



J O R N A D A

Gestión de Emergencias **UNE-ISO 22320**



UNE-ISO 22320
GESTIÓN DE EMERGENCIAS
RESPUESTA A INCIDENTES
ASPECTOS BÁSICOS E IMPLANTACIÓN

UNE-ISO 22320

GESTIÓN DE EMERGENCIAS

RESPUESTA A INCIDENTES

Sobre este documento

Este documento contiene un resumen ejecutivo de la ponencia “La Norma UNE-ISO 22320:2013 sobre Gestión de Emergencias” con la que Start Up participó en la Jornada sobre Gestión de Emergencias celebrada el 28 de marzo de 2014 en AENOR (Madrid).

Su objetivo es doble: por un lado, señalar los aspectos más destacados de la Norma ISO 22320 y su relación con la gestión corporativa y, por otro, presentar brevemente la metodología de implantación que Start Up utiliza en todo sus proyectos.

Para la elaboración del mismo se han tenido en cuenta los trabajos desarrollados por AENOR, CEN E ISO, la legislación de referencia (especialmente, la Ley 8/2010 de Protección de Infraestructuras Críticas, con la que los operadores públicos y privados que sean caracterizados como críticos habrán de adoptar sistemas de gestión de su seguridad global, basados fundamentalmente en los estándares normativos internacionales existentes), así como la propia experiencia de Start Up en la implantación de sistemas de gestión de emergencias y continuidad.



Sobre los autores

Andrés Álvarez. Ingeniero de Minas de con más de 20 años de experiencia en gestión de proyectos. En la actualidad es Director de Seguridad Integral de Start Up.

andres.alvarez@gestionemergencias.es

Milenka MacDowall. Ingeniera Informática y Auditora de sistemas de gestión según normas ISO 27001, 20000-1 y 22321 por AENOR, BSI, ITSMF e ISACA (CISA, CRISC, ITIL). En la actualidad es Consultora Sénior en Start Up.

milenka.macdowall@seguridadinformacion.com

ÍNDICE

1. Introducción
2. Normalización
3. La Norma ISO 22320
4. Implantación de un sistema de gestión de emergencias
5. Beneficios

Sobre Start Up

1. INTRODUCCIÓN

A raíz de los **ataques terroristas del 11 de septiembre** de 2001 en los **Estados Unidos** y de los posteriores en **España** y el **Reino Unido**, la sociedad internacional fue consciente de la necesidad de tomar medidas de seguridad, en todos los ámbitos posibles, con el fin de contribuir a proteger a los ciudadanos frente a diferentes tipos de situaciones de riesgo, ya sean éstas generadas por el hombre, de manera intencionada o no, o por la propia naturaleza.

Asimismo, las consecuencias de los desastres naturales de los últimos años -el **terremoto de Haití**, el **tsunami de Indonesia**, las **inundaciones** y los **ciclones** en **Australia**, el terremoto en **Nueva Zelanda**, el terremoto y posterior tsunami y **desastre nuclear** en **Japón**, o los más cercanos terremotos acontecidos en **Lorca** (España) e **Italia**- también han puesto de manifiesto la necesidad de mejorar la gestión de los riesgos asociados al comportamiento de las fuerzas naturales y de las situaciones que estos pueden producir.

Por otro lado, la creciente complejidad de la interacción humana está dando paso a la aparición de nuevos riesgos y, sobre todo, está despertando el interés de las principales instituciones del mundo acerca de cómo poder minimizar, en todo lo posible, las situaciones lesivas que puedan producirse, de manera intencionada o no, como consecuencia de los mismos. Los **ataque ciberterroristas** de los últimos años (a Estados, empresas o ciudadanos), la **gestión de aglomeraciones** y **posibles emergencias** (la tragedia de la **Love Parade** en Duisburgo en el año 2010, el **Madrid Arena**, ...), o **accidentes** como el acontecido en las vías de **Angrois**, por ejemplo, son algunos de los hechos que ponen de relieve la necesidad de trabajar de manera exhaustiva en la gestión y coordinación de la respuesta a incidentes.

El interés por mejorar la gestión de la seguridad de los ciudadanos por parte de sus instituciones representativas ha ido parejo al incremento de la preocupación por parte de otros organismos (tanto públicos como privados) cuya participación activa en la gestión es imprescindible, aunque, a priori, esto pueda suponer un esfuerzo importante en las tareas de coordinación y preparación.

Fruto de esta preocupación por la seguridad considerada de una forma integral, tanto lógica como física, se han desarrollado distintas normas internacionales entre las que se encuentra la **Norma UNE-ISO 22320:2013, Protección y Seguridad de los Ciudadanos. Gestión de emergencias. Requisitos para la respuesta a incidentes**, así como diversas

iniciativas legislativas, entre las que cabe destacar la Directivas europeas SEVESO o más recientemente la Ley 8/2011 sobre Protección de Infraestructuras Críticas, promovida por el Gobierno de España y dirigida a la prevención y protección de aquellos servicios básicos para la ciudadanía, como pueden ser el suministro eléctrico, de agua o las telecomunicaciones, entre otras. Esta Ley obliga a que los operadores públicos y privados que sean caracterizados como críticos adopten sistemas de gestión de su seguridad global, basados fundamentalmente en los estándares normativos internacionales existentes. Entre ellos, el que entendemos como fundamental para todas aquellas organizaciones que puedan verse involucradas en actuaciones de respuesta a incidentes con riesgos importantes para la sociedad, es la Norma UNE-ISO 22320 de Gestión de Emergencias.

“El objetivo consiste en salvar vidas, mitigar daños y perjuicios, así como garantizar un nivel de base de la continuidad de las funciones esenciales de la sociedad. Dichas funciones incluyen la salud, los servicios de rescate, el suministro de agua, alimentos, electricidad y combustible. Mientras que en el pasado el centro de respuesta a incidentes tenía un ámbito nacional, regional o incluso a nivel de organizaciones individuales, hoy y para el futuro, hay una necesidad de enfoque transversal debido a que, la mayor parte de las veces, la respuesta ante emergencias requiere la involucración de muchas organizaciones tanto públicas como privadas”.

Fuente: <http://lascertificaciones.blogspot.com.es/2013/02/iso-22320-sistema-de-gestion-de.html>

2. INICIATIVAS DE NORMALIZACIÓN

Las iniciativas que se han puesto en marcha desde el ámbito de la normalización, tanto a nivel internacional como a nivel europeo y español, han sido impulsadas para facilitar la coordinación de todas las partes interesadas e implicadas en la protección civil y poner a su disposición las mejores herramientas de gestión aceptadas internacionalmente.

Por un lado, **ISO** se moviliza por iniciativa principalmente del organismo norteamericano, ANSI, y se toma la decisión de crear un órgano de máximo nivel asesor del Consejo Técnico en materia de Seguridad (ISO/TMB SAG "Security"). Este órgano, además de proponer el inicio de trabajos de normalización en campos ya cubiertos por comités técnicos existentes (detectores radiológicos/nucleares; detectores de ántrax; Normas de ciber-seguridad; Biométrica de entrada/salida; Sensores químicos/de explosivos; Simulación y análisis; Formación para responsables de emergencias; Comunicaciones interoperables, etc.), también ha reactivado el **comité ISO/TC 223 "Societal Security"**, originalmente denominado "Civil Defence" y que en la actualidad cuenta con 47 países participantes.

Por su parte, la **Comisión Europea** ha preparado en los últimos tiempos numerosos documentos dirigidos a promover la utilización de la normalización europea como apoyo al desarrollo de iniciativas reglamentarias orientadas a aumentar la protección y la seguridad de los ciudadanos de la Unión Europea. Así mismo, es igualmente destacable el enorme presupuesto destinado por el 7º Programa Marco para investigación pre-normativa en el campo de la Seguridad. Como consecuencia de las solicitudes de colaboración de la Comisión al **Comité Europeo de Normalización (CEN)**, se creó en 2005 un grupo de trabajo asesor del Consejo Técnico que ha dado lugar al comité **CEN/CT 391** denominado "**Protection and Security of the Citizen**".

En **España**, con el fin de realizar el seguimiento de todos estos trabajos y elaborar normas y guías nacionales, se creó en 2008, a petición de **AENOR** y por resolución de la Dirección General de Desarrollo Industrial del Ministerio de Industria, el comité de Normalización **AEN/CTN 196, Protección y seguridad de los ciudadanos** cuya responsabilidad se centra en la normalización en el área de la seguridad de los ciudadanos, con el objetivo de incrementar la capacidad de gestión de crisis mediante consideraciones técnicas, humanas, de organización, de operación y gestión, así como la concienciación de todas las partes implicadas.

Para ello, en el seno de AENOR se elaborarán documentos normativos tanto para prevenir como para responder ante riesgos de crisis y desastres causados de manera intencionada o no o por la propia naturaleza, que alteren y tengan consecuencias en las funciones de la sociedad, considerando todo tipo de riesgos y cubriendo las fases de gestión de crisis y emergencias, antes, durante y después de un incidente que afecte a la seguridad de los ciudadanos

ISO/TC 223 Societal Security

Normas aprobadas	
ISO 22300:2012	Societal security. Terminology
ISO 22301:2012	Societal security. Business continuity management systems. Requirements
ISO 22311:2012	Societal security. Video-surveillance. Export interoperability
ISO/TR 22312:2011	Societal security. Technological capabilities
ISO 22313:2012	Societal security. Business continuity management systems. Guidance
ISO 22320:2011	Societal security. Emergency management. Requirements for incident response (*)
ISO 22398:2013	Societal security. Guidelines for exercises

Normas en elaboración	
ISO/DIS 22315	Societal security. Mass evacuation. Guidelines for planning
ISO/NP 22316	Societal security -- Organizational resilience -- Principles and guidelines
ISO/WD 22317	Societal security. Business continuity management systems. Business impact analysis (BIA)
ISO/WD TS 22318	Societal Security. Business continuity management. Guidance for supply chain continuity
ISO/DIS 22322	Societal security -- Emergency management -- Public warning
ISO/DIS 22324	Societal security. Emergency management. Colour-coded alert
ISO/CD 22325	Societal security. Emergency management. Guidelines for emergency management capability assessment
ISO/DTR 22351	Societal security. Emergency management. Message structure for exchange of information
ISO/FDIS 22397	Societal security. Guidelines for establishing partnering arrangements

Fuente: www.iso.org /Consultado 2014-03-24/

(*) Versión española: UNE-ISO 22320:2013. *Protección y Seguridad de los Ciudadanos. Gestión de emergencias. Requisitos para la respuesta a incidentes*. Disponible en www.aenor.es

3. LA NORMA ISO 22320

La Norma **ISO 22320, Protección y Seguridad de los Ciudadanos. Gestión de emergencias. Requisitos para la Respuesta a Incidentes**, recoge las mejores prácticas para proporcionar una respuesta eficaz ante un incidente de acuerdo con una serie de requisitos mínimos aplicables a cualquier tipo de organización y describe las pautas para el establecimiento de las estructuras organizativas y procedimientos para el mando y el control, apoyo a la decisión, la trazabilidad y la gestión de la información en la gestión de situaciones de emergencia, independientemente del marco legal en el que opere.

La norma también ayuda a asegurar que la información es operativa, oportuna, pertinente y precisa para los procesos, sistemas de trabajo e información especificados.

Asimismo, establece las bases para la coordinación y la cooperación, asegurando que todas las partes pertinentes actúan alineadas durante un desastre, lo que minimiza el riesgo de malentendidos y garantiza un uso más eficaz de los recursos combinados (la interoperabilidad entre las organizaciones involucradas es esencial para el éxito de respuesta ante incidentes).

El estándar proporciona ejemplos de los roles y las responsabilidades habituales, aunque éstos deban ser adaptados a la estructura local de respuesta a incidentes y de los tipos de incidentes posible. Señala, a su vez, los requisitos mínimos para establecer procesos de gobierno, facilitar el flujo de información y coordinar a todos los implicados en la resolución de emergencias.

Las **actividades principales para dar respuesta eficaz ante un incidente pasan por diferentes etapas:**

- En primer lugar, un momento previo en el que se deben evaluar y categorizar los riesgos, y en función de ello elaborar unos planes y protocolos de actuación frente a cada escenario.
- A continuación, el momento en el que se desata el suceso perturbador, que es detectado a través de la activación de las alarmas correspondientes, se da paso a los procesos de mando y control, de información operacional, así como a la coordinación y cooperación con el objetivo de mitigar de inmediato los efectos negativos.
- Una vez transcurrido el incidente, el objetivo es trabajar en la recuperación y capacidad de la organización para restablecer la normalidad de la actividad lo antes posible.

Para la norma ISO 22320 la gestión de emergencias se compone de las tres fases de un evento disruptivo (antes, durante y después) que deben ser gestionadas de acuerdo a un sistema estructurado de mando y control.

Fases de la gestión de emergencias

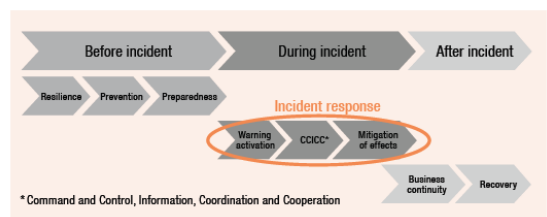


Figure 1: Phases of emergency management.

Fuente: Ernst-Peter Döbbling. 2012. ISO

Un **sistema estructurado de mando y control** permite:

- un entendimiento común de los fines y objetivos;
- una imagen operativa común de la situación;
- vínculos con otras organizaciones fuera de la línea de mando;
- el nombramiento y la designación de administradores y entidades competentes;
- la organización y control de los servicios de emergencia públicos y privados.

El proceso de mando y control sigue el principio PDCA (Plan-Do-Check-Act) de mejora continua. Este proceso se ajusta continuamente debido al impacto de las medidas de respuesta (positiva) o para la evaluación del incidente (negativo).

La **información operacional** proporciona la base para la evaluación de la situación y la toma de decisiones. La producción, integración y difusión de la información operativa, son elementos esenciales en el mando y control. En caso de emergencia o de crisis, las rutas normales de información y comunicación pueden ser interrumpidas y, la información en sí misma, puede ser intencionalmente manipulada o mal transmitida y/o entendida, por lo que disponer de instrumentos eficaces para su permanente control es una actividad básica para asegurar la correcta gestión de las emergencias.

Proceso para proporcionar información adicional



Fuente: Ortiz, 2013. AENOR

La **cooperación** es otro de los conceptos claves que se tratan en la norma. Se define como el acuerdo para trabajar o actuar en conjunto de acuerdo a los intereses generales y valores comunes.

La cooperación, como cualquier otro proceso, tiene que ser evaluado, preparado, establecido, y probado de antemano sobre la base del análisis de riesgos. Esto facilita las oportunidades para la planificación de respuestas a incidentes de manera eficaz y económica. La cooperación permite optimizar recursos y mejorar la respuesta de la comunidad ante situaciones de crisis reduciendo, además, la creciente complejidad de la colaboración pública y privada, nacional e internacional, en la gestión de emergencias

ISO 22320 también facilita una buena **coordinación de respuesta a incidentes** entre las organizaciones gubernamentales y la industrias y es aplicable a todas las organizaciones del sector público y privado que puedan estar implicadas en la respuesta a emergencias. Una organización puede utilizar este estándar para identificar los requisitos de desempeño individuales y organizar la toma de decisiones en situaciones de crisis, cuando la toma de decisiones jerárquica normal, se interrumpe. La norma permite planificar e implementar un completo y bien estructurado sistema de respuesta a incidentes bajo las premisas de coordinación, cooperación y colaboración público-privada.

OTRAS NORMAS

Como se ha indicado, la **Norma ISO 22320** da respuesta a la necesidad planteada en la gestión de emergencias de una estructura de gobierno y control, coordinación y cooperación para efectiva y eficaz. Esta norma proporciona los requisitos mínimos para establecer procesos de gobierno, facilitar el flujo de información y coordinar a todos los implicados en la resolución de emergencias.

No obstante, para abordar adecuadamente las adversidades a las que se puede estar expuesto se debe hacer uso de una metodología de gestión de riesgos para comprender y acometer con total fundamento cualquier situación crítica. En este sentido, la norma **ISO 31000, Gestión de Riesgos. Principios** se utilizará como marco genérico para la gestión de todos los riesgos asociados, no sólo a situaciones de emergencia sino también a cualquier otro tipo de riesgo corporativo.

La preparación para responder a las incidencias y los programas de continuidad operacional se realizarán con la Norma **ISO 22301, Seguridad social. Sistemas de gestión de continuidad. Requisitos** que especifica los requisitos para planificar, establecer, implementar, operar, monitorizar, revisar, mantener y mejorar continuamente un sistema de gestión documentado para reducir la probabilidad de ocurrencia, prepararse, responder, recuperarse y protegerse de y contra incidentes perturbadores. Esta norma establece los requisitos de un sistema de gestión para tratar emergencias alineado con el resto de sistemas de gestión ISO.

Asimismo, también deben ser tenidas en cuenta todas las normas elaboradas por el comité ISO/TC 223 así como la legislación y guías prácticas de referencia.

4. IMPLANTACIÓN

¿Por qué implantar la Norma UNE-ISO 22320?

La Norma UNE-ISO 22320 es una herramienta que cualquier organización implicada en la respuesta a incidentes: pública o privada, pequeña o grande, puede utilizar para mejorar sus capacidades y habilidades para manejar todo tipo de emergencias. Y no sólo mejorar las suyas sino mejorar la capacidad conjunta de actuación fortaleciendo la coordinación y cooperación con otros agentes intervinientes.

Dentro de las organizaciones que pueden verse implicadas en la respuesta a incidentes, podemos diferenciar aquellas que por la naturaleza de sus actividades van a participar en las diferentes actuaciones de emergencia (centros de coordinación público; fuerzas y cuerpos de seguridad del estado; unidades de intervención militar; sector sanitario; bomberos;...) y aquellas que por incidentes en sus instalaciones pueden verse afectadas por una situación de emergencia y tienen que estar preparadas para actuar frente a ellas. Dentro de este segundo grupo podemos diferenciar los operadores de infraestructuras críticas; es decir aquellas proporcionan servicios esenciales a la población.

Es importante que todas las organizaciones que “se puedan” ver involucradas en la respuesta a incidentes tengan unos criterios de intervención ordenados bajo un sistema de gestión de la seguridad, pero es esencial que las organizaciones que “están” involucradas en la respuesta a incidentes y los operadores de las infraestructuras críticas los tengan.

En esta línea están evolucionando los nuevos marcos normativos, destacando la Ley 8/2011 PIC de Protección de Infraestructuras Críticas que fomentará la adopción de sistemas de gestión integral de la seguridad basados en estándares internacionales como la Norma UNE-ISO 22320.

Por nuestra experiencia, a pesar de las grandes inversiones y gastos que en materia de seguridad asumen las diferentes organizaciones que se pueden ver sometidas a situaciones de emergencia, existe una relajación y desatención respecto a los aspectos normativos que les aplican y una falta de organización y sistematización acusada en sus protocolos y procedimientos de actuación.

Por ejemplo es muy frecuente que los Planes de Autoprotección o Planes de Emergencia estén desfasados y/o se hayan elaborado con la única perspectiva de un cumplimiento administrativo sin que sean un documento que se corresponda con la realidad de la organización y su forma de proceder. De igual modo, diferentes aspectos de la Norma Básica de Autoprotección o de las normas específicas sectoriales se descuidan en la práctica: Programas de formación y divulgación; programas de mantenimiento de los medios de extinción y seguridad;... Por otra parte, no existe conocimiento ni por lo tanto coordinación con los Planes de Autoprotección de otras organizaciones subordinados o principales,....

Estas cuestiones que aparentemente suponen únicamente un incumplimiento normativo con repercusiones tan solo en el ámbito administrativo, pueden cobrar un protagonismo de una relevancia excepcional si se tiene la desgracia de que ocurra un suceso grave. La perspectiva de estas cuestiones no tengan duda, lo estamos viendo en otras catástrofes, será totalmente distinta y las responsabilidades, por activa o pasiva, puede pasar a otro plano nada deseable.

Desde un punto de vista más práctico, por qué recomendamos la implantación de la Norma UNE-ISO 22320:

- **A los agentes “activos” en las emergencias**, además de para la mejora de sus capacidades, fundamentalmente para la adopción de un lenguaje común que será básico para una adecuada coordinación y cooperación con el resto de agentes.
- **A los operadores críticos**, porque estarán obligados a adoptar un sistema de gestión integral de la seguridad y la adopción de la UNE-ISO 22320 les dará respuesta a una gran parte de los requerimientos a los que estarán sujetos.
- **Al resto de organizaciones** que se puedan ver implicadas en actuaciones de respuesta a incidentes para reforzar la atención sobre aspectos que la improbabilidad de que aquellas puedan materializarse, puede derivar en un descuido de sus obligaciones.



Implantar un Sistema de Gestión de Emergencias de acuerdo a la Norma ISO 22320 obligará a la organización a someterse anualmente a una auditoría de revisión o certificación que, como premisa inicial, verificará el cumplimiento del marco normativo y servirá de acreditación frente a terceros de tal circunstancia y del compromiso de la organización con la vigilancia de tales aspectos.

Asimismo implantar un Sistema de Gestión de Emergencias de acuerdo a la Norma ISO 22320 permitirá optimizar los procedimientos y ajustarlos a la realidad mejorando la coordinación de todos los posibles agentes intervinientes. Como en muchos otros aspectos, en la mayoría de las ocasiones se trata de proceder a los protocolos que ya se siguen en la organización.

¿En qué consiste?

Como hemos señalado, la implantación de la Norma UNE-ISO 22320 supone adaptar las actuaciones de respuesta a incidentes en nuestra organización a las mejores prácticas disponibles y hacerlo en las tres fases de un incidente: antes, durante y después. La respuesta a incidentes comprenderá un conjunto de acciones para detener las causas de un peligro inminente, para mitigar sus consecuencias y para recuperarse de sus efectos.

Cualquier organización debe disponer de unos planes de actuación ante las emergencias que se puedan producir en sus instalaciones ya que nuestra normativa prevé su elaboración tanto en preceptos de carácter general, como es la Norma Básica de Protección, como en las reglamentaciones específicas que afectan a determinadas actividades e instalaciones.

La Norma UNE-ISO 22320 basa la respuesta a incidentes, en cualquiera de sus tres fases (antes, durante y después), en tres pilares básicos:

- **Establecimiento de una estructura y un proceso de mando y control;**
- **Definición de procesos para la gestión de la información operacional;**
- **Requisitos para la cooperación y coordinación entre las distintas organizaciones implicadas.**

De esta manera, implantar la Norma UNE-ISO 22320 no supone más que adaptar los Planes existentes en la organización a estos requisitos de la Norma.

Se puede entender fácilmente que esta adaptación será tanto más sencilla cuanto mayor sea el grado de “cumplimiento” de la normativa actual. Es decir, que la organización cuente con unos Planes de Emergencia actualizados, que respondan a la realidad operativa de la organización y que sean conocidos por sus miembros.

¿Cómo se implementa?

Destacaremos en primer lugar que para implantar la Norma UNE-ISO 22320 no es necesario, aunque sí recomendable, contar con sistemas de gestión que cumplan con otros estándares normativos. Es más, adoptar esta Norma no supone desarrollar un sistema de gestión de nuestras actuaciones de respuesta a incidentes entendido éste en un sentido amplio. No obstante, es evidente nuestra recomendación de integrar estos procedimientos con los sistemas de gestión de nuestra actividad, si se dispone de ellos, o de desarrollar, en su caso, un sencillo Plan de Gestión de las actuaciones de respuesta a incidentes con la elaboración de un manual que incluya por una parte los procedimientos que prescribe la Norma UNE-ISO 22320 y, por otro, que incluya los procedimientos el seguimiento y control de nuestra propia gestión, en cuanto al control documental, gestión de no conformidades y acciones correctivas y preventivas, auditorías internas, gestión de recursos humanos y revisión del sistema.

Podemos distinguir cuatro fases para la implantación de la Norma:

Evaluación/Auditoría de diagnóstico: donde se tiene en cuenta la documentación existente: Planes de respuesta a emergencias propios y externos, procesos y procedimientos internos, y legislación de referencia,

Definición de alcance y desarrollo de política de respuesta a emergencias. La política es un documento de alto nivel, que establece las metas y objetivos generales de la organización en materia de gestión de emergencias.

Elaboración e implantación de procedimientos alineados con los planes y documentación:

Procedimiento de mando y control; Procedimiento de gestión de la información operacional; Procedimiento de cooperación y coordinación.

Plan de mejora y **revisión de cumplimiento del sistema.**

Las 4 fases de Start Up

1. Evaluación inicial / Auditoría de diagnóstico

El punto de partida para la implantación de la Norma será el análisis y revisión de toda la documentación existente en la organización relativa a las actuaciones de respuesta a incidentes:

- Planes de emergencia o de autoprotección existentes en la organización.
- Planes de actuación subordinados o principales de organizaciones que dependan o en las que se integre la nuestra.
- Planes de mantenimiento; formación; divulgación; programa de auditorías e inspecciones; de simulacros; de sustitución de medios y recursos;...
- Acuerdos y contratos con agentes bien subordinados o principales que intervengan en la respuesta a incidentes.
- Y en general cualquier otra documentación que determine o que afecte a las actuaciones de respuesta a incidentes o a su preparación.

De este análisis se deducirá la necesidad de actualización y/o modificación de su contenido para que cumpla con los requisitos normativos que le aplican y para que responda a la realidad de las instalaciones de la organización y a su sistemática de actuación frente a incidentes.

2. Definición de alcance y desarrollo de política de respuesta a emergencias

En el alcance se define el ámbito de actuación de la norma y sus límites. Abordará aspectos generales de lo que pretende la organización con la implantación de la norma, como por ejemplo:

- Establecer las metas y objetivos en materia de respuesta a emergencias así como definir su compromiso en materia de gestión de emergencias
- Conocer y disponer de los medios necesarios para responder a las emergencias.
- Informar y formar al personal para actuar con eficacia y rapidez ante las situaciones de emergencia.
- Analizar y prevenir las causas de posibles emergencias.
- Establecer una mejora continua de los sistemas y planes de respuesta a emergencias.

La Declaración de Política, deberá estar formalmente aprobada por la Dirección y distribuida y comunicada a todas las partes interesadas.

3. Elaboración e implantación de procedimientos

Procedimiento de mando y control

Como paso previo para definir la estructura de mando, se deberá establecer una clasificación de las posibles situaciones de emergencia y los distintos niveles de “alerta” en las mismas. Los procedimientos de mando y control determinarán qué personas ocupan cada nivel jerárquico definido en cada estadio de la emergencia que hayamos definido. Se deben establecer sus responsabilidades y los perfiles para saber quién puede hacerse cargo de esa responsabilidad.

La Norma nos determina los aspectos a incluir en los procesos de mando y control durante todas las fases de un incidente, de manera que quien tome la decisión lo haga con el mayor y mejor conocimiento posible de la situación en el menor tiempo posible y que las ordenes que se deriven se transmitan fielmente y produzcan los efectos deseados.

La toma de decisiones debe ser lo más clara y transparente posible. La toma de decisiones debe ser comunicada dentro de la organización y a otras organizaciones interesadas, así como al público, en su caso.

El sistema de gestión debe establecer los lugares e instalaciones apropiados para la ubicación de los responsables de la toma de decisiones; es decir, centros de mando o control. Se podrá establecer un único centro de mando o varios, pero, en este último caso, tendrán una clara dependencia jerárquica. Los centros de mando facilitarán la recepción y gestión de la información y la aplicación de las órdenes y adecuado uso de los recursos disponibles.

Respecto a los recursos humanos necesarios para las acciones de respuesta a incidentes en cada tipo de emergencia y en sus diferentes fases, el sistema de gestión deberá prever su organización de manera que su intervención se produzca en el menor tiempo posible. Se primará la participación del personal que participe en la gestión “ordinaria” de la empresa en el momento que se produzca el incidente. El sistema de gestión determinará la forma de alertar y adscribir otros recursos.

Como hemos indicado el sistema de gestión establecerá los perfiles profesionales de los miembros de la estructura de mando pero, además, indicará la formación necesaria de cada actuante para prever las necesidades formativas a establecer.

El sistema de mando y control, se centrará en los aspectos de competencia de la propia organización y los de agentes sobre los que tenga ascendencia, para los que serán vinculantes. Será recomendable que los procedimientos, aunque sólo tenga efectos meramente informativos, contemplen la cadena de mando general en actuaciones de envergadura en la que se requiera una intervención más amplia. Aunque los procedimientos son escalables e integrables, un conocimiento de un espectro más amplio que el que es estrictamente de nuestra competencia.

Procedimiento de gestión de información operacional

El segundo pilar básico de la Norma ISO 22320 está constituido por los procesos de información operacional. La información operacional proporcionará la base para la evaluación de la situación y por lo tanto, para la adecuada toma de decisiones, la organización de los recursos y las actividades de control. En definitiva, la información operacional en la respuesta a incidentes es necesaria para gestionar de forma eficaz las actividades de respuesta.

La Norma introduce el calificativo de operacional para distinguir la información que manejaremos en la gestión de emergencias de la información en general que podemos tener a disposición.

Se distinguen principalmente dos tipos de información:

- Estática: Información previa al incidente que viene recogida en los propios Planes y sus Anexos o que puede tener disponible previamente alguna organización colaboradora (por ejemplo; planos, recursos humanos y técnicos, información de contacto, etc.).
- Dinámica: Es la información que se genera y gestiona durante la situación de emergencia.

La Norma establece unos procedimientos de transformación de manera que del conjunto de información disponible obtengamos una información operacional que sea útil a nuestros propósitos. La información disponible será tanto la que podamos tener de manera previa relativa al lugar en el que ocurre el incidente, información estática; como la información dinámica que se vaya generando en el desarrollo de las actuaciones de emergencia. En momentos en los que la toma de decisiones tiene que ser muy rápida se tienen que preestablecer sistemas de tratamiento de la información para que en cada estadio de la toma de decisiones se tenga la información necesaria y suficiente. Un exceso de información puede entorpecernos la toma de decisiones tanto como un defecto. De esta manera, la norma caracteriza la información operacional y establece marcos para su gestión..

La Norma ISO 22320 determina la adopción, en el sistema de gestión de actuaciones, de un proceso continuo para proporcionar información operacional, incluyendo las siguientes actividades:

- a) Planificación y dirección: La información operacional deberá ser planificada y preparada como parte del proceso de mando y control.
- b) Recopilación: se deberán identificar y validar las fuentes de las que podremos obtener información y determinar la manera de registrarla.
- c) Tratamiento y explotación: se determinan procedimientos para tratar la información recopilada y que esta pueda ser utilizada fácilmente por los responsables de la toma de decisiones en todos los niveles y también por otros participantes que la necesiten en sus actuaciones.
- d) Análisis y producción: Durante el análisis y la producción, toda la información procesada disponible estará integrada, evaluada, analizada, e interpretada para crear información operacional. La información generada deberá atender a las prioridades en los requerimientos o solicitudes de información del mando del incidente.
- e) Difusión e integración: Durante la difusión e integración, la información operacional se entrega en función de su categorización y uso por los responsables en la toma de decisiones y otros usuarios. La difusión se ve facilitada por una variedad de medios. Los medios estarán determinados por las necesidades de los usuarios, las implicaciones y la criticidad de la información operacional, y los medios de transmisión disponibles.
- f) Evaluación y retroalimentación: Durante la evaluación y la retroalimentación, la organización llevará a cabo una evaluación a todos los niveles para ver como se llevan a cabo las actividades relacionadas con el suministro de información operacional. Basándose en estas evaluaciones, y la retroalimentación resultante, deberían iniciarse acciones correctivas, según sea necesario, para mejorar el proceso.

Los procesos anteriores establecidos dentro del sistema de gestión para obtener la información operacional deben establecerse atendiendo a los siguientes criterios: Calidad; Perspectiva; Sincronización; Integridad; Coordinación y Cooperación; Priorización; Predicción; Agilidad; Colaboración y Fusión.

Procedimiento de cooperación y coordinación

La coordinación es el objetivo fundamental que persigue esta Norma. Podemos decir que el resto de procedimientos se ponen al servicio de este objetivo superior.

La coordinación es la forma en que estas diferentes organizaciones trabajan juntas para lograr un objetivo común.

Cada organización tiene su propia línea de jerarquía, mando e información. El reto consiste en integrar las respuestas individuales para lograr una sinergia en la medida en que la respuesta a incidentes tiene un objetivo unificado y un proceso de consenso en la toma de decisiones.

Respecto a la Cooperación y en la medida que sea posible nos deberemos ajustar a las prescripciones de la Norma de manera que podamos llevar a cabo las siguientes actuaciones:

- Evaluar la necesidad de la cooperación con otras organizaciones, actores y partes interesadas para preparar una eficaz respuesta a incidentes,
- Establecer acuerdos de cooperación sobre la base de la evaluación,
- Permitir la integración de los socios de la cooperación en el proceso de mando y control mediante el intercambio de expertos en su caso, y
- Testar, evaluar y revisar los acuerdos de cooperación a intervalos especificados por la organización.

El cumplimiento de esos aspectos de la Norma lo atenderemos con la referencia al Marco legal de Cooperación y/o Planes de Ámbito Superior respecto de los agentes Públicos, y a los contratos con agentes privados que puedan participar en las actuaciones de respuesta a incidentes (empresa de seguridad; subcontratas; empresas con las que se establezcan compromisos de puesta a disposición de medios en caso de emergencias;...).

Respecto a la coordinación se propiciarán todo tipo de actuaciones que permitan a los agentes que puedan verse implicados en actuaciones conjuntas de respuesta a incidentes a conocer sus respectivas organizaciones y sistemas de gestión y, en especial, con la realización de simulacros conjuntos.

4. Plan de mejora y revisión de cumplimiento

En base a una autoevaluación guiada por el equipo consultor, o a través de la realización de una auditoría interna, se evalúa el grado de cumplimiento y consistencia del sistema, indicando los puntos fuertes que hay que tratar de mantener y las áreas de mejora que permitan a la organización planificar acciones y medidas que ayuden a la cumplir con los requisitos de la norma.

Para cada acción se define:

- Descripción de la acción
- Responsables
- Plazos
- Prioridad
- Recursos necesarios

Esta fase permite comprobar la correcta implantación de los procedimientos y verificar el cumplimiento de los requisitos de la norma para que la organización esté preparada para afrontar la auditoría de certificación.

5. BENEFICIOS

La certificación de la Gestión de Emergencias según las directrices propuestas por la Norma ISO 22320, se dirige a cualquier tipo de organización -privada, pública, gubernamental o sin ánimo de lucro-, pero diferenciando dos enfoques distintos en función de la actividad de la organización. En primer lugar, aquellas organizaciones dedicadas profesionalmente a gestionar emergencias en su día a día, como organizaciones del ámbito sanitario o de las fuerzas de seguridad y protección, ya sean públicas o privadas. Y, en segundo lugar, organizaciones responsables que estén comprometidas con dar una respuesta de forma eficiente y eficaz ante emergencias que les puedan afectar, pensando en minimizar el impacto del incidente y asegurar su continuidad.

Esta certificación es compatible con otros sistemas de gestión como el de Gestión Ambiental ISO 14001, el de Seguridad y Salud en el Trabajo OHSAS 18001 o la nueva especificación AENOR EA 31 Sistemas de Gestión del Riesgo, ya que comparte con ellos algunas herramientas comunes a cualquier sistema de gestión, como la planificación, establecimiento de objetivos y metas, o acciones correctivas, añadiendo, en este caso, una perspectiva completa en cuanto a la respuesta ante incidentes, no cubierta íntegramente en otros sistemas de gestión.

En general, las organizaciones que implantan un Sistema de Gestión de Emergencias en su organización según la Norma ISO 22320 consiguen, sobre todo, desarrollar y mejorar sus capacidades para dar respuesta ante cualquier tipo de emergencia, independientemente de la dimensión de la misma; esto es, ya sea un incidente, una crisis, interrupciones de la actividad o un desastre. Se garantiza que la información operativa es veraz y fiable, ya que se establecen procesos de gestión de información y datos; y se minimizan los malentendidos al establecer una base de coordinación y cooperación entre las partes implicadas, así como una gestión más eficiente de los recursos compartidos.

En aquellas organizaciones en las que su actividad principal consiste en participar e intervenir en situaciones de emergencia, la certificación ISO 22320 aporta seguridad en el desarrollo de su actividad profesional. Asimismo, reconoce el compromiso de dar una respuesta eficaz a través de los objetivos de respuesta planteados, así como una gestión más eficiente de sus medios y recursos.

Con este certificado se reconocerá a las organizaciones responsables implicadas en la respuesta eficaz ante cualquier tipo de incidente de manera más óptima y eficiente junto con todas las partes implicadas.

La Norma UNE- ISO 22320 además de permitir mejorar nuestra capacidad de respuesta frente a situaciones de emergencia supondrá:

- **Mejora de la organización, coordinación y toma de decisiones** en la gestión de emergencias:
- **Mejora las relaciones con las autoridades, administraciones y partes interesadas** y mejora la imagen que éstas tienen de nuestra organización.
- **Alineación con los programas europeos** y con los **requisitos legales sobre Planes de Emergencia**.
- **Mejorar la imagen de la organización** pudiendo ser utilizada como herramienta de marketing.
- La certificación en la norma, que ahora es un **argumento diferenciador**, podría convertirse en un elemento a valorar para acceder a los contratos del sector público en materia de servicios relacionados con la respuesta a emergencias.
- En la **práctica jurídica**, la certificación ISO 22320 puede ayudar a demostrar que el empresario se ha preocupado por la eficacia de las medidas organizativas utilizando para su gestión las mejores prácticas disponibles en las normas internacionales de referencia

ISO 22320 recoge las mejores prácticas mundiales para el establecimiento de mando y control de las estructuras de organización y procedimientos, apoyo a las decisiones, trazabilidad y gestión de la información.

Ayuda a garantizar la información oportuna, relevante y precisa operación por procesos que especifican, sistemas de trabajo, captura de datos y la gestión.

Establece las bases de coordinación y cooperación, lo que garantiza que todas las partes relevantes están en la misma página durante un desastre, lo que minimiza el riesgo de malentendidos y garantiza un uso más eficaz de los recursos combinados.



Sobre Start Up

Start Up es una compañía española con sede social en Asturias especializada en la implantación de estándares normativos internacionales ligados al cumplimiento legal y a la gestión de la seguridad de la información y de la continuidad de negocio.

En este campo, es la empresa líder en España, tanto en el asesoramiento a la Administración Pública a través de la asistencia en el cumplimiento de la Ley Orgánica de Protección de Datos y la implantación del Esquema Nacional de Seguridad, como en el asesoramiento al sector privado en la implantación de la Norma ISO 27001.

Asimismo, Start Up ha desarrollado la mayoría de proyectos de implantación de la norma internacional ISO 22320 que han sido certificados en España.

Servicios

Gestión de Seguridad de la Información
Esquema Nacional de Seguridad
Esquema Nacional de Interoperabilidad
Gestión de Servicios de TI
LOPD
Análisis y Gestión de Riesgos
Gestión de Continuidad de Negocio
Hacking Ético
Calidad en el Desarrollo del Software
Buen Gobierno TIC
Protección de Infraestructuras Críticas
Integración de Sistemas de Gestión
Gestión de Emergencias - Respuesta a Incidentes
Gestión de evidencias electrónicas

El equipo de profesionales de Start Up se encuentra formado por un conjunto de expertos en Sistemas de Gestión, Tecnologías, Seguridad de la Información y Gestión de Riesgos Corporativos. Todos ellos están certificados por entidades acreditadas a nivel internacional, tales como AENOR, BSI, Lloyd's, Applus, Microsoft (MCSA), ITIL o ISACA (CISA, CISM y CRISC) como Expertos Implantadores y Auditores de Sistemas de Seguridad de la Información, Sistemas de Gestión de Servicios de TI y Sistemas de Gestión de la Calidad.

Start Up

Dirección: Ildefonso Sánchez del Río 10, 1ºB
33001 - Oviedo - Asturias
Teléfono: 985 20 75 59
Móvil: 609 67 76 49
Fax: 985 20 71 98
Email: info@seguridadinformacion.com



Escanee el código y acceda a nuestra lista de Clientes