecidas.

Como todo recurso, estos también tendrían que ser gestionados para obtener su mejor aprovechamiento y potencial.

Los sistemas de información que utiliza un centro de atención y respuesta a emergencias podrían considerarse activos tangibles. Se podrían identificar y clasificar estos sistemas de acuerdo a los niveles de funcionamiento donde operan. De esta manera, en el nivel operativo se tendrían los siguientes:

- Sistema de Recepción de Llamadas de Emergencia
- Sistema de generación de ficha, código y número de registro
- Sistema de Información Geográfica (GIS)
- Sistema de monitoreo y geolocalización de unidades de respuesta (AVL)
- Sistema de Despacho Asistido Computarizado (CAD)
- Sistema de radiocomunicaciones móviles (*trunking*)
- Sistema de monitoreo y análisis de imágenes por video vigilancia
- Sistema de alertas
- Sistema automatizado de datos para instancias judiciales

Los que se utilizarían en el nivel táctico:

- Sistema de estadísticas (*data warehouse*)
- Sistema de gestión de calidad
- Sistema de seguridad de la información
- Sistema de gestión documental
- Sistemas geográficos de información
- Sistema de control del mal uso del servicio
- Sistema de información financiera

Uno de los sistemas que se utilizaría en el nivel estratégico sería:

- Cuadro de Mando Integral (CMI)

Un sistema de emergencia y seguridad requiere de sistemas seguros de información, que soporten el acopio, almacenamiento, procesamiento y uso de la información para el apoyo en las operaciones de emergencias, la toma de decisiones, la administración y el control, la comunicación, la transparencia y la rendición de cuentas**.**

7.1.4. Productos y servicios

Los productos y servicios informativos se tendrían que generar de acuerdo con las necesidades y requerimientos de los usuarios, los funcionarios/as operativos y de quienes gestionan el Sistema, y la proyección de la mejora continua del servicio.

A su vez, la elaboración de estos dependería de la arquitectura de la información y tecnológica con la cual se hubiera diseñado el sistema de emergencia y seguridad (ver Capítulo III de esta Guía).

Estos también tendrían que quedar registrados como parte el diagnóstico informacional.

7.2. Ciclo de la información

Una vez realizado el diagnóstico, existirían varios modelos para la gestión de la información. Esta sección se enfoca en la gestión de la información orientada a procesos, sobre la base de un ciclo continuo de siete actividades relacionadas entre sí:

1. Identificación de necesidades de información
2. Adquisición de información
3. Organización y almacenamiento
4. Desarrollo de productos o servicios de información
5. Distribución y acceso a la información
6. Uso de la información
7. Monitoreo y evaluación

Para su funcionamiento, el modelo para la gestión de la información de un sistema de emergencia y seguridad, requeriría contar, mínimamente, con protocolos, procedimientos y herramientas dirigidos a:

- La clasificación de la información y el control de la documentación
- La seguridad de la información
- La asignación y el control de accesos diferenciados a la información
- El uso aceptable de los activos y las consecuencias de su uso no autorizado
- La evaluación y el tratamiento de riesgos
- La revisión, actualización, resguardo y destrucción de la información

Este modelo de gestión permitiría potenciar los recursos de información como soporte de los procesos de toma de decisión y como insumo para la obtención de los objetivos y las metas establecidas en el plan estratégico.

Adicionalmente, impulsaría la generación de conocimiento, el aprendizaje y adaptación frente a un entorno cambiante, y facilitaría la sinergia con el talento humano.

7.3. Niveles de funcionamiento de la información

En cada uno de los tres niveles de funcionamiento de un sistema de emergencia y seguridad: nivel estratégico, nivel táctico y nivel operativo, sería necesario contar con fuentes, flujos, recursos, productos y servicios de información para guiar la toma de decisiones.

- **Nivel estratégico:** La toma de decisiones en este ámbito se centra en definir los grandes lineamientos que guíen la gestión, la dirección o re-direccionamiento del Sistema, y su posicionamiento.

  La toma de decisiones de este tipo recae en las autoridades de alto nivel, incluyendo a funcionarios/as del área de planificación.

  Este nivel actúa a partir de los flujos externos de información, información interna e información institucional, y el conocimiento que se hubieran generado desde la experiencia y en el nivel táctico.

- **Nivel táctico:** En este nivel, la toma de decisiones está enfocada en la planificación y elaboración de planes, programas y proyectos, para lo cual emplea información proveniente del flujo interno e información institucional.

  Este tipo de decisiones recaería en las autoridades de nivel alto y medio, y se serviría de la información y el conocimiento o aprendizajes producidos en el nivel operativo.

- **Nivel operativo:** Abarcaría las decisiones que se toman cotidianamente para el funcionamiento diario del Sistema. De este nivel provendrían los dato**s** capturados a través del sistema de mando y control, integrado por otros subsistemas incluyendo el de llamadas, video vigilancia, u otros mecanismos de alerta.

Cada uno de estos niveles de funcionamiento tendría que contar con un ciclo de información, conformado por las seis actividades mencionadas anteriormente. Cada ciclo tendría que quedar plasmado en protocolos y procedimientos que, a su vez posibilitarían la realización de ejercicios objetivos de revisión, ajustes e introducción de mejoras, así como también efectuar eventuales auditorías.

7.4. Identificación de necesidades de información

Las necesidades de información podrían definirse en función de temas, problemas y contingencias.

Tabla 23: Identificación de Necesidades de Información

Tema	Problema	Contingencia
Generación de Información oportuna y confiable	Capacidad de generación de datos; vulneración de los sistemas de generación y transacción de datos; velocidad de transacción de datos; consumo de información, entre otros.	Proponer planes, programas y proyectos de información, basada en la plataforma transaccional del servicio.
Interoperabilidad	Consumo de información segura con las instituciones articuladas y vinculadas; Fuga o filtración de información; mantenimiento de la cadena de custodia; demora en las solicitudes para consumo de información, entre otros.	Integrar plataformas informáticas de las instituciones articuladas asociadas a la gestión de emergencias o vinculadas en casos específicos.

Retroalimentación de la gestión del servicio de atención de emergencias	Monitoreo de estándares operativos y tecnológicos, entre otros.	Generar información estadística de la gestión del servicio de atención de emergencias.
Tiempos y variables de atención (Instituciones articuladas)	Identificación de tiempos de atención en territorio; número de recursos disponibles; mapas de calor, entre otros.	Estimar el tiempo y multivariables de las situaciones de peligro vinculadas a la gestión operativa de las instituciones articuladas.
Niveles de priorización	Identificación de incidentes o eventos; asignación de roles institucionales; reporte de recursos en el Sistema, entre otros.	Estimar la magnitud de situaciones de peligro vinculadas a la gestión operativa de las instituciones articuladas.
Desempeño de atención de emergencia	Cumplimiento de estándares internacionales en atención de emergencias, entre otros.	Evaluar y controlar la gestión operativa de la atención de emergencias.
Situaciones de peligro (instituciones articuladas)	Retroalimentación no adecuada de las situaciones en territorio; estado de los recursos, entre otros.	Evaluar las situaciones de peligro vinculadas a la gestión operativa de las instituciones articuladas, entre otros.

Fuente: Servicio Integrado de Seguridad ECU-911, 2020.

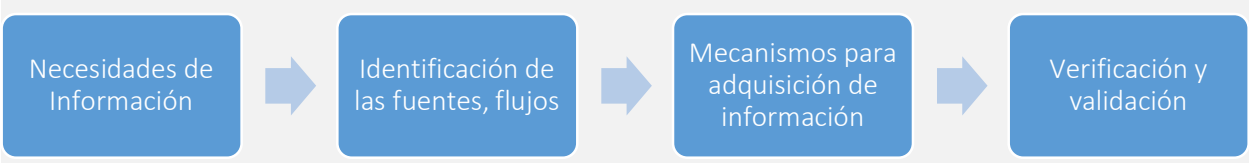
Existirían varios mecanismos y herramientas para identificar las necesidades de información, incluyendo análisis de brecha, auditorías de información (ver Sección 7.9 de este Capítulo), evaluaciones de desempeño y revisiones después de la acción, entre otros.

7.5. Adquisición de información

A partir de las necesidades identificadas, se buscaría recabar todos los datos y la información requerida para cubrirlas. Para esto se tendrían que tener en cuenta las fuentes, los flujos y los recursos de información existentes y considerar la posibilidad de incorporar nuevos.

Los datos y la información que se generen, tendrían que estar sometidos a algún mecanismo de verificación y validación que aseguren los aspectos mínimos de calidad.

Figura 24: Adquisición de la información



Fuente: Servicio Integrado de Seguridad ECU-911, 2020.

7.6. Organización y almacenamiento

La organización, almacenamiento y custodia de la información podría llevarse a cabo mediante la creación, mantenimiento y actualización constante de repositorios. Estos repositorios, a su vez, contribuirían a la memoria institucional del sistema de emergencia y seguridad.

A modo de ejemplo, se podrían considerar los siguientes repositorios: biblioteca virtual, informes (de gestión, atención, financieros, de proyectos), de consultas o pedidos de información realizados por otras entidades y terceras personas, entre otros.

Para la clasificación de la información en los repositorios, podría tomarse en cuenta el estándar ISO/IEC 27001 que simplifica este proceso en cuatro pasos:

i. Ingresar activos en un repositorio

ii. Criterios de clasificación

iii. Clasificación por activo (etiquetación)

iv. Tratamiento de la información clasificada

Los activos de información de un sistema de emergencia y seguridad podrían quedar clasificados según los siguientes criterios: tipo, ubicación, tiempo de conservación, tamaño, almacenamiento, medidas de seguridad y otros atributos. Adicionalmente, se tendría que especificar la/s persona/s que fungiría/n como custodio/s o responsable/s de esos activos, aplicando principios de racionalización, economía y depuración.

- Tipo de activo
- Ubicación
- Tiempos de conservación, particularmente en lo que respecta a documentos y archivos
- Tamaño
- Almacenamiento o soporte
- Acceso/Uso
- Seguridad
- Responsabilidad

Existirían varios criterios para clasificar la información en cuanto a su acceso y uso. Lo anterior dependerá, entre otros factores, de la legislación vigente, la realidad de cada país, así como de las necesidades y circunstancias específicas de cada sistema de emergencia y seguridad.

A pesar de lo anterior, en términos generales, los criterios para la clasificación de la información en cuanto acceso, tendrían que quedar establecidos sobre la base de los contenidos de la misma y los usos que se le dará. En ese sentido, se podría pensar en la siguiente clasificación de la información:

- **Confidencial.** Los sistemas de emergencia y seguridad capturan información individual de cada persona que tendría que resguardarse y protegerse.
- **Reservada o restringida.** Por lo general, la clasificación de “reservada” atañe a información vinculada con la seguridad pública y de Estado.
- **Uso interno.** Accesible única y exclusivamente por el personal autorizado del Sistema.

- **Uso interinstitucional.** Accesible para interactuar con otras instituciones del sector público, tanto en lo que respecta a la atención y respuesta a emergencias, así como insumo para el diagnóstico de problemas, el diseño de políticas de intervención para abordarlos, y el monitoreo y evaluación de estas.
- **Uso público.** Información de dominio público como la que se encuentra en la página web o es publicada por medios de comunicación y difusión para efectos de transparentar la gestión y rendir cuentas. Esta tendría que estar regida por el plan de comunicación de la entidad (ver Capítulo IX de esta Guía).

En lo que respecta al tratamiento de la información clasificada, particularmente como confidencial y restringida, sería conveniente establecer mecanismos de seguridad para protegerla de posibles riesgos, incluyendo daño, filtración o mal uso, entre otros. Algunas de las herramientas más comunes utilizadas para resguardar este tipo de información serían:

- Cifrar la información
- Generar y guardar copias de seguridad
- Diferenciar y limitar los accesos según perfiles y funciones
- Acuerdos de confidencialidad entre la entidad y otras instituciones públicas, así como entre la entidad y el personal.
- Reglamentar la entrega de información interinstitucional.

7.7. Desarrollo de productos o servicios de información

En esta etapa del ciclo, los datos y la información disponibles se procesarían, analizarían y empaquetarían, según corresponda, en productos y/o servicios dirigidos a una diversidad de audiencias internas y externas:

- Usuarios en general
- Públicos específicos
- Tomadores de decisión del propio Sistema, en los tres niveles de funcionamiento
- Tomadores de decisión en otras instituciones del estado. Entre estas últimas se podrían mencionar a los Ministerios de Salud y Seguridad, Observatorios del Delito y Protección Civil, entre otros

Habría una variedad de servicios o productos informativos que se podrían elaborar, a modo de ejemplo:

Tabla 25: Desarrollo de Servicios y/o Productos

Necesidades Específicas	Servicios y/o Productos
Mejorar la calidad del servicio a partir de la evaluación y monitoreo de la atención de emergencias.	Informes de satisfacción de los usuarios del sistema de emergencia y seguridad. Informes estadísticos vinculados a la atención de emergencias.
Mantener la cadena de custodia de los datos que podrían convertirse en evidencia o prueba en procesos judiciales.	Suministro de información a través del Sistema Automatizado de Entrega de Información a la función judicial

Brindar acceso a la información pública. Mejorar el nivel de preparación de la comunidad, incluyendo grupos y subgrupos en situación de vulnerabilidad.	Informes de gestión vinculados al funcionamiento del sistema de emergencia y seguridad. Análisis socio-demográfico de la población e identificación de riesgos de la población, grupos y subgrupos en situación de vulnerabilidad frente a emergencias.

Fuente: Servicio Integrado de Seguridad ECU-911, 2020.

7.8. Intercambio, distribución, acceso y uso de la información

El intercambio, distribución y el acceso a la información estarían sujetos, entre otros elementos, a:

- Leyes y acuerdos interinstitucionales que se hubieran establecido,
- Los lineamientos, protocolos y herramientas internos relativos al ciclo de información,
- La calificación y clasificación de la información en cuanto acceso y confidencialidad,
- Los planes de comunicación, incluyendo los componentes de transparencia y rendición de cuentas, y
- Los flujos de información y los responsables a cargo de la gestión de la información, entre otros.

La disponibilidad de la información de manera oportuna y en el formato adecuado, promueve la toma informada de decisiones, cataliza el aprendizaje de la propia entidad, facilita el reconocimiento de nuevos enfoques y la revelación de nuevos problemas/soluciones. De esta manera el sistema de emergencia y seguridad podría tornarse más resiliente, con mayor capacidad de ajustarse o adaptarse a los cambios.

Dependiendo del uso que se le piensa dar a la información, la misma podría distribuirse y tornarse accesible de diferentes maneras, en una variedad de formatos y haciendo uso de diversos canales o medios.

7.8.1. Interoperabilidad e intercambio de la información

La disponibilidad oportuna, efectiva y automática de datos, información, documentos y objetos digitales entre las instituciones articuladas (o de primera respuesta) es una funcionalidad clave para brindar a la población un servicio de calidad.

La recomendación sería que el sistema de emergencia y seguridad cuente con un diseño que asegure la interoperabilidad, con base en una o varias plataformas informáticas que permitan la transferencia de datos e información.

El intercambio de información (entrega y uso) tendría que tomar en cuenta normas y estándares internacionales y nacionales, como los elaborados por la Organización Internacional para la Estandarización (ISO, por su acrónimo en inglés), la Organización de Estándares Nacionales de Información de Estados Unidos (NISO, por su acrónimo en inglés) o el Instituto Estadounidense de Estándares Nacionales (ANSI, por su acrónimo en inglés).

Adicionalmente, también se tendrían que establecer reglamentaciones, protocolos y procedimientos internos, así como convenios de colaboración interinstitucionales para el intercambio de información, más aún si ese intercambio está mandatado por ley. Estos tendrían que especificar, entre otros aspectos, el tipo de información, el formato, los canales, la necesidad, los fines y las autorizaciones necesarias para habilitar los pedidos y los envíos de información.

7.8.2. Desarrollo y mejora continua de las operaciones

Para el fortalecimiento de las capacidades, el desarrollo institucional y la mejora continua de la entidad, el personal directivo precisaría manejar información estratégica acerca del funcionamiento del Sistema, incluyendo el componente financiero.

Esta información podría quedar disponible por medio de un tablero de control con información sobre objetivos, metas e indicadores. Los informes de gestión, de servicio, financieros y de proyectos también podrían estar al alcance del nivel directivo a través de un sistema de gestión de documentos (repositorio), ordenados por tema y período temporal de referencia.

A partir de las herramientas utilizadas por la entidad para recibir retroalimentación, ya sea por parte de los usuarios (por ejemplo: encuestas de satisfacción) y de las instituciones articuladas y vinculadas (por ejemplo: sesiones de revisión después de la acción), se podrían generar insumos informativos para la dirección. Estos podrían integrarse al sistema de gestión de documentos, al tablero de control o a un repositorio de información vinculado con la gestión de calidad y mejora continua.

7.8.3. Instancias prejudiciales y judiciales

La disponibilidad y entrega de datos e información generados o capturados por un sistema de emergencia y seguridad podrían servir de insumos clave para instancias prejudiciales o administrativas e instancias judiciales.

Respecto al primer tipo de instancia, se tendrían que utilizar las políticas, protocolos y procedimientos que se hubieran establecido para el intercambio y entrega de información interinstitucional.

Para instancias judiciales, la legislación de cada país podría haber establecido los mecanismos y procedimientos para compartir información de relevancia para las diferentes etapas que integran un proceso judicial. Dentro de ese marco, sería recomendable prever una herramienta específica para entregar y compartir los datos y la información que pudieran servir como evidencia en procesos judiciales. De esta manera se podría resguardar la autenticidad e integridad del indicio y así contribuir a garantizar la calidad probatoria del mismo (cadena de custodia).

En este sentido, se recomendaría que la entrega se hiciera por medio de los mecanismos que garantizan la interoperabilidad, es decir, prever el desarrollo de una plataforma que permita el envío de oficio o a petición de parte (sea el juez o fiscal), de la información que pudiera servir de evidencia en relación a presuntos hechos punibles detectados o denunciados. De esta manera, la información sería enviada de forma directa (de punto a punto), encriptada y sin intermediarios. La información se tornaría legible al ser descargada por la autoridad competente (juez o fiscal), pasando la custodia, uso y administración a la instancia judicial. Los riesgos de filtraciones, ataques cibernéticos y virus se verían reducidos.

En caso de no contar o de no poder desarrollar una plataforma específica, en el marco de lo que establece la ley, se podrían adoptar acuerdos interinstitucionales con los operadores de justicia para definir el procedimiento de entrega de información. Uno de los principales objetivos de estos acuerdos sería el de precautelar la cadena de custodia de la información y de esta manera conservar la validez de la prueba al momento de ser considerada como evidencia en un proceso judicial.

En estos instrumentos que se expidan para reglamentar el tratamiento y el intercambio de información con valor evidenciario, se tendrían que establecer los tiempos, plazos o términos de respuesta a las solicitudes de información realizadas por parte de los operadores de justicia, asegurando la protección y la celeridad en los diferentes procedimientos. De igual manera se tendrían que definir los tiempos en que la información tendría que permanecer archivada dentro del sistema de emergencia y seguridad.

Adicionalmente, sería necesario introducir mecanismos de control jurídico y tecnológico con la finalidad de conservar a buen recaudo la información que podría ser utilizada para fines judiciales. Estos mecanismos tendrían que venir acompañados de directrices claras para su resguardo, evitando la filtración, comercialización o cualquier acto que pudiera resultar en la invalidez de la información dentro de un proceso judicial.

7.8.4. Comunicación, transparencia y rendición de cuentas

A partir del plan de comunicación que se elabore (ver Capítulo IX de esta Guía), y de los objetivos, metas y actividades comunicacionales que se hubieran planteado en el mismo, y basándose en la arquitectura de la información e informática con la que se hubiera diseñado el sistema de emergencia y seguridad, este podría producir información de interés y de utilidad para el público interno (funcionarios/as del propio Sistema) y el público externo (general y específico), atendiendo a una variedad de propósitos:

- Informativos
- Educativos
- Preventivos
- Vinculantes
- Para generar fidelidad y sentido de pertenencia entre el personal
- Para generar confianza y legitimidad entre la población
- Para transparentar la gestión y el funcionamiento del Sistema, y rendir cuentas

Existirían varios canales o medios para realizar la distribución y facilitar el acceso a dicha información, incluyendo la intranet, la plataforma web, boletines (digitales y/o impresos), informes y publicaciones (digitales y/o impresos), entre otros.

7.8.5. Proceso de políticas públicas

Los datos y la información que genera el sistema de emergencia y seguridad, particularmente aquellos relacionados con la atención y respuesta a emergencias, también podrían convertirse en insumos relevantes para otras dependencias de la administración pública. Entre esas dependencias se podrían mencionar aquellas que trabajan en temas de salud, seguridad, violencia doméstica y contra las mujeres, desastres naturales y antrópicos, vialidad, transporte y movilidad, por mencionar algunas.

Estos insumos y los análisis que se deriven de los mismos, podrían alimentar y dar soporte a todo el ciclo de política pública, desde el diagnóstico, pasando por el diseño, la implementación y el monitoreo, hasta la evaluación.

Existirían varias maneras de tornar disponibles los datos y la información generados por el Sistema a partir de las emergencias recibidas y atendidas. Respecto a las entidades articuladas y vinculadas, se podría pensar en contar con sistemas interoperables. Si esto no fuera posible, el sistema de emergencia y seguridad podría generar informes de servicio, con información sobre la atención y respuesta a emergencias, elaborados mensual, trimestral o cuatrimestral, semestral y/o anualmente. Esta información tendría que venir desagregada por atributos útiles para el diseño de intervenciones de política pública, incluyendo sexo, edad, ubicación de los incidentes, tipo de lugar de los incidentes y tipo de incidente, entre otros.

Este tipo de participación o colaboración que podría brindar un sistema de emergencia y seguridad más allá de su zona directa e inmediata de acción, lo colocaría como parte de la gobernanza para la seguridad pública y, de manera más amplia, de la gobernanza pública.

7.9. Auditorías de la información

La sexta actividad del ciclo está enfocada en evaluar la gestión de la información.

Es por ello que, con base en las normas ISO 30401 u otras similares que se hubieran adoptado, y a los protocolos y los procedimientos que se hubieran establecido para la gestión de la información, incluyendo su clasificación, respaldo y protección, sería recomendable llevar a cabo auditorías para:

- Evaluar el grado de cumplimiento y observancia de esos instrumentos.
- Medir la efectividad y eficiencia del ciclo de la información y de cada una de sus seis actividades.

Así como para identificar:

- Las necesidades de información, por niveles y áreas.
- Las inconsistencias, duplicidades y puntos débiles.
- Nuevos/as o potenciales fuentes, flujos, recursos, productos/servicios, usos y usuarios que podría tener la información.

Existirían varios tipos de metodologías para llevar a cabo este tipo de ejercicios. La elección quedaría a criterio de cada sistema de emergencia y seguridad, pero podrían tenerse en cuenta los siguientes lineamientos mínimos:

- Presentar de forma clara los objetivos y propósitos de la auditoría.
- Conocer la estructura organizacional, niveles de funcionamiento, las fuentes, los flujos, los recursos y los servicios/productos de información e identificar a las personas claves en la organización en materia de información.
- Diseñar la metodología con la cual será llevada a cabo la auditoría: recolección y análisis de datos, entrevistas, grupos focales, entre otras técnicas.
- Elaborar y comunicar las recomendaciones.
- Dar seguimiento a la implementación de las recomendaciones.
- Medir y valorar los cambios generados a partir de las mismas.

Las auditorías podrían ser consideradas como herramientas para, desde un enfoque de gestión de la calidad (ver Capítulo IV de esta Guía), apuntar hacia la mejora continua del manejo de la información dentro de la entidad, superando a tiempo y de manera informada cualquier divergencia, brecha o desviación identificada con respecto a las normas, protocolos y procedimientos establecidos en la materia.

CAPÍTULO VIII. GESTIÓN DE LA SEGURIDAD

Introducción

En este Capítulo se presentan directrices relativas a la gestión de la seguridad que aplicarían para un sistema de emergencia y seguridad. La seguridad podría ser considerada como un recurso o medio clave para garantizar la prestación de los servicios.

La gestión de la seguridad de un sistema de emergencia y seguridad tendría que estar arraigada en las políticas, protocolos y herramientas institucionales establecidos para tal fin. Los estándares internacionales y nacionales de otros países en materia de seguridad podrían servir de referencia. Estos brindarían lineamientos y parámetros a seguir, adaptándolos a las realidades de cada Sistema y de cada país.

La seguridad de un sistema que atiende y responde a emergencias tendría que abordarse con un enfoque multidimensional, poniendo atención tanto en las condiciones básicas de funcionamiento de un centro operativo como en la continuidad de los servicios. En ese sentido, las múltiples dimensiones de la seguridad abarcarían la información, las comunicaciones, los sistemas informáticos, la seguridad física y de la infraestructura, y la seguridad del personal, entre otras.

En este capítulo, además de brindar directrices generales para la gestión de la seguridad y lineamientos para asegurar el funcionamiento de un centro de atención a emergencias desde múltiples dimensiones, también se aborda el análisis de riesgos y vulnerabilidades para resguardar y asegurar la continuidad operacional y la entrega de servicios en situaciones de crisis.

8.1. Seguridad de la información

La base legal para la gestión de la seguridad de la información tendría que remitirse a todas las normas nacionales que garantizan derechos y obligaciones de las personas y de las instituciones públicas para la prestación de un servicio. También cabría considerar el valor de la información, de hacerla pública y accesible en el marco de sociedades y regímenes políticos democráticos. Esto resulta especialmente relevante para conducir ejercicios de supervisión, transparencia, veeduría, auditoría y rendición de cuentas (temas que se abordan en el Capítulo X de esta Guía).

La seguridad de la información involucraría la adopción de medidas y acciones preventivas, proactivas y reactivas encaminadas a proteger la información del centro de atención a emergencias. Tendría que estar construida sobre tres principios básicos: la confidencialidad, la disponibilidad y la integridad de datos.

Además de ser un fin en sí mismo, la seguridad de la información tendría que ser considerada como un proceso continuo. Como tal, precisaría ser gestionado por un equipo especializado (dentro del área funcional para la Gestión de la Seguridad mencionada en el Capítulo III de esta Guía), y guiado por un conjunto de políticas y protocolos establecidos por la propia entidad para tales efectos. Estos tendrían que estar dirigidos a evitar el acceso, (re)uso, divulgación, intercambio, interrupción y destrucción no autorizados de los datos y la información que maneja el sistema de emergencias y seguridad, en diferentes formatos, formas y medios.

8.1.1. Políticas y estándares para la seguridad de la información

Las políticas y protocolos de seguridad tendrían que funcionar como instrumentos rectores para guiar, estandarizar y sistematizar el trabajo en esta área. Podrían ceñirse a normas y parámetros internacionales como, por ejemplo, la ISO 27000 y la familia de estándares asociados a la certificación de Sistemas de Gestión de la Seguridad de la Información (SGSI), entre otros. Asimismo, también tendrían que alinearse

con las normas nacionales relacionadas a la protección de datos, transparencia, propiedad intelectual, entre otros temas.

En cuanto a contenidos, podrían incluir aspectos generales tales como:

- Controles del acceso, sobre la base de roles y responsabilidades diferenciados
- Tratamiento de la información
- Seguridad física y ambiental

Entre los aspectos más específicos que podrían ser contemplados y regulados por las políticas y protocolos de seguridad de la información, vinculados al funcionamiento de un centro de atención a emergencias, se podrían mencionar los siguientes:

- Definición y gestión de perfiles y cuentas de usuarios/as (con grados/niveles diferentes de accesos y seguridad)
- Uso y gestión de las cuentas de acceso
- Uso de los servicios de mensajería
- Uso de licencias de *software* y definición de *softwares* no autorizados
- Protección de datos y privacidad
- Control de acceso físico
- Control de acceso remoto
- Descarga de ficheros (red externa/interna)
- Retención de registros y copias de seguridad
- Uso de los servicios de red
- Uso de informática y comunicaciones en movilidad
- Uso de controles criptográficos

Las políticas y protocolos que se elaboren en materia de seguridad de la información, tendrían que ser difundidos y socializados entre el personal, así como entre las personas externas que visitan las instalaciones de un centro de atención a emergencias.

A partir de las políticas y protocolos que se diseñen e implementen, el área funcional encargada de la seguridad de un centro de atención a emergencias, podría auditar su gestión en materia de sistemas de información y tecnologías afines. Para ello, podría utilizar como referencia las directrices establecidas por la guía: Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT, por sus siglas en inglés), desarrollado por la Asociación de Auditoría y Control de Sistemas de la Información (ISACA, por sus siglas en inglés).

8.1.2. Tratamiento de la documentación física y digital

El sistema de emergencia y seguridad tendría que establecer un proceso de control de la información documentada, en línea con las normas ISO 15489 e ISO 30301, que establecen instrucciones y pasos para la gestión de los documentos.

Los procedimientos tendrían que obedecer a un tratamiento seguro y consistente con la importancia de la información interna e institucional, aplicables en todas las etapas: (a) almacenamiento, (b) uso y reutilización (c) acceso y flujo, (d) digitalización y resguardo, y (e) destrucción.

También tendría que disponer de medidas de seguridad y de protocolos para el manejo de la información que se genere o acceda a través de: (a) suite ofimática, (b) mensajería de correo electrónico, (c) portales, (d) sistemas de bases de datos, (e) discos duros y/o externos, (f) multimedia (voz, video, cintas) y (g) tecnologías en la nube, u otros medios.

8.2. Seguridad de la infraestructura tecnológica para la información y la comunicación

Uno de los focos de la gestión de la seguridad de la información tendría que ser el sistema informático, particularmente la protección de los activos informáticos del sistema de atención a emergencias. Estos se podrían clasificar en:

- ***Hardware*:** elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, DVDs, entre otros).
- ***Software*:** conjunto de programas que se ejecutan sobre el *hardware*, tanto si es el propio sistema operativo como las aplicaciones instaladas en él.
- **Datos:** información lógica que procesa el *software* haciendo uso del *hardware*. En general serán informaciones estructuradas en bases de datos o paquetes de información que se intercambian por la red.
- **Otros**, por ejemplo: elementos fungibles, que son aquellos que se usan o gastan, incluyendo la tinta y el papel para las impresoras, los soportes tipo DVD u otros. Al ser elementos externos al sistema informático, no son críticos para su seguridad.

Entre estos, el más crítico son los datos. Los datos están almacenados en el *hardware* y son procesados por las aplicaciones *software* para apoyar la prestación de los servicios del sistema de atención a emergencias. Todo lo demás se podría reponer, mientras que la recuperación de datos es crítica para el funcionamiento del Sistema. Haría falta elaborar protocolos de protección que establezcan los pasos y las medidas que se tendrían que adoptar para:

- Recuperarlos en el menor plazo de tiempo posible y,
- Tornarlos utilizables, en el estado más próximo al momento de la pérdida.

La familia de estándares asociados a la certificación de Sistemas de Gestión de la Seguridad de la Información (SGSI), incluye también un conjunto de mecanismos básicos y medidas para salvaguardar los datos dentro de un sistema informático, que podría servir de referencia para un centro de atención a emergencias.

8.2.1. Referente a los sistemas informáticos

Las políticas y protocolos para la seguridad informática tendrían que estar estrechamente vinculados con los lineamientos para garantizar la confidencialidad, integridad y disponibilidad de la información que la entidad maneja. Su implementación tendría que apuntar a evitar brechas de seguridad y mantener los datos a salvo.

La seguridad informática respecto al *hardware* tendría que estar dirigida a proteger todos los elementos físicos que componen una red, haciendo uso de herramientas que permitan escanear y controlar el tráfico. Entre esas herramientas se podrían mencionar las siguientes: *firewalls*, cortafuegos y servidores *proxy*, entre otras.

Servidores, impresoras, *firewalls* y *proxys* tendrían que cumplir con las normas y requerimientos establecidos en las políticas de seguridad informática. Tendrían que quedar inventariados en formatos físicos y electrónicos. El *hardware* tendría que estar protegido contra problemas de suministro eléctrico. Adicionalmente, el uso de dispositivos de almacenamiento externo tendría que quedar sujeto a procedimientos estandarizados de protección, control y seguridad.

En relación a los servidores, la arquitectura de los mismos tendría que estar diseñada sobre la base de un modelo de redundancia y alta disponibilidad. Esto significa que todo lo que se aloja en su infraestructura sería resistente a las interrupciones y fallas del sistema eléctrico.

Para construir una infraestructura de alta disponibilidad se podría tomar como referencia el capítulo DSS04 del COBIT, particularmente la sección 7, asociada a la gestión de acuerdos de respaldos. Como mínimo, se tendrían que considerar los siguientes componentes: sistemas redundantes, matrices o arreglos de discos redundantes, red redundante, fuente de poder redundante, interruptores de transferencia automática (ATS, por sus siglas en inglés).

La seguridad informática respecto al software tendría que sustentarse en protocolos de vigilancia y testeos periódicos. Asimismo, tendría que considerar la validación de parches y actualizaciones e incorporar un software antivirus que esté conectado a la red interna. Al igual que con el *hardware*, sería recomendable inventariar todos los activos de software tales como sistemas operativos, *software* de servicio, paquetes de *software* base (ofimática, cliente de correo, mensajería instantánea, videoconferencia, edición de video, aplicaciones de bases de datos, entre otros).

Algunos mecanismos básicos para la seguridad de los sistemas informáticos que se podrían considerar serían:

- **Autenticación:** Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.
- **Autorización:** Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la entidad.
- **Administración:** Define, mantiene y elimina las autorizaciones de los/as usuarios/as del Sistema, los recursos del Sistema y las relaciones usuarios-recursos del Sistema.
- **Auditoría:** Continua vigilancia de los servicios en producción, para lo cual se recaba y analiza información.
- **Registro:** Mecanismo que captura y guarda cualquier intento de violar las reglas de seguridad establecidas por el sistema de atención a emergencias, en una base de eventos que luego podría ser analizada.
- **Mantenimiento de la integridad de la información:** Procedimientos establecidos para evitar o controlar que los archivos no sufran cambios no autorizados y que la información enviada desde un punto llegue al destino indicado, sin haber sufrido alteraciones en el camino.

8.2.2. Seguridad de las comunicaciones

Los sistemas de atención a emergencias exigen cada vez un número mayor de aplicaciones (sistemas de entrega de correo electrónico y navegadores, entre otros) y de equipos terminales (teléfonos, ordenadores centrales, computadores personales y teléfonos móviles, entre otros) conectados a las redes. Es por ello que la seguridad de las comunicaciones en redes de datos y en redes móviles resultan fundamentales para la gestión de la seguridad.

La capacidad de las redes o de los sistemas de información para resistir los accidentes o acciones malintencionadas que pongan en riesgo los correspondientes servicios que ofrecen o tornan accesibles, depende de la protección e interceptación del tráfico de comunicaciones y de sus puntos críticos.

La seguridad de las comunicaciones abarca los sistemas de almacenamiento, y de procesamiento y transmisión de datos. Estos a su vez están compuestos por mecanismos de transmisión (cables, enlaces inalámbricos, satélites, enrutadores y conmutadores, entre otros) y de servicios de apoyo (sistema de nombres de dominio incluidos los servidores raíz, servicio de identificación de llamadas y servicios de autenticación, entre otros).

Este tipo de seguridad, enfocada en las comunicaciones, buscaría evitar que interceptores no autorizados accedan a las telecomunicaciones de forma inteligible, sin dejar de entregar el contenido a los destinatarios previstos. Para ello se podría recurrir a los siguientes mecanismos: criptoseguridad, seguridad de transmisión, seguridad de emisiones, seguridad de flujo de tráfico y seguridad física de los equipos.

Es importante proteger el tráfico clasificado y no clasificado en las redes de comunicaciones, incluidos voz, video y datos. Voz sobre protocolo de Internet seguro (VOIP, por sus siglas en inglés), se habría convertido en el estándar de facto para asegurar la comunicación de voz, reemplazando la necesidad de equipos análogos.

Para estos propósitos vinculados a resguardar la seguridad de las comunicaciones, se podrían tomar en cuenta, mínimamente, los siguientes lineamientos:

- **Referente a las cuentas de correo.** El nombre de usuario y contraseña que se utilizan para acceder a los sistemas informáticos tendrían que ser individuales, y las contraseñas construidas de acuerdo con una serie de criterios para promover mayores niveles de seguridad.
- **Referente a la mensajería electrónica**. Tendrían que implementarse medidas de protección para mensajes clasificados, encriptar los contenidos y/o información sensible que pudieran compartirse y monitorear los mensajes.
- **Referente a las telecomunicaciones**. Los requerimientos (*switches*, enrutadores, puntos de acceso inalámbrico, entre otros) y servidores (web, FTP, correo y otros) podrían regirse por los estándares de la norma ANSI/TIA 942-A u otra regulada por el órgano especializado en cada país.

8.3. Seguridad física

La seguridad física es un subcomponente de la seguridad de las instalaciones e involucra los mecanismos de prevención y detección para proteger físicamente los recursos del Sistema, desde los activos físicos hasta el personal.

Además de las normas técnicas de diseño, edificación y habilitación de áreas y dependencias para el trabajo de funcionarios/as públicos/as vigentes en cada país, se tendrían que considerar al menos las siguientes acciones:

- Diagnosticar el estado actual y futuro del centro operativo.
- Analizar y evaluar de manera periódica el estado de funcionamiento y los riesgos que podría enfrentar el sistema de emergencia y seguridad en su operación diaria.
- Elaborar, revisar y ajustar un plan de seguridad física con las medidas con que cuenta la instalación, y las instrucciones y ejercicios de simulacro dirigidos al personal.

En cuanto a la seguridad física se tendrían que considerar, mínimamente, los siguientes elementos:

i. **Seguridad física e infraestructura:**

- Perímetro de seguridad física
- Controles físicos de entradas y salidas
- Seguridad de oficinas, despachos e instalaciones
- Protección contra amenazas externas y de origen ambiental
- Protección contra incendios (ver como referencia la norma NFPA 101), incluyendo sistemas de detección y alarma (ver como referencia la norma NFPA 72), sistema de rociadores (ver como referencia la norma NFPA 13), instalación de puertas contra incendios (ver como referencia la norma NFPA 101) y cortafuego (ver como referencia la norma NFPA 80)
- Rutas de evacuación y salidas de emergencia debidamente señalizadas

ii. **Seguridad del equipamiento o de los equipos:**

- Emplazamiento y protección de equipos, por ejemplo, contra incendios, eventos sísmicos e hidrometeorológicos, entre otros.
- Instalaciones de suministro de electricidad y agua, entre otros servicios.
- Seguridad del cableado
- Mantenimiento de los equipos
- Seguridad de los equipos fuera de las instalaciones
- Reutilización o retirada segura de equipos

iii. **Acceso a las instalaciones y sitios autorizados**

Las personas externas al Sistema tendrían que quedar debidamente identificadas y registradas antes de ingresar a las instalaciones, ya sea a pie, en vehículo, o por algún otro medio. El registro tendría que incluir, entre otros elementos, los siguientes datos: fecha y hora de ingreso, nombre completo, documento de identidad, motivo del ingreso, persona a visitar, así como la fecha y hora de salida. Se podría también tomar un registro fotográfico y generar credenciales o pases que tendrían que quedar visibles durante la presencia de la persona dentro de las instalaciones.

En el ingreso, las personas visitantes también podrían pasar por un arco detector o por un detector manual de metales. Adicionalmente, bultos y paquetes podrían ser inspeccionados por máquina de rayos X.

Las zonas restringidas tendrían que quedar visualmente identificadas, y el acceso a las mismas tendría que quedar reglamentado por un proceso interno de autorización, teniendo en cuenta los cargos y responsabilidades del personal.

8.4. Riesgos y vulnerabilidades

La gestión de la seguridad también implicaría la identificación de riesgos o eventualidades que pudieran afectar el funcionamiento y la continuidad de operaciones de un sistema de emergencia y seguridad.

En ese sentido, se recomendaría implementar procesos y herramientas que permitan identificar vulnerabilidades y potenciales riesgos sobre tres componentes principales del Sistema: información y

comunicaciones, soporte informático e infraestructura. Este diagnóstico serviría de insumo para diseñar los planes de mitigación y contingencia, continuidad de operaciones y recuperación.

La recomendación sería desarrollar un enfoque proactivo de la gestión de riesgos. Este enfoque demandaría prever, reducir o evitar riesgos y tomar las medidas de preparación necesarias para que se puedan restablecer las operaciones del sistema de emergencia y seguridad en el menor tiempo posible, en caso de darse alguna de las contingencias identificadas. Para ello, habrían al menos tres herramientas claves que se podrían considerar: el análisis de riesgos, un plan de continuidad de operaciones (PCO) y un plan de recuperación ante desastres.

8.4.1. El análisis de riesgos

El análisis de riesgos es clave para saber qué medidas de prevención, mitigación y respuesta introducir para que el sistema de emergencia y seguridad pueda seguir brindando sus servicios, sin importar las circunstancias.

Para ello sería necesario realizar una identificación de riesgos que pudieran afectar a cada uno de los sistemas y servicios críticos, incluyendo el equipamiento tecnológico y de comunicación que le da soporte y viabiliza su funcionamiento. Luego sería necesario evaluar la posibilidad de que ocurran, y valorar el tipo y nivel de impacto que acarrearían. Esta información podría quedar sistematizada en una matriz de riesgo.

La matriz de riesgo es una herramienta de gestión que ayuda a determinar objetivamente cuáles son los riesgos relevantes para la seguridad. Al posicionar los diferentes tipos de riesgo en la matriz, se podrían visualizar con claridad dónde estarían las prioridades, y hacia dónde tendrían que estar dirigidos los esfuerzos y los recursos. (En el Capítulo II de esta Guía, se abordó el empleo de este instrumento vinculado al plan estratégico). A continuación, se presenta un ejemplo de una matriz de riesgo:

Tabla 26: Ejemplo de matriz de riesgo

Riesgo	Probabilidad	Impacto	Mitigación	Responsable(s)
Interrupción del sistema eléctrico/de respaldo de la información entre los distintos centros de atención	Alta en ciudades de la costa pacífico	Reducción de la interoperabilidad	Equipos de respaldo	Departamento de planificación, logística y presupuesto

Fuente: Sistema Nacional de Atención a Emergencias y Seguridad 9-1-1, República Dominicana, 2020.

La identificación y el análisis de riesgos tendrían que venir acompañados de un plan de contención y mitigación de las vulnerabilidades asociadas, con acciones específicas a tomar, y que incluya los siguientes elementos:

- La designación de responsables, hasta el nivel de unidades y equipos, para que todas las partes del Sistema sepan cómo reaccionar y qué hacer en caso de ocurrencia de los riesgos identificados,
- La asignación de presupuesto y,
- El establecimiento de plazos.

8.4.2. Plan de continuidad de las operaciones (PCO)

Este tipo de planes contribuiría a que los sistemas de soporte, esenciales o críticos, para el funcionamiento del centro de atención a emergencias, estén disponibles cuando sean necesarios, apoyando la prestación de los servicios, sin importar las circunstancias del contexto.

El PCO es un plan de emergencia con el objetivo de mantener la funcionalidad a un nivel mínimo aceptable durante una contingencia o crisis. En caso de que se produzca esa eventualidad, que impactaría negativamente sobre las operaciones del Sistema, dicho plan tendría que contemplar todas las medidas de reacción y recuperación para responder efectivamente.

El objetivo del PCO es mantener al centro de atención y respuesta a emergencias funcionando. Esto daría lugar a la necesidad de priorizar las operaciones que son críticas para mantener la continuidad de su funcionamiento, en todo momento, bajo cualquier tipo de contingencia que se esté enfrentando.

Algunos beneficios y/o ventajas de contar con este tipo de plan serían los siguientes:

- Identificación temprana y oportuna de procesos y activos críticos, otorgando prioridad a su protección o garantía de funcionamiento durante una crisis.
- Definición de tiempos y plazos críticos de recuperación para volver al estado anterior, señalando planes y protocolos de contingencia.
- Prevención y minimización de pérdidas humanas y económicas, y de afectación al personal que labora en un Centro.

Para el diseño del PCO sería recomendable considerar los siguientes pasos y aspectos:

- Formar un comité y un equipo de trabajo multidisciplinario para prever y analizar riesgos.
- Realizar evaluaciones de riesgos (probabilidad de ocurrencia e impacto).
- Identificar los procesos y la criticidad de cada uno de estos para el funcionamiento del Sistema.
- Modularizar cada componente informático crítico del Sistema, para así garantizar la recuperación de la operación ante cualquier contingencia.
- Desarrollar y documentar procedimientos, indicando el objetivo y el alcance, considerando los tiempos de recuperación para cada actividad a ejecutar.
- Asignar responsables por cada acción a ejecutar, para así garantizar la continuidad casi inmediata.
- Desarrollar estrategias de recuperación para posibles escenarios de contingencia donde se vean interrumpidos los procesos críticos, incluyendo la definición de procedimientos, y roles que se tendrían que activar para responder y operar en situaciones de emergencia.
- Difundir y socializar el plan entre el personal y entrenar al personal de las áreas funcionales donde se hubieran identificado puntos y procedimientos críticos. Esta capacitación tendría que brindarse independientemente de la mitigación de riesgos que se hubiera llevado a cabo, pues siempre existirá un riesgo residual.
- Definir el plan de comunicación de crisis (ver Capítulo IX de esta Guía).
- Definir el calendario de pruebas y de simulación para el restablecimiento de los procesos críticos, con base en el plan de recuperación ante desastres.
- Documentar y actualizar constantemente el plan. Realizar pruebas al plan al menos una vez al año, analizar y documentar los resultados, e introducir ajustes y mejoras. Sería útil crear una base de conocimiento de las lecciones aprendidas durante las pruebas, así como también luego de su implementación frente a una crisis.

8.4.3. Planes de contingencia y de recuperación

La planificación de la contingencia es un proceso básico para la gestión de la seguridad en un sistema de atención de emergencias, y parte sustantiva del control interno que se establece para gestionar la disponibilidad de los procesos y equipos críticos en el caso de una interrupción. El principal objetivo sería minimizar el tiempo fuera de servicio y maximizar el tiempo de recuperación. Un modelo de referencia para la planificación de la contingencia y la recuperación podría ser el Análisis de Impacto en el Negocio (BIA, por sus siglas en inglés).

Para el Plan de Recuperación ante Desastres (PRD), cabría considerar las directrices y recomendaciones relativas al Plan de Continuidad de las Operaciones (PCO) y prestar especial atención a los siguientes puntos:

- Enfocarse en los procesos y equipos considerados críticos para los servicios de emergencia y seguridad.
- Desarrollar ejercicios prospectivos sobre escenarios que pudieran afectar la disponibilidad de los servicios de emergencia y seguridad.
- Definir las acciones de respaldo de la infraestructura tecnológica y de comunicaciones, que brindan soporte a los procesos y equipos críticos de los servicios de emergencia y seguridad, especificando la frecuencia y la ubicación de esos respaldos.
- Definir protocolos de actuación sobre la base de procesos y la priorización de los mismos.
- Definir roles y responsabilidades.
- Definir aquella información mínima que resulta necesaria para continuar operando.
- Generar una base de conocimiento con las lecciones aprendidas a partir del diseño, pruebas e implementación del plan.

8.5. Seguridad y salud del personal

En la seguridad laboral y prevención de riesgos de trabajo se conjugarían varias disciplinas profesionales con el fin específico de eliminar o reducir los riesgos propios de las actividades laborales. Estos riesgos podrían ser causantes tanto de enfermedades como de accidentes laborales.

El tema fue introducido, brevemente, en la Sección 6.8 del Capítulo VI sobre Gestión del Talento Humano, cuando se hizo referencia a la salud y seguridad ocupacional del personal, en función de la naturaleza, dinámica y condiciones de trabajo en un centro de atención a emergencias. Adicionalmente, se enumeraron otros aspectos que una política de seguridad y salud ocupacional de un centro de atención a emergencias podría abordar, que se presentan brevemente en esta sección, incluyendo:

- **Condiciones de trabajo**: Se refieren a factores sociales, técnicos, organizacionales en un lugar de trabajo, y a los factores de riesgo que pudieran surgir en el ambiente laboral. Estos, a su vez, podrían generar, de manera inmediata o a largo plazo, consecuencias negativas o positivas en el bienestar, la salud y la seguridad de los/as funcionarios/as.

  Normativas internacionales y nacionales disponen que es obligación del Estado establecer condiciones de trabajo seguras y adecuadas para un correcto y saludable desarrollo de las actividades por parte de los/as funcionarios/as.

- **Factores de riesgo:** Se determina como factor de riesgo laboral a cualquier condición que se encuentra presente en el desarrollo de una actividad laboral y que pudiere producir accidentes, enfermedades e inclusive la muerte de la persona.

- **Accidentes de trabajo:** Se podrían definir como todo suceso imprevisto y repentino que sobrevenga por causa, consecuencia o en ocasión de realizar la actividad laboral relacionada con el puesto de trabajo, y que ocasione en la persona lesión corporal, perturbación funcional, incapacidad, o muerte (inmediata o posterior).

- **Enfermedades laborales:** Estas podrían entenderse como afecciones crónicas, causadas de una manera directa por el ejercicio del puesto de trabajo u ocupación que realiza la persona en el ámbito laboral y como resultado de la exposición a factores de riesgo, y que podrían producir incapacidad laboral.

  La Organización Internacional del Trabajo (OIT) ha producido una lista de enfermedades ocupacionales, organizadas por causa, que podrían servir como referencia para este punto.

  La clave radicaría en comprobar la relación causa-efecto entre el trabajo desempeñado y la enfermedad crónica resultante, y de ser así, introducir medidas para erradicar o mitigar las causas identificadas.

- **Ausentismo laboral:** La Organización Internacional del Trabajo (OIT) lo define como "la práctica realizada por un trabajador de no asistencia al trabajo por un período de uno o más días de los que se pensaba que iba a asistir, quedando excluidos los periodos vacacionales, las huelgas, períodos gestacionales y privación de la libertad."

- **Sistemas de prevención y vigilancia epidemiológica:** La prevención de enfermedades que pudieran presentarse dentro del ámbito laboral y en el desempeño de las actividades laborales son un punto importante para la prevención de riesgos laborales, la seguridad y salud del personal. En ese sentido, la vigilancia epidemiológica sería un instrumento de vital importancia. Tendría que ser concebido como un proceso dinámico utilizado para identificar, medir y analizar los problemas de salud que pudieran afectar a la población laboral. Es a partir de esa vigilancia epidemiológica que se podría generar información para la toma de decisiones orientadas a promocionar la salud, prevenir las enfermedades o, en su defecto, contener y controlar los problemas sanitarios que ya se hubieran presentado al interior de un centro de trabajo.

8.5.1. Factores de riesgo

Es necesario partir del reconocimiento de que el principal factor para que exista un accidente laboral es el factor humano. Esto podría deberse a varios motivos, incluyendo: la ejecución de un acto inseguro o de una condición insegura, ya sea por desconocimiento al momento de la ejecución de la/s tarea/s, por exceso de confianza en la ejecución de la misma, o por fallas técnicas. Es así que para asegurar el éxito en la prevención de riesgos laborales se tendrían que tomar en cuenta los siguientes pasos:

- Identificación y evaluación de riesgos laborales en los puestos de trabajo, mediante herramientas e instrumentos avalados y reconocidos internacionalmente, incluyendo la Guía Técnica Colombiana (GTC) 45, la Norma Técnica de Prevención (NTP) 330, Identificación de Peligros y Evaluación de Riesgos (IPER), entre otras.

- Evaluación de riesgos específicos como, por ejemplo, la evaluación de riesgos psicosociales, riesgos ergonómicos, riesgos físicos, mecánicos y químicos, entre otros, que pudieran afectar la salud y el bienestar del personal.

- Definición de medidas para prevenirlos, mitigarlos o eliminarlos, incluyendo capacitaciones, de acuerdo al puesto de trabajo, a los riesgos existentes y cómo evitarlos.

Entre los factores de riesgo ocupacional más comunes en un centro de atención a emergencias, se presentan aquellos asociados a tres tareas operativas básicas: recepción de solicitudes, llamadas o reportes de auxilio y monitoreo de cámaras de video vigilancia, y atención de las emergencias en terreno. Cada tipo de riesgo tendría que estar acompañado de una serie de recomendaciones que podrían ser consideradas para su mitigación.

Tabla 27: Riesgos y recomendaciones en la recepción de llamadas y monitoreo de cámaras

Tipo de Riesgo: Ergonómico	Recomendaciones
• Digitación constante del teclado y uso prolongado de mouse o joystick. • Se mantiene posición sentada por períodos prolongados de tiempo. • Uso prolongado de pantallas.	• Asignación de tiempo para pausas activas (descanso y ejercicios de estiramiento) y descansos visuales. • Dotación de protectores visuales. • Ajuste de la altura e inclinación del teclado. • Reposabrazos y descansos para las palmas de las manos. • Dotación de sillas ergonómicas. • Posturas correctas frente al computador y al momento de sentarse.
Tipo de Riesgo: Psicosocial	**Recomendaciones**
• Alta responsabilidad. • Altos niveles de estrés. • Estado de alerta constante. • Carga de trabajo. • Dificultad para balancear vida profesional y personal. • Jornada de trabajo, trabajo nocturno, rotación, horas extras, trabajo fuera del horario laboral.	• Actividades para la descarga emocional. • Mejora en la comunicación. • Seguimiento psicológico con profesionales.

Fuente: Servicio Integrado de Seguridad ECU-911, 2021.

Tabla 28: Riesgos y recomendaciones en la respuesta a emergencias en terreno

Tipo de Riesgo: Ergonómico	Recomendaciones
• Postura sentada por tiempo prolongado durante la actividad de conducción.	• Asientos ergonómicos para vehículos.
Tipo de Riesgo: Mecánico	**Recomendaciones**
• Uso de vehículos. • Desplazamiento en medios de transporte terrestre. • Accidentes viales, atrapamientos, desmembramientos, muerte.	• Mantenimiento preventivo de vehículos de manera periódica. • Capacitación sobre leyes de tránsito y temas relacionados. • Capacitación de manejo defensivo. • Concientización al volante.

Tipo de Riesgo: Psicosocial	Recomendaciones
• Alta responsabilidad. • Altos niveles de estrés. • Estado de alerta constante. • Carga de trabajo. • Dificultad para balancear vida profesional y personal. • Jornada de trabajo, trabajo nocturno, rotación, horas extras, trabajo fuera del horario laboral.	• Actividades para la descarga emocional. • Mejora en la comunicación. • Seguimiento psicológico con profesionales.

Fuente: Servicio Integrado de Seguridad ECU-911, 2021.

8.6. Mejora continua

En línea con el modelo de gestión de calidad integral que se desarrolló en el Capítulo IV de esta Guía, sería necesario establecer acciones de mejora en todos aquellos aspectos que hacen a la seguridad del sistema de emergencia. Para ello, basándose en las políticas y protocolos de seguridad establecidos, se tendrían que establecer mecanismos de evaluación y medición que permitan identificar desvíos, deficiencias y debilidades en los procesos actuales y, como resultado, introducir actualizaciones o ajustes que los mantengan confiables y seguros.

En el marco del modelo de gestión de calidad integral, para poder generar un círculo continuo de mejoras, sería necesario considerar los siguientes pasos:

i. Definir procesos de monitorización que recolecten y entreguen datos para medir, procesar, analizar e implementar mejoras en la seguridad de la información, informática, comunicacional, física y del personal.

ii. Diseñar reportes e informes que permitan identificar fallos o vulnerabilidades recurrentes, y así ajustar las políticas de seguridad existentes.

iii. Identificar obsolescencia tecnológica y comunicacional.

iv. Establecer un proceso con el que se pueda evaluar el cumplimiento y medición constante de las políticas y protocolos de seguridad.

v. Priorizar las áreas de oportunidad identificadas y generar planes de acción para atender dichos hallazgos.

CAPÍTULO IX. GESTIÓN DE LA COMUNICACIÓN

Introducción

La comunicación y la información podrían ser consideradas como recursos estratégicos para los sistemas de emergencia y seguridad, tanto en lo que respecta a la comunicación institucional como operativa. La primera estaría ligada al posicionamiento, a la imagen y a la "marca" de un sistema de emergencia y seguridad. Incluiría una serie de acciones comunicacionales dirigidas al relacionamiento con el personal así como con el público externo desde una perspectiva estratégica. La segunda estaría vinculada con la comunicación al interior del sistema de emergencia y seguridad, y de este con actores del entorno, en atención y respuesta a emergencias de baja y alta magnitud. Es por ello que su planificación y gestión resultan fundamentales.

La planificación y la gestión de la comunicación tendría que pensarse en dos ejes: un eje estratégico, relacionado con la comunicación institucional, y otro eje más operativo, vinculado al funcionamiento del sistema de emergencia y seguridad en la atención y respuesta a emergencias. Adicionalmente, la planificación y la gestión de la comunicación tendría que darse en dos planos: al interior de la organización y en relación con el entorno. Por último, la planificación y la gestión de la comunicación tendría que ser concebida para emergencias de baja intensidad, relativas al operar diario del Sistema, y a emergencias de alta intensidad, relacionadas con desastres naturales o antrópicos que afectan de manera simultánea a un elevado número de personas y áreas geográficas.

Como resultado del proceso de planificación, se tendría que elaborar un plan de comunicación que serviría de hoja de ruta para orientar la gestión de las comunicaciones. El Capítulo presenta una serie de lineamientos para guiar la estructura, componentes y contenidos mínimos que se podrían considerar para elaborar un plan de comunicación.

Luego se exponen algunos canales y herramientas que podrían ser tenidos en cuenta para el manejo de las comunicaciones en un sistema de emergencia y seguridad, incluyendo: la creación de una vocería, el uso de las redes, los medios de comunicación y sociales, la vinculación con la población y las comunidades, y los mensajes pregrabados.

El Capítulo también ofrece directrices para guiar la planificación y la gestión de la comunicación en situaciones de crisis de alto impacto, que afectan a nivel nacional, subnacional y zonal. Finalmente, el Capítulo concluye con la presentación de tres desafíos comunicacionales, frente a los cuales se proponen algunas medidas de mitigación.

9.1. La planificación de la comunicación

Las acciones comunicacionales tendrían que formar parte de un proceso estructurado de diseño, ejecución y evaluación.

La comunicación tendría que tener un alcance integral. A su vez, la planificación y la gestión de la comunicación tendrían que estar integradas en la gestión global de la entidad y podrían tener diferentes niveles de complejidad, dependiendo del tipo de modelo de funcionamiento adoptado por el sistema de emergencia y seguridad (estos modelos fueron presentados en el Capítulo III de esta Guía).

Toda la actividad comunicacional tendría que responder a una planificación previa que contribuya a garantizar los resultados y el impacto buscados. Adicionalmente, tendría que estar alineada a los objetivos estratégicos del Sistema, a los diferentes tipos de emergencias y necesidades operacionales, a los requerimientos informativos de la población, las diferentes audiencias o públicos específicos y al ecosistema de medios de comunicación, entre otros elementos.

Todo estos aspectos tendrían que quedar refrendados en un documento técnico y de referencia transversal. El plan de comunicación serviría de instrumento conductor. La planificación tendría que abordar dos dimensiones necesarias y complementarias de la actividad comunicacional: la organizacional/institucional, con un fuerte componente estratégico, y la operativa.

9.2. La planificación de la comunicación organizacional

En la dimensión organizacional, la planificación de la comunicación implicaría adoptar un enfoque estratégico. Es una actividad instrumental de apoyo al plan estratégico de una entidad. Tendría que considerar las acciones comunicacionales que buscan el fortalecimiento del Sistema, tomando en cuenta la misión, visión y objetivos estratégicos planteados (ver Capítulo II de esta Guía).

Asimismo, la comunicación organizacional tendría que abordarse como parte integral de la planificación estratégica, intentando capitalizar las fortalezas y oportunidades, y haciendo frente a las debilidades y amenazas identificadas. Tendría que estar guiada por sus propios objetivos y metas, alineados con el plan estratégico, e incorporar indicadores para medir los resultados alcanzados.

En este nivel resultarían necesarias distintas estrategias de comunicación. Cada una ofrecería un marco conceptual y práctico para responder a una situación determinada, aplicable en diferentes momentos. Asimismo, cada una sería el fruto de una planificación de la gestión de flujos comunicacionales al interior de la entidad, acorde a sus objetivos, valores y expectativas.

La planificación de la comunicación organizacional determinaría de qué forma se tendrían que estructurar y coordinar las comunicaciones, buscando:

- La integración de los flujos y procesos comunicacionales con los objetivos estratégicos perfilados en la planificación de la entidad.
- El establecimiento de procesos y flujos comunicacionales que permitan crear valor, construir símbolos y significados compartidos, elaborar mensajes, posicionar al sistema de emergencia y seguridad y generar relación de cercanía/pertenencia con la población, de manera sistematizada y sostenida en el tiempo.
- El involucramiento y la coordinación entre el proceso gerencial y los otros procesos organizacionales.
- La participación de todo el personal en la consolidación, desarrollo y fortalecimiento del sistema de emergencia y seguridad.
- La transparencia y la rendición de cuentas del funcionamiento y la gestión del Sistema (ver Capítulo X de esta Guía).

Esta planificación, así como su ejecución, quedarían a cargo del área funcional especializada en el tema, integrada por un equipo de funcionarios/as con la formación y experiencia necesarias para desempeñarse en el área.

9.3. La planificación de la comunicación operativa

La gestión comunicacional en el ámbito operativo tendría que contemplar el modelamiento de los elementos mínimos de un plan de comunicación, dirigido a apoyar la prestación de los servicios en atención y respuesta a emergencias, y consolidar la relación del Sistema con la población usuaria y las distintas audiencias identificadas.

La planificación de la comunicación operativa tendría que considerar al menos dos dimensiones: la temporalidad y la audiencia.

Respecto a la primera dimensión, resultaría importante pensar en objetivos y estrategias de comunicación para tiempos "normales" de funcionamiento del sistema de emergencia y seguridad. Adicionalmente, también sería pertinente planificar la comunicación operativa para tiempos de emergencias de gran magnitud y alto impacto. (Este tema se desarrolla en la Sección 9.6 de este Capítulo). Particularmente, se la tendría que vincular con la continuidad de los servicios, antes, durante y después de incidentes críticos.

En relación a la segunda dimensión, la planificación de la actividad comunicacional operativa podría subdividirse en dos componentes: un componente interno y otro externo.

La comunicación interna haría referencia al proceso comunicacional que se gesta para consumo de la propia entidad. Involucraría la identificación de audiencias internas, el desarrollo de contenidos, diseño de imágenes y elaboración de productos, y la identificación y activación de medios/canales de comunicación.

Estas acciones estarían dirigidas a:

- Apuntalar la calidad, eficiencia y eficacia de los servicios prestados.
- Fomentar un buen clima laboral y relaciones colaborativas de trabajo.
- Informar y mantener actualizado al personal sobre decisiones tomadas, adopción de nuevos estándares y cambios de políticas y protocolos, entre otros temas de interés.

La comunicación externa estaría dirigida a la población en general y a las diferentes audiencias o públicos que se hubieran identificado. Buscaría mantenerlos informados respecto a temas vinculados con la atención y respuesta a las emergencias, eventos programados, y al funcionamiento del propio Sistema, a través de campañas y otras acciones comunicacionales. Para ello es indispensable que, de acuerdo con los objetivos establecidos en el plan de comunicación, se formulen los mensajes, se elijan los canales, los tiempos y la frecuencia con la que estos serán divulgados, y se utilice un lenguaje comprensible y sencillo, evitando tecnicismos.

Respecto a los eventos programados, estos no necesariamente están vinculados a la planificación de la comunicación operativa. Estos son eventos cuya ocurrencia está prevista. Pueden tener alcance nacional, subnacional o zonal. En ocasiones requieren que el sistema de emergencia y seguridad se active anticipadamente, desde un enfoque preventivo, operativo y comunicacional. Implicaría la coordinación con las entidades de respuesta para el monitoreo de cámaras de videovigilancia y el despliegue de unidades en lugares estratégicos para la atención oportuna de posibles incidentes que pudieran derivarse del evento, entre otras acciones. Asimismo, demandaría acciones de comunicación para informar al público acerca del desarrollo del evento, utilizando para ello los canales disponibles, incluyendo: ruedas de prensa, redes sociales, mensajería instantánea, mensajes pre-grabados, entre otros medios.

9.4. Plan de comunicación

El plan de comunicación podría ser concebido como un programa detallado de la actividad comunicacional que un sistema de emergencia y seguridad llevará a cabo. Tendría que delinear de forma clara y precisa los objetivos y metas a alcanzar, las acciones comunicacionales que se diseñarán, los públicos o audiencias a los cuales esas acciones irían dirigidas, los tiempos/frecuencia de exposición, los canales/medios a utilizar, y las personas responsables de cada una de las tareas.

Adicionalmente, el plan tendría que venir acompañado de un cronograma de acción y su ejecución tendría que apoyarse en un conjunto de indicadores con los cuales se intentarían medir los resultados alcanzados.

A los efectos de poder diseñar un plan de comunicación, resultaría importante iniciar con al menos dos pasos:

- Entender cuál es la estructura de medios tradicionales y sociales, y tener claro cuál es la cobertura y penetración de los mismos, así como la frecuencia e intensidad de uso entre la población.
- Identificar y conocer cuáles son los diferentes tipos, características, necesidades y formas de comunicación de los públicos o audiencias a los cuales el plan de comunicación y sus acciones irían dirigidos.

Independiente de cuál sea el modelo de funcionamiento adoptado por el sistema de emergencia y seguridad, es importante que la comunicación en el sistema de emergencia y seguridad se maneje sobre la base de un único plan, consensuado por todos los actores articulados al Sistema, y con una clara definición de liderazgos, pautas de acción, vocerías y herramientas de seguimiento y evaluación.

El documento tendría que ser elaborado anualmente, tomando en cuenta la coyuntura por la que atraviesa el sistema de emergencia y seguridad. Adicionalmente, se podrían estipular revisiones cada mes, con una evaluación final que permita estimar o medir su efectividad, alcance e impacto.

Entre los elementos mínimos con los que tendría que contar un plan de comunicación, se podrían mencionar los siguientes:

- Diagnóstico de comunicación, incluyendo análisis del entorno y contextualización
- Objetivos de comunicación
- Segmentación de los públicos
- Estrategia creativa y mensajes claves
- Estrategia de medios de comunicación
- Diseño y elaboración de piezas y productos comunicacionales y publicitarios
- Acciones de comunicación
- La oportunidad o el momento (timing), la frecuencia y la duración
- Presupuesto
- Control y evaluación

Cada plan de comunicación incluiría una serie de acciones de comunicación que se tendrían que implementar para intentar alcanzar los objetivos de comunicación planteados, con base en la estrategia creativa y de mensajes claves, especificando los mecanismos y medios comunicativos que serán utilizados, y haciendo uso de las piezas o productos comunicacionales y publicitarios diseñados.

En términos de acciones comunicacionales, se podrían considerar los siguientes ejemplos:

- Campañas
- Agendas y giras de medios
- Eventos con participación de la comunidad y autoridades
- Visitas a escuelas o tours para recibir a escuelas
- Simulacros en la vía pública de atención y respuesta a emergencias

Con respecto a las campañas, a continuación, se presentan algunos parámetros básicos que se podrían considerar al momento de diseñarlas:

- Las campañas tendrían que ser informativas.
- El lenguaje tendría que ser sencillo y claro.
- Tendrían que estar basadas en los temas o problemas que hubieran sido detectados a partir del análisis de la información que el propio sistema de emergencia y seguridad hubiera generado (ver Capítulo VII de esta Guía).

Si el plan incluye acciones con los medios tradicionales, se recomendaría realizar acercamientos con los principales medios y mantener los contactos y las relaciones con estos al día.

La elaboración del plan comunicacional tendría que estar a cargo del área funcional correspondiente y luego validado y aprobado por la máxima autoridad del sistema de emergencia y seguridad para su implementación.

A continuación, a modo de ejemplo, se comparte una propuesta de estructura y contenidos mínimos de un plan de comunicación:

Tabla 29: Ejemplo de plantilla para el desarrollo de un Plan de Comunicación

PRESENTACIÓN INSTITUCIONAL	
Nombre:	[Del sistema de emergencia y seguridad que corresponda]
Misión:	Gestionar la atención de las situaciones de emergencia de la población, reportadas a través de un número único (si lo hubiera) y las que se generen por video vigilancia, monitoreo de alarmas o algún otro medio, mediante el despacho de recursos de respuesta especializados, pertenecientes a organismos públicos y privados articulados al Sistema, con la finalidad de contribuir, de manera permanente, a la consecución y mantenimiento de la seguridad.
Visión:	Ser una institución líder y modelo en la coordinación de servicios de emergencia y seguridad, utilizando tecnología de punta en sistemas y telecomunicaciones, comprometidos con la calidad, seguridad, salud en el trabajo y el medio ambiente, que permitan brindar un servicio de alto nivel a la población, de manera continua y sostenida.
Eje sectorial:	Seguridad
CANALES INTERNOS Y EXTERNOS	
Canal	**Descripción**
Facebook:	El uso de fotografías y videos podrían ser productos comunicacionales con posibilidad de generar mayor atracción, interés, actividad e interacción dentro de la cuenta y entre los/as seguidores/as.
Twitter:	Brinda la posibilidad de publicar mensajes sencillos, cortos y de manera oportuna. Otra característica valiosa de esta red social es la inmediatez con la que se publican los mensajes. Todas las características mencionadas anteriormente, lo convierten en una posible fuente de información para medios de comunicación tradicionales. La utilización de etiquetas *hashtag* permitiría agrupar contenidos de acuerdo a eventos o situaciones específicas, facilitando su búsqueda y en casos de noticias o acontecimientos importantes, posicionar mensajes y tendencias.

YouTube:	Tener una cuenta oficial donde alojar y organizar los videos producidos por la institución, de acuerdo a su contenido. Esto facilitaría la navegación y la búsqueda de información por parte de la población y públicos específicos. Los videos podrían ser tipo documentales, programas sobre casos exitosos, resúmenes de noticias, entrevistas, entre otros géneros, producidos por la propia institución o con apoyo de una agencia externa. Los videos podrían utilizarse para complementar la información que se le quiere brindar al público. Adicionalmente, en otras redes sociales, se podrían colocar enlaces a los videos. Esto resulta útil, particularmente, cuando las redes sociales tienen un límite máximo de capacidad y caracteres.
Instagram:	El contenido en Instagram tendría que ser visual. Fotografías o videos con calidad y capacidad autoexplicativa, y lo suficientemente interesantes/llamativos para generar interacciones. Se podrían utilizar descripciones cortas, complementadas con un *hashtag*, para brindar una idea del contenido que se está compartiendo.
Página web:	Permite brindar información de manera detallada, con datos oficiales, de las entidades que participan en la coordinación de una emergencia. El contenido escrito podría complementarse con fotos y videos. Podría utilizarse para publicar y poner a disposición del público, información de carácter administrativo y operativo que den cuenta y contribuyan a transparentar la gestión y el funcionamiento de un sistema de emergencia y seguridad.
Pantallas en áreas de servicio:	Especificar cantidad y lugares donde están posicionadas (centros comerciales, salas de espera o de atención de entidades públicas, estaciones de buses o trenes, entre otras posibles ubicaciones estratégicas).
Medios o programas de comunicación propios:	Radio o programa de radio en FM o digital. Canal o programa de televisión de señal abierta (público, privado o comunitario). Periódico o contribución (semanal o mensual) a través de una columna/artículo de opinión. Revista o contribución a través de una columna/artículo, de acuerdo a la periodicidad de publicación del medio o con base en una frecuencia preestablecida.

PLAN DE COMUNICACIÓN

JUSTIFICACIÓN (Tendría que responder a la pregunta: ¿Por qué es relevante contar con un plan de comunicación?)

Para dar a conocer y posicionar los servicios del sistema de emergencia y seguridad entre la población, las formas de contacto para acceder a los servicios, y la necesidad de hacer un uso responsable de los mismos.

Ante la posibilidad de enfrentar situaciones de emergencia de baja y alta envergadura, sería necesario preparar a la población y a grupos en situación de vulnerabilidad para que sepan qué hacer y cómo responder ante esas situaciones.

También sería necesario para generar una comunicación consistente, continua y confiable, independientemente de cuál sea el modelo de funcionamiento adoptado. Un plan de comunicación se torna aún más relevante en situaciones de crisis para contener la ansiedad, incertidumbre y confusión entre la

población, y contrarrestar la desinformación (información falsa), la información errónea y la información maliciosa.	
OBJETIVOS (En esta parte se tendría que describir qué se quiere alcanzar con un plan de comunicación. La pregunta que se tendría que responder sería: ¿para qué?)	
Objetivo general:	Posicionar imagen positiva y de confianza del sistema de emergencia y seguridad entre la población.
Objetivos específicos:	• Atraer positivamente la atención de aliados estratégicos nacionales e internacionales. • Reforzar la relación con los medios de comunicación e incrementar la presencia institucional en los medios. • Crear sentido de pertenencia en los funcionarios de la institución. • Consolidar al sistema de emergencia y seguridad como centro de referencia en el marco de incidentes de alto impacto. • Transparentar la gestión y el funcionamiento del sistema de emergencia y seguridad.
Acciones de Comunicación:	• Campañas en redes sociales. • Intervenciones en medios tradicionales. • Visitas a escuelas. • *Tours* guiados para escuelas. • Simulacros en la vía pública de atención y respuesta a emergencias.
Fuente: Servicio Integrado de Seguridad ECU-911, 2020.	

9.5. Manejo de la comunicación

Un sistema de emergencia y seguridad enfrenta diferentes tipos de emergencias. Estas no tienen horarios ni días específicos, excepto por los incidentes programados. La mayoría de las emergencias son inesperadas y sorpresivas, es por eso que la planificación y las acciones de comunicación tendrían que poder adaptarse a esta naturaleza propia de las emergencias, buscando brindar a la población información útil para preservar la vida y la seguridad, en todo momento. La comunicación de y para emergencias, tendría que practicarse como un proceso dinámico y ajustable a las características de los eventos que se presenten.

En una situación de emergencia, la posibilidad de brindar información útil, actualizada, veraz y de manera continua, dependerá de la planificación y la preparación comunicacional que haya desarrollado, previamente, el sistema de emergencia y seguridad.

En función de la naturaleza y dinámicas de las emergencias, la comunicación relativa a estas tendría que realizarse casi en tiempo real. Este es uno de los principales motivos por los que la comunicación tendría que estar basada en seis premisas básicas:

- Que sea clara
- Que sea sencilla
- Que sea concreta
- Que sea concisa
- Que sea constante

- Que sea oportuna

A partir del plan de comunicación, su implementación y el manejo diario de la comunicación, tendrían que recaer en un área funcional específicamente dedicada al tema. El área tendría que estar integrada por un equipo de funcionarios/as con una formación especializada, ciertas competencias predefinidas y una serie de actitudes necesarias para poder desempeñarse en los puestos relacionados al tema.

La comunicación en situaciones de emergencia podría manejarse a través de diferentes canales y herramientas:

9.5.1. Vocería

Debido a las características y dinámicas de un servicio de emergencia y seguridad, sería propicio contar con uno o varios voceros.

Los/as voceros/as podrían ser entendidos como personas específicamente designadas para cumplir con la función de comunicar; representan la voz y la imagen oficial de la entidad.

Resultaría pertinente definir claramente las funciones de los/as voceros/as, así como también las competencias y actitudes que se buscarían para ese perfil de cargo. Ese sentido, mínimamente tendrían que:

- Conocer el funcionamiento del sistema de emergencia y seguridad.
- Estar informados/as acerca de la situación y evolución respecto a la atención de emergencias.
- Expresarse de forma sencilla y clara.

Quienes atienden, articulan y dan respuesta a las emergencias tendrían que estar siempre en contacto con los/as voceros/as y el equipo de comunicación. La integración y la complementariedad de su trabajo podría marcar una diferencia en el desempeño y la imagen del sistema de emergencia y seguridad. El papel de la vocería cobra especial importancia en situaciones de emergencias de gran magnitud y alto impacto.

De ser posible, y en función de los cambios del ecosistema comunicacional y de las propias emergencias, tendría sentido considerar incluir en el programa de capacitación continua de la entidad (ver Capítulo VI sobre la Gestión de Talento Humano), un curso o taller de especialización/actualización en vocería, particularmente ligada al sector de emergencias.

9.5.2. Redes

A continuación se presentan dos tipos de redes (externa e interna), que podrían ser aprovechadas por el sistema de emergencia y seguridad como parte de sus planes y acciones de comunicación. Las redes tendrían como ventaja:

- La ampliación de la visibilidad y del alcance de las acciones y mensajes,
- La actualización frecuente de contenidos sin mayores costos, y
- La facilidad de comunicar información de forma inmediata, directa y a un gran número de personas de manera simultánea, por mencionar solo alguna de ellas.

9.5.2.1. Plataforma web (externa)

El sitio web tendría que considerarse como la "carta" de presentación del sistema de emergencia y seguridad en el plano digital. Es allí donde los/as internautas podrían encontrar, mínimamente, los siguientes elementos informativos, desde el punto de vista comunicacional del Sistema:

- Información institucional, incluyendo visión, misión, objetivos, año de creación, equipo de trabajo, modelo de gestión y de funcionamiento adoptados
- Presentación y descripción sobre los servicios que presta
- Formas de contacto para emergencias y consecuencias por el mal uso del Sistema
- Acciones de comunicación y boletines de prensa
- Eventos realizados y los que están por venir
- Datos abiertos, datos y boletines estadísticos e informes
- Información institucional de contacto y de cuentas en redes sociales

Varios de estos elementos informativos también podrían ser utilizados en medios tradicionales y sociales de comunicación.

El diseño y mantenimiento del sitio web tendría que responder a algunos criterios básicos, incluyendo:

- Esquema de página web sencillo y de fácil navegación.
- Información confiable y de calidad, actualizada de manera constante, presentada de manera clara y ordenada.
- Uso de imágenes y videos de alta resolución para ilustrar y complementar la información escrita.
- Enfoque inclusivo, desde el punto de vista tecnológico (tipo de conexión, velocidad o ancho de banda, navegador y sistema operativo, entre otros) y desde el punto de vista de las discapacidades de los/as internautas.
- Compatibilidad para su visualización y navegación desde dispositivos móviles.
- Recaudos de protección y seguridad en línea con las políticas y protocolos establecidos por el sistema de emergencia y seguridad (ver Capítulo VIII de esta Guía sobre Gestión de la Seguridad).

9.5.2.2. Intranet (interna)

La intranet es uno de los mecanismos o canales de comunicación e información dirigido al personal administrativo y operativo de un sistema de emergencia y seguridad. En este espacio digital interno, el personal podría encontrar información actualizada, relacionada con el desempeño de la entidad, noticias y novedades, eventos y actividades, así como herramientas administrativas y operativas que pudieran facilitar la gestión y el funcionamiento del Sistema (incluyendo: políticas y protocolos vigentes, nuevos o actualizados; formularios; explicación de cómo llevar a cabo determinadas tareas o trámites internos, entre otros).

Entre los lineamientos que se podrían proponer para la estructura y contenidos de una intranet para un sistema de emergencia y seguridad destacarían los siguientes:

- Permitir diferentes contenidos y niveles de acceso de acuerdo con las distintas funciones y cargos del personal.
- Facilitar los dos principales tipos de servicios o aplicaciones de internet:
    - Los que permiten la comunicación, incluyendo: buzón de sugerencias; mensajería instantánea; llamadas de audio y video; noticias internacionales, nacionales, locales e institucionales; grupos de discusión internos; y reproductor de imágenes y sonido en tiempo real.
    - Los que permiten buscar y organizar información: archivos o ficheros compartidos; directorios con información de contacto; acceso y consulta a bases de datos internas y externas y buscador.

9.5.3. Medios de comunicación

Los medios de comunicación son canales para llegar al público general. Transmiten mensajes que se difunden a un gran número de receptores de manera simultánea, a través de diferentes técnicas y tecnologías. Cada uno presenta características específicas en relación a: tipo de audiencia, cobertura, formas publicitarias, ventajas y costos, entre otras.

9.5.3.1. Medios tradicionales

La relación con los medios de comunicación tradicionales implicaría vincularse institucionalmente con editores, periodistas, entrevistadores y reporteros. Esta relación tendría que concebirse como una alianza estratégica, por cuanto permite que las acciones y el desempeño del sistema de emergencia y seguridad se evidencie de forma masiva y llegue a distintos tipos de audiencias de manera simultánea, de acuerdo con los objetivos comunicacionales planteados. Estos objetivos podrían estar asociados con la comunicación externa en el plano operativo, así como también con la comunicación organizacional, dirigida a trabajar sobre la percepción pública respecto al valor de los servicios, la confianza, la transparencia y la rendición de cuentas del sistema de emergencia y seguridad,.

Los mensajes tendrían que estar orientados a informar y concientizar al público. El enfoque comunicacional podría ser preventivo, educativo o vinculante.

9.5.3.2. Medios Sociales

Las redes sociales tendrían que considerarse como un canal de comunicación directo con la población. Existen en la actualidad varias redes sociales, incluyendo Twitter, Facebook, Instagram, entre otras.

A través de las redes sociales sería especialmente importante compartir información de utilidad para la población como el estatus de vías, accidentes, evolución/estado de eventos relevantes (fichas informativas e imágenes), entre otras.

De igual manera también se podrían aprovechar para difundir campañas diseñadas para brindar información, recomendaciones, recordatorios sobre fechas o eventos destacados, crear conciencia sobre determinados riesgos o el uso adecuado del Sistema, entre otras acciones, y hacerlo de forma oportuna y a bajo costo.

Para alimentar las cuentas de redes sociales, mantenerlas activas y relevantes, resultaría preferible elegir la información más "atractiva" o de interés para la población. Generalmente el contenido audiovisual tiene mayor impacto y tiende a generar más interacciones.

A diferencia de los medios tradicionales de comunicación, las redes sociales habilitan una comunicación horizontal y de doble (e inclusive, en algunos casos, de múltiples) vías. A través de las redes sociales, el público también podría expresar su conformidad o inconformidad con el servicio.

A continuación, se presentan algunos lineamientos generales a tener en cuenta para el manejo de las cuentas en redes sociales por parte de un sistema de emergencia y seguridad:

- No participar en discusiones con cualquier persona.
- Todo mensaje a nombre de la institución tendría que contar con la autorización de la persona encargada de la comunicación de la entidad.
- Evitar sincronizar las cuentas oficiales de la institución con alguna aplicación, cuenta de Twitter personal, o cualquier juego o programa que pudiera publicar contenido automáticamente.
- Evitar publicar opiniones personales a nombre de la institución.
- Publicar fotos y videos con prudencia, precaución y respeto.

9.5.4. Vinculación con la población y la comunidad

En la vinculación con el entorno, un sistema de atención y respuesta a emergencias tendría que considerar un componente de relacionamiento con el público y las comunidades, y otro componente de monitoreo y alerta temprana.

El componente de relacionamiento con el público y las comunidades tendría como propósito activar y consolidar su involucramiento e interacción con el sistema de emergencia y seguridad. Los mensajes, eventos y demás acciones comunicacionales que se lleven cabo como parte de este componente, tendrían que reflejar y abordar preocupaciones, opiniones, problemas y riesgos específicos de la población y las comunidades a los cuales irían dirigidos. De esta manera, se estaría brindando información útil y focalizada para que puedan tomar mejores decisiones al momento de enfrentar situaciones de emergencias.

Adicionalmente, esa vinculación también podría tener como propósito movilizar a la comunidad para introducir cambios positivos de comportamiento y hábitos, conducentes a preservar la salud, el bienestar y la vida de las personas.

Los objetivos de la vinculación con la población y la comunidad, podrían plantearse en el corto, mediano y largo plazo. A modo de ejemplo, en el corto plazo, la vinculación con la población y con las comunidades podría estar dirigida a:

- Concientizar a las personas respecto al buen uso del servicio, particularmente a los niños/as, adolescentes y jóvenes quienes, a mediano y largo plazo, se convertirán en potenciales usuarios del sistema.
- Capacitar respecto a cómo actuar y qué hacer frente a diferentes tipos de emergencias.
- Instruir respecto a cómo prepararse y actuar frente a incidentes de alto impacto.

En el mediano y largo plazo, los objetivos de la vinculación con la población y la comunidad podrían plantearse en términos de fortalecer la imagen y la legitimidad social del sistema de emergencia y seguridad.

La vinculación con la población y con las comunidades tendría que estar sustentada en al menos cuatro premisas:

- Respeto en el trato que se le da a los/as usuarios y a la población en general.
- Empatía y sensibilidad respecto a las situaciones y problemas que las personas, a nivel individual o colectivamente, pudieran estar enfrentando.
- Cercanía y constancia en el vínculo con las personas y las comunidades.
- Profesionalismo en el servicio que se le brinda a la población, demostrando preparación, coordinación, eficiencia y eficacia.

Estas premisas contribuirían a generar confianza y relación de pertenencia con el sistema de emergencia y seguridad, en línea con el objetivo de mediano y largo de plazo mencionado anteriormente.

La vinculación puede ser presencial, mediante la implementación de programas y proyectos de acuerdo con las condiciones y necesidades de cada comunidad; así como también virtual, facilitada por el uso y la expansión de las redes sociales.

A su vez, la interacción constante con la población y la comunidad estaría ligada al componente de monitoreo y alerta temprana. Este segundo componente podría concebirse como un proceso de escucha de doble vía, que incluye el análisis, seguimiento y recopilación de información por parte del sistema de emergencia y seguridad respecto a la población y las comunidades sobre:

- Necesidades, problemas y desafíos que enfrentan en materia de atención y respuesta a emergencias. Esta información serviría como insumo para plantear soluciones asertivas y oportunas.
- Rumores e información falsa en torno a potenciales riesgos y peligros que pudieran afectar negativamente la labor del sistema de emergencia y seguridad. Estas situaciones podrían contenerse y contrarrestarse con campañas de información basadas en datos, hechos y evidencia.
- El nivel de conocimiento y de satisfacción, y el tipo de opinión y percepción que la población y las comunidades tienen respecto al sistema de emergencia y seguridad. Esta información podría servir de insumo para orientar la introducción de cambios y mejoras en la lógica del enfoque de gestión de calidad integral (presentado en el Capítulo IV de esta Guía).

9.5.5. Mensajes pregrabados

Además de los canales y herramientas ya presentados, los mensajes pregrabados podrían ser una opción eficiente para comunicar e informar a la población acerca de situaciones de emergencia en curso y eventos programados. Estos tendrían que estar configurados de acuerdo a la capacidad tecnológica de cada Sistema, y ajustarse al marco normativo que cada Estado hubiera establecido en el ámbito de las telecomunicaciones.

9.6. La planificación y gestión de la comunicación en emergencias de gran magnitud

Las situaciones de emergencia de gran escala son escenarios de alta sensibilidad técnica, política y social, donde la operación de un sistema de emergencia y seguridad tendría que estar acompañada de un plan de comunicación de crisis, que incluya a las entidades articuladas (o de primera respuesta) y vinculadas, y que esté dirigido a la población en general y a las audiencias o públicos específicos identificados.

En situaciones de emergencia de alta envergadura, la información es un recurso sumamente valioso para la toma de decisiones. Comunicar la información disponible resulta clave para movilizar recursos nacionales e internacionales y permite brindar una respuesta oportuna y adecuada a la población.

La comunicación de crisis es un componente estratégico de la planificación de las actividades de comunicación y, asimismo, un componente de la gestión del riesgo. Así como la mayoría de los incidentes de magnitud y los riesgos pueden ser objeto de un análisis y se podrían anticipar, la gestión de la comunicación tendría que considerar la planificación y la preparación ante eventos de magnitud.

La planificación y preparación de la comunicación de crisis tendría que cristalizarse en un plan de comunicación. Este plan podría formar parte del plan integral o maestro de comunicación, o podría elaborarse como un plan aparte pero vinculado al primero. En ambos casos, permitiría gestionar y guiar las acciones de comunicación en circunstancias excepcionales. Esta tarea comunicacional de crisis tendría que apuntalar la respuesta a la emergencia de gran escala. Adicionalmente, tendría que estar en línea con la matriz de riesgo, el plan para la continuidad de operaciones y el plan de recuperación frente a desastres (ver Capítulo VIII de esta Guía).

El plan tendría que contener, mínimamente los siguientes elementos:

- Los pasos necesarios para elaborar comunicados en crisis
- Estrategias de comunicaciones y mensajes
- Evaluación del plan, luego de haber superado la crisis

La planificación de la comunicación de crisis permitiría a las autoridades del sistema de emergencia y seguridad contar con lineamientos, procesos y procedimientos establecidos para comunicar de manera efectiva a la población en general y a públicos específicos, sobre la naturaleza, estado y evolución del riesgo. En ese sentido el diseño de acciones comunicacionales focalizadas y segmentadas, haciendo uso de diferentes canales de comunicación disponibles y de acuerdo a las necesidades de los públicos identificados, podrían contribuir a la asertividad y a la receptividad del mensaje.

Un instrumento oportuno para situaciones de gran afectación, a nivel nacional, subnacional o zonal, es la difusión de alertas de emergencia. Este tipo de alertas son mensajes de difusión masiva, instantánea y rápida, que precisan del apoyo del sector de telecomunicaciones para garantizar la disponibilidad simultánea de los diferentes canales de comunicación. Los mensajes de alerta tendrían que variar según el tipo de incidente predefinido. La previsión de esto permitiría elaborar, de manera anticipada, plantillas de mensajes para su eventual uso.

Adicionalmente, en el marco de este tipo de situaciones de alta envergadura e impacto, es altamente probable que se activen no solo las entidades articuladas sino las vinculadas también. Debido al mayor número de entidades, la coordinación en la respuesta y en la comunicación se tornan aún más cruciales. La homologación de los mensajes para difundir a la población y la necesidad de que todas las entidades involucradas en la respuesta a la emergencia manejen la misma información, adquieren una mayor relevancia y tornan aún más necesario contar con un único plan de comunicación de crisis.

Todas las entidades tendrían que alinearse a las acciones de comunicación previstas en el plan de comunicación de crisis, evitando mensajes contradictorios o una competencia mediática y comunicacional. De esta manera se torna posible mantener mensajes consistentes y un flujo constante y continuo de información actualizada, válida y creíble.

Adicionalmente, la planificación de la comunicación en crisis, también tendría que considerar el plano operativo de la respuesta. En ese sentido, tendría que establecer un conjunto de lineamientos, procesos y procedimientos que faciliten la comunicación para la interacción, el intercambio de información y la coordinación en distintos niveles, entre: autoridades, entidades articuladas y vinculadas, equipos de emergencias y públicos interesados (científicos, académicos, profesionales de salud pública y comunicadores, entre otros).

En lo que respecta a la gestión de la comunicación en crisis se podrían considerar los siguientes lineamientos:

- Constituir un centro o nodo centralizado de comunicaciones, a cargo de manejar todas las solicitudes de información y preparar los comunicados para los medios de prensa, medios sociales, otras instituciones, el público en general y públicos específicos.
- Definir cadena de autorización para la comunicación y divulgación de la información.
- Establecer un calendario de comunicaciones.
- Elaborar plantillas o guiones pre-armados de mensajes.

Estas últimas podrían diseñarse basándose en los siguientes tres componentes:

- Públicos o audiencias a los/as que van dirigidos
- Mensaje principal
- Instrucciones para más información

El Sistema de Comando de Incidentes (SCI), específicamente el capítulo de comunicación, podría ofrecer lineamientos y pautas a seguir para la comunicación en emergencias. Adicionalmente, otras fuentes de referencias podrían ser: la "Guía para la planificación de comunicaciones en crisis" y las "Recomendaciones para comunicarse con las partes interesadas durante una crisis", ambas elaboradas por *Mission Critical Partners* (2020).

9.7. Desafíos comunicacionales

La comunicación en la gestión de emergencias y seguridad puede cambiar todos los días y a todas horas debido a la naturaleza misma de los incidentes. Además de este desafío, la comunicación de y para emergencias enfrenta al menos tres desafíos adicionales.

i. Desafío 1: Grupos en situación de vulnerabilidad

Las medidas de atención y respuesta a emergencias tendrían que tener en cuenta las necesidades específicas de las personas en situación de vulnerabilidad, marginalidad o con algún tipo de discapacidad. La falta de consideración de las dificultades de interacción con los medios y dispositivos de comunicación, y la distancia social, física y cultural de estos grupos, emergen como obstáculos reales al momento de brindar protección, atención y respuesta ante emergencias.

Frente a este desafío, en la planificación de las acciones comunicacionales, un sistema de emergencia y seguridad podría considerar los siguientes elementos:

- Identificar cuáles son los grupos en situación de vulnerabilidad (incluyendo: personas analfabetas, en situación de marginalidad, pertenecientes a etnias con costumbres y lenguajes distintos al dominante u oficial y personas con alguna discapacidad física o mental, entre otros). Entender cuáles son sus características sociodemográficas, su ubicación geográfica (si fuera aplicable) y sus necesidades en relación a aspectos comunicacionales en situaciones de emergencias de baja y alta intensidad.
- Analizar ventajas y oportunidades en el empleo de diferentes medios de comunicación.
- Diseñar acciones de comunicación y mensajes orientados a cada una de las audiencias especiales identificadas, para reducir la vulnerabilidad de dichas personas y aumentar la eficacia de los esfuerzos de atención y respuesta a emergencias.

ii. Desafío 2: Desinformación

- Información falsa, errónea o engañosa (misinformation)
- Información incompleta, inexacta o tergiversada/manipulada (disinformation)
- Aseveraciones que dejan de basarse en hechos y datos objetivos, información factual y la evidencia y, en cambio, apelan a las emociones, creencias o deseos del público ("postverdad")

En un contexto de postverdad, en donde fluye la información falsa y manipulada, aumentan las posibilidad de que se produzcan "desórdenes informativos" que, a su vez, podrían generar desesperación y zozobra social. Frente a este escenario, un sistema de emergencia y seguridad podría considerar los siguientes lineamientos para la gestión de la comunicación:

- Evitar la improvisación o la verdad contada a medias.
- Evitar que las imágenes en una atención de emergencias caigan en espectáculo con el afán de llamar la atención.
- Establecer mecanismos de verificación de datos sobre una emergencia, antes de entregarlos a los medios.
- Contar con directrices de comunicación e información para la difusión.
- Cuidar la forma de comunicar, respetar ante todo la dignidad humana de las víctimas.

iii. Desafío 3: Mayor incidencia de desastres o catástrofes de alto impacto

Ante el aumento en la frecuencia y la intensidad de desastres de alto impacto provocados, por ejemplo, por el cambio climático y de origen antrópico, es cada vez más probable que los sistemas de emergencia y seguridad tengan que enfrentarse con mayor asiduidad a este tipo de situaciones. Frente a ese escenario, se presentan algunos lineamientos para la planificación y gestión de la comunicación:

- Fortalecer la planificación y la revisión de planes de comunicación asociados a la preparación.
- Establecer mecanismos de cooperación, intercambio de lecciones aprendidas, buenas prácticas y entrenamiento en conjunto con otras entidades sobre cómo actuar frente a este tipo de eventos.
- Adoptar herramientas para la emisión de alertas de emergencia[9] (cuando esto fuera posible), el seguimiento de las comunicaciones, y la evaluación de los planes y las acciones de comunicación.

[9] Ver Protocolo de Alerta Común.

CAPÍTULO X. TRANSPARENCIA Y RENDICIÓN DE CUENTAS

Introducción

La transparencia y la rendición de cuentas podrían ser consideradas, simultáneamente, como valores y principios a sostener, objetivos a alcanzar y procesos a seguir. En todo caso, los tres enfoques son sustantivos en y para la gobernanza democrática y las políticas asociadas a la gestión pública, incluyendo en el ámbito de la seguridad y, la atención y respuesta a emergencias.

Este tipo de servicio, al ser brindado por el Estado y al estar enfocado en la protección y salvaguardia de la vida humana, requeriría facilitar la responsabilización por la gestión y los resultados obtenidos, poniendo a disposición de las instituciones públicas, los medios de comunicación, sectores académicos y privados, la sociedad civil y la población, una serie de datos e información para el legítimo ejercicio del control horizontal y vertical. Hacerlo no sólo colocaría al sistema de emergencia y seguridad en línea con las leyes de cada país, sus normas y políticas internas sino que también contribuiría a aumentar su nivel de aprobación, confianza y legitimidad entre la población.

Por la naturaleza de los contenidos y el fin que persigue, la transparencia y la rendición de cuentas tendrían que ser parte del diseño del Sistema y de la planificación estratégica orientada a su fortalecimiento. Esto implicaría la creación de protocolos, procesos y mecanismos para brindar, de manera proactiva, información sobre el funcionamiento y la gestión del Sistema, así como facilitar el acceso a la información que contribuya a la veeduría, la generación de conocimiento, la creación de valor público y la innovación.

En este Capítulo se abordan la transparencia y la rendición de cuentas desde la necesidad de su planificación, vinculándola, particularmente, con la planificación estratégica (Capítulo II de esta Guía) y la planificación de la comunicación organizacional (Capítulo IX de esta Guía). Luego describe un conjunto de mecanismos y herramientas concretos para el ejercicio de la transparencia y la rendición de cuentas, incluyendo: consultas y solicitudes de información pública, datos cuantitativos, indicadores y datos abiertos, sistema de reportería, compras y contrataciones públicas de bienes y servicios, auditorías internas/externas y el plan de comunicación de la entidad.

El plan de comunicación (cubierto en el Capítulo IX de esta Guía), se presenta como una herramienta clave para incorporar objetivos, metas, resultados y acciones comunicacionales relativos a la transparencia y la rendición de cuentas, aprovechando información disponible a través de los anteriores mecanismos mencionados.

Finalmente, el Capítulo se refiere a dos instrumentos adicionales: el Código de Ética y al Código de Conducta (introducidos en el Capítulo VI de esta Guía). Estos, acompañados de sesiones de inducción y capacitación, así como de un esquema de incentivos y sanciones en razón de su cumplimiento o incumplimiento, buscarían inculcar e infundir la transparencia y la rendición de cuentas como valores y principios rectores del accionar del sistema de emergencia y seguridad así como de su personal.

10.1. Planificación para la transparencia y la rendición de cuentas

La planificación para garantizar altos niveles de transparencia y la rendición de cuentas por parte de un sistema de emergencia y seguridad, podría comenzar con una justificación. De esta manera se podrían explicitar las razones por las cuales un sistema de emergencia y seguridad procuraría una actuación transparente y la rendición de cuentas sobre las actividades realizadas ante las demás entidades públicas, públicos específicos y la población.

A modo de ejemplo, estas razones podrían estar ligadas a:

- Garantizar la eficacia y eficiencia del Sistema, contribuyendo a la gobernanza,

- Respetar el derecho al acceso de información pública de las personas, y
- La necesidad de velar por la integridad del funcionamiento y de la gestión del Sistema, y evitar y enfrentar la corrupción.

Un proceso de planificación también permitiría definir los objetivos que se procurarían alcanzar, por ejemplo:

- Conseguir un alto nivel de confianza y credibilidad por parte de la población.
- Convertirse en una referencia o fuente nacional (e internacional) de información confiable y actualizada.

Así mismo, permitiría pensar y establecer de manera sistematizada las metas e indicadores de desempeño que se podrían acordar para medir avances y logros en la consecución de los objetivos establecidos en materia de transparencia y rendición de cuentas. Esto a su vez podría servir para la comunicación, demostración y publicación de resultados, y la responsabilización por las metas y logros alcanzados, así como por los no alcanzados.

La planificación podría resultar en un plan que, para su implementación, precisaría de una serie de procesos, procedimientos y mecanismos. El plan tendría que estar alineado con las leyes nacionales de transparencia y de acceso a la información pública, los planes de gobierno abierto vigentes en cada país, y los otros planes (estratégico y operativo) elaborados por el sistema de emergencia y seguridad.

En función de los objetivos y de las metas establecidas, un Sistema podría considerar la aplicación de una serie de mecanismos internos y externos para cumplir con ellos, incluyendo:

- Consultas y solicitudes de información pública
- Datos cuantitativos, indicadores y datos abiertos
- Reportería (informes)
- Publicación de procesos de compras y contrataciones públicas
- Auditorías internas/externas
- Plan de comunicación

10.2. Consultas y solicitudes de información pública

Un sistema de emergencia y seguridad tendría que contar con procesos y mecanismos estipulados para la recepción de consultas y pedidos de información por parte de la población y de públicos específicos, en línea con el marco legal vigente en el país.

Algunas consideraciones a tener en cuenta para estandarizar y facilitar los procesos de consultas y pedidos de información:

- Habilitar varios canales o medios, incluyendo: vía telefónica, por correo electrónico, presencial o a través del sitio web del sistema de emergencia y seguridad. Resultaría importante diferenciar claramente estos canales de aquellos utilizados para reportar emergencias.
- Diseñar un formulario físico y digital para que el público pueda realizar sus consultas o solicitar la información que precisa.

- Definir un procedimiento interno para el tratamiento de esa consulta o pedido de información, incluyendo:
    - Clasificar el tipo de información que se puede compartir y divulgar.
    - Formato con el que será presentada la información solicitada.
    - Plazos para dar respuesta a la consulta o al pedido de información realizado.
    - Autorizaciones necesarias para entregar la información solicitada.
    - Guión para la atención de este tipo de llamadas.
    - Plantillas de correo pre-armadas para responder automáticamente a este tipo de pedidos o solicitudes.
    - Certificación física y digital dejando constancia de que se atendió la consulta y se entregó la información solicitada. En caso de no entregarla, se sugeriría brindar una explicación conforme a la legislación del país o al marco normativo de la entidad.
- Funcionarios/as del sistema de emergencia y seguridad específicamente entrenados y dedicados a cumplir con este tipo de tareas.

Dado que un sistema de emergencia y seguridad maneja datos personales resultaría importante encontrar un equilibrio entre la transparencia y la rendición de cuentas, y la privacidad y confidencialidad de la información identificable de los/as usuarios/as. Así mismo, sería importante que la información que genera y gestiona un sistema de emergencia y seguridad también esté sujeta a una tipología y proceso de clasificación (al respecto, ver Capítulo III y VII de esta Guía).

La tipología de clasificación de la información tendría que estar en línea con los parámetros establecidos en las leyes de cada país, considerando también cuestiones de seguridad interna como la no divulgación de datos que pudieran generar algún tipo de riesgo, incluyendo: comprometer la operación del sistema de emergencia y seguridad, generar vulnerabilidades a los sistemas informáticos y de las comunicaciones de la entidad, y comprometer la integridad física de los/as funcionarios/as, entre otros aspectos.

Adicionalmente, en línea con las políticas y protocolos establecidos por la entidad en materia de seguridad de la información, la comunicación y los sistemas informáticos, los datos personales también tendrían que estar protegidos para evitar su mal uso, filtraciones y fugas de información. (Sobre este tema, remitirse al Capítulo VIII de esta Guía).

10.3. Datos cuantitativos, indicadores y datos abiertos

Es fundamental que los servicios públicos, incluyendo un sistema de emergencia y seguridad, pongan a disposición de los/as interesados/as información para la valoración del funcionamiento del Sistema, de los servicios prestados y de los resultados alcanzados.

Es por ello que, en un primer momento, un sistema de emergencia y seguridad podría poner a disposición del público dos grandes tipos de datos e indicadores, ya procesados o con algún grado de intervención:

- Datos cuantitativos e indicadores sobre el uso de los fondos públicos: nóminas, presupuesto, balance general, entre otros temas.
- Datos cuantitativos e indicadores sobre el funcionamiento y los servicios brindados: casos atendidos, número de personas atendidas (desagregadas por sexo y edad), tipo de eventos atendidos, zonas de atención, entre otras variables.

En un segundo momento, se tendría que tomar en cuenta un enfoque más reciente, que pone particular interés en los datos abiertos, es decir, en datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que fueron publicados digitalmente.

El sistema de emergencia y seguridad tendría que publicar regularmente datos abiertos para facilitar y promover su uso, reuso y distribución por parte del público general y audiencias específicas, sin imponer restricciones con base en los derechos de autor o de reproducción.

Para el caso de datos abiertos, resultaría importante definir, por ejemplo:

- El origen, cómo y dónde se obtuvieron
- La frecuencia de publicación de los datos actualizados y exhaustivos
- El formato, incluyendo para que sean legibles por máquina, interoperables y comparables
- La forma en que se tendría que citar la fuente
- El lugar dentro del sitio Web del sistema de emergencia y seguridad donde podrían publicarse

Además de propiciar la transparencia y la rendición de cuentas, los datos abiertos fomentarían la participación pública y la generación de conocimiento a partir del procesamiento y análisis de los datos que se ponen a disposición del público. Adicionalmente, podrían contribuir a la gobernanza y a la confianza en el sistema de emergencia y seguridad. Aún más, podrían ser fuentes para la innovación frente a problemas y desafíos comunes que precisan de soluciones informadas.

10.4. Sistema de reportería

En función de la arquitectura de información con la cual haya sido diseñado el sistema de emergencia y seguridad, los sistemas informáticos que den soporte a su funcionamiento y las bases de datos que hayan sido creadas (ver Capítulo III de esta Guía), se podría contar con una serie de informes útiles para la rendición de cuentas.

Entre ellos se podrían mencionar los siguientes:

- **Informes de gestión.** Darían cuenta del funcionamiento administrativo del Sistema, el uso de los recursos económicos, el cumplimiento de la planificación estratégica y operativa, y los resultados alcanzados. Estos podrían elaborarse con una frecuencia semestral y/o anual.
- **Informes de servicio.** Brindarían información sobre la atención y respuesta a emergencias. Podrían elaborarse mensual, trimestral o cuatrimestral, semestral y/o anualmente.
- **Informes financieros**, basados en los presupuestos de ingresos y gastos. Ofrecerían un balance de la ejecución y grado de cumplimiento. Podrían elaborarse con una frecuencia trimestral o cuatrimestral, semestral y/o anual.
- **Informes de proyectos**. Presentarían el nivel de avance de los proyectos activos, fechas estimadas de cierre, niveles de ejecución financiera de los mismos, entre otra información relevante. Podrían publicarse trimestral o cuatrimestralmente.

Estos informes, a su vez, podrían formar parte del plan de comunicación de la entidad. Podrían ser divulgados a través de diferentes medios o canales, incluyendo: el sitio web, las cuentas de redes sociales, eventos presenciales o virtuales y publicaciones, entre otros. (Sobre la gestión de la comunicación para un sistema de emergencia y seguridad, dirigirse al Capítulo IX de esta Guía).

10.5. Procesos de compras y contrataciones públicas de bienes y servicios

La transparencia también tendría que incorporarse a todos los procesos de adquisiciones de bienes y servicios, cumpliendo con las normas establecidas en cada país y garantizando las mismas oportunidades para todos los proveedores.

Para transparentar los procesos de compras y contrataciones sería recomendable:

- Disponer de una sección dentro del sitio web del sistema de emergencia y seguridad donde se publiquen todos los concursos y licitaciones, detallando los requerimientos, condiciones y plazos. Esta información también podría publicarse en otros medios, según lo establezcan las leyes en cada país.
- Contar con un equipo de compras que revise los procesos de adquisición de bienes y servicios y que apruebe sólo aquellos que estén en consonancia con lo establecido por la ley y sus procedimientos, los requisitos y las bases publicados. Sería recomendable que este equipo estuviera conformado por la máxima autoridad de la entidad, un asesor/a jurídico/a, un/a funcionario/a del área de planificación, un funcionario/a del área de administración y finanzas y, si lo hubiera, un/a funcionario/a encargado de los temas de transparencia y rendición de cuentas.
- Recurrir a técnicos y peritos especializados en cada bien o servicio objeto de un proceso de compra o contratación, para que puedan brindar recomendaciones y una opinión informada sobre requisitos y especificaciones, y su cumplimiento por parte de los proveedores.

A través de la plataforma web (externa), el sistema de emergencia y seguridad podría publicar los resultados de los procesos de compra y contratación (incluyendo concursos y licitaciones). Adicionalmente, se podría considerar llevar a cabo y publicar evaluaciones técnicas de los proveedores y de los bienes y servicios comprados o contratados.

10.6. Auditorías internas/externas

Otro mecanismo disponible para evidenciar la transparencia y la gestión institucional es la ejecución periódica de procesos de auditorías. Estas permitirían identificar a tiempo, desviaciones tanto financieras como operativas, formular medidas de corrección e implementarlas por medio de planes de acción.

Las auditorías podrían ser tanto internas como externas. Las internas tendrían que ser realizadas por un área técnica de la organización, especializada en el tema. Las auditorías externas tendrían que ser realizadas por un ente regulador o empresa contratada para tales propósitos. El fin de este proceso sería evidenciar de manera objetiva la observancia de las disposiciones legales y normativas que aplican a la entidad, así como el desempeño y el grado de cumplimiento de los objetivos planteados. Esta verificación podría ser de índole financiera, tecnológica, de gestión institucional, del manejo de datos y de seguridad, entre otros.

Sería importante que la entidad, de manera transparente, publique los resultados de las auditorías como parte de las acciones estipuladas en el plan, tomando en cuenta la clasificación de la información institucional. De esta manera, se facilitaría el proceso de control horizontal y vertical, incluyendo las veedurías por parte de la población, organizaciones de la sociedad civil y otras audiencias específicas, respecto a la gestión del sistema de emergencia y seguridad.

10.7. Plan de comunicación

El plan de comunicación de un sistema de emergencia y seguridad, particularmente en lo que respecta a su componente organizacional, tendría que incorporar objetivos, metas, resultados y acciones comunicacionales vinculados a la transparencia y a la rendición de cuentas.

Tendría que aprovechar el empleo de las redes (plataforma web externa y la intranet), los medios (tradicionales y sociales) y otros canales disponibles para, con base en los datos e informes que produce el sistema de emergencia y seguridad, poder comunicarlos y difundirlos en aras de la transparencia y la rendición de cuentas institucionales.

En línea con lo anterior, y a modo de ejemplo, la plataforma web podría utilizarse para la publicación y disponibilización digital de los datos e indicadores, los informes (de gestión, servicio, financiero y de proyectos), los procesos de compras y contrataciones (de principio a fin, atravesando y acompañando todas sus etapas, incluyendo la evaluación de proveedores y contratistas), los resultados de las auditorías realizadas, las conferencias y comunicados de prensa institucionales, entre otros contenidos relevantes para la transparencia y la rendición de cuentas del servicio de emergencia y seguridad.

A través de los medios de comunicación tradicionales y sociales se podría brindar a la población balances de gestión y de los servicios brindados, los resultados de licitaciones y auditorías realizadas, entre otras acciones comunicacionales posibles.

En todo caso, el plan de comunicación podría ser otro de los mecanismos para promover la transparencia y rendición de cuentas por parte de un sistema de emergencia y seguridad.

10.8. Mecanismos adicionales

Adicionalmente a estos procesos y mecanismos específicos para contribuir a la transparencia y a la rendición de cuentas de un sistema de emergencia y seguridad, se podrían mencionar al menos dos herramientas más:

- El Código de Ética y el Código de Conducta (ambos introducidos en el Capítulo VI de esta Guía)
- La formación de los/as funcionarios/as sobre la base de esos dos Códigos, en aras de propiciar conductas y acciones profesionales fundadas en valores éticos, vinculados con la honestidad, la integridad y la transparencia

La aplicación de la transparencia y la rendición de cuentas tendría que ser transversal al funcionamiento del Sistema. Para ello, resultaría pertinente contar con un Código de Ética que consolide los principios y los valores que tendrían que guiar las actuaciones consideradas altamente deseables por parte del sistema de emergencia y seguridad. Adicionalmente, también se tendría que disponer de un Código de Conducta que defina los comportamientos deseables a nivel individual y en lo que respecta a las relaciones interpersonales, entre quienes trabajan para un sistema de emergencia y seguridad.

Estos Códigos podrían formar parte del proceso de inducción de nuevos/as funcionarios/as, sin importar el tipo de contrato o cargo, para que conozcan los propósitos y contenidos de ambos instrumentos, así como las consecuencias de no respetarlos. Es posible que a lo largo de la carrera profesional de los/as funcionarios/as de un sistema de emergencia y seguridad, resulte necesario actualizar, refrescar o profundizar la formación en valores éticos, incluyendo cursos en liderazgo basado en altos valores. Adicionalmente, ambos Códigos podrían estar disponibles para el personal a través de la intranet así como para el público general, a través de la plataforma web (externa).