UNIVERSIDAD POLITÉCNICA DE VALENCIA
Departamento de Ingeniería Hidráulica y Medio Ambiente

Master Oficial en Ingeniería Hidráulica y Medio Ambiente

Detección de eventos de contaminación en redes de abastecimiento de agua mediante el Control Estadístico de Procesos

TESIS

Trabajo para optar por el Título de
Máster en Ingeniería Hidráulica y
Medio Ambiente

Presentada por

Joanna Alicia Gutiérrez Pérez

Dirigida por

Dr. Rafael Pérez García
Dr. Joaquín Izquierdo Sebastián

Valencia, España. Junio de 2010

UNIVERSIDAD POLITÉCNICA DE VALENCIA

Departamento de Ingeniería Hidráulica y Medio Ambiente

Master Oficial en Ingeniería Hidráulica y Medio Ambiente

Título:

Detección de eventos de contaminación en redes de abastecimiento de agua mediante el Control Estadístico de Procesos

Autor:

Joanna Alicia Gutiérrez Pérez

Directores:

Dr. Rafael Pérez García

Dr. Joaquín Izquierdo Sebastián

Resumen

Los sistemas de abastecimiento de agua potable son infraestructuras críticas que están expuestas a daños por causas naturales y por ataques deliberados, que pueden poner de manifiesto las debilidades del sistema. Tales sistemas son muy vulnerables a una variedad de amenazas, como la contaminación deliberada o accidental de la red de distribución. La intrusión contaminante es difícil de predecir, especialmente si es deliberada, debido a la dispersión espacial del sistema, lo que puede comprometer seriamente su capacidad para entregar agua potable segura. En este sentido, la implementación de un sistema de monitorización puede ser de gran ayuda, no tanto para prevenir la contaminación del agua, sino para alertar de forma temprana en el caso de que aparezca.

Bajo esta perspectiva, el estudio de eventos de intrusión deliberada en una red de abastecimiento no ha sido abordado hasta el momento utilizando teorías y técnicas de Control Estadístico de Procesos, (*Statistical Process Control - SPC*), las cuales permiten detectar y medir desajustes significativos de la variable deseada en el tiempo. La presente tesis, propone analizar la respuesta de una red de distribución de agua ante una cierta concentración de un contaminante inyectado en un punto de la red, implementando gráficos de control estadístico que permitan representar los desajustes en el parámetro de la calidad del agua debido a la presencia del contaminante. Una vez observado su comportamiento y en función de los límites establecidos, se podrían definir los nodos críticos en los que la variación de la calidad del agua ha provocado una serie de alarmas.

Palabras clave: *Vulnerabilidad / Control Estadístico de Procesos / Sistemas de Abastecimiento de Agua / Acciones de mitigación / Amenazas*

Abstract

Water supply systems are critical infrastructures exposed to damages due to natural causes and deliberate attacks, as well, which can unveil the weaknesses of the system. Such systems are highly vulnerable to a variety of threats, such as deliberate or accidental intrusion of pollutants into the distribution network. Contaminant intrusion is difficult to predict, especially if it is deliberate, due to the spatial dispersion of the system, which can seriously compromise its ability to deliver safe drinking water. In this sense, the implementation of a monitoring system may be of great help, not just to prevent water contamination, but to early alert in the event it appears.

Under this perspective, deliberate intrusion events in a supply network have not been approached using theories and techniques of *Statistical Process Control (SPC)*, which allow detecting and measuring significant temporal imbalances of any variable of interest. This thesis proposes implementing statistical control charts to analyze the response of a water supply network under the event of intrusion of a certain concentration of a pollutant being injected through a point of the network. This allows to represent imbalances of the water quality parameter due to the presence of the contaminant. After observing the behavior of this indicator and depending on the established limits, there might be defined critical nodes where the variation of the water quality has caused the alarms.

Palabras Clave: *Vulnerability / Statistical Process Control / Drinking water supply systems / Mitigation actions / Threats*

Resum

Els sistemes d'abastiment d'aigua potable són infraestructures crítiques que estan exposades a danys per causes naturals i per atacs deliberats, que poden posar de manifest les debilitats del sistema. Tals sistemes són molt vulnerables a una varietat d'amenaces, com la contaminació deliberada o accidental de la xarxa de distribució. La intrusió contaminant és difícil de predir, especialment si és deliberada, a causa de la dispersió espacial del sistema, la qual cosa pot comprometre seriosament la seua capacitat per a entregar aigua potable segura. En este sentit, la implementació d'un sistema de monitorització pot ser de gran ajuda, no tant per a previndre la contaminació de l'aigua, sinó per a alertar de forma primerenca en el cas que aparega.

Davall esta perspectiva, esdeveniments d'intrusió deliberada en una xarxa d'abastiment no han sigut abordats utilitzant teories i tècniques de Control Estadístic de Processos, (Statistical Process Control - SPC), les quals permeten detectar i mesurar desajustos significatius de la variable desitjada en el temps. La present tesi, proposa analitzar la resposta d'una xarxa de distribució d'aigua davant d'una certa concentració d'un contaminant injectat en un punt de la xarxa, implementant gràfics de control estadístic que permeten representar els desajustos en el paràmetre de la qualitat de l'aigua degut a la presència del contaminant. Una vegada observat el seu comportament i en funció dels límits establits, es podrien definir els nodes crítics en què la variació de la qualitat de l'aigua ha provocat una sèrie d'alarmes.

Palabras Clave: *Vulnerabilitat / Control Estadístic de Processos / Sistemes d'abastiment d'aigua potable / Accions de mitigació / Amenaces*

"Detección de eventos de contaminación en redes de abastecimiento de agua mediante el Control Estadístico de Procesos"

Índice

Lista de Figuras

Lista de Tablas

1. INTRODUCCIÓN

1.1. PREÁMBULO

El abastecimiento de agua potable es una de las actividades fundamentales para el desarrollo de una ciudad y su calidad de vida. El sistema de abastecimiento tiene ciertas características en su funcionamiento que lo hacen especial frente a otros servicios, ya que el suministro puede verse amenazado y, como consecuencia, ser interrumpido, ya sea de manera parcial o total por un período de tiempo, provocando graves efectos en todos los sectores de la población.

Minimizar los posibles impactos, tanto en la salud pública como económicos, es objeto de diversas investigaciones en el ámbito de la seguridad del abastecimiento de agua potable, que se han enfocado en la mejora de los sistemas de monitorización y detección de contaminantes (químicos, biológicos y radiológicos).

En la última década se ha incrementado el interés en el desarrollo de nuevos sistemas de seguridad para enfrentar las intrusiones, tanto deliberadas como accidentales, en una red de abastecimiento. Diversos algoritmos y modelos de optimización se han desarrollado para identificar los sitios más eficientes en la ubicación de sensores. Algunas de esas contribuciones son de Alzamora y Ayala (2006), que sugirieron un marco general para la localización de sensores usando algoritmos topológicos. Dorini *et al*. (2006) propusieron un marco de optimización multiobjetivo. Eliades y Polycarpou (2006) sugirieron una solución multiobjetivo utilizando un algoritmo de soluciones de Pareto. Ghimire y Barkdoll (2006) proponen un enfoque heurístico basado en la demanda, en el que los sensores se ubican en los nodos de mayor consumo. Guan *et al.* (2006) propusieron una metodología de optimización mediante la simulación de un algoritmo genético. Éste se basó en una sola función objetivo, en la que se integraron cuatro objetivos de diseño. Sobre la misma línea de métodos de localización de sensores, Gueli (2006) sugirió un modelo "depredador-presa" de tipo evolutivo para resolver el problema de optimización multiobjetivo planteado. Mientras, Huang *et al.* (2006) establecieron el campo de aplicación en la minería de datos. Krause *et al*. (2006) aplicaron un algoritmo para la localización de sensores, usando una función de maximización submodular. Ostfeld y Salomons (2006) y Preis y Ostfeld (2006), usaron el esquema del algoritmo genético ordenado, multiobjetivo no dominado II (NSGA-II). Proparto y Piller (2006) utilizaron programación mixta-entera con una relajación lineal para resolver la localización de los sensores. Trachman (2006), sugirió un enfoque de ingeniería "hombre de paja", tomando en consideración factores como la distribución de la población, la presión del sistema y los patrones de flujo. Wu y Walski (2006), utilizaron una formulación de optimización multiobjetivo, basada en algoritmos genéticos, con eventos de

contaminación generados aleatoriamente (usando simulaciones de Monte Carlo). Chastain Jr. (2006), desarrolló una metodología heurística para identificar localizaciones estratégicas, que pueden ser establecidas como puntos de detección crítica para eventos de contaminación.

Bajo este contexto de propuestas estadísticas y de aprendizaje automático para la mejora de la seguridad de los sistemas de abastecimiento, este trabajo analiza la respuesta ante una intrusión contaminante en una red de distribución de agua. Asimismo, introduce la utilización de técnicas de Control Estadístico de Procesos (*Statistical Process Control –SPC)* para observar las variaciones en el valor del parámetro de la calidad del agua.

1.2. OBJETIVOS DE LA TESIS

Este proyecto de tesina plantea el estudio de eventos de intrusión deliberada en una red de abastecimiento de agua, mediante la utilización de técnicas de *SPC*, como un primer acercamiento para la definición de puntos potencialmente críticos dentro de la red.

El objetivo principal de este trabajo es la detección de variaciones en la calidad del agua en una red de abastecimiento. Para alcanzarlo, se utiliza el *SPC* como herramienta para establecer los posibles estados de alerta en los que la red se pudiera encontrar. Con el fin de alcanzar tal objetivo, se plantea lo siguiente:

- **a)** Plantear las bases de un escenario teórico de entrada de contaminantes que servirá de caso base para el estudio.
- **b)** Obtener los datos del comportamiento de la red de abastecimiento de agua, bajo el escenario de contaminación que se ha definido.
- **c)** Aplicar la técnica de control estadístico de procesos para analizar la evolución del contaminante en el tiempo y determinar los nodos potencialmente críticos.
- **d)** Establecer las conclusiones y recomendaciones generales.
- **e)** Sentar las bases para el planteamiento de la investigación doctoral.

1.3. ORGANIZACIÓN DEL DOCUMENTO

A continuación se describe brevemente el contenido de cada uno de los capítulos que forman la presente tesis:

En el **capítulo 1** se describe la justificación y los objetivos que se pretenden alcanzar con la realización del presente trabajo.

El **capítulo 2** se enfoca a las principales características de los sistemas de abastecimiento de agua, a los conceptos básicos del sistema de abastecimiento de agua como una "infraestructura crítica" y a la descripción de los principales eventos que la amenazan.

En el **capítulo 3** se aborda el concepto de vulnerabilidad en el contexto de los sistemas de abastecimiento de agua y se señalan los puntos más vulnerables de un sistema de abastecimiento. Asimismo, se describen algunos de los modelos más conocidos de evaluación de la vulnerabilidad.

El **capítulo 4** se centra en la mejora de la seguridad de los sistemas de abastecimiento de agua potable, en el contexto de los Sistemas de Alerta Temprana, mencionando las principales características que debe cumplir un sistema de monitorización.

Dentro del **capítulo 5** se dan los fundamentos conceptuales de las técnicas de Control Estadístico de Procesos. Se define el de control y los criterios para su construcción. Asimismo, se destaca su utilización como posible herramienta para la detección de anomalías fuera del ámbito industrial.

El **capítulo 6** trata sobre el desarrollo del caso de estudio. Se dan las características físicas de la red, las consideraciones para el planteamiento de los escenarios de contaminación y la construcción de los gráficos de control.

El **capítulo 7** corresponde a los resultados obtenidos. Se presentan los gráficos de control para cada uno de los eventos de contaminación planteados, así como la información relevante de los mismos. Además, se habla de las posibles acciones de respuesta y se comparan los resultados de un evento.

En el **capítulo 8** se dan las principales conclusiones sobre el trabajo realizado y se hace una propuesta de los trabajos y líneas de investigación sobre el tema.

Finalmente, en el **capítulo 9,** se indexan las referencias bibliográficas sobre las que se ha basado el desarrollo del presente trabajo.

2. ANTECEDENTES

2.1. EL CONCEPTO DE INFRAESTRUCTURA CRÍTICA

De acuerdo con información de la *OECD* Organización para la Cooperación y el Desarrollo Económico (*Organisation for Economic Co-operation and Development-OECD,* 2008), una *infraestructura crítica* es definida, en diversos planes nacionales de muchos países, como bienes físicos e intangibles, cuya destrucción o interrupción quebrantaría seriamente la salud pública, el orden social y el cumplimiento de las principales responsabilidades del gobierno. Debido a su importancia, tales infraestructuras han recibido especial atención en los cambios a las políticas de inversión nacional en algunos países, con el fin de crear estrategias para protegerlas. En relación con lo anterior, un daño a esas infraestructuras generalmente sería catastrófico y de largo alcance, ya que las causas de riesgo podrían ser naturales (como terremotos o inundaciones) o hechas por el hombre (como terrorismo o sabotaje), siendo estás últimas las más difíciles de predecir.

En un documento de la *OECD,* se presentan las definiciones de "infraestructura crítica" usadas por los gobiernos de distintos países en el contexto nacional o regional de los programas de protección. En la Tabla 2.1 se muestran las definiciones del concepto usadas en seis planes de protección de infraestructuras críticas publicados. La revisión de las definiciones considera separadamente las dos palabras bajo estudio: por un lado, el término "infraestructura" tiende a ser amplio; ya que los gobiernos de los seis países mostrados hacen referencia a la estructura física, pero la mayoría incluye también bienes intangibles, de producción o redes de comunicación. Por otro lado, las definiciones utilizadas de la palabra "crítica", se refieren a los medios que proporcionan un apoyo fundamental para el bienestar social y económico, para la seguridad pública y para el funcionamiento de las principales responsabilidades del gobierno.

Tabla 2.1. *Definiciones Nacionales de Infraestructura Crítica*

Australia	*"Infraestructura crítica es definida como aquellas instalaciones físicas, cadenas de suministro, tecnologías de información y redes de comunicación las cuales, si se destruyen, degradan o inutilizan por un largo período de tiempo, impactaría significativamente en el bienestar económico y social de la nación, o afectaría la capacidad de Australia para conducir la defensa nacional y garantizar la seguridad nacional."*
Canadá	"*Las infraestructuras críticas de Canadá consisten en aquellas instalaciones físicas y tecnologías de información, redes, servicios y bienes, los cuales, si se interrumpen o destruyen, tendrían un severo impacto en los servicios sanitarios, en la estabilidad o el bienestar económico de los Canadienses o en el funcionamiento eficaz de los gobiernos en Canadá."*

Alemania	*"Las instalaciones críticas son organizaciones o instalaciones de mayor importancia para la comunidad cuyo fallo o deterioro causaría una prolongada escasez de los suministros, importantes perturbaciones del orden público u otras consecuencias dramáticas."*
Holanda	*"Infraestructura critica se refiere a productos, servicios y procesos vinculados que, en el evento de interrupción o fallo, causaría un importante alteración social. Esto podría resultar en un gran número de muertes y daños económicos graves …"*
Reino Unido	*"La Infraestructura Crítica Nacional comprende aquellos bienes, servicios y sistemas que soportan la vida económica, política y social del Reino Unido cuya importancia es tal que su pérdida podría: 1) causar grandes pérdidas de vida; 2) tener un serio impacto en la economía nacional; 3) tener otras consecuencias sociales graves para la comunidad; o 4) ser de interés inmediato para el gobierno nacional."*
Estados Unidos	La definición general de infraestructura crítica en el plan general de infraestructuras críticas de los Estados Unidos es: *"sistemas y bienes, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de esos sistemas y bienes, tendría un impacto debilitador en la seguridad, la estabilidad económica nacional, la salud pública nacional o los servicios sanitarios, o cualquier combinación de estos temas."* Para fines de política de inversión, esta definición es más precisa: *sistemas y bienes, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de esos sistemas y bienes tendría un impacto debilitador en la seguridad nacional."*

Fuente: (OECD, 2008)

En la Tabla 2.2., se hace referencia a una lista en la que se muestran los sectores identificados como de preocupación nacional, en la protección de las infraestructuras críticas, dentro de los programas de los países señalados anteriormente, así como también para la Comisión Europea. Esas listas muestran que la mayoría de los gobiernos adoptan una amplia perspectiva sectorial incluyendo sectores que normalmente no serían considerados, como lo son, los sectores de alimentación, de salud, de gobierno y de finanzas.

Tabla 2.2. *Cobertura de los planes sectoriales de infraestructura crítica*

Sector	Australia	Canadá	Holanda	Reino Unido	Estados Unidos	Unión Europea
Energía (incluyendo la nuclear)	X	X	X	X	X	X
Tecnología de la Información y Comunicación	X	X	X	X	X	X
Finanzas	X	X	X	X	X	X
Salud	X	X	X	X	X	X
Alimentación	X	X	X	X	X	X
Agua	X	X	X	X	X	X
Transporte	X	X	X	X	X	X
Seguridad	Servicios de emergencia	X	X	Servicios de emergencia	Servicios de emergencia	X
Gobierno		X	X	X	X	X
Químicos		X	X		X	X

Defensa industrial	X		X		X	
Otros sectores y actividades	Reuniones públicas, íconos nacionales		Legal/Judicial		Embalses, instalaciones comerciales, monumentos nacionales	El espacio y las instalaciones de investigación

Fuente: (OECD, 2008)

En Moteff *et al.* (2003) se dice que en los últimos años, una serie de documentos relacionados con las infraestructuras críticas han ofrecido definiciones generales de las mismas y han proporcionado información sobre cuales infraestructuras debieran ser incluidas. Sin embargo, ninguna de esas listas o definiciones se puede considerar definitiva. La definición general y el criterio para determinar qué puede ser una infraestructura crítica y cuáles pueden calificarse así, ha crecido con el paso del tiempo; desde aquellas que en un principio se consideraron fundamentales para la defensa, la seguridad económica de la nación y la continuidad de gobierno (cuyas interrupciones prolongadas pudieran causar daños militares y económicos importantes), hasta incluir aquellas consideradas vitales para la seguridad y salud pública, así como para la moral de la nación, como los monumentos nacionales y la industria química.

En ese contexto, como una respuesta a la creciente amenaza de terrorismo a finales de los 90, el Gobierno Federal de los Estados Unidos de Norteamérica, bajo la presidencia de Bill Clinton, estableció la Comisión Presidencial para la Protección de Infraestructuras Críticas (*President's Commission on Critical Infrastructure Protection-PCCIP*), y en la Orden Ejecutiva publicada (E.O. 13010), se definió el término "infraestructura" como: "El marco de redes interdependientes y de sistemas que abarcan determinadas industrias, instituciones (incluyendo gente y procedimientos), y capacidades de distribución que proporcionan un flujo confiable de productos y de servicios esenciales para la defensa y la seguridad económica de los Estados Unidos, el buen funcionamiento del gobierno en todos los niveles, y de la sociedad en conjunto."

Posteriormente, debido a que la seguridad nacional de los Estados Unidos se calificó como de prioridad nacional alta, el término "infraestructura crítica" se fue desarrollando dentro de una mayor preocupación política. En la misma Orden Ejecutiva 13010, se habló acerca de lo que hace que una infraestructura sea crítica y fue señalado lo siguiente: *"Ciertas infraestructuras nacionales son tan vitales que su incapacidad o destrucción tendría un impacto debilitante en la defensa o seguridad económica de los Estados Unidos"*. Dentro de la Orden, de acuerdo con los inventarios básicos de infraestructuras críticas, se definieron ocho sectores de prestación de servicios esenciales a la sociedad, los cuales son:

- Telecomunicaciones
- Sistemas de energía eléctrica
- Almacenamiento y transporte de gas y petróleo.

- Banca y finanzas
- Transporte
- Sistemas de abastecimiento de agua
- Servicios de emergencia (incluyendo servicios médicos, de rescate, policía y bomberos)
- Continuidad del Gobierno

Del mismo modo, se destacó un grupo de bienes clave como: los monumentos nacionales, las plantas de energía nuclear, los embalses, las instalaciones de gobierno y los bienes comerciales.

Asimismo, en el reporte de la comisión, quedaron determinadas las infraestructuras de cada uno de los sectores mencionados anteriormente, tal como se describe a continuación:

- Banca y Finanzas: Entidades tales como el comercio minorista y organizaciones comerciales, instituciones de inversión, intercambio de acciones, casas de cambio, y sistemas de reserva y las organizaciones con operaciones asociadas, operaciones de gobierno y actividades de soporte que están involucradas en todo tipo de transacciones monetarias (incluyendo su almacenamiento con propósito de ahorro, su inversión para propósitos de rentabilidad, su cambio para propósitos de pago y su gasto en forma de préstamos y otros instrumentos financieros).

- Sistemas de Energía Eléctrica: Se consideran a las estaciones de generación de energía, a las redes de transmisión y distribución, que generan y abastecen de electricidad a los usuarios finales, y los medios que logran y mantienen su funcionamiento nominal, incluyendo el transporte y almacenamiento del combustible necesario para ese sistema.

- Servicios de Emergencia: Tales como médicos, policíacos, bomberos, sistemas de rescate y personal necesario una vez que un individuo o comunidad requiere respuesta a una emergencia.

- Producción, Almacenamiento y Transporte de gas y petróleo: La producción e instalaciones para el gas natural, petróleo crudo y refinado y combustibles derivados del petróleo, las instalaciones de refinamiento y procesamiento para esos combustibles y las tuberías, barcos, camiones y los sistemas ferroviarios que transportan a esos productos desde su fuente hasta los sistemas que dependen del gas y petróleo en alguna de sus formas.

- Información y Comunicaciones: Equipo informático y de telecomunicaciones , software, procesos y gente que lleva a cabo el procesamiento, almacenamiento y transmisión de datos e información; los procesos y la

gente que convierte los datos en información y la información en conocimiento y, los datos y la información para sí mismos.

- Transporte: Sistemas físicos fundamentales de distribución para apoyar la seguridad nacional y el bienestar económico de la nación, incluyendo los sistemas del espacio aéreo, las compañías aéreas, las aeronaves y aeropuertos; caminos y carreteras, camiones y vehículos personales; puertos y vías navegables y los buques que operan; tránsito masivo tanto por ferrocarril como por autobús; tuberías, incluyendo de gas natural, de petróleo y de otros materiales peligrosos; transporte ferroviario de mercancías y pasajeros; y otro servicios de distribución.

- Sistema de Abastecimiento de Agua: Las fuentes de agua, los embalses, instalaciones, acueductos y otros sistemas de conducción, filtración, sistemas de limpieza y tratamiento, tuberías, sistemas de refrigeración y otros mecanismos de suministro que se proporcionan para usos domésticos e industriales, incluyendo sistemas para tratar el agua de escorrentía, aguas residuales y extinción de incendios.

En este sentido, una infraestructura crítica, tanto en los Estados Unidos como en el mundo, abarca una amplia gama de bienes y sistemas de ingeniería. Si bien ningún sistema es más importante que otro, el carácter interdependiente de su funcionamiento es lo que interesa. Como se mencionó anteriormente, si un solo sistema es interrumpido, existe el potencial para fallos secundarios en infraestructuras interdependientes. Como resultado, existe una importante necesidad de medir y supervisar la confiabilidad y las debilidades potenciales de tales sistemas. Además, la capacidad de modelar los efectos de un fallo de la infraestructura es un aspecto importante en el diseño de redes, de los planes de recuperación de desastres y de la identificación de infraestructuras críticas y su refuerzo. Dada la fuerte presencia en el mundo industrializado de redes económicas, de transporte, de telecomunicaciones, de energía y servicios médicos, es fundamental tener una visión de las técnicas capaces de identificar las vulnerabilidades potenciales en los elementos de una sola red, o las debilidades sistemáticas más generalizadas, para ser protegidas o reforzadas.

En la misma línea, Murray y Grubesic (2007) señalan que los conceptos de *fiabilidad* y *vulnerabilidad* son especialmente importantes cuando se analiza la capacidad de una infraestructura crítica para proporcionar continuidad en el funcionamiento. La *fiabilidad* se refiere a la probabilidad de que un determinado elemento, en una infraestructura crítica, funcione en un momento dado. Es decir, la fiabilidad es una medida probabilística de los elementos en una infraestructura crítica y su capacidad para no fallar o funcionar mal, de acuerdo con una serie de patrones establecidos o normas de de funcionamiento. Contrario a la fiabilidad, la *vulnerabilidad* es un concepto más amplio con implicaciones mucho más extensas. Pues mientras que la fiabilidad se enfoca en la posibilidad de mantener el funcionamiento de los elementos de la infraestructura crítica, la vulnerabilidad se centra en el potencial para alterar esos elementos o degradarlos hasta un punto

donde el funcionamiento es disminuido. Por otro lado, vulnerable no siempre significa poco fiable, y a su vez, poco fiable no necesariamente es ser vulnerable. Sin embargo, tanto la fiabilidad como la vulnerabilidad son importantes para determinar la continuidad de las operaciones de una infraestructura crítica

2.2. LA INFRAESTRUCTURA DE ABASTECIMIENTO DE AGUA

La infraestructura de abastecimiento de agua es una colección de sistemas de abastecimiento interdependientes, sirviendo cada uno a comunidades en un área geográfica limitada (Haimes *et al.,* 1998). De forma general, los sistemas de abastecimiento de agua están constituidos por fuentes de agua, tuberías de distribución (desde la fuente de agua), plantas de tratamiento y redes de distribución (Li, 2007).

Asimismo, la red de abastecimiento puede considerarse como el conjunto de elementos. Dispositivos y mecanismos empleados para llevar el agua desde los puntos de captación hasta los puntos de consumo. Forman parte de la red de abastecimiento de agua los elementos necesarios para que el suministro de agua en los puntos de consumo se realice en las condiciones de caudal, presión y calidad suficientes para cada uno de los usos.

En un sistema de abastecimiento de agua el proceso completo, desde la captación hasta el consumo final por parte del abonado, puede entenderse como un sistema compuesto de varias etapas, claramente diferenciadas. Estas son:

- Etapa de captación.
- Etapa de transporte.
- Etapas de tratamiento. La etapa encargada de la depuración y potabilización del agua captada para dejarla en condiciones adecuadas para el consumo humano.
- Etapa de almacenamiento y regulación
- Etapa de distribución

En la Figura 2.1., se presenta un esquema general del servicio de abastecimiento de agua, mostrando el sistema de distribución de agua como un subsistema del servicio, el cual está constituido por tres componentes principales: estaciones de bombeo, almacenamiento y tuberías de distribución**.** Estos componentes pueden ser divididos en más subcomponentes, que a su vez pueden dividirse en sub-subcomponentes. Por ejemplo, la estación de bombeo consiste en los componentes estructurales, eléctricos, tuberías, y los subcomponentes de la unidad de bombeo. La unidad de bombeo puede ser dividida, además, en sub-subcomponentes como la bomba, los controles, los transmisores de energía, etc. La definición exacta de los componentes, subcomponentes y sub-subcomponentes, depende del nivel de detalle que requiera el análisis y en gran medida de la disponibilidad de los datos (Mays, 2004).

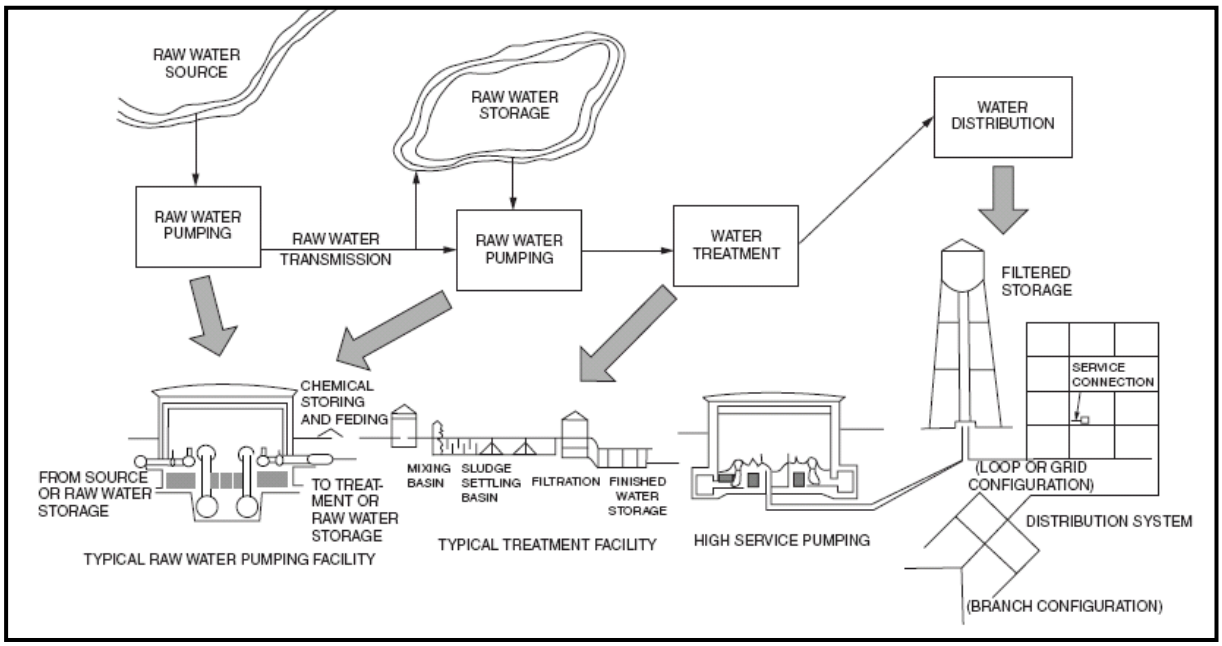

Figura 2.1. *Esquema general de un Sistema de Abastecimiento de Agua (Mays, 2004)*

Esta división de los componentes en subcomponentes y sub-subcomponentes, define una jerarquía de construcción de bloques utilizados para construir el sistema de distribución de agua. Esta relación jerárquica del sistema de distribución de agua, se puede observar en la Figura 2.2.

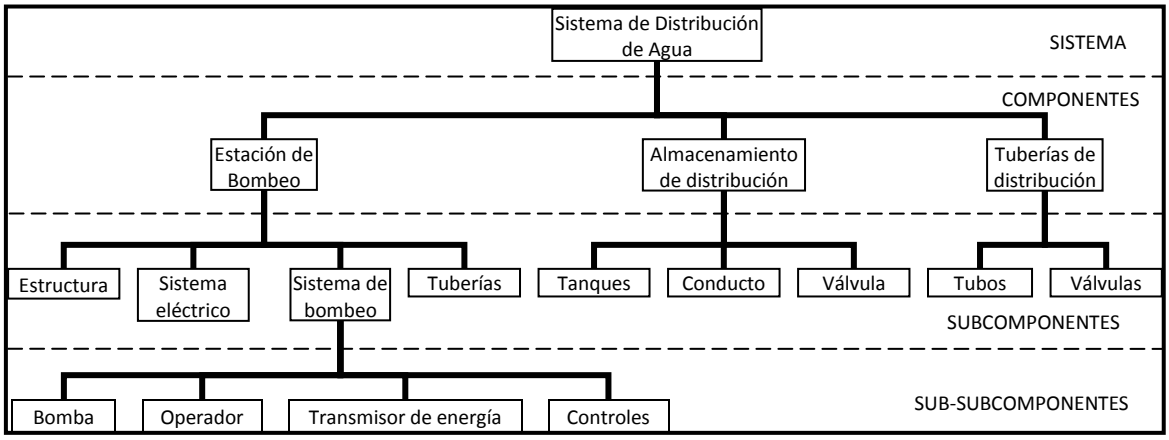

Figura 2.2. *Jerarquía de construcción de bloques en los sistemas de distribución de agua. (Mays, 2004)*

2.2.1. La distribución del agua

El suministro del agua se lleva a cabo mediante la red de distribución, que es la parte del sistema de abastecimiento que transporta el agua directamente hacia los puntos de consumo (edificios, industrias, bocas de riego e incendio, etc.). Está constituida por todo un conjunto de tuberías, piezas especiales y elementos

dispuestos y ordenados de forma conveniente para garantizar el abastecimiento. Los elementos más característicos de la red de distribución, en su etapa final de abastecimiento a los abonados, son las tuberías, las válvulas, los elementos de medición y control del sistema y los elementos encargados de generar el consumo final del sistema.

Las tuberías son el elemento principal de la red de distribución, así como el más numeroso. La gran mayoría de los problemas de diseño, operación, mantenimiento y rehabilitación se encuentran relacionados directa o indirectamente con tales elementos. Las válvulas, otro de los elementos más numerosos en las redes de distribución se emplean, en su mayoría, para aislar determinados tramos de la red en caso de que sea necesario realizar algún trabajo de rehabilitación, reparación o mantenimiento. No obstante, en la red de distribución también existen otros tipos de válvulas que cumplen funciones diferentes. En cuanto a los elementos de medida y control, su instalación a lo largo de la red de distribución es una buena práctica para tener monitorizado y controlado gran parte del abastecimiento; la finalidad es conocer los valores de las diferentes variables hidráulicas que indican el estado de la red. Dentro de los elementos de medida y control, los más importantes dentro de la red de distribución son los contadores domésticos. Finalmente, los elementos encargados de generar el consumo final del sistema, son toda una serie de componentes que constituyen el tramo final donde termina la red de distribución, los cuales son: desagües, bocas o hidrantes de riego, hidrantes de extinción de incendios y acometidas. En la Figura 2.3 se muestra una representación de una red de distribución.

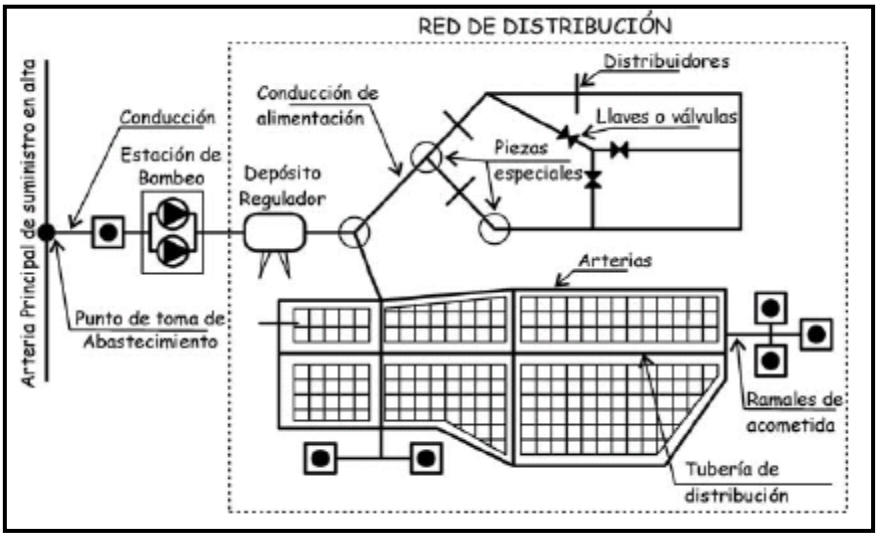

Figura 2.3. *Elementos que componen una red de distribución*

2.3. EL SISTEMA DE ABASTECIMIENTO DE AGUA COMO INFRAESTRUCTURA CRÍTICA

A través de la historia, el agua ha sido un objetivo estratégico en conflictos armados. Estos conflictos han sido, de acuerdo con la clasificación de Gleick (2008), por las siguientes razones:

a) por el control de los recursos hídricos cuando el abastecimiento de agua o el acceso a ella es el origen del problema;

b) por el uso del agua como herramienta militar, debido a que los recursos hídricos o los sistemas de agua son usados por una Nación o Estado como un arma durante una acción militar;

c) por el uso del agua como una herramienta política, donde los recursos hídricos o los propios sistemas de agua son utilizados por una Nación, Estado o ente no estatal como un objetivo político;

d) por actos relacionados con el terrorismo, cuando los recursos hídricos o los sistemas de abastecimiento de agua, o bien, son objetivos de ataque, o son instrumentos de violencia o de coerción de actores no estatales;

e) porque se considera el agua como un blanco militar, ya que los sistemas de recursos hídricos o los sistemas de abastecimiento de agua son blancos de acciones militares de Naciones o Estados; y

f) por controversias Estatales y no Estatales; en las que los recursos hídricos o los sistemas de abastecimiento son un motivo importante de conflicto en el contexto del desarrollo económico y social de una nación.

En lo que se refiere específicamente a la infraestructura de abastecimiento de agua, ya en 1941 el entonces director del *FBI (Federal Bureau of Investigation)*, de los Estados Unidos, J. Edgar Hoover escribió: "*Se ha reconocido desde hace mucho que entre los servicios públicos, los sistemas de suministro de agua son un punto particularmente vulnerable para el ataque de agentes extranjeros, debido a la posición estratégica que ocupan manteniendo en marcha las ruedas de la industria y preservando la salud y la moral del pueblo americano".*

En relación con la cita anterior, una vez establecida la *PCCIP* en 1996, la Agencia de Protección Ambiental de los Estados Unidos (*Environmental Protection Agency of the USA-US-EPA*) ha sido la agencia que, hasta la fecha actual, se encarga de centralizar todas las estrategias de protección sobre los servicios de agua.

Pérez *et al.* (2008) señalan que el concepto de servicio estratégico referido al abastecimiento de agua prevalece en prácticamente todos los países. Como muestra, el Consejo Europeo aprobó, a propuesta de la Comisión, la iniciativa del Programa Europeo para la Protección de Infraestructuras Críticas (*European Programme for Critical Infrastructure Protection-EPCIP*) en diciembre de 2004, siendo asimismo el abastecimiento de agua una de las infraestructuras incluidas en la iniciativa. Posteriormente, en noviembre de 2007, el Gobierno español

aprobó la creación del Centro Nacional de Protección de Infraestructuras Críticas (*CNPIC*), que se ocupa de un catálogo de más de 4000 instalaciones o sistemas considerados como tales, aunque la lista es secreta debido a la lógica discreción que rige las actuaciones en materia de seguridad, es obvio suponer que en la lista se incluyen a todos los sistemas de abastecimiento de agua, incluyendo la captación, potabilización y sistema de distribución de las ciudades de cierto tamaño.

Por otro lado, como ya se mencionó, las infraestructuras de abastecimiento de agua están expuestas a daños por causas naturales y por actos humanos malintencionados y, aunque el agua es potabilizada en la planta de tratamiento antes de su abastecimiento, su calidad puede deteriorarse dentro del sistema de distribución y causar enfermedades a la población que la consume. Dentro de las principales causas que resultan en brotes de enfermedades transmitidas por el agua, además de los peligros naturales, están los fallos en el sistema, la entrada de contaminantes en el sistema de distribución, errores de operación y ataques malintencionados.

En la mayoría de los sistemas de abastecimiento de agua el riesgo potencial de los fallos en la calidad del agua potable nunca es cero, ya que los fallos pueden suceder en diferentes maneras. Por lo tanto, el diseño y mantenimiento de sistemas robustos son importantes para garantizar agua segura incluso cuando múltiples fallos ocurran simultáneamente. En relación con esto último, el concepto de "agua potable segura" significa que la gente no debe morir o enfermarse gravemente por usarla o beberla. Sin embargo, no significa que no exista un riesgo asociado a la misma. La seguridad no es una condición absoluta, sino más bien relativa y en la práctica, la premisa de que el agua es segura, significa que el agua está a un nivel de riesgo tan bajo que los consumidores no tienen que preocuparse por contraer una enfermedad a través de ella (Hrudey y Krewski, 1995 citado por Lee, 2006).

2.3.1. Peligros y amenazas en los sistemas de abastecimiento de agua

De forma general, una "amenaza" es un peligro latente asociado a un fenómeno físico, ya sea de origen natural, tecnológico o antrópico, el cual puede manifestarse en un sitio específico y en un tiempo determinado produciendo efectos adversos en las personas, los bienes, los servicios y el medio ambiente. Una amenaza se expresa como la probabilidad de ocurrencia de un evento con una cierta intensidad en un sitio determinado y en un período de tiempo específico.

Por otro lado, una amenaza o un peligro es un evento anormal o extremo, ya sea en el entorno natural o en el creado por el hombre, que tiene efectos adversos en los sistemas de ingeniería, e incluso en la vida humana (Coburn *et al., 1994* citado por Li, 2007). Sin embargo, en los sistemas de abastecimiento de agua, los peligros o amenazas no necesariamente tienen eventos de tipo anormal o extremo, ya que como señala Li (2007), el

riesgo puede ser alto incluso si el peligro es moderado debido a las altas vulnerabilidades de los componentes del sistema.

Las amenazas a los sistemas de abastecimiento de agua incluyen peligros naturales y amenazas relacionadas con actos humanos. Existen diferencias sensibles entre uno u otro tipo de causas, puesto que, como indica Matalas (2005), citado por Pérez (2008), las causas naturales pueden afectar a una porción importante del sistema, pero la extensión e intensidad del daño está íntimamente ligada a la probabilidad de ocurrencia del fenómeno que conduce al daño, lo que dicho en otras palabras, hace que el fenómeno sea dependiente de situaciones pasadas que permitan valorar la probabilidad del suceso (Pérez *et al.* 2008). Los peligros naturales se han estudiado extensivamente por lo que existe suficiente información disponible para poder calcular la probabilidad de ocurrencia con cierto grado de fiabilidad, así como calcular la probabilidad de ocurrencia y valorar el daño producido, por lo que se podrá tener una buena estimación del riesgo.

En cuanto a las amenazas por causas humanas, estas envuelven incertidumbres inherentes y en el caso de los daños producidos de forma deliberada, no existe la posibilidad de establecer un patrón probabilístico. Los motivos por los cuales no se puede establecer un patrón de comportamiento al respecto, son: a) pese a la repercusión de los actos deliberados (entre ellos los actos terroristas), en los medios y en la sociedad, el impacto real es muy inferior a su impacto psicológico, ya que el número de víctimas que han dejado queda muy por debajo de las que producen los accidentes de tráfico o el cáncer, por ejemplo; y b) los ataques deliberados constituyen un conjunto de eventos independientes entre sí, más condicionados por la coyuntura socio-política y por la oportunidad que por la cronología previa de otros ataques (Pérez *et al.* 2008).

Los peligros y amenazas que son frecuentemente mencionados y sus posibles consecuencias en un sistema de abastecimiento se agrupan, a manera de resumen, en la Tabla 2.3.

Tabla 2.3. *Peligros y amenazas en un sistema de abastecimiento de agua*

Tipo de Amenazas o Peligros		**Consecuencias**
Peligros Naturales	Terremoto	• Rotura de tuberías • Pérdida de presión • Colapso de la estructura
	Inundación	• Pérdidas de la planta de tratamiento • Contaminación del sistema de distribución
	Sequía	• Escasez de agua • Exceso de polvo • Problemas de la calidad del agua
	Viento (huracanes, tornados)	• Problemas inducidos por las inundaciones • Daños en la estructura • Pérdida de energía
	Clima severo (frío, calor, nieve, hielo)	• Tuberías heladas • Interrupciones y pérdidas (fugas)

			• Aumento de la demanda del agua
Amenazas por causa humana	Ataques (terrorismo, vandalismo, sabotaje)	Físicos	• Destrucción física de los bienes del sistema o interrupción del abastecimiento de agua. • La pérdida de presión del agua compromete las capacidades de los servicios contra incendios y podría llevar a una posible acumulación de bacterias en el sistema • Potencial para crear un fenómeno transitorio mediante la apertura y cierre de las válvulas de control más importantes y encendido y apagado muy rápido de las bombas que pudiera provocar roturas simultáneas de la tubería.
		Cibernéticos	• Interrupción física de la red de Supervisión, Control y Adquisición de Datos *(Supervisory Control and Data Acquisition-SCADA)* • Ataques en el sistema de control central para provocar fallos simultáneos • Ataques usando virus y gusanos informáticos • Cambiar u ocultar datos para neutralizar la cloración o no añadir desinfectantes permitiendo la aparición de microbios
		Químicos y Biológicos	• Afectación grave a la calidad del agua • Problemas de salud y muertes entre los usuarios del sistema • Pánico • Pérdida de la confianza en los consumidores
	Accidentes (transportación, construcción, liberación de materiales peligrosos, incendios)		• Contaminación de fuentes de agua • Pérdida de instalaciones y estructuras vitales • Roturas e interrupciones del suministro
	Fallos (del sistema, de energía)		• Pérdida de la capacidad y funcionalidad del sistema. • Pérdida del control del sistema.
	Amenazas psicológicas (desinformación, falsas llamadas de emergencia)		• Pérdida de la confianza pública. • Incitación al pánico

Fuente: Mays (2004) y Grigg (2003)

2.3.1.1. Peligros Naturales

Dentro de los peligros que provienen de fenómenos físicos originados por la naturaleza y sus elementos, los terremotos, las inundaciones y las sequías son los eventos más importantes que pueden causar grandes daños y pérdidas en el servicio de abastecimiento.

Terremotos

Los principales peligros de un terremoto incluyen fallos en el terreno debido a la licuefacción o deslizamiento de tierras. Además, producen asentamientos, que traen efectos sobre las instalaciones y el equipo por el temblor de la tierra y ruptura superficial de la falla. Los sistemas de abastecimiento resultan muy dañados por los terremotos, ya que la mayoría de los perjuicios son a las tuberías de transmisión y distribución en áreas que experimentaron deformación en el terreno, como resultado de licuefacción o ruptura de la falla. Las tuberías

fabricadas de materiales quebradizos como por ejemplo, asbestos, cemento o concreto han sufrido más averías que las tuberías soldadas o de acero dúctil.

En un terremoto, las instalaciones de la potabilizadora de agua también experimentan daños, pero son mucho menores que el daño producido a las tuberías. Sin embargo, el potencial para liberar gas clorhídrico puede ser una importante preocupación de seguridad en las plantas de tratamiento. Los sistemas de abastecimiento de agua son esenciales cuando ocurren incendios a causa de terremotos, porque pueden ser necesarias grandes cantidades de agua para extinguirlos. Por ejemplo, tanto el terremoto de San Francisco en 1906, como el terremoto de Loma Prieta de 1989, en los Estados Unidos, dañaron el sistema de agua municipal, afectando los esfuerzos de lucha contra incendios. En relación con esto, uno de los aspectos más importantes a considerar, en cuanto a las características de los sistemas de abastecimiento, es la respuesta de las paredes de las tuberías de gran diámetro, a la propagación de las ondas sísmicas. Los métodos para mejorar la caracterización de la interacción suelo-tubería son necesarios, junto con la validación de los ensayos a gran escala (NESS, 2003).

Inundaciones

Las inundaciones son fenómenos naturales que tienen como agentes a la lluvia o el crecimiento anormal de la marea, provocando el aumento de los niveles de los ríos y los cuerpos de agua. En general, los daños ocasionados por inundaciones a los sistemas de agua potable se pueden asociar a la destrucción total o parcial de captaciones localizadas en ríos o barrancos, azolve y colmatación de componentes por arrastre de sedimentos, pérdida de captación por cambio del cauce del río, rotura de tuberías expuestas en la zona de captación, rotura de tuberías de distribución y conexiones en las áreas costeras debido al agresión de marejadas y en áreas próximas a cauces , contaminación del agua en las cuencas, daño de equipos de bombeo al entrar en contacto con el agua, colateralmente hay impactos indirectos como la suspensión de energía eléctrica y comunicaciones.

Sequías

Las sequías son períodos secos prolongados en ciclos climáticos naturales que se originan en un conjunto complejo de elementos meteorológicos que actúan en el suelo y en la atmósfera. Esto determina la alteración en el balance hídrico de una zona o localidad, haciendo que los recursos hídricos sean insuficientes para satisfacer los requerimientos de consumo para riego, generación de energía eléctrica y (lo más importante) para agua potable. Por tanto, esta escasez adquiere diferentes matices en función del clima y de las posibilidades de regulación natural, de la fase del ciclo hidrológico en estudio, de la infraestructura hidráulica o de la gestión del medio. Los daños que provocan son difícilmente cuantificables ya que no son, generalmente, estructurales y aparecen en diferentes sectores. Debido a la diversidad de los impactos y a la imprecisión en el tiempo de inicio y fin del fenómeno, la concepción de las sequías se plantea con términos poco precisos, los cuales son adaptados a las necesidades de los diferentes gestores y planificadores. Los efectos esperados en los

sistemas de abastecimiento de agua potable son: la pérdida o disminución del caudal de agua superficial y/o subterránea, el racionamiento y/o suspensión del servicio de abastecimiento, el incremento en los costos del agua debido a que el usuario tiene que comprarla ya sea embotellada o en camiones tanque, con la consecuente pérdida de su calidad.

La experiencia de los servicios de abastecimiento de agua en cuanto a inundaciones y terremotos es extensa, y la mayoría de las consecuencias han sido identificadas y estudiadas. El viento es un peligro común, pero el daño más importante al servicio debido al viento, son las inundaciones provocadas por este. Otros desastres naturales, como el clima extremo y los rayos o relámpagos de las tormentas también amenazan al sistema, pero no tan significantemente como un terremoto.

2.3.1.2. Amenazas intencionales

En Grigg (2003), se clasifica a las amenazas por causa humana en cuatro grupos que son: accidentes, fallos amenazas psicológicas y ataques.

Accidentes

Los accidentes envuelven acciones no intencionales contra el servicio, pudiendo causar importantes daños o desperfectos. Por ejemplo, la contaminación producida por un accidente en una planta nuclear; un accidente de construcción que deshabilite un embalse, una tubería principal, o una planta de tratamiento; un accidente en el transporte de sustancias como el petróleo que introduzca un vertido que contamine una fuente de agua.

Fallos

En cuanto a los fallos en un sistema de abastecimiento de agua se incluyen, entre otros: roturas, fallos en el propio sistema y fallos en el suministro de energía o en el sistema de cómputo. Los fallos son amenazas de origen humano en el sentido de que estos se deben a una disminución del rendimiento deseado de un componente o sistema.

Amenazas psicológicas

Las amenazas psicológicas si bien no son la principal preocupación, deben ser controladas antes de provocar el caos en la población.

Ataques

Los ataques a los sistemas de abastecimiento son las amenazas de mayor importancia y preocupación, ya que pueden ser causados por actos de terrorismo, vandalismo o sabotaje. Los ataques incluyen el uso de varios grados de violencia, fuerza, terror, intimidación o medios tecnológicos para amenazar o dañar ilícitamente al

sistema de agua. La protección básica contra dichos ataques (o amenazas de ataques) es el sistema de seguridad; esto incluye, la evaluación del peligro, la evaluación de la vulnerabilidad, plantear las medidas de mitigación, la planificación de las acciones de respuesta y las comunicaciones en caso de crisis. Por lo tanto, las claves de la seguridad son la detección, el retraso y la respuesta.

Los ataques a los sistemas de agua se clasifican en tres tipos: **ataques físicos, ataques cibernéticos** y **ataques químicos y biológicos** (Haimes, 2006; Quiao, 2005; Mays, 2004; Grigg, 2003; Li, 2007). Cada escenario de ataque tiene características únicas y requiere de una evaluación de la vulnerabilidad y de esfuerzos de mitigación diferentes. Las consecuencias potenciales de esos tipos de ataques no son necesariamente mutuamente excluyentes, ya que la destrucción física de uno o más componentes podría resultar en una catástrofe

Ataques Físicos

Son blancos de los ataques físicos: las tuberías, las estaciones de bombeo, tanques de almacenamiento y otras instalaciones, lo que alteraría el diseño de la red de distribución por la destrucción o degradación de una parte de la misma (Quiao, 2005). Los escenarios de ataques físicos que destruyen o alteran los componentes de un sistema de agua son más probables en comparación con otros, porque para su realización se requiere un mínimo nivel de conocimiento ya sea para el uso de materiales explosivos o herramientas.

Ataques Cibernéticos

Los avances en las tecnologías de cómputo, especialmente durante la década de los 90 han ayudado a los servicios de abastecimiento de agua a automatizar varios aspectos de los mismos como el abastecimiento, la distribución y los sistemas del manejo de la información (Panguluri *et al.* 2004). Esto ha llevado a que los sistemas estén cada vez más expuestos a las amenazas.

Un ataque cibernético ha sido definido como un ataque de ordenador a ordenador que mina la confidencialidad, integridad o disponibilidad del ordenador o de la información contenida en él (O'Shea, 2003 citado por Panguluri *et al.,* 2004). La definición anterior es limitada, pues excluye a los ataques hechos directamente por algún individuo no autorizado que pudiera tener acceso a la máquina. La protección contra los modos de ataque más obvios es muy importante, ya que estos pueden ser tan simples como que un individuo use el teclado de un equipo aparentemente sin uso, pero encendido y conectado al ordenador principal, o que inserte un disco con un determinado virus incrustado que lance un ataque directo al sistema principal (Panguluri *et al.* 2004)

La trascendencia de la infraestructura de los sistemas informáticos de un sistema de abastecimiento de agua, de tamaño medio a grande, por lo general, incluye a otros sistemas como al Sistema Financiero, al Sistema de

Recursos Humanos, al Sistema de Gestión de Información de Laboratorio, al *SCADA*, al Sistema Computarizado de Mantenimiento y Gestión, etc. Dichos sistemas son considerados una parte de la infraestructura de Tecnología de la Información (*Information Tecnology-IT*) de los servicios de abastecimiento. Los ciber-ataques a la infraestructura de *IT* pueden causar importantes daños financieros e interrupciones de las operaciones internas del servicio, pero esos daños no se presentan inmediatamente en el abastecimiento de agua. Sin embargo, los ataques al sistema *SCADA* podrían tener un grave impacto inmediato en el abastecimiento de agua. Asimismo, una prolongada interrupción de la infraestructura de la *IT* podría también provocar complicaciones en el abastecimiento de agua

Los ataques cibernéticos son principalmente al *SCADA*, ya que este permite a los operadores del servicio supervisar y controlar los procesos entre diversos sitios remotos (Quiao, 2005), asimismo, los ataques son a la información y al sistema de gestión de la infraestructura del agua, para provocar pérdida de datos, dañar la información y los equipos informáticos.

Evaluaciones realizadas por la *US-EPA* a los sistemas *SCADA,* de un determinado número de empresas de agua de los Estados Unidos, señalaron una lista de sus vulnerabilidades más importantes (Panguluri *et al.,* 2004), que son las siguientes:

1. El operador de la estación inicia sesión en el sistema y permanece conectado incluso cuando no está presente en la estación de trabajo, lo que hace inútil el proceso de autentificación.
2. El acceso físico al equipo que opera al sistema *SCADA,* es relativamente fácil.
3. Acceso no protegido a la red de *SCADA* desde lugares remotos a través de *Digital Subscriber Lines* (*DSL*) y /o módem de líneas *dial-up.*
4. Puntos inseguros de acceso inalámbrico en la red.
5. Muchas redes del *SCADA* conectadas directa o indirectamente a *Internet*.
6. No existe un cortafuegos instalado o la configuración del mismo es débil o no está verificada.
7. No se da seguimiento al sistema de registros de eventos.
8. No se utilizan los sistemas de detección de intrusos.
9. No se aplican frecuentemente parches de *software* de seguridad a los sistemas operativo y *SCADA*.
10. La configuración de la red y/o *router* es insegura; no se han cambiado las contraseñas predeterminadas por los fabricantes

Diversas metodologías y herramientas de evaluación de la vulnerabilidad han sido desarrolladas para determinar las debilidades potenciales en la infraestructura del sistema de cómputo del servicio de abastecimiento de agua. Esas metodologías ayudan a evaluar la susceptibilidad para potenciales ataques e identificar acciones correctivas que puedan mitigar el riesgo y la gravedad de las consecuencias de tales

ataques (Panguluri *et al.,* 2004). Esa evaluación de la vulnerabilidad debe cubrir tanto la infraestructura de *IT* como del sistema de *SCADA*

Al respecto, la Metodología de Evaluación del Riesgo para el Agua *(Risk Assessment Methodology for Water-RAM-W)*, fue desarrollado específicamente para la industria del agua por la *American Waterworks Association Research Foundation* (*AWWARF*) y los Laboratorios Nacionales *Sandia*. Uno de los componentes del proceso de la *RAM-W* es el "árbol de fallos" del *SCADA* el cual, es una representación gráfica que muestra cada punto de vulnerabilidad que puede ser usado por un ciber-atacante para destruir y/o deshabilitar los componentes críticos del sistema *SCADA* o interferir con la operación normal del servicio de abstecimiento (Panguluri *et al.* 2004). Los árboles de fallos del *SCADA* son usados también, junto con los cálculos del riesgo, para categorizar y seleccionar las acciones de mejoras en lo que a seguridad se refiere. Por otro lado, la evaluación de la vulnerabilidad del sistema de *IT* no se aborda al mismo nivel como la evaluación del *SCADA* por medio de la *RAM-W*. Sin embargo, es esencial asegurar a los sistemas de *IT,* junto con los sistemas *SCADA,* especialmente si están conectados entre sí, ya que las debilidades en los sistemas de *IT* pueden ser utilizados para deshabilitar o interrumpir las operaciones del sistema *SCADA.*

Schneier (1999) desarrolló una metodología formal de "árbol de ataques", muy similar al análisis de árbol de fallos utilizada por *RAM-W.* El objetivo es analizar la seguridad de sistemas y subsistemas basado en diferentes ataques. Los ataques contra un sistema son representados en una estructura de árbol, teniendo como objetivo el "nodo raíz" y las diferentes maneras de llegar a él, que son los "nodos hojas". Esta metodología propone otra manera de abordar el tema de la seguridad, ya que parte de la idea de que la seguridad no es un producto, sino más bien un proceso, y los árboles de ataque son la base para entender tal proceso.

Asimismo*, DIONIX* y *PlantData Technologies* desarrollaron una metodología denominada "Llamadas de Defensa". En esta metodología la red de *IT* y la seguridad del sistema *SCADA* son desplegadas en varias capas. Se considera que la configuración adecuada de las "llamadas" debe ser flexible y el empleo de un conjunto de capas integrado y coordinado es la clave en el diseño de una guía de seguridad (Panguluri *et al.* 2004).

Otro método de evaluación de la vulnerabilidad recomienda la evaluación de los cuatro niveles del sistema *SCADA* (Munshi, 2003 citado por Panguluri *et al.,* 2004). El Nivel uno de evaluación controla las vulnerabilidades del equipo de campo, como el *PLCs, RTUs* y caudalímetros. El Nivel dos de evaluación determina las vulnerabilidades de los medios de comunicación como las Redes de Área Local *(Local Area Networks-LAN*), *dial-up*, y el DSL *(Digital Subscriber Line-DSL)*. Por último, el nivel tres de evaluación examina el subsistema *SCADA host.* Y por último, el Nivel cuatro de evaluación observa a toda la empresa para encontrar debilidades.

El objetivo de tales metodologías es conducir al desarrollo, documentación y refuerzo de una seguridad efectiva, la cual es única para cada sistema, ya que una misma medida para todos no sería eficaz. Además, aunque se invierta una gran cantidad de tiempo y dinero en evaluar la vulnerabilidad de un sistema, a menudo es casi imposible garantizar todas las vulnerabilidades en un sistema. Por lo tanto, es importante determinar las consecuencias de tipos específicos de ciber-amenazas y asegurar el sistema para esas amenazas específicas.

Ataques químicos y biológicos

Los ataques químicos y biológicos generalmente no afectan la estructura de la red de distribución, pero amenazan la vida humana propagándose a través del agua. Sin embargo, las estrategias que reducen la vulnerabilidad para un tipo de ataque pueden incrementar la vulnerabilidad de otro. Por ejemplo, el aumento de la redundancia para disminuir las consecuencias de un ataque físico podría aumentar la conectividad entre los elementos de la red de distribución de agua y el riesgo de contaminación intencional (Quiao, 2005).

La contaminación química o biológica en los sistemas de abastecimiento de agua es considerada como la amenaza potencial más grave. Los agentes biológicos pueden ser dispersados a través del sistema de distribución y llegar hasta los consumidores ocasionando daños en su salud e incluso la muerte, ya que algunos contaminantes no son detectados hasta que se presentan una serie de síntomas. Incluso sin que haya impactos severos en la salud, el hecho de saber que ha sido violada la seguridad del sistema, trae como consecuencia la pérdida de confianza de los usuarios en cuanto al servicio.

Existen diversas substancias que pueden contaminar el agua. Sin embargo, son de especial interés aquellos contaminantes que no son fácilmente detectados por el consumidor, los cuales pueden causar un cierto grado de morbilidad o mortalidad; así como también, que sean agentes capaces de originar una contaminación de un gran volumen de agua en comparación con el suministro en un área pequeña. Cabe diferenciar agentes que ocasionan un efecto agudo y agentes de efecto crónico. Los primeros producen daños a corto plazo y los segundos a largo plazo. Los contaminantes que producen una respuesta aguda son de mayor preocupación debido a que presentan las características necesarias para ser utilizados como armas en un ataque, es decir, que presenta alta solubilidad, dividido o suspendido en el agua, es incoloro, inodoro, insípido, altamente tóxico, resistente a desinfectantes en concentraciones normales, resistente a la ebullición durante uno a tres minutos, es de fácil adquisición y transporte y no requiere de equipos sofisticados para su uso.

Respecto a los agentes químicos contaminantes, debido al desarrollo de la industria química, un gran número de ellos presentan características altamente peligrosas que así como pueden amenazar y dañar el medioambiente, también son considerados "armas químicas de guerra", y son utilizados para amenazar la seguridad y la salud de una población. Estos agentes son clasificados de acuerdo con su efecto fisiológico en "agentes mortales", que son aquellos que fueron creados para causar un gran número de muertes. Estos a su

vez se dividen en cuatro tipos: agentes neurotóxicos, agentes vesicantes, agentes asfixiantes y agentes sanguíneos. Otros químicos denominados "agentes de hostigamiento" no necesariamente causan muertes, pero sí provocan incapacitación de distintas maneras. Entre estos agentes se encuentran los siguientes: lacrimógenos, vomitivos, depresores, alucinógenos y estimulantes (Chastain, 2004).

En la Tabla 2.4., se presentan algunos de los agentes y venenos químicos industriales que son más factibles de causar impactos en un sistema de abastecimiento.

Tabla 2.4. *Eficacia potencial de productos químicos en sistemas de abastecimiento de agua*

Agentes químicos (mg/L *a menos que se indique lo contrario*)	**Concentración Aguda 0.5 L**	Directrices recomendadas	
		5 L/day	**15 L/day**
Agentes químicos de guerra:			
Cianuro de Hidrógeno	25	6.0	2.0
Tabun (GA, μg/L)	50	70.0	22.5
Sarin (GB, μg/L)	50	13.8	4.6
Soman (GD, μg/L)	50	6.0	2.0
VX (μg/L)	50	7.5	2.5
Lewisite (fracción de arsénico)	100-130	80.0	27.0
Sulfuro de Mostaza (μg/L)		140.0	47.0
Bencilato de 3-quinuclidinilo (BZ, µg/L)		7.0	2.3
Dietielamida de Ácido Lisérgico	0.050		
Venenos químicos Industriales			
Cianuros	25	6.0	2.0
Arsénico	100-130	80.0	27.0
Fluoruro	3000		
Cadmio	15		
Mercurio	75-300		
Dieldrina	5000		
Fluoroacetato de Sodim		No proporcionado	
Parathion		No proporcionado	

Fuente: Mays (2004)

En cuanto a las amenazas biológicas, existe una gran variedad de agentes patógenos clasificados principalmente en: bacterias *(rickettsias)*, protozoos, virus y toxinas (tales como biotoxina botulínica, aflatoxina, ricina y otras) que son potencialmente resistentes a la desinfección por cloración, además de ser relativamente estables en agua durante largos períodos de tiempo. Aunque el agua proporciona dilución, una partícula flotante de cualquier tamaño podría ser usada para dispersar patógenos en los sistemas de agua potable. Otros sistemas más sofisticados como las microcápsulas también podrían ser usados para dispersar patógenos en los sistemas de abastecimiento de agua (Mays, 2004).

El Centro para el Control y Prevención de Enfermedades de los Estados Unidos, *(Center for Disease Control and Prevention-CDC)*, divide a los agentes biológicos en tres clases: A, B y C. Esta clasificación está relacionada con su peligrosidad y su probabilidad de uso, siendo los más dañinos los de clase A. En la Tabla 2.5 se detalla cada una de las clases y los agentes que incluyen.

Tabla 2.5. *Clasificación de agentes biológicos, según el CDC*

Categoría A
Agentes de alta prioridad, incluyen organismos que suponen un riesgo para la seguridad nacional debido a que: • pueden ser fácilmente diseminados o transmitidos de persona a persona, • causan altas tasas de mortalidad, y tienen el potencial de provocar un gran impacto en la salud pública, • pueden causar pánico y disturbios sociales, • requieren de acciones especiales para lograr que el sistema de salud pública esté preparado para enfrentarlos. Agentes (Enfermedad/agente): • Carbunco (Antrax) *(Bacillus anthracis)* • Botulismo *(Toxina de Clostridium botulism)* • Peste *(Yersinia pestis)* • Viruela *(variola mayor)* • Tularemia *(Francisella tularensis)* • Fiebre hemorrágica viral *(Filovirus*, p.ej. Ebola*; Arenavirus,* p.ej. virus Lassa y Machupo*; Bunyavirus, Flavivirus)*
Categoría B
Agentes de segunda prioridad, se incluyen aquellos que: • son moderadamente fáciles de dispersar, • causan moderadas tasas de morbilidad y bajas tasas de mortalidad, • requieren mejoras específicas en la capacidad de diagnóstico del *CDC* y sistemas mejorados para la vigilancia de enfermedades. Agentes (Enfermedad/Agente): • Brucelosis *(especies de Brucella)* • Toxina Epsilon de *Clostridium perfringens* • Amenazas para la seguridad de los alimentos *(especies de Salmonella, E. Coli O157:H7, Shigella)* • Muermo *(Burkholderia pseudomallei)* • Psitacosis *(Chlamydia psittaci)* • Fiebre Q *(Coxiella burnetii)* • Toxina de ricino *(Ricinus communis*-semillas de ricino) • Enterotoxina estafilocócica B • Tifus *(Rickettsia prowazekii)* • Encefalitis viral *(alfavirus,* p.ej., la encefalitis equina venezolana, la encefalitis equina oriental, la encefalitis equina occidental*)* • Amenazas contra la seguridad del agua *(Vibrio cholerae, Cryptosporidium parvum)*
Categoría C
Agentes que tienen la tercera más alta prioridad, incluyen los patógenos emergentes que pueden ser manipulados para su diseminación masiva en el futuro, debido a su: • disponibilidad, • facilidad de producción y dispersión, • potencial de causar altas tasas de morbilidad y mortalidad y un gran impacto en la salud pública.

Agentes (Enfermedad/Agente):

- Enfermedades infecciosas emergentes como el virus *Nipah* y el *Hantavirus*
- Tuberculosis multiresistente
- Virus de la encefalitis transmitida por garrapatas
- Virus de la fiebre hemorrágica transmitida por las garrapatas
- Fiebre amarilla

Fuente: Centros para el Control y la Prevención de Enfermedades (*CDC-Centers for Desease Control and Prevention)*

Se puede decir que, de acuerdo con la clasificación anterior, los agentes de mayor interés corresponden a los considerados dentro de la Categoría B, ya que incluyen principalmente a los patógenos transmitidos por agua y alimentos.

A modo de resumen, en la Tabla 2.6, se presenta información acerca de los agentes anteriormente citados y otros relevantes. Aunque se conoce mucho sobre ellos, todavía existe la necesidad de investigar más para caracterizar completamente su impacto, su estabilidad y su tolerancia al cloro.

Tabla 2.6. *Amenaza potencial de los agentes de armas biológicas: Resumen*

Agente	Tipo	Amenaza en agua	Estabilidad en agua	Tolerancia al Cloro
Antrax	Bacteria	Si	*2 años* (esporas)	Resistente (esporas)
Brucelosis	Bacteria	Probable	*20-72* días	Desconocida
C. Perfringens	Bacteria	Probable	Común en alcantarillado	Resistente
Tularemia	Bacteria	Si	Hasta 90 días	Desactivada, 1 ppm, 5 min.
Glanders	Bacteria	Poco probable	*Hasta 30* días	Desconocida
Meliodosis	Bacteria	Poco probable	Desconocido	Desconocida
Shigellosis	Bacteria	Si	*2-3* días	Desactivada, 0.05 ppm, 10 min.
Cólera	Bacteria	Si	Buena supervivencia	Fácil eliminar
Salmonella	Bacteria	Si	8 días, agua dulce	Desactivada
Peste	Bacteria	Si	16 días	Desconocida
Fiebre Q	Rickettsia	Posible	Desconocida	Desconocida
Tifus	Rickettsia	Poco probable	Desconocida	Desconocida
Psitacosis	Rickettsia	Posible	*12-24* horas, agua marina	Desconocida
Encefalomielitis	Virus	Poco probable	Desconocida	Desconocida
Fiebre hemorrágica	Virus	Poco probable	Desconocida	Desconocida
Viruela	Virus	Posible	Desconocida	Desconocida
Hepatitis A	Virus	Si	Desconocida	Desactivada, *0.4* ppm, 30 min.
Cryptosporidiosis	Protozoo	Si	Estable durante días o más	Oocistos resistentes
Toxinas botulimicas	Biotoxina	Si	Estable	Desactivada, 6 ppm, 20 min.
T-2 micotoxina	Biotoxina	Si	Estable	Resistente
Aflatoxina	Biotoxina	Si	Probablemente estable	Probablemente tolerante
Ricina	Biotoxina	Si	Desconocida	Resistente a 10 ppm
Enterotoxinas estafilocócicas	Biotoxina	Si	Probablemente estable	Desconocida

Microcistinas	Biotoxina	Si	Probablemente estable	Resistente 100 ppm
Anatoxina A	Biotoxina	Probable	Desactivada en días	Desconocida
Tetrodotoxina	Biotoxina	Si	Desconocida	Desactivada, 50 ppm
Saxitoxina	Biotoxina	Si	Estable	Resistente a 10 ppm

Fuente: (Clark y Deininger, 2000)

2.4. IDEAS PRINCIPALES DEL CAPÍTULO

- Una *infraestructura crítica* abarca una amplia gama de bienes y sistemas de ingeniería. Se define, en diversos planes nacionales de muchos países, como bienes físicos e intangibles, cuya destrucción o interrupción quebrantaría seriamente la salud pública, el orden social y el cumplimiento de las principales responsabilidades de un gobierno. Debido a su importancia, tales infraestructuras han recibido especial atención en los cambios a las políticas de inversión nacional en algunos países, con el fin de crear estrategias para protegerlas.

- Los sistemas de abastecimiento son considerados como una infraestructura crítica. Ocupan una posición estratégica, debido a que mantienen a otras infraestructuras y principalmente, una población.

- Debido a que son un punto particularmente vulnerable, están expuestos tanto a daños por causas naturales, (terremotos, inundaciones, sequías, viento, condiciones climáticas extremas), como por actos humanos (ataques, accidentes, fallos y amenazas psicológicas), ya sean estos últimos malintencionados o no.

- Las causas naturales son posibles de predecir, debido a que están directamente ligadas a sucesos pasadas que permiten evaluar su probabilidad de ocurrencia. Por el contrario, las amenazas por causas humanas, envuelven incertidumbres inherentes y en el caso de los daños producidos de forma deliberada, no existe la posibilidad de establecer un patrón probabilístico.

- Los ataques a los sistemas de abastecimiento de agua son considerados la amenaza de mayor importancia, ya que pueden deberse a terrorismo, vandalismo o sabotaje. De forma general, se clasifican en ataques físicos, ataques cibernéticos y ataques químicos y biológicos. La contaminación química o biológica es considerada como la amenaza potencial más grave.

- La protección básica contra ataques o amenazas de ataques, es un sistema de seguridad; que incluye, la evaluación del peligro, la evaluación de la vulnerabilidad, el diseño de medidas de mitigación, la planificación de las acciones de respuesta y las comunicaciones en caso de crisis. Por lo tanto, las claves de la seguridad son la detección, el retraso y la respuesta.

3. VULNERABILIDAD DE LOS SISTEMAS DE ABASTECIMIENTO DE AGUA

3.1. CONCEPTO DE VULNERABILIDAD

Existen diversas definiciones del término vulnerabilidad, entre las que se citan la de la Real Academia de Lengua Española, que la define como la cualidad de ser vulnerable, es decir, la posibilidad de ser herido o recibir alguna lesión física o moral. Por otro lado, la Estrategia Internacional para la Reducción de Desastres (EIRD), indica que vulnerabilidad son las condiciones determinadas por factores o procesos físicos sociales, económicos y ambientales, que aumentan la susceptibilidad de una comunidad al impacto de amenazas. Otra definición adoptada es la de la Administración Nacional Oceánica y Atmosférica (*National Oceanic and Atmospheric Administration-NOAA*), como la susceptibilidad de los recursos o bienes a los impactos negativos de eventos amenazantes (Thomas, 2006).

En otro contexto, la vulnerabilidad es definida como la debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: es la debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza (ISO27000,).

Tales definiciones han sido extendidas a varias aplicaciones de la ingeniería y sus sistemas; por ejemplo en Corburn *et al.* (1994), citado por Li (2007), la vulnerabilidad es definida como el grado al cual es probable que sea dañada o interrumpida una comunidad, estructura o área geográfica por el impacto del daño de un fenómeno particular con un determinado nivel de severidad.

En el ámbito de los sistemas industriales, Einarsson y Rausand (1998), citados por Li (2007), definen a la vulnerabilidad como las propiedades de un sistema industrial cuyos inmuebles, instalaciones, y equipo de producción, incluyendo sus recursos humanos, organización y todo el software, hardware y mercancía neta, pueden debilitarse o limitar su capacidad para soportar amenazas y sobrevivir a sucesos accidentales los cuales se originan tanto dentro como fuera de las fronteras del sistema

Boudou (2006) señala que es difícil definir vulnerabilidad, y considera que este concepto requiere de otros dos que son el peligro y el azar Con respecto a un riesgo natural, el peligro es un evento potencialmente peligroso, un fenómeno natural o físico es representado, por lo general, por su período de retorno y sus características físicas como por ejemplo su magnitud e intensidad.

Una definición matemática del concepto, es la que se muestra en la fórmula de Doré (2004), citado por Boudou (2006), en la cual la vulnerabilidad es expresada por:

$$V = \frac{PxC}{E} \quad (1)$$

Donde *V* es la vulnerabilidad, *P* es la probabilidad de accidente, *C* representa el nivel de las consecuencias del accidente, y *E* es el estado de preparación de cara al accidente. El producto de *P* por *C*, representa el riesgo y *E* es el estado de preparación contra este riesgo. Por lo tanto, la vulnerabilidad podría ser expresada matemáticamente como la relación de un factor de riesgo y un factor de disponibilidad para hacer frente a este riesgo.

Sin embargo, por su parte, Ezell (2007) asegura que la vulnerabilidad es confundida con el riesgo, ya que señala que diversos autores utilizan términos como "susceptible a", "hacer frente y ocuparse" o simplemente como una "colección de riesgos" para definir el concepto de vulnerabilidad. Asimismo, señala la relación que existe entre vulnerabilidad y riesgo, y concluye que la vulnerabilidad resalta la noción de susceptibilidad a un escenario, mientras que el riesgo se enfoca en la severidad de las consecuencias dentro del contexto de un escenario y que por lo tanto, la vulnerabilidad es una condición del sistema que debe ser evaluada dentro del contexto de un escenario, o bien, una medida de la susceptibilidad frente a un o unos escenarios.

Por su lado, Apostolaskis y Lemon (2005) definen vulnerabilidad como la manifestación de los estados inherentes del sistema (p.ej. físico, técnico, organizacional y cultural) que puede ser explotado por un adversario para averiar o dañar el sistema.

3.2. FRAGILIDAD DE LOS SISTEMAS DE ABASTECIMIENTO DE AGUA

Un accidente, una catástrofe natural o un ataque deliberado pueden poner de manifiesto las debilidades del sistema. Es difícil, tal vez imposible, proteger globalmente el sistema de abastecimiento de agua contra todo tipo de contingencias. Sin embargo, sí es posible analizar y estudiar todas las posibilidades de fallo y sus consecuencias, como medio para prevenir los efectos adversos de cualquier suceso que implique un riesgo para los usuarios, de forma directa o indirecta, tanto si proviene de una causa accidental como deliberada. (Pérez *et al.*, 2008)

En una primera clasificación, los daños en un sistema de abastecimiento de agua pueden incluirse dentro de tres grandes categorías:

1. **Daños físicos en el sistema**, que dejen fuera de servicio la totalidad o parte del mismo. En esta categoría estarían incluidos los daños en las fuentes de abastecimiento, plantas de tratamiento, depósitos de almacenamiento, estaciones de bombeo, y los sistemas de conducción, transporte y distribución.

2. **Daños en los sistemas de información y comunicaciones**, incluyendo elementos de medida y seguridad, líneas de transmisión y todo el *software* y *hardware* empleado para la operación y control del sistema.

3. **Daños a los usuarios del sistema**, apartado en el que se incluyen todos las anomalías en la calidad del agua servida, bien sea por fuentes biológicas, químicas o radiactivas.

3.2.1. Puntos vulnerables en los sistemas de abastecimiento de agua

Todas las infraestructuras críticas, en cierto grado, son vulnerables a cualquier amenaza natural o tecnológica. Con respecto a esto, se han identificado áreas potencialmente vulnerables en un sistema de abastecimiento con diferente grado de vulnerabilidad (Figura 3.1) Cada uno de los componentes y subsistemas que constituyen un sistema de abastecimiento de agua, ofrecen grandes oportunidades tanto para causas naturales como humanas, ya que la mayoría de ellos son espacialmente diversos y accesibles.. Esos subsistemas son:

1. **Fuentes de agua:** ríos, embalses, cuerpos de agua, pozos e infraestructuras.
2. **Plantas de Tratamiento:** que remueven impurezas y agentes nocivos, haciendo el agua apta para el consumo doméstico y otros usos.
3. **Transporte y distribución:** el conjunto de diferentes tuberías y otros elementos que permiten la disponibilidad del agua potable desde las fuentes hasta los grifos de los consumidores, como tuberías de transmisión, canales, bombas, válvulas, etc.
4. **Almacenamientos:** como tanques.
5. **Sistemas de medición, control y comunicación:** todos los dispositivos de medición y monitorización de flujos, presión, calidad del agua y otros parámetros operacionales, incluyendo también elementos de control y software computacional, como el *SCADA.*

Cada uno de esos subsistemas es un punto vulnerable en todo el sistema de abastecimiento de agua, porque un severo desajuste, ruptura o avería de cualquiera de ellos podría deshabilitar el sistema (Pérez *et al.,* 2008). Sin embargo, la red de distribución es la parte más vulnerable de todo el sistema de agua ya que, por ejemplo, cualquier individuo puede forzar la entrada de un contaminante dentro de la red, con una bomba o equipo relativamente pequeño y fácilmente adquirible, desde lugares ventajosamente accesibles y privados como lo

son una casa, un hidrante de extinción de incendios o una estación de bombeo. Los efectos de un suceso tal, dependerán del diseño hidráulico de la red de distribución y de sus condiciones de demanda.

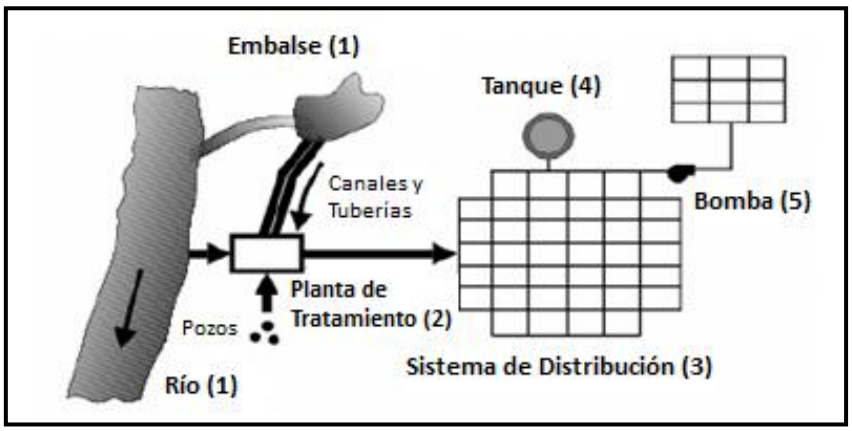

Figura 3.1. *Elementos y puntos vulnerables en un sistema general de abastecimiento de agua (Haestad et al. 2003 citado por Li, 2007)*

3.3. EVALUACIÓN DE LA VULNERABILIDAD

Dentro del contexto de la evaluación de la vulnerabilidad de los sistemas de abastecimiento de agua, la medición de la vulnerabilidad evalúa la resistencia a un ataque, un fallo o un desastre y determina las consecuencias adversas. La identificación de la criticidad, detecta los componentes principales de la red, cuyo deterioro o remoción puede resultar en importantes consecuencias negativas. Finalmente, la mejora de la seguridad, reduce la vulnerabilidad mediante la modificación de la topología del sistema y/o la asignación de recursos de seguridad disponibles.

La Asociación Nacional de Recursos Hídricos (*National Water Resources Association-NWRA*) define la evaluación de la vulnerabilidad como la identificación de las debilidades en cuanto a seguridad se refiere, enfocándose en identificar las amenazas que puedan comprometer la capacidad para proporcionar un servicio.

A su vez, Baker (2003) señala que la evaluación de la vulnerabilidad es un importante subconjunto de los procesos de evaluación del riesgo, incluye la búsqueda en el sistema de elementos y sus modos de fallo, basados en un conjunto dado de amenazas.

En lo que se refiere al proceso de evaluación de la vulnerabilidad en los sistemas de abastecimiento de agua, Mays (2004) señala los siguientes elementos comunes:

- Caracterización del sistema de abastecimiento, incluyendo su misión y objetivos,
- Identificación y priorización de las consecuencias adversas a evitar,
- Determinación de los bienes críticos que pudieran ser objeto de actos malintencionados, que podrían provocar consecuencias no deseadas,
- Evaluación del riesgo (probabilidad cualitativa) de tales actos malintencionados,
- Evaluación de las medidas existentes,
- Análisis de los riesgos actuales y el desarrollo de un plan de prioridades para la reducción de riesgos.

3.3.1. El proceso de medición de la vulnerabilidad

Para el proceso de medición, es necesaria la realización de un análisis de vulnerabilidad previo, para determinar los componentes críticos o débiles de un sistema y las medidas de emergencia y mitigación contra determinadas amenazas. En este proceso existen metodologías para cada amenaza con la finalidad de que los componentes sean reforzados y para que sean capaces de resistir futuros impactos.

En el caso de un sistema de abastecimiento de agua, uno de los aspectos que deberá resolver un análisis de vulnerabilidad es la resistencia de cada uno de sus componentes ante el impacto de las amenazas en una cierta región. El resultado, definirá las medidas de mitigación necesarias y los procedimientos de emergencia o respuesta al impacto (si este se presentara anticipadamente). Por lo tanto, el análisis de vulnerabilidad es la base para el establecimiento de los planes de emergencia y de mitigación necesarios para organizar la preparación, la actuación durante la emergencia y la rehabilitación de los sistemas. Muestra lo que se debe hacer antes, durante y después del impacto de una amenaza. Asimismo, el manejo de datos e información actual y confiable acerca del funcionamiento del sistema es un requerimiento fundamental para la realización de un análisis de vulnerabilidad efectivo. A partir de un análisis estadístico matemático de la información, se pueden obtener los componentes más vulnerables del sistema y conocer el riesgo para una determinada amenaza.

3.3.2. Modelos sobre vulnerabilidad

En los últimos años se han desarrollado varios modelos y metodologías relacionados con la vulnerabilidad de los sistemas de abastecimiento de agua, orientados principalmente a su medición, a la caracterización de la condición de las tuberías y a la rehabilitación del sistema de conducciones. Sin embargo, la complejidad de la medición de la vulnerabilidad se debe a que varía en función del diseño y operación de los sistemas de abastecimiento.

A continuación se detallan algunos de los modelos más importantes, citados por: Pérez *et al.* (2009), Li (2007), Moglia *et al.* (2006) y Mays (2004):

- ***UTILNETS***: Es un Sistema de Apoyo a la Decisión *(Decision Support System - DSS*) para la planificación de la rehabilitación y para la optimización del mantenimiento de las tuberías de un sistema de abastecimiento. El modelo valora la fiabilidad de las tuberías a partir de predicciones estadísticas sobre su vida útil, y sirve para determinar las consecuencias del mantenimiento para optimizar la política de rehabilitación. El modelo ha sido producto de un proyecto europeo de investigación dentro del programa *BRITE-EURAM*, que comenzó aproximadamente en 1993.

- ***KANEW***: El modelo está dirigido a los mismos objetivos de planificación de la rehabilitación del sistema de conducciones, basado en la edad y material de las tuberías. El modelo es producto de un proyecto de investigación de la *AWWARF* de Estados Unidos (1998).

- ***WARP***: Se trata de una aplicación prototipo desarrollada inicialmente sobre *MS-Excel* y posteriormente convertida en un programa independiente. El desarrollo ha sido realizado por el Consejo Nacional de Investigación *(National Research Council - NRC)* de Canada desde 2000. La aplicación *D-WARP* (*Distribution Water mAins Renewal Planner*) permite analizar estadísticas de rotura de tuberías y proyectar futuras tasa de roturas, así como estimar costes y planificar escenarios. El modelo tiene en cuenta factores temporalmente dependientes, tales como la temperatura, humedad del suelo y precipitación.

- ***PARMS***: Acrónimo de *Pipeline Asset and Risk Management System*, es un conjunto de modelos para el apoyo de la gestión de sistemas de abastecimiento, realizado por la *Commonwealth Scientific and Industrial Research Organization (CSIRO)* de Australia a partir de 2002. Utiliza modelos estadísticos para predecir fallos en las tuberías a partir de factores como el tipo de suelo, presión del agua, edad, material y diámetro de la tubería y otros.

- ***CARE-W***: El modelo nace en 2002 de una iniciativa de investigación sobre la rehabilitación de sistemas de tuberías dentro del V Programa Marco Europeo de I+D, con la participación de investigadores de varios países europeos. El modelo platea un enfoque proactivo para el reemplazo de tuberías (mantenimiento preventivo) mediante el análisis de fiabilidad de las tuberías y el planteamiento de una metodología de priorización. Cabe destacar el modelo *CARE-S* para sistemas de saneamiento, que se comienza a realizar en 2003 en el mismo marco.

- ***Metodología para la Medición del Riesgo para los Servicios de Agua.* (*Risk Assessment Methodology for Water Utilities-RAM-W^{SM}*).** Fue desarrollada en colaboración con el Departamento de Energía de los Laboratorios Nacionales *Sandia*, financiado por la *US-EPA*. Esta herramienta compara los componentes del sistema entre sí para determinar cuáles son los más críticos. En este método, la vulnerabilidad es definida como una explotación de la debilidad o deficiencia de seguridad en una instalación. La medición de la vulnerabilidad se realiza sobre la base del análisis de las características de eventos indeseables la accesibilidad de los eventos indeseables, características de la seguridad y de las políticas, medidas de protección, etc. Los resultados de la evaluación, son usados para generar la valoración del riesgo para los componentes del sistema.

- ***Herramienta de Autoevaluación de la Vulnerabilidad* (*Vulnerability Self-Assessment Tool-VAST*).** Esta herramienta fue desarrollada por la Asociación de Agencias Metropolitanas de Alcantarillado *(Association of the Metropolitan Sewerage Agencies-AMSA)* en colaboración con dos empresas de consultoría y con financiamiento de de la *US-EPA*. Este método se basa sobre la evaluación cualitativa del riesgo. La vulnerabilidad es evaluada en una escala cualitativa (por ejemplo, muy alto, alto, moderado y bajo) mediante la consideración de las medidas ya establecidas. Posteriormente, los resultados son usados para generar puntuaciones críticas a partir de las cuales los niveles de riesgo de los activos pueden ser evaluados. Este método se puede utilizar para tomar medidas para los eventos extremos, responde si ocurren los acontecimientos extremos y restablece a las condiciones normales en aquel momento.

- ***Programa de Investigación Conjunto de Evaluación de Vulnerabilidad y Amenazas* (*Threat Ensemble Vulnerability Assessment Research Program – TEVA*).** Este programa del Centro de Investigación de Seguridad Nacional (*National Homeland Security Research Center – NHSRC)*, se formó en el año 2003. Está conformado por un grupo interdisciplinario de científicos pertenecientes a la *US-EPA,* a la Universidad de Cincinnati, a los Laboratorios Nacionales *Sandia* y al Laboratorio Nacional de Argonne. El objetivo del grupo es investigar el potencial de los impactos de eventos de contaminación en los sistemas de abastecimiento de agua y buscar nuevas técnicas y métodos para reducirlos. Se enfocan principalmente en el desarrollo de herramientas informáticas, específicamente en el diseño y evaluación de métodos de mitigación. Dentro de las herramientas desarrolladas por *TEVA,* se encuentra la Herramienta de Optimización para la Ubicación de Sensores (*Sensor Placement Optimization Tool – TEVA-SPOT)* y el *Software* para Detección de Eventos (*CANARY*), que analiza en tiempo real los datos de salida sensores de monitorización (*US-EPA,* 2010).

- La Asociación Nacional Rural del Agua *(National Rural Water Association-NRWA)* y La Asociación de Administradores de Agua Potable del Estado *(Association of State Drinking Water Administrators-*

ASDWA) con asistencia de la *US-EPA*, desarrollaron la Guía de Autoevaluación de la seguridad para sistemas de abastecimiento pequeños de entre 3.300 y 10.000 consumidores. Esta guía proporciona un inventario de los componentes críticos del sistema y cuestiones generales de la evaluación de la vulnerabilidad. Una vez que las cuestiones han sido resueltas, entonces se obtiene la vulnerabilidad de los componentes y se hace la priorización de acciones.

- ***Estudio de la Seguridad Automatizada y Herramienta de Evaluación. (Automated Security Survery & Evaluation Tool-ASSET),*** fue desarrollado por la Asociación de Obras de Agua de Nueva Inglaterra *(New England Water Works Association* (*NEWWA*) en conjunto con la *US-EPA* y otras consultoras privadas. Esta herramienta está dirigida a sistemas que sirven entre 3.300 y 50.000 usuarios (sistemas pequeños y medianos). Este es una herramienta de software-basado, el cual fue implementado en todos los sistemas de abastecimiento de Inglaterra. Consiste en un programa de auto-guía diseñado para ayudar a los sistemas de agua potable en la realización de una medición completa de la vulnerabilidad, así como mejorar la seguridad para un rango de amenazas. La evaluación comprende ocho pasos, que son la recolección de información, la identificación de la misión y los objetivos, determinación de los componentes críticos, evaluación de la amenaza, seguridad física y medidas existentes, análisis del riesgo, plan de prioridades para la reducción del riesgo y un reporte final.

3.4. IDEAS PRINCIPALES DEL CAPÍTULO

- La medición de la vulnerabilidad de los sistemas de abastecimiento de agua evalúa la resistencia a un ataque, un fallo o un desastre y determina las consecuencias adversas. La identificación de la criticidad, detecta los componentes principales de la red, cuyo deterioro o eliminación puede resultar en consecuencias negativas.

- Dentro de un sistema de abastecimiento de agua potable existen áreas potencialmente vulnerables con diferente grado de vulnerabilidad, como son: fuentes de agua, plantas de tratamiento, transporte y distribución, almacenamientos, sistemas de medición, control y comunicación. Sin embargo, la red de distribución es la parte más vulnerable de todo el sistema.

- En los últimos años, se han desarrollado varios modelos y metodologías relacionados con la vulnerabilidad de los sistemas de abastecimiento de agua, orientados principalmente a su medición, a la caracterización de la condición de las tuberías, a la rehabilitación del sistema de conducciones y principalmente, a la detección de eventos de contaminación y a su mitigación.

4. LA SEGURIDAD DE LOS SISTEMAS DE ABASTECIMIENTO DE AGUA

4.1. INTRODUCCIÓN

Debido a la diversidad espacial de los sistemas de abastecimiento de agua, limitar el acceso físico a todos los componentes clave del sistema, además de ser prácticamente imposible, no es suficiente para reducir efectivamente el riesgo asociado a un posible ataque. Por lo que un evento tal puede ocurrir en cualquier momento y lugar en todo el sistema.

En este contexto, diversas investigaciones en el ámbito de la seguridad del abastecimiento de agua potable, se han enfocado en la mejora de los sistemas de monitorización y detección de contaminantes para minimizar los posibles impactos tanto económicos, como en la salud pública. Un enfoque para evitar o mitigar los impactos por contaminación consiste en llevar a cabo la monitorización en el contexto de un Sistema de Alerta Temprana *(Early Warning System-EWS),* cuyo objetivo es identificar, en tiempo y de manera fiable, eventos de contaminación de baja probabilidad y de alto impacto, para permitir una respuesta local eficaz que reduzca o evite completamente los impactos adversos que puedan resultar de un evento de tales características. En este sentido, un EWS debe ser una parte integral de la operación de un sistema de abastecimiento de agua, siendo capaz de detectar no sólo contaminaciones introducidas de forma intencional, sino también contaminación por accidente o como resultado de eventos naturales. Por lo tanto, un sistema de monitorización en línea es considerado un posible medio de protección de un sistema de abastecimiento, contra los impactos de un evento de contaminación. Dentro de las consideraciones para el diseño de un EWS están la localización y la densidad de cobertura de los sensores (Hasan *et al.*, 2004). Estos aspectos están determinados por los resultados previos de la caracterización completa del sistema y de la evaluación de la vulnerabilidad. Sin embargo, la complejidad y naturaleza dinámica de los sistemas de distribución complica la selección de la ubicación de los sensores. Es por ello, que se ha incrementado el interés en el desarrollo de metodologías para hacer frente a dichas amenazas.

La base de un *EWS* es una tecnología de monitorización que pueda detectar o visualizar una variedad de substancias tóxicas o microorganismos infecciosos Un *EWS* eficaz es, en realidad, un sistema integrado para desplegar la tecnología de monitorización, analizar e interpretar los resultados y estos a su vez, utilizarlos para la toma de decisiones y el diseño de un plan acciones de respuesta, que protejan a la salud de la población y a la infraestructura misma. Según Grayman *et al.* (2004), un *EWS* debe incluir un amplio rango de mecanismos

que deben trabajar en conjunto para prevenir la entrada de contaminantes al sistema de distribución de agua; esos componentes son:

- Un mecanismo para detectar la probable presencia de un contaminante en la fuente de agua.
- Un medio de confirmación de la presencia de contaminación, determinando la naturaleza del evento y predecir cuándo afectará a la fuente de agua en los sitios de toma y la intensidad de la contaminación en la toma.
- Un marco institucional generalmente conformado por una unidad central que coordine los esfuerzos asociados con la gestión del evento de contaminación.
- Vínculos de comunicación para la transferencia de información.
- Diversos mecanismos para responder a la presencia de contaminación en la fuente de agua, con el fin de mitigar su impacto en los usuarios.

En cuanto a las características de un *EWS* ideal*,* los requerimientos mínimos que este debe cumplir son los siguientes (Clark *et al.,* 2004):

a) *Tiempo de respuesta rápido.* Advertir con tiempo suficiente para responder al evento de contaminación y prevenir la exposición de los usuarios al contaminante. El tiempo de respuesta de un *EWS*, es el período de tiempo desde el punto al cual el contaminante tiene contacto con el sensor, hasta el punto cuando se produce un reporte y se inicia una respuesta. El tiempo de respuesta requerido dependerá de un cierto número de factores, tales como el punto en el cual el contaminante es introducido dentro del sistema, las características de la planta de tratamiento y los tiempos de retención, y de las propiedades del contaminante. En algunos casos, no es necesario un tiempo de respuesta rápido, mientras que en otros, el tiempo de respuesta deberá ser inmediato.

b) *Automatización.* Idealmente, un *EWS* debe requerir poca o nula intervención de un operador, además de estar funcionando continuamente durante 24 horas. Asimismo, el sistema debe permitir la operación de manera remota tal que, una respuesta en un sensor lejano sería transmitida de forma inmediata a un sistema central de manejo de datos. En el caso de que un contaminante sea detectado, el *EWS* debe inmediatamente de activar una alarma y avisar al operador por vía electrónica, teléfono o fax.

c) *Cobertura de un amplio rango de contaminantes.* Debido a que existe un gran número de agentes que son una amenaza potencial si son introducidos al sistema de abastecimiento, es casi imposible saber anticipación cuál agente contaminante puede ser usado. Por ello, el *EWS* debe tener la capacidad de abarcar un amplio rango de agentes. Sin embargo, puede suceder que los métodos que son efectivos para

un gran número de agentes, no lo son para distinguir entre substancias peligrosas y substancias benignas. Por lo tanto, debe haber un balance entre la necesidad y la especificidad.

d) *Específico para contaminantes de interés.* Un *EWS* debe identificar positivamente agentes específicos que suponen una amenaza para la salud de los usuarios; y a su vez, ser capaz de diferenciar entre esas substancias y otras estrechamente relacionadas, aunque no dañinas.

e) *Identificación del punto en el cual fue introducido el contaminante.*

f) *Sensibilidad Suficiente.* El *EWS* debe ser lo suficientemente sensible para proporcionar un nivel de detección y cuantificación de un agente específico, para el nivel de concentración más bajo que se considere una amenaza para la salud.

g) *Baja ocurrencia de resultados falsos.* Se consideran resultados falsos cuando un *EWS* indica un falso positivo o un falso negativo. En el caso de un falso positivo, el *EWS* señala la presencia de un contaminante que en ese momento no está presente; por el contrario, un falso negativo es cuando no se detecta un contaminante que está presente a niveles que son significativos para la salud. Para ambos errores el porcentaje de ocurrencia debería ser cero, sin embargo, dado que siempre existe la probabilidad de que cualquier tipo de error ocurra, es necesario que se establezca un porcentaje de aceptación para el error, tal que no afecte en la toma de decisiones.

h) *Confiable y Robusto.* El sistema remoto de monitorización debe ser capaz de soportar diversos factores externos. Es decir, el sistema puede verse expuesto a situaciones como: cortes de energía, eventos climáticos extremos, actos de vandalismo o el continuo ensuciamiento de los componentes de los sensores.

i) Dotar de vigilancia continua durante todo el año.

j) Producir resultados con una precisión aceptable.

k) *Mínimo conocimiento y entrenamiento*. El equipo que se utilice en el *EWS*, no debe requerir de un excesivo entrenamiento y conocimiento para la operación, el mantenimiento y la interpretación de los resultados.

l) *Costo asequible.* Que sea asequible para la mayoría de las empresas de abastecimiento de agua.

Sin embargo, un *EWS* con algunas de esas características es poco viable, pero existen algunas tecnologías que pueden ser utilizadas para construir un sistema de alerta temprana que pueda cumplir con ciertos criterios

mínimos, como: dar una rápida respuesta, mantener suficiente sensibilidad y funcionar como un sistema automatizado que permita la monitorización remota. Cualquier sistema de monitorización que no cumpla esos aspectos, no puede ser considerado un *EWS* eficaz.

4.2. TECNOLOGÍAS DE MONITORIZACIÓN

En la actualidad se dispone de monitores de la calidad del agua, incluyendo el análisis físico, químico, radiológico y microbiológico, así como los sistemas de bio-monitorización que utilizan organismos vivos como indicadores de cambios en la calidad del agua.

Algunos de los métodos de monitorización físicos y químicos más comunes, que han sido propuestos para usarse en un *EWS*, incluyen pruebas puntuales simples como turbidez, pH, temperatura, olor, conductividad, oxígeno disuelto; pruebas conjuntas como por ejemplo inmunoensayos para herbicidas y monitorización más avanzada para químicos como fluorescencia para aceites, cromatografía para petróleo y sus componentes, productos químicos orgánicos volátiles y fenoles (Hassan *et al.,* 2004).

Por otro lado, existe un importante esfuerzo de investigación en el desarrollo de sensores más robustos y confiables para ser usados en el sistema de abastecimiento de agua. Un ejemplo es la utilización de la tecnología basada en los satélites, ya que pueden ser útiles para la identificación de agentes químicos y biológicos en las fuentes de agua o para la transmisión rápida de datos desde las estaciones de monitoreo. Asimismo, se desarrollan otras tecnologías, como por ejemplo, el bio-análisis por medio de sensores de chip, que ofrecen incrementar el acceso automatizado a datos en tiempo real para su inclusión en un *EWS*.

4.3. MONITORIZACIÓN DE LA RED DE DISTRIBUCIÓN

El sistema de distribución representa la mayor vulnerabilidad de todo un sistema de agua potable. El riesgo de contaminación (deliberada o accidental) es alto, y las consecuencias pueden ser graves. Por ello, el mecanismo de protección más viable, ante un evento tal, es la monitorización. Sin embargo, su implementación y funcionalidad dependen de aspectos como: la suciedad y obstrucción de las tuberías, su gran distribución geográfica, del poco conocimiento de sus variables hidráulicas, la variabilidad de la calidad del agua, la alimentación de una sola tubería por múltiples fuentes, la presencia de desinfectantes químicos, el poco o nulo financiamiento y la localización de las estaciones de monitorización, entre otros.

4.4. IDEAS PRINCIPALES DEL CAPÍTULO

- La mejora de la seguridad, reduce la vulnerabilidad de un sistema de abastecimiento de agua potable.

- La monitorización es un componente crítico en cualquier programa de seguridad del agua potable, ya que no existe otra manera factible de hacer frente a un evento de contaminación, especialmente si es en el sistema de distribución.

- Debido a que la red de distribución es el punto más vulnerable, frente a un evento de contaminación, dentro de un sistema de abastecimiento de agua potable, es necesaria la implementación de un sistema de seguridad, específicamente un sistema de monitorización de alerta temprana.

- La monitorización temprana, dentro del sistema de distribución, identifica en tiempo eventos de contaminación. Asimismo, permite evitar o mitigar los impactos adversos ocasionados por un evento tal.

- Prevenir la entrada de contaminantes en el sistema de abastecimiento, requiere que un *EWS* tenga, como mínimo, los siguientes mecanismos: un mecanismo de detección, un medio de confirmación, una unidad de control o unidad central de coordinación, vínculos de comunicación de información y mecanismos de respuesta de mitigación.

- Un *EWS* debe cumplir con los siguientes criterios mínimos: dar una respuesta rápida, sensibilidad suficiente y funcionar como un sistema automatizado que permita la monitorización remota.

5. El CONTROL ESTADÍSTICO DE PROCESOS

5.1. INTRODUCCIÓN

Las técnicas de Control Estadístico de Procesos *(Statistical Process Control-SPC),* fueron desarrolladas en los años 20's por el Doctor Walter A. Shewhart y su utilización fue de gran importancia durante la Segunda Guerra Mundial en las industrias de armamento. Estas técnicas, típicamente usadas para la monitorización y control de la calidad de los procesos industriales, pueden detectar cambios en la media del proceso, cambios en la varianza y en la relación entre múltiples variables.

Los métodos de *SPC* son una colección de técnicas de gran alcance para la resolución de problemas, las cuales son comúnmente usadas para monitorizar procesos de producción. Entre sus métodos, los gráficos de control son la herramienta más común y han sido utilizados para el seguimiento de procesos, análisis de tendencias y obtención de alertas en el estatus del proceso. Gráficos de *SPC* convencionales, como los gráficos de control de *Shewhart*, los gráficos de suma acumulada *(Cumulative Sum-CUMSUM)* y los gráficos de promedio móvil ponderado exponencialmente *(Exponentially Weighted Moving Average-EWMA)* están bien fundamentados para el control de procesos distribuidos normalmente, con la variación aleatoria del proceso. La aplicación concreta del *SPC* está basada en el conocimiento y seguimiento del proceso a través de datos históricos, por lo que el nivel del promedio del proceso y la dispersión del proceso, pueden ser monitoreadas para poder tomar medidas al respecto (Wang *et al.,* 2008).

Los métodos tradicionales del *SPC* proporcionan un grupo de pruebas estadísticas de hipótesis general, las cuales mantienen que el valor de la media de la característica de calidad de un proceso o la media de un proceso, es consistente en su nivel objetivo (Fallah y Akhavan, 2009)

5.1.1. Gráficos de Control

En Prat *et al*. (1997), se define como gráfico de control, aquel en el que se representa de forma cronológica el comportamiento de un proceso, y cuyo objetivo principal, es la detección rápida de cambios en un proceso debido a causas no comunes o asignables; es decir; cualquier evidencia de que la media y la variabilidad del proceso no se han mantenido constantes a lo largo de un intervalo de tiempo. Lo anterior, se consigue minimizando el tiempo que transcurre desde que se produce un desajuste hasta que se detecta. Por lo tanto, se deben considerar los siguientes puntos:

1. El riesgo que se está dispuesto a admitir cada vez que se decida que una causa asignable ha entrado en el proceso.
2. El cambio mínimo en el valor del parámetro que se desea detectar
3. El tiempo medio esperado entre los desajustes.

Existen varios tipos de gráficos de control, cada una de ellos usa ecuaciones algo distintas entre sí y son apropiadas para diferentes tipos de datos. En relación con esto, una clasificación general de los tipos de gráficos de control que existen se describe en la Tabla 5.1. Determinar cual tipo de gráfico de control se debe usar, depende de la identificación del tipo de datos que se vayan a representar, ya sean continuos o discretos. Con respecto a lo anterior, las distribuciones estadísticas más comunes son la normal, la binomial y la Poisson, siendo estas las más apropiadas para describir a la mayoría de procesos.

Tabla 5.1. *Clasificación General de los Gráficos de Control.*

Por Variables (Datos continuos)	▪ Gráficos para $\overline{X}$ y *R,* ▪ Gráfico de observaciones ▪ Gráfico de rangos móviles individuales ▪ Gráfico de medias móviles
Por Atributos (Característica no medible)	▪ Gráfico *P* ▪ Gráfico *NP* ▪ Gráfico C ▪ Gráfico *U*
Con Memoria	▪ Gráfico *CUMSUM* (*Cumulative Sum*) ▪ Gráfico *EWMA* (*Exponentially Weighted Moving Average*)

Los gráficos por atributos se aplican cuando existen situaciones en las que la variable o característica de calidad que interesa controlar no es una característica medible en una escala continua o cuantitativa. En estos casos, cada unidad puede calificarse como conforme o disconforme, de acuerdo con si posee o no ciertos atributos, o según el número de defectos que presenta

Los gráficos por variables son utilizados para datos continuos o para la característica de calidad de un proceso. Si la característica del proceso puede medirse y expresarse como un número en una escala de medición continua, tales como el contenido en cm^3, peso, viscosidad, intensidad, temperatura, etc., esta será considerada una variable, cuando el proceso está en estado de control, se distribuyen en general como una distribución normal. Cuando se trata con una característica de la calidad que es una variable, por lo general es necesario monitorear tanto el valor medio de la característica de la calidad como su variabilidad

Tanto los gráficos por variables como por atributos, son útiles para detectar cambios en la media de más de más de dos desviaciones estándar, pero pueden tardar mucho en detectar un cambio más pequeño. Ante esto,

los gráficos denominados con memoria, son más rápidos en detectar cambios de pequeña magnitud, pero más lentos en detectar cambios de mayor magnitud.

En la Figura 5.1, se muestra el formato general de un gráfico de control. Para su construcción, los datos son agrupados en intervalos de tiempo y ordenados a su vez en subgrupos de forma cronológica. En el gráfico se pueden observar tres líneas que lo dividen, estás líneas se denominan Línea Central (*LC*), Límite de Control Superior (*LCS*), Límite de Control Inferior (*LCI*). Estos límites ayudan a definir la tendencia y variabilidad natural del proceso. La *LC* suele ser la media aritmética o el valor esperado de la variable representada, de modo que aproximadamente la mitad de los valores del subgrupo caerán en cada lado, si el estado del proceso es bajo control, (es decir, cuando únicamente se presentan causas comunes o fortuitas). Los límites superior e inferior son, generalmente, más y menos tres desviaciones estándar, con respecto a la media.

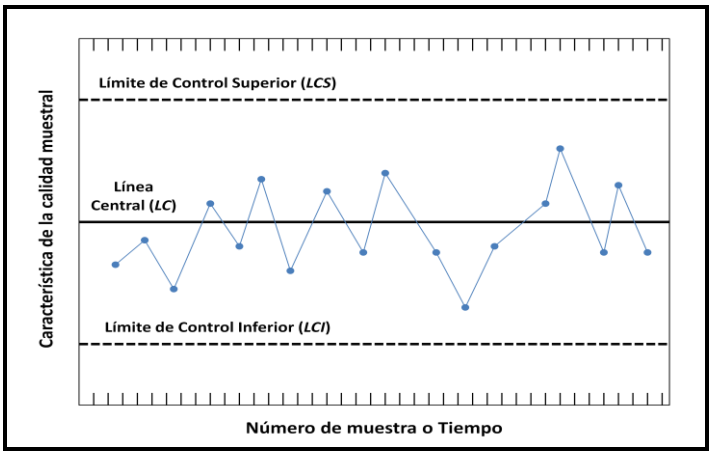

Figura 5.1. *Formato General de un Gráfico de Control*

5.1.1.1. Criterios generales en el diseño de un gráfico de control

Dentro de los principales aspectos en el diseño de un gráfico de control están, la selección del tamaño de la muestra, la frecuencia del muestreo y la definición de los límites de control.

En cuanto a la selección del tamaño de la muestra, por lo general, las muestras grandes facilitan la detección de desfases pequeños en el proceso. Sin embargo, la elección del tamaño de la muestra está en función del tipo de cambio a detectar; es decir, si el cambio en el proceso es relativamente grande, se usan tamaños de muestra más pequeños que los que se emplean para detectar un cambio menor. La determinación de la frecuencia de muestreo, para la detección de variaciones, se relaciona con el tamaño de la muestra, esto es, tomar muestras pequeñas en intervalos cortos o bien tomar muestras más grandes en intervalos más largos.

La especificación de los límites de control, en el diseño del gráfico, es una de las decisiones a tomar más significativas. En la definición de los límites de control, una práctica común es determinar estos límites como un múltiplo de la desviación estándar del estadístico graficado. El múltiplo que generalmente se elige es tres; por lo tanto, se acostumbra emplear límites de Tres sigma, independientemente del tipo de gráfico empleado. Además de que se considera que han dado buenos resultados en la práctica, (Montgomery, 2004).

Para la definición de los límites de control se considera, por lo general, que se tiene un estadístico muestral *w* que mide alguna característica de la calidad de interés, y se supone que la media de *w* es μ_w, y que la desviación estándar de *w* es σ_w. Por lo tanto, el *LCS,* el *LC* y la *LC* se definen por las ecuaciones:

$$LCS = \mu_w + L\sigma_w \tag{5.1}$$

$$LC = \mu_w \tag{5.2}$$

$$LCI = \mu_w - L\sigma_w \tag{5.3}$$

Donde *L* es la distancia de los límites de control a la línea central, expresada en unidades de desviación estándar.

En relación con los límites de control, algunos analistas sugieren el uso de dos conjuntos de límites: límites exteriores o límites de acción (de tres sigma, por ejemplo), y límites interiores o de advertencia (por lo general, con amplitud de dos sigma). Los primeros se consideran así debido a que cuando se localiza un punto fuera de ellos, se hace una búsqueda de una causa asignable y se emprende una acción correctiva. En cuanto a los segundos, si se presentara una situación en la que uno o más puntos se localizan entre los límites de advertencia y los límites de control, o muy cerca del límite de advertencia, podría significar que el proceso no está operando correctamente. El uso de límites de advertencia puede aumentar la sensibilidad del gráfico; es decir, puede permitir que el gráfico señale con mayor rapidez una variación en el proceso. Sin embargo, una de las desventajas de su uso es que pueden resultar confusos en su interpretación, ya que a pesar de mejorar la sensibilidad del gráfico, pueden dar como resultado un incremento de falsas alarmas.

Cabe comentar que un gráfico de control da "falsas alarmas" cuando las observaciones de un proceso en estado de control llevadas al gráfico, son interpretadas erróneamente como señales de aparición de causas asignables. Para que esto no ocurra con frecuencia, se debe tener la seguridad de que el proceso o la variable a cambiado. Para ello, en el caso de una distribución normal los *LCS* y *LCI* se deben establecer, como ya se ha mencionado, a una distancia del *LC* de tres desviaciones estándar del estadístico que se registra en el gráfico.

5.1.1.2. Reglas de control

Es posible aplicar simultáneamente varios criterios de control o sensibilización a un gráfico de control, para determinar si el proceso está fuera de control. El criterio base es el de uno o más puntos fuera de los límites de control. En ocasiones, se emplean criterios suplementarios para aumentar la sensibilidad del gráfico frente a variaciones tan pequeñas en el proceso, con el fin de poder responder con mayor rapidez a la causa asignable. En la Tabla 5.2. se enlistan algunas de las reglas de control más comunes en la práctica, que se aplican en los gráficos de control, especialmente en los gráficos de *Shewhart* $\overline{X}$. Al inspeccionar un gráfico de control con esas reglas, se puede concluir que el proceso está fuera de control si se satisface una o más de ellas.

Tabla 5.2. *Reglas de control o de sensibilización más comunes aplicadas a los gráficos de control de Shewhart*

Señal acción estándar →	**1.** Uno o más puntos fuera de los límites de control **2.** Dos de tres puntos consecutivos fuera de los límites de advertencia dos sigma pero aún dentro de los límites de control *LCS* y *LCI* **3.** Cuatro de cinco puntos consecutivos fuera de los límites de una sigma	**Reglas de *Western Electric***
	4. Una racha de ocho puntos consecutivos fuera de los límites de una sigma **5.** Seis puntos seguidos que se incrementan o se decrementan de manera sostenida **6.** Quince puntos seguidos en la zona C (tanto arriba como debajo de la *LC)* **7.** Catorce puntos seguidos alternándose arriba y abajo. **8.** Ocho puntos seguidos en ambos lados de la línea central, pero ninguno de ellos en la zona C. **9.** Un patrón inusual o no aleatorio en los datos **10.** Uno o más puntos cerca de un límite de control o límite de advertencia	

Sin embargo, los expertos recomiendan usar las reglas de control con precaución, ya que un número excesivo de falsas alarmas puede ser perjudicial para un programa de *SPC* efectivo. O bien se puede provocar la aparición de un *Error Tipo I* (Concluir que el proceso está fuera de control cuando en realidad está bajo control), o de un *Error Tipo II* (Concluir que el proceso está bajo control cuando en realidad está fuera de control). Asimismo, al aplicar más reglas suplementarias de sensibilización, el proceso de decisión de hace más complejo, perdiéndose la simplicidad inherente del gráfico de control

5.2. EL CONTROL ESTADÍSTICO DE PROCESOS COMO HERRAMIENTA DE DETECCIÓN

La mayoría de las aplicaciones de los métodos del *SPC* se encuentran dentro del marco industrial, orientado a productos. Sin embargo, los principios de tales técnicas son, en sí mismos, generales, y por lo tanto, existen muchas otras aplicaciones no industriales, o del sector de la industria de servicios. Tales aplicaciones fuera del ámbito de la manufactura no difieren substancialmente de las aplicaciones industriales más comunes. Por ejemplo, un gráfico de control utilizado para reducir la fracción de tarjetas de circuitos impresos disconformes,

producidas por una planta de productos electrónicos, podría aplicarse con igual facilidad, para reducir los errores de facturación en una operación de tarjetas de crédito bancarias. Unos gráficos $\overline{X}$ y *R* aplicados a un proceso de manufactura de anillos para pistones de motor, podrían usarse para monitorear y controlar el tiempo de flujo de las cuentas por pagar a través de una función financiera.

Los gráficos de control para variables han encontrado una aplicación frecuente en escenarios tanto industriales como no industriales. Sin embargo, se cree erróneamente que estos gráficos no son aplicables a escenarios fuera de la manufactura debido a que el "producto es diferente". En realidad, si es posible hacer mediciones del producto que reflejen la calidad, la función o el desempeño, entonces la naturaleza del producto no tiene relación alguna con la aplicabilidad general de las cartas de control. Existen, sin embargo, dos diferencias que es común encontrar entre las situaciones de manufactura y las de no manufactura: **1)** en un escenario fuera de las manufacturas los límites de las especificaciones rara vez se aplican al producto, por lo que la noción de capacidad del proceso frecuentemente no está definida; y **2)** puede requerirse de una mayor inventiva para seleccionar la variable o variables apropiadas que deben medirse.

Se ha encontrado que, una vez que el sistema se ha definido adecuadamente y se ha desarrollado un sistema de medición válido, la mayoría de las herramientas del *SPC* pueden aplicarse fácilmente a un amplia variedad de operaciones como por ejemplo, financieras, comerciales, de diseño, desarrollo de programas informáticos, etc.

En relación con lo anterior, Beneyan (1998) muestra el uso de los gráficos de control en el ámbito de la medicina, por ejemplo, para encontrar el número de errores en la medicación de los pacientes, para determinar la tasa de infecciones en hospitales o para saber el número de recaídas de los pacientes en un período de tiempo.

Otra aplicación de los gráficos de control es la realizada por Ye *et al.* (2003). En su trabajo, propone la detección de intrusiones informáticas (*cyber intrusions*) a través de los gráficos de control *EWMA*, (para datos correlacionados y no correlacionados), con el fin de proteger a los sistemas de información de intrusiones y asegurar la confiabilidad y la calidad del servicio. La importancia de su contribución se debe a que, tal y como lo señala, distintas anomalías en los sistemas informáticos han sido estudiadas con técnicas basadas en inteligencia artificial, pero no han sido extensamente estudiadas utilizando teorías y técnicas de ingeniería de la calidad.

Por otro lado, en los últimos años, se han propuesto diversos métodos para la detección temprana de defectos o desajustes, (por ejemplo, basados en Minería de datos, en Redes neuronales, aplicando la *Transfomada de Fourier*, etc.). Entre ellos, el desarrollo del *SPC* se ha enfocado al control de procesos multivariados, para los

procesos de monitorización. En relación a esto, Wang *et al.* (2008) propone la identificación temprana de defectos aplicando métodos de *SPC,* junto con un modelo de auto-regresión, para la identificación temprana del punto de inicio donde se produce un defecto, en un proceso en el que no existe información previa o datos históricos y el proceso es dejado funcionando inalterado hasta que se presenta un fallo. En su trabajo señala que la variación del proceso no puede ser aleatoria después de un cierto período de tiempo, y que tal variación puede deberse a causas especiales; lo que significaría que el proceso puede mostrar una tendencia. A su vez, hace una comparación entre los gráficos de control que utilizó para identificar el punto inicial de un defecto, incluyendo el gráfico de *Shewhart,* y los gráficos de media móvil.

5.3. IDEAS PRINCIPALES DEL CAPÍTULO

- Los métodos de *SPC* son una colección de técnicas para la resolución de problemas, que son comúnmente usadas para monitorizar procesos de producción. Sin embargo, recientemente el desarrollo del *SPC* se ha enfocado al control de procesos de monitorización y a la detección temprana de anomalías en campos como la medicina o la informática.

- Entre los las técnicas del *SPC*, los gráficos de control son la herramienta más común y son utilizados en el seguimiento de procesos, el análisis de tendencias y la obtención de alertas. De forma general, los gráficos de control se clasifican en gráficos de control por variables y gráficos de control por atributos.

- En el diseño de un gráfico de control, se deben considerar los siguientes aspectos principales: la selección del tamaño de la muestra, la frecuencia del muestreo y la definición de los límites de control, es decir la Línea Central (*LC*), el Límite de Control Superior (*LCS*) y el Límite de Control Inferior (*LCI*).

6. CASO DE ESTUDIO

6.1. DESCRIPCIÓN DE LA RED

Con el objetivo de demostrar la aplicación y el análisis del *SPC,* como herramienta de detección de eventos de contaminación, se eligió una red de abastecimiento que corresponde al Ejemplo 3 de *EPANET,* (Figura 6.1), y el cual está disponible en la página *web* de la *US-EPA*. La red consta de dos fuentes de abastecimiento (un río y un lago), tres tanques de almacenamiento elevados, 117 tuberías, 92 nodos y dos estaciones de bombeo. Asimismo, está sujeta a cinco patrones de demanda y su período de simulación fue de 24 horas. En lo que se refiere al entorno del sistema (los detalles de consumos, los patrones de demanda, las características y los valores de las tuberías y las bombas, los volúmenes de los tanques, las reglas de operación) permanecen constantes.

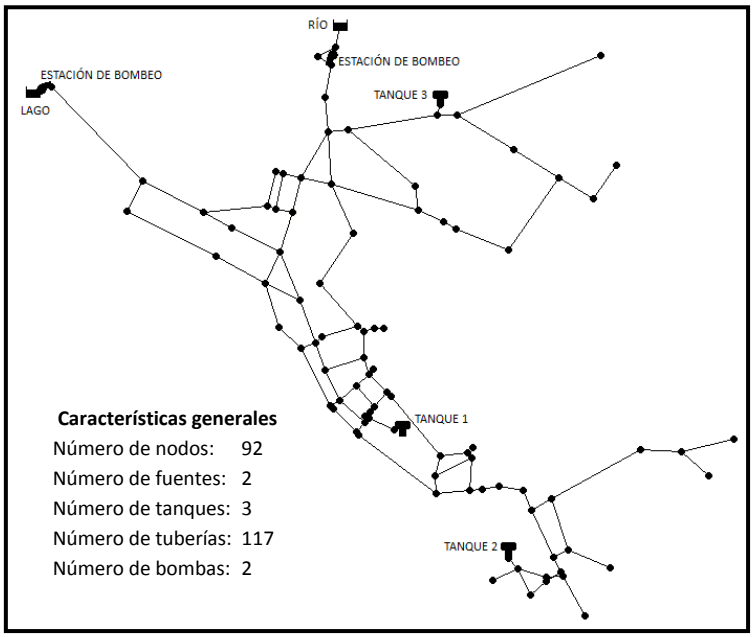

Figura 6.1. *Esquema general de la red de estudio: Ejemplo 3 de EPANET*

6.2. BASES EL ESCENARIO DE CONTAMINACIÓN

El trabajo se desarrolla a partir de un escenario de contaminación factible, donde se generan los datos de la intrusión, que es el objetivo del estudio. Asimismo, para realizar el análisis del comportamiento de la red de

abastecimiento, esta debe estar previamente modelada y calibrada hidráulicamente en un período de tiempo suficiente para representar su funcionamiento normal.

Las consideraciones generales asumidas para el desarrollo del escenario de contaminación siguen a las propuestas por Chastain, (2006) y son las siguientes:

a) Se considera un solo agente contaminante de entrada en la red. Su selección, se basa en sus propiedades toxicológicas y métodos de detección. Asimismo, se supone de fácil adquisición transporte y dispersión.
b) El contaminante elegido es capaz de provocar una contaminación masiva y se considera que no es detectado durante su consumo.
c) El contaminante se asume como un agente conservativo y se considera resistente a los procedimientos normales de desinfección, por lo que su tiempo de permanencia en el agua y su eficacia potencial se suponen altas.
d) El patrón de inyección del contaminante se define con un tiempo de inicio y duración.
e) La entrada del contaminante a la red puede ocurrir en cualquiera de los nodos de la red y con igual probabilidad de ocurrencia.
f) Cada evento de contaminación ocurre con una inyección en un solo nodo de la red, con una duración y concentración del contaminante establecidas.

Por otro lado, para que efectivamente un agente químico o biológico cause daño o muerte debido a su presencia en el agua potable, debe tener ciertas características como son:

- Posibilidad de ser utilizado como un arma, es decir, que pueda ser introducido y dispersado en cantidades suficientes que provoquen el efecto deseado.
- Peligrosidad en el agua, debido a su toxicidad y su nivel de contaminación.
- Estabilidad en el agua, es decir, que mantenga sus efectos estructurales y tóxicos.
- Resistencia a la cloración, esto es, que no se oxide en presencia de cloro libre disponible en el agua. Aquí, cabe mencionar la evidente necesidad de asegurar las plantas potabilizadoras para evitar la inactivación de los sistemas de cloración.

6.3. CONSTRUCCIÓN DE LOS EVENTOS DE CONTAMINACIÓN

Con base en los criterios descritos en el apartado anterior y a la revisión bibliográfica realizada, se asumió, para propósitos del análisis, que la red de distribución estaría sujeta a eventos de contaminación química. Tales eventos fueron simulados como una inyección deliberada de una sustancia química, de carácter conservativo.

Para lo cual, se consideró el *Caso Base A* de Ostfeld *et al.* (2008), que asume inyectar durante dos horas una concentración de 230.000 mg/L afectada por una tasa de flujo de inyección de 125L/h.

Las inyecciones del contaminante se realizaron en el Nodo 159, cuya ubicación se muestra en la Figura 6.2 .El nodo de inyección se eligió basándose en el trabajo de Ostfeld *et al.* (2004). Asimismo, los eventos de contaminación se realizaron, de manera independiente, en las siguientes horas: 01:00, 02:00, 12:00 y 13:00, que como se puede observar en la Figura 6.3, corresponden a horas significativas dentro del patrón general de demanda de la red.

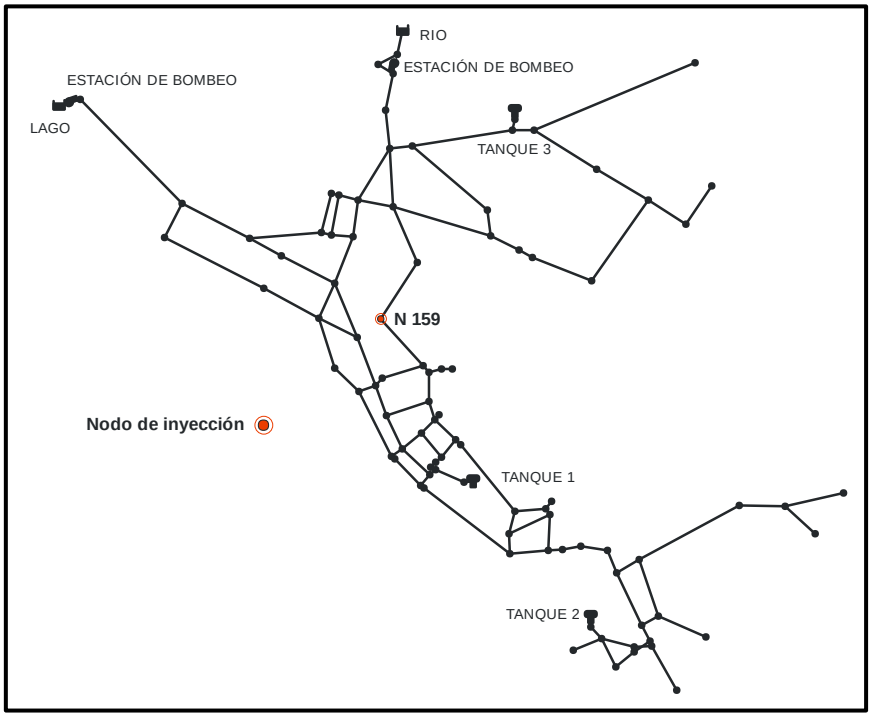

Figura 6.2. *Localización del punto de inyección en la red de abastecimiento*

Una vez planteados los escenarios de contaminación, se realizaron las simulaciones para la obtención de los datos de calidad, conservando los parámetros y condiciones hidráulicas originales de la red, pero introduciendo el tipo de contaminante, sus propiedades y el tipo de fuente de calidad, como se especifican en la Tabla 6.1. Para la realización de los cálculos, se utilizó la *EPANET-MATLAB toolkit*, la cual se encuentra disponible en el sitio *web* http://eldemet.wordpress.com.

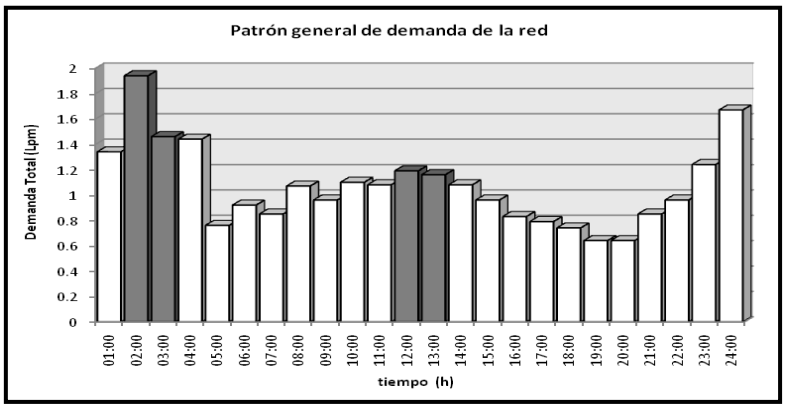

Figura 6.3. *Horas de los eventos de inyección, representadas en el patrón general de demanda*

Tabla 6.1. *Parámetros de entrada para la simulación del evento de contaminación*

Parámetro	Detalle
Período Total de simulación	24 horas
Hora de inicio de la simulación	00:00 horas (12:00am)
Período hidráulico	1 hora
Período del informe	1 hora
Período de calidad	1 hora
Estatus inicial de las bombas	cerradas
Tipo de contaminante	químico
Propiedades del químico	conservativo
Tipo de fuente de calidad	caudal másico

6.4. CONSIDERACIONES PARA LA CONSTRUCCIÓN DE LOS GRÁFICOS DE CONTROL

Como se mencionó en el capítulo anterior, la elección de los datos y la definición de los límites de control son importantes en el diseño de un gráfico de control. Para obtener los límites de control se requiere primero elegir los datos adecuados para el análisis, por ejemplo, los datos del estado normal del proceso (que puede no conocerse al momento). Existen dos métodos para determinar los datos. Uno es elegir la parte de los datos basándose en la sugerencia de expertos y el otro es mediante el estudio de los propios datos.

6.4.1. Datos y límites de control

En el presente trabajo, se parte de que no existe ningún indicio del contaminante en el agua de la red. Esto significa, que el nivel del contaminante en la red es de 0 mg/L, en un estado de funcionamiento normal.

Sin embargo, como ya se mencionó, es recomendable establecer un límite de advertencia, que permita realizar acciones preventivas o de mitigación. Por esto, se determinó que el límite de advertencia estuviera en función de los niveles máximos permitidos para el tipo de contaminante inyectado.

Otro aspecto considerado para la determinación del límite de advertencia, es la pertenencia del químico al grupo de agentes sanguíneos. Éste es un material extremadamente peligroso y venenoso, debido a que actúa rápidamente. Entre sus propiedades se encuentra que es altamente soluble y estable en agua, es incoloro y aunque desprende un olor similar a almendras amargas puede no ser detectado. Es altamente tóxico si se ingiere o si es absorbido por la piel. Debido a que la Concentración Aguda (*CA*), a partir de la cual se presentan consecuencias graves es de 50 mg/L, se propone un Límite de Advertencia (*LA*) de 25 mg/L, donde sus efectos son menores.

6.4.2. Fundamentos estadísticos del gráfico de control

Cuando se trabaja con una característica de la calidad que puede expresarse como una medición, se acostumbra monitorear tanto el valor medio de la característica de la calidad como su variabilidad. Así, el control sobre la calidad promedio puede realizarse por medio del gráfico de control de promedios $\overline{X}$.

Con la finalidad de identificar la presencia del contaminante en los nodos y la evolución del mismo en el tiempo, debido a los eventos producidos, se determinó el uso de la teoría convencional del *SPC.* Asimismo, por simplicidad, se eligió el gráfico de control de $\overline{X}$ y se asumió que los datos observados se distribuyen normalmente.

Los fundamentos estadísticos para la construcción de los gráficos $\overline{X}$, suponen considerar que la característica de calidad o variable tiene una distribución normal con media μ y desviación estándar σ, donde ambas son conocidas. Si $x_1,\ x_2, \dots,\ x_n$ es una muestra de tamaño n, entonces el promedio de la muestra es:

$$\overline{x} = \frac{x_1 + x_2 + \cdots + x_n}{n} = \frac{1}{n}\sum_{i=1}^{n} x_i \qquad (6.1)$$

Además, se supone que por un lado, $\overline{x}$ sigue una distribución normal con media μ y desviación estándar $\sigma_{\overline{X}} = \frac{\sigma}{\sqrt{n}}$. Por otro lado, se considera una probabilidad igual$1 - \alpha$ a, donde α señala el nivel de confianza en los análisis, para que cualquier media muestral se localice entre:

$$\mu + Z_{\alpha/2}\alpha_{\overline{x}} = \mu + Z_{\alpha/2}\frac{\sigma}{\sqrt{n}} \qquad (6.2)$$

$$\mu - Z_{\alpha/2}\alpha_{\overline{x}} = \mu - Z_{\alpha/2}\frac{\sigma}{\sqrt{n}} \tag{6.3}$$

Por lo tanto, si se supone que se conocen μ y σ y que la característica de la calidad tienen una distribución normal, las ecuaciones 6.2 y 6.3 podrían usarse como *LCS* y *LCI*, respectivamente. Siendo $Z_{\alpha/2} = 3$ ya que, como se ha señalado, en la práctica se acostumbra trabajar con límites de tres sigma (o lo que es igual a una confianza del 99%). A su vez, μ puede ser usada como la *LC* del gráfico de control.

Por otro lado, si se supone que se cuenta con m muestras, cada una de las cuales contiene n observaciones de la característica de la calidad, se tiene que $\overline{x}_1,\ \overline{x}_2, \dots,\ \overline{x}_m$ son los promedios de cada una de las muestras. Por lo tanto, el promedio del proceso es igual al promedio agregado, definido por la ecuación 6.4, que sería la *LC* del gráfico de control $\overline{X}$.

$$\overline{\overline{x}} = \frac{\overline{x}_1 + \overline{x}_2 + \cdots + \overline{x}_m}{m} = \frac{1}{m}\sum_{i=1}^{m}\overline{x}_i \tag{6.4}$$

Cabe mencionar que los límites de control pueden ser estimados, como se ha mencionado hasta ahora, a partir de las desviaciones estándar o bien, por los rangos de las m muestras. La estimación a partir de los rangos supone que si $x_1,\ x_2, \dots,\ x_n$ es una muestra de tamaño n, entonces el rango de la muestra es la diferencia entre la observación menor y mayor, esto es:

$$R = x_{máx} - x_{mín} \tag{6.5}$$

Ahora, sean $R_1,\ R_2, \dots,\ R_m$ los rangos de las m muestras. El rango promedio está dado por:

$$\overline{R} = \frac{R_1 + R_2 + \cdots + R_m}{m} = \frac{1}{m}\sum_{i=1}^{m}R_i \tag{6.6}$$

Con base en lo anterior, se definen las ecuaciones para obtener los límites de control del gráfico $\overline{X}$:

$$LCS = \overline{\overline{x}} + A_2\overline{R} \tag{6.7}$$

$$LC = \overline{\overline{x}} \tag{6.8}$$

$$LCI = \overline{\overline{x}} - A_2\overline{R} \tag{6.9}$$

Donde A_2 se tabula como una constante, en función de las n observaciones de la muestra m, de acuerdo con los valores proporcionados en una tabla de factores para construir gráficos de control. La tabla puede consultarse en el Apéndice VI de Montgomery, (2004).

7. RESULTADOS

7.1. INTRODUCCIÓN

Los resultados que se presentan en este capítulo, corresponden a los gráficos de control obtenidos para cada evento de contaminación. Una vez realizadas las simulaciones en diferentes escenarios, se construyeron los gráficos de control mediante el programa *MATLAB*, bajo las consideraciones descritas en el apartado anterior.

Los gráficos obtenidos representan los nodos que exceden los límites establecidos, así como su evolución durante el período de simulación. La información que proporcionan permite determinar las horas en las que el contaminante alcanza su mayor concentración, el tiempo de duración del evento y, a su vez, el tiempo del cual se dispone para planear y efectuar acciones que mitiguen o eviten la dispersión del contaminante. Asimismo, se puede evaluar si tales acciones de respuesta fueron suficientes para lograr detener el efecto del contaminante, disminuyendo así, los daños potenciales asociados a la intrusión.

7.2. EVENTOS DE CONTAMINACIÓN

A continuación, se presentan los gráficos de control para cada uno de los escenarios de contaminación planteados y se analizan sus principales aspectos.

7.2.1. Evento de contaminación a las 01:00 h

En la Figura 7.1 se muestra el gráfico de control del evento de contaminación de las 01:00 h. En él se puede observar que el efecto de haber inyectado el contaminante a las 01:00 h se manifiesta a partir de las 02:00 h y empieza a disminuir en concentración hasta las 11:00 h. Por lo tanto, se puede decir que el evento tiene una duración de nueve horas. También es importante notar que a las 06:00 h se sobrepasa el *LA* de 25 mg/L, por lo que se tienen cuatro horas para tomar medidas correctivas antes de alcanzar las máximas concentraciones que se presentan a las 07:00, 09:00 y 10:00 horas (Tabla 7.1).

Tabla 7.1. *Resultados principales de la evolución del contaminante: evento a las 01:00 h*

Concentración inyectada (mg/L)	Hora de inyección	Hora de detección del contaminante	Hora en la que se pasa el *LA*	Horas de máxima concentración
230.000	01:00	02:00 h	06:00	07:00, 09:00 y 10:00

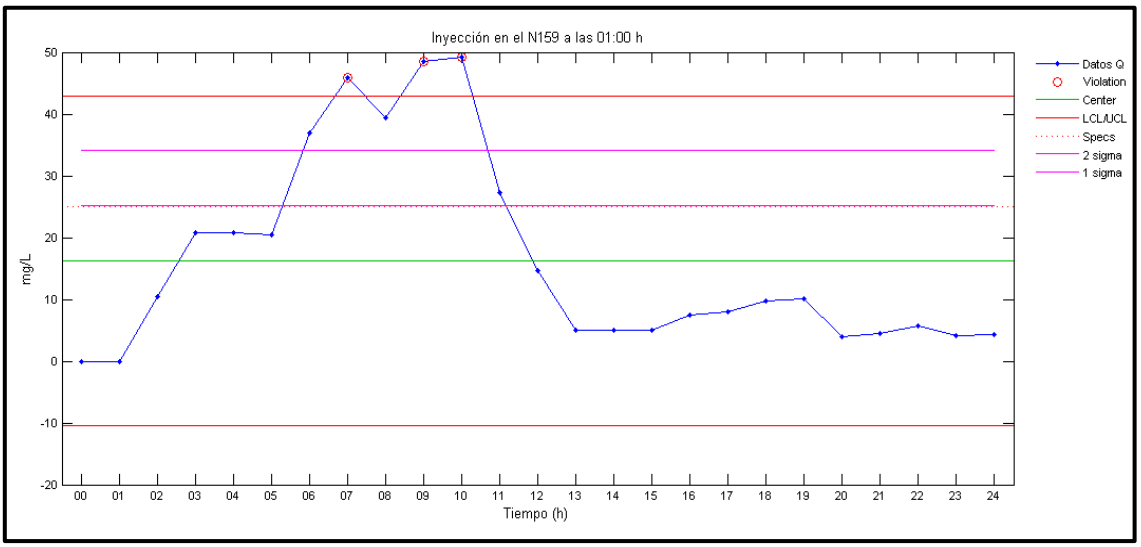

Figura 7.1. *Gráfico de control: Evolución del contaminante del evento de contaminación en el N159 a las 01:00 h*

Por otro lado, en el gráfico de control presentado en la Figura 7.2 se muestran cuáles son los nodos que son afectados, de tal manera que se puede ver la relación que existe entre el nodo en el que fue introducido el contaminante y los demás nodos de la red. Cabe señalar que en el gráfico los nodos están ordenados en relación con sus etiquetas y no en función de su situación física en la red (Tabla 7.2).

Tabla 7.2. *Datos principales de los nodos afectados: evento a las 01:00 h*

Concentración inyectada (mg/L)	Hora de inyección	Nodos que pasan el *LA*	Nodos con la máxima concentración
230.000	01:00	163, 239, 241, 249, 265, 269	35, 159, 161, 164, 167, 169, 171, 173, 181, 199, 201, 203, 271, 273, 275

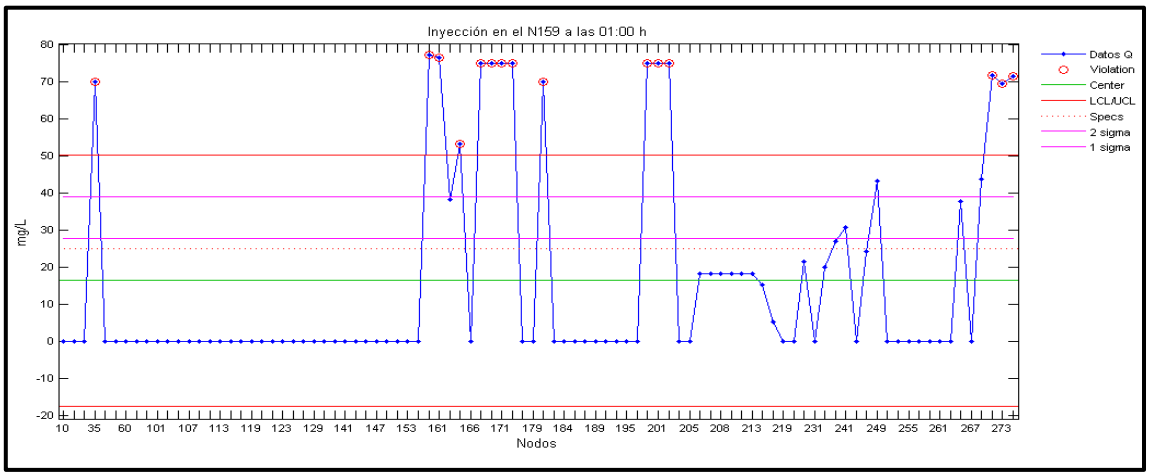

Figura 7.2. *Gráfico de control: Nodos afectados en el evento de contaminación del N159 a las 01:00 h*

7.2.2. Evento de contaminación a las 02:00 h

Como puede observarse en la Figura 7.3, el evento de contaminación de las 02:00 h tiene un comportamiento similar al de las 01:00 h. Para este evento, el gráfico detecta la presencia del contaminante en la red a partir de las 03:00 h y se puede ver que se sobrepasa el *LA* a las 07:00 h. Alcanza las máximas concentraciones a las 08:00, 10:00 y 11:00 horas (Tabla 7.3. También, se puede apreciar que la disminución del contaminante empieza a las 12:00 h, por lo que el período de mayor contaminación tiene una duración de nueve horas.

Tabla 7.3. *Resultados principales de la evolución del contaminante: evento a las 02:00 h*

Concentración inyectada (mg/L)	Hora de inyección	Hora de detección del contaminante	Hora en la se pasa el *LA*	Horas de máxima concentración
230.000	02:00	03:00	07:00	08:00, 10:00 y 11:00

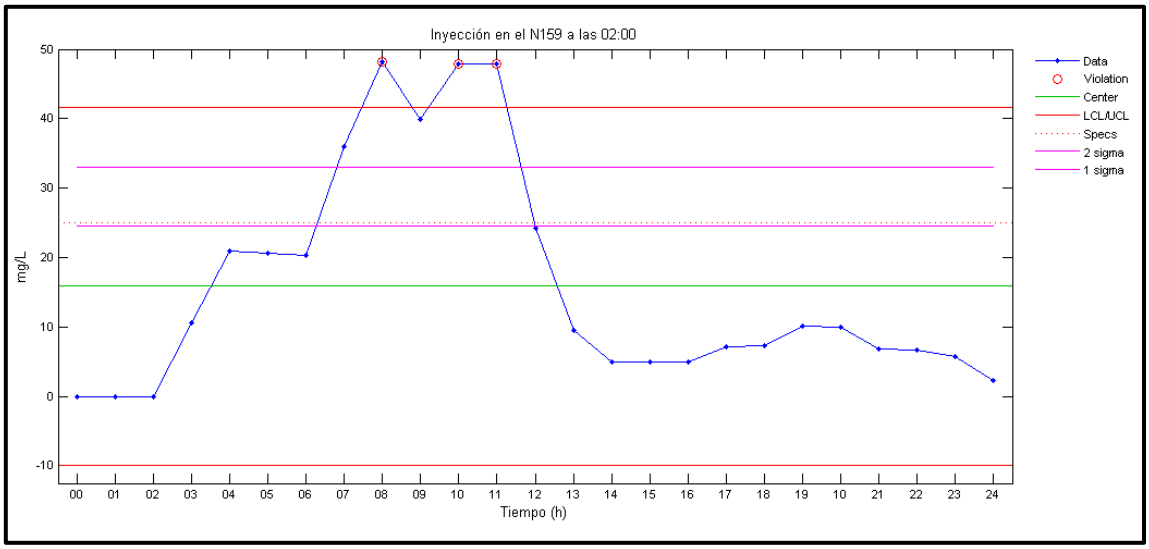

Figura 7.3. *Gráfico de control: Evolución del contaminante del evento de contaminación en el N159 a las 02:00 h*

El gráfico de control de la Figura 7.4 muestra los nodos afectados por el contaminante, tanto los que sobrepasan el *LA*, como los que exceden el *LCS* con las máximas concentraciones. La información principal del gráfico de control para los nodos, se presenta en la Tabla 7.4.

Tabla 7.4. *Datos principales de los nodos afectados: evento a las 02:00 h*

Concentración inyectada (mg/L)	Hora de inyección	Nodos que pasan el *LA*	Nodos con la máxima concentración
230.000	02:00	161, 163, 164, 239, 241, 249	35, 159, 167, 169, 171, 173, 199, 201, 203, 265, 269, 271, 273, 275

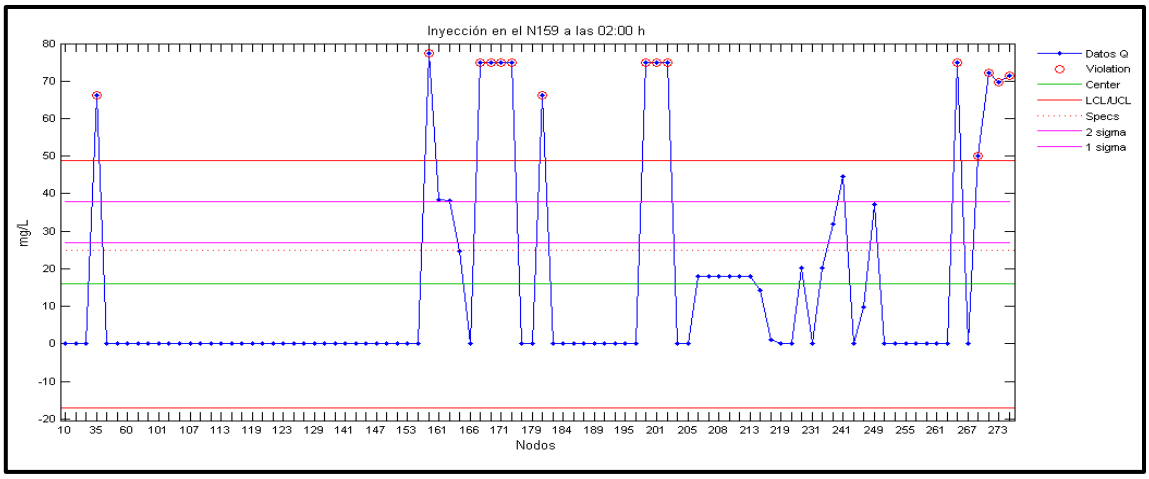

Figura 7.4. *Gráfico de control: Nodos afectados en el evento de contaminación del N159 a las 02:00 h*

7.2.3. Evento de contaminación a las 12:00 h

El evento de contaminación de las 12:00 h tiene como resultado el gráfico de control de la Figura 7.5. En él, se observa que la detección del contaminante es a las 13:00 h. En este caso, solo se cuenta con una hora desde que es detectada la presencia del contaminante hasta superar el *LA,* a las 14:00 h. Lo anterior, implicaría la ejecución de acciones rápidas antes de alcanzar las máximas concentraciones que se presentan a las 18:00, 19:00, 20:00 y 21:00. Un punto de atención en el gráfico, es que a pesar de que se percibe una disminución de la concentración del contaminante a las 22:00 y 23:00 horas, se aprecia nuevamente un aumento a las 24:00 h que sobrepasa el *LA*. Lo cual, de nuevo podría poner de en estado de alerta al sistema de abastecimiento (Tabla 7.5).

Tabla 7.5. *Resultados principales de la evolución del contaminante: evento a las 12:00 h*

Concentración inyectada (mg/L)	Hora de inyección	Hora de detección del contaminante	Hora en la que se pasa el *LA*	Horas de máxima concentración
230.000	12:00	13:00	14:00,	18:00, 19:00, 20:00 y 21:00

Por otro lado, la información correspondiente a los nodos en los que se presentan alarmas, debido a la presencia del contaminante, y que pasan el *LA* y el *LCS,* se presenta en la Figura 7.6 y en la Tabla 7.6.

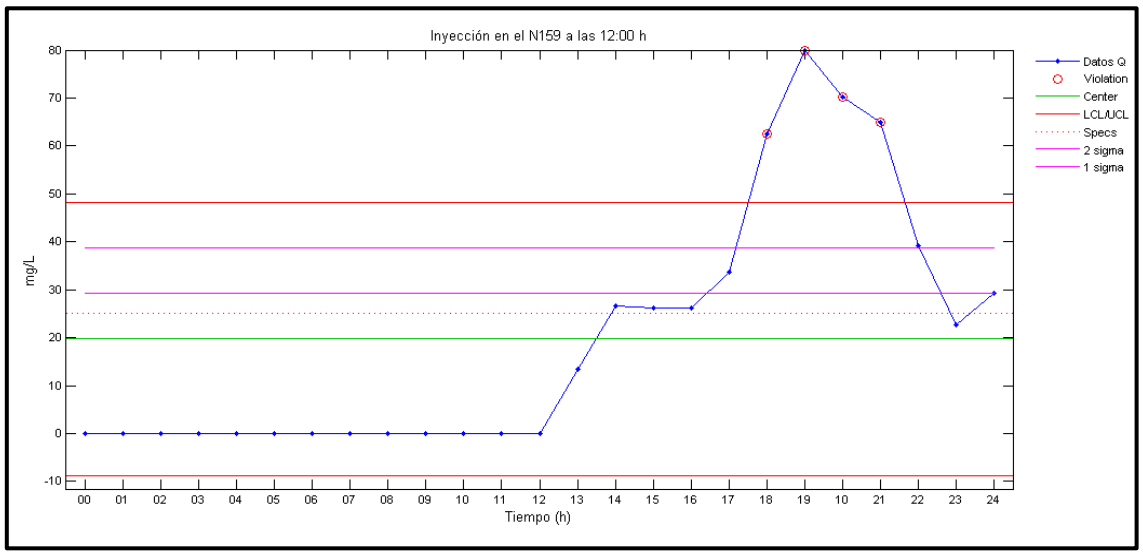

Figura 7.5. *Gráfico de control: Evolución del contaminante del evento de contaminación en el N159 a las 12:00 h*

Tabla 7.6. *Datos principales de los nodos afectados: evento a las 12:00 h*

Concentración inyectada (mg/L)	Hora de inyección	Nodos que pasan el *LA*	Nodos con la máxima concentración
230.000	12:00	35, 164, 177, 179, 184, 185, 187, 201, 204, 205, 207, 267, 273, 275	159, 161, 163, 167, 169, 171, 173, 181, 183, 189, 199, 265, 269, 271

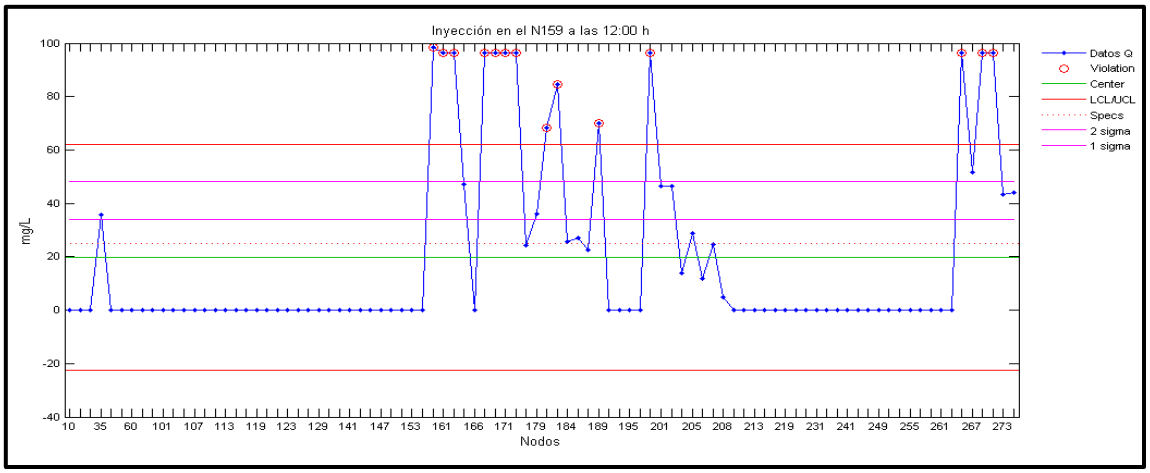

Figura 7.6. *Gráfico de control: Nodos afectados en el evento de contaminación del N159 a las 12:00 h*

7.2.4. Evento de contaminación a las 13:00 h

En lo que se refiere al evento de contaminación de las 13:00 h, un primer aspecto que se puede observar es que se presentan concentraciones más altas con respecto a los sucesos anteriores.

Se observa que la evolución del contaminante durante las 24 horas de simulación, tiene su máxima concentración a las 20:00 h. La primer alarma, cuando sobrepasa el *LA,* se presenta a las 15:00 h y a partir de ahí, empieza a incrementar la concentración. El nivel de concentración del contaminante comienza a disminuir hasta las 23:00 h (Tabla 7.7). Asimismo, el grafico de control de este evento de contaminación, (Figura 7.7), permite determinar que la red de abastecimiento está fuera de control durante 11 horas debido a la presencia del contaminante.

Tabla 7.7. *Resultados principales de la evolución del contaminante: evento a las 13:00 h*

Concentración inyectada (mg/L)	Hora de inyección	Hora de detección del contaminante	Hora en la que se pasa el *LA*	Horas de máxima concentración
230.000	13:00	14:00	15:00	19:00, 20:00, 21:00 y 22:00

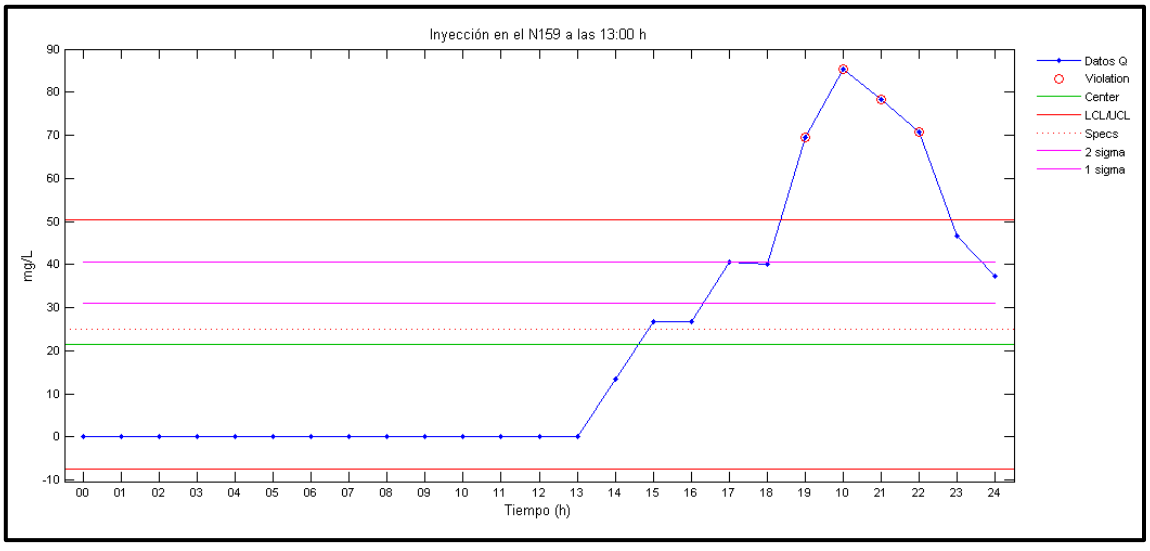

Figura 7.7. *Gráfico de control: Evolución del contaminante del evento de contaminación en el N159 a las 13:00 h*

En relación con lo anterior, el gráfico de control de la Figura 7.8 muestra los nodos que presentan alarmas, porque han excedido el *LCS* y que registran las concentraciones más altas. Asimismo, en la Tabla 7.8, se detallan los nodos que pasan el *LA* y los de máxima concentración.

Tabla 7.8. *Datos principales de los nodos afectados: evento a las 13:00 h*

Concentración inyectada (mg/L)	Hora de inyección	Nodos que pasan el *LA*	Nodos con la máxima concentración
230.000	13:00	35, 177, 179, 181, 184, 185, 187, 193, 195, 199, 201, 267, 273, 275	159, 161, 163, 167, 169, 171, 173, 183, 189, 203, 265, 269, 271

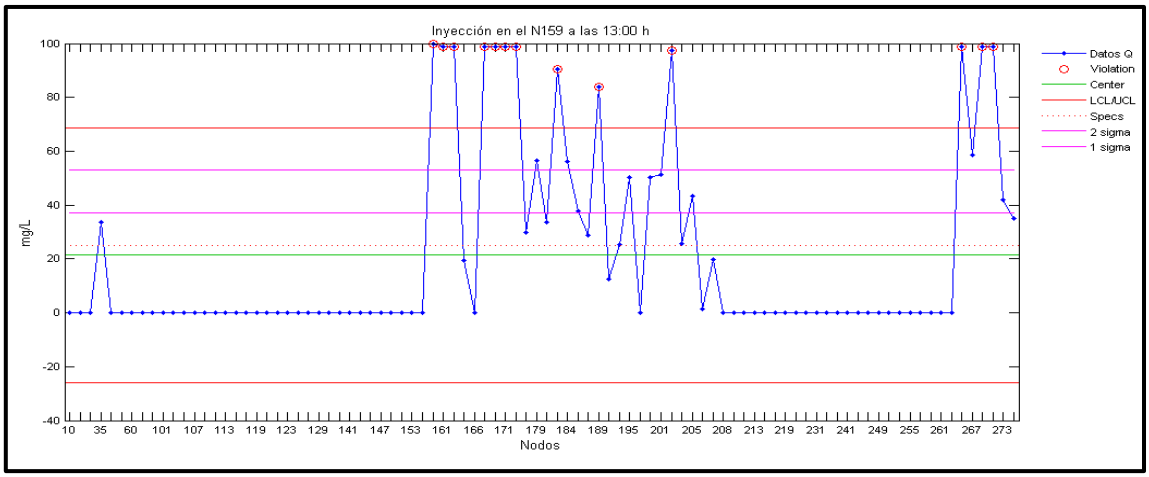

Figura 7.8. *Gráfico de control: Nodos afectados en el evento de contaminación del N159 a las 13:00 h*

7.3. ACCIONES DE MITIGACIÓN Y RESPUESTA

Pérez *et al.* (2008) introducen el contexto de la seguridad y los planes de emergencia, destacando un nuevo concepto asociado a la vulnerabilidad, que es la *resilencia*. Se entiende como tal la capacidad de recuperación del sistema después de haber sufrido un daño. Se parte de la hipótesis de que, al contrario que los eventos accidentales o los fenómenos naturales, es imposible predecir los ataques deliberados, como lo es un evento de contaminación. Ante esta perspectiva, la tendencia que predomina actualmente, es la de incrementar la *resilencia* del sistema. Por tanto, una vez conocidas las vulnerabilidades del sistema, el siguiente paso sería la planificación de las posibles acciones que deben llevarse a cabo en el caso de que se produzca cualquier tipo de daño en el sistema.

En la misma línea, Burns *et al.* (2004) señalan que las acciones de mitigación para reducir la vulnerabilidad del sistema, ante actos deliberados es muy similar a los métodos utilizados para mitigar actos de vandalismo o peligros naturales. Sin embargo, las acciones de mitigación también incluyen elementos que previenen el acceso indebido a los componentes de un sistema, los cuales, en algunos casos, puede ser contrario a facilitar el acceso que es necesario para la mitigación de un desastre involuntario. El grado en que estas medidas se

aplican depende directamente de la cantidad de riesgo aceptable y de la probabilidad de materialización del riesgo.

Los elementos y puntos vulnerables de un sistema de abastecimiento de agua pueden ser menos susceptibles a un daño si se realizan acciones de mitigación, es decir, acciones enfocadas a eliminar o reducir los efectos perjudiciales de cualquier contingencia. Las acciones de mitigación cubren una amplia variedad de actividades y pueden ser tan complejas como la readaptación de una planta de tratamiento, o tan simples como levantar muros. Sin embargo, las acciones de mitigación dependerán del tipo de peligro y del análisis de las vulnerabilidades del sistema.

Dependiendo de las características de la vulnerabilidad para un sistema de abastecimiento de agua dado, un plan de respuesta debe ser preparado para definir las medidas que serán implementadas para minimizar la probabilidad de un evento indeseable o aminorar su impacto. Los cambios en la seguridad del sistema, prácticas de monitorización, instalaciones físicas y operaciones dependen de la naturaleza de amenazas particulares.

En relación con lo anterior, este apartado trata sobre la mitigación de la vulnerabilidad a través de una propuesta de cierre de válvulas, instaladas en ciertas tuberías de la red de estudio. Con esto, se busca dificultar el paso del flujo contaminado, reduciendo el caudal que transmiten los nodos infectados a nodos sin infectar.

Las válvulas, que se localizan en las tuberías: 177, 184, 204, 215 y 225 (Figura 7.9), corresponden a las válvulas denominadas de "compuerta" o "retención". La decisión de utilizar ese tipo de válvulas, se debe a que estas válvulas que cierran o abren completamente las tuberías, no se consideran como elementos separados, sino que se incluyen como una característica de la tubería en la que se encuentran. De esta manera, no fue necesario alterar la red físicamente, ni su número de elementos.

El objetivo es analizar si el cierre de válvulas logra reducir el número de horas de los eventos de contaminación, el número de alarmas, los niveles del contaminante en la red y el número de nodos afectados.

Con base en lo anterior, se realizaron nuevamente las simulaciones de los eventos de contaminación en las horas ya establecidas, pero con la condición de cierre de las válvulas. Para ello, se establecieron las reglas de control de la hora de cierre en función del evento de contaminación y de la información proporcionada por los gráficos de control. Por lo que se determinó que las horas de cierre fueran las 03:00, 04:00, 14:00 y 15:00 horas, para cada evento respectivamente.

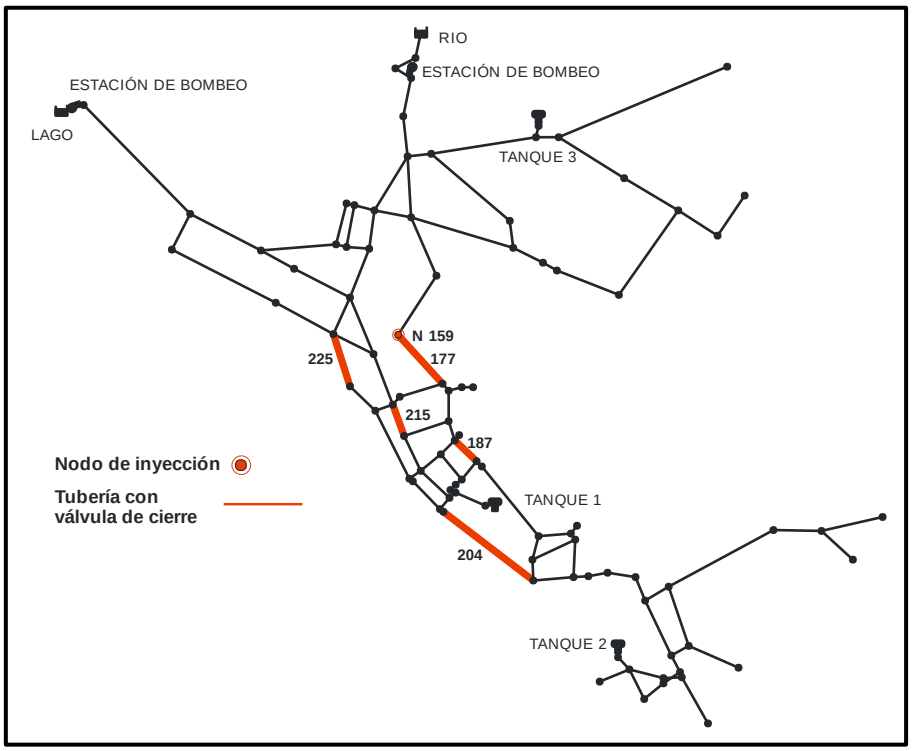

Figura 7.9. *Esquema de la red que indica las tuberías con las válvulas de cierre*

A continuación, se presentan los resultados de los gráficos de control obtenidos. Los gráficos representan tanto la evolución del contaminante en el mismo período de simulación de 24 horas, como a los nodos de la red afectados. Cabe mencionar que se conservó el mismo valor del *LA* y todas las condiciones iniciales ya descritas. Igualmente, se conservaron los criterios para la construcción de los gráficos de control.

7.3.1. Evento de contaminación a las 01:00 h

Los principales aspectos que se observan en el gráfico de control de este evento, (Figura 7.10), son: las concentraciones del contaminante son más bajas a lo largo del período de simulación, no se presentan alarmas por sobrepasar el *LA* y, finalmente, el sistema comienza estabilizarse a partir de las 13:00 h (en que las concentraciones tienden a cero). En relación con esto, en la Tabla 7.9 se resumen los principales datos del gráfico anteriormente descrito y se comparan con los resultados obtenidos de la simulación del mismo evento sin cierre de válvulas.

Tabla 7.9. *Tabla de comparación para el evento de contaminación de las 01:00 h, con base en las horas de simulación*

Estado de las válvulas	Sin cierre	Con cierre
Hora de detección del contaminante	02:00	02:00
Horas que sobrepasan el *LA*	06:00	ND
Horas de máxima concentración	07:00, 09:00 y 10:00	02:00 y 03:00
Duración del evento	9 horas	3 horas
μ del evento de contaminación	16.2783	2.24816
σ del evento de contaminación	85.2953	18.0316

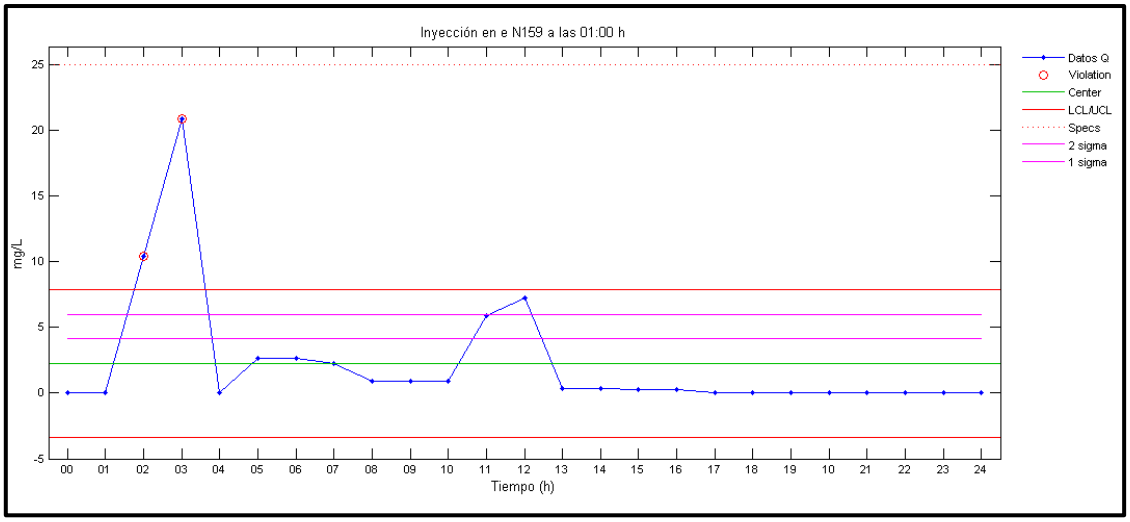

Figura 7.10. *Gráfico de control: Evolución del contaminante del evento de contaminación en el N159 a las 01:00h con cierre de válvulas*

En la Tabla 7.10 se especifican los nodos que fueron mayormente afectados durante el evento de contaminación de las 01:00 h. Además, estos resultados se comparan con los obtenidos anteriormente sin el cierre de las válvulas

Tabla 7.10. *Tabla de comparación para el evento de contaminación de las 01:00 h, con base en nodos afectados*

Estado de las válvulas	Sin cierre	Con cierre
Nodos que sobrepasan el *LA*	163, 239, 241, 249, 265, 269	159, 161, 164
Nodos con la máxima concentración	35, 159, 161, 164, 167, 169, 171, 173, 181, 199, 201, 203, 271, 273, 275	159, 161, 164, 169, 265
Duración del evento	9 horas	3 horas

μ del evento de contaminación	16.2783	2.24816
σ del evento de contaminación	56.4715	9.11826

En lo que respecta a los nodos de la red que fueron afectados, la Figura 7.11 representa el gráfico de control correspondiente a los puntos vulnerables en el evento. En este caso, se observa una disminución en el número de nodos afectados por el contaminante, debido al cierre de las válvulas, lo cual indica que con esta acción se aisló suficientemente al resto de nodos de la presencia del contaminante. Al permanecer menos puntos contaminados se facilita su control y manejo.

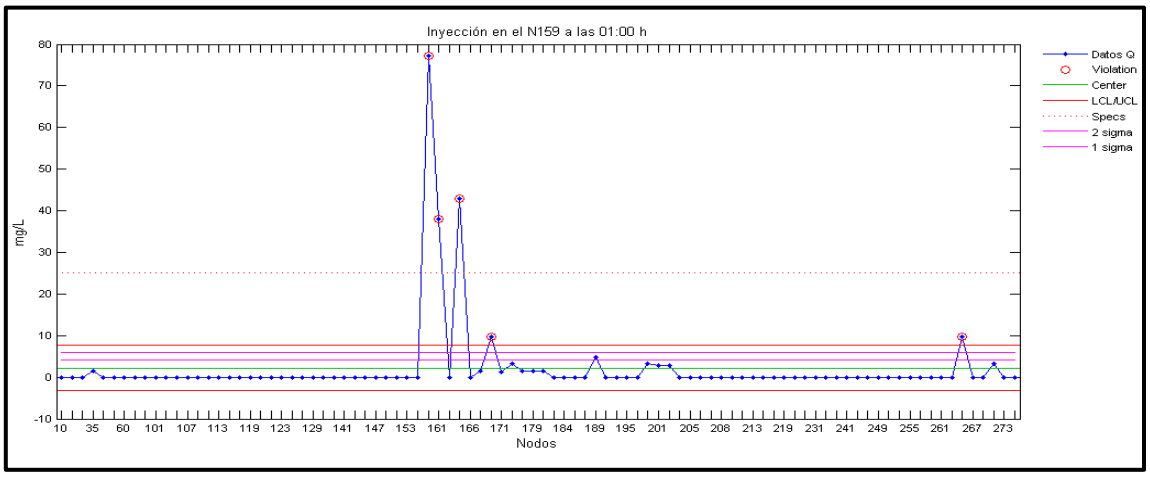

Figura 7.11. *Gráfico de control: Nodos afectados en el evento de contaminación del N159 a las 01:00 h con cierre de válvulas*

7.3.2. Evento de contaminación a las 02:00 h

De acuerdo con el gráfico de control de este evento, (Figura 7.12), la propagación del contaminante durante las 24 horas solo presenta dos horas en las que se registran concentraciones por encima del *LCS,* pero no excede el *LA*. Se advierte que, con el cierre de las válvulas, la duración del evento disminuyó de nueve a tres horas ya que a las 05:00 h la concentración del contaminante cae a cero y continúa con valores muy bajos, hasta estabilizarse a las 14:00 h. En relación con esto, la Tabla 7.11 resume la información más significativa del gráfico de control y se contrasta también, con los resultados obtenidos sin la acción de mitigación de cierre de válvulas.

Tabla 7.11. *Tabla de comparación para el evento de contaminación de las 02:00 h, con base en las horas de simulación*

Estado de las válvulas	Sin cierre	Con cierre
Hora de detección del contaminante	03:00	03:00
Horas que sobrepasan el *LA*	07:00	ND
Horas de máxima concentración	08:00, 10:00 y 11:00	03:00 y 04:00
Duración del evento	9 horas	3 horas
μ del evento de contaminación	15.8657	1.69349
σ del evento de contaminación	82.5285	13.2958

Además de lo anterior, en el gráfico de control de la Figura 7.13 y en la Tabla 7.12 se muestran los detalles de los nodos en los que se detectó mayormente la presencia del contaminante. En comparación con los resultados obtenidos sin el cierre de válvulas, el número de nodos con altas concentraciones se redujo, al igual que los nodos que sobrepasan el *LA,* de seis a dos nodos.

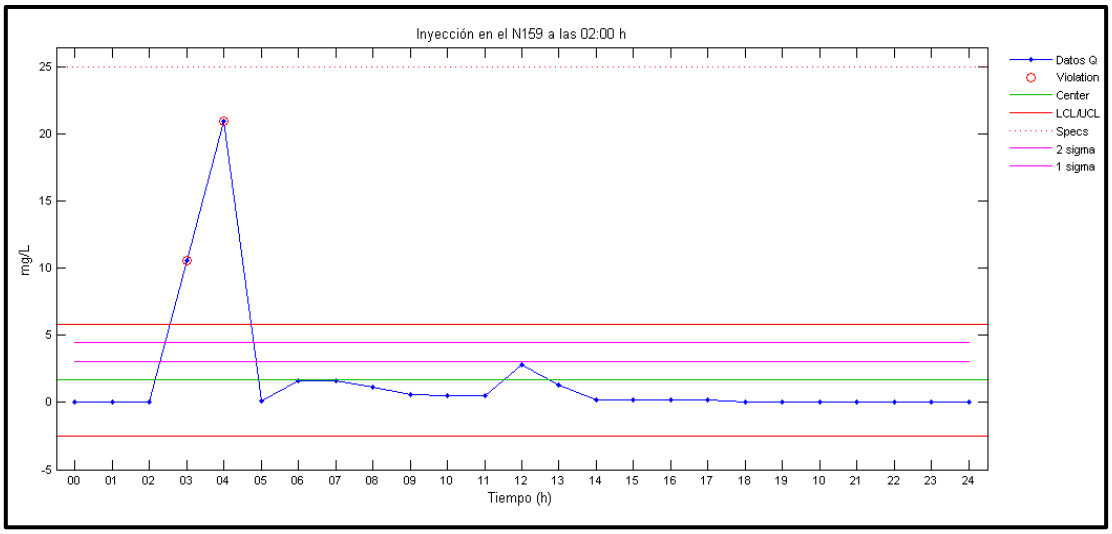

Figura 7.12. *Gráfico de control: Evolución del contaminante del evento de contaminación en el N159 a las 02:00h con cierre de válvulas*

Tabla 7.12. *Tabla de comparación para el evento de contaminación de las 02:00 h, con base en nodos afectados*

Estado de las válvulas	Sin cierre	Con cierre
Nodos que sobrepasan el *LA*	161, 163, 164, 239, 241, 249	159, 161
Nodos con la máxima concentración	35, 159, 167, 169, 171, 173, 199, 201, 203, 265, 269, 271, 273, 275	159, 161, 164, 169, 265
Duración del evento	9 horas	3 horas
μ del evento de contaminación	15.8657	1.69349
σ del evento de contaminación	55.004	6.9331

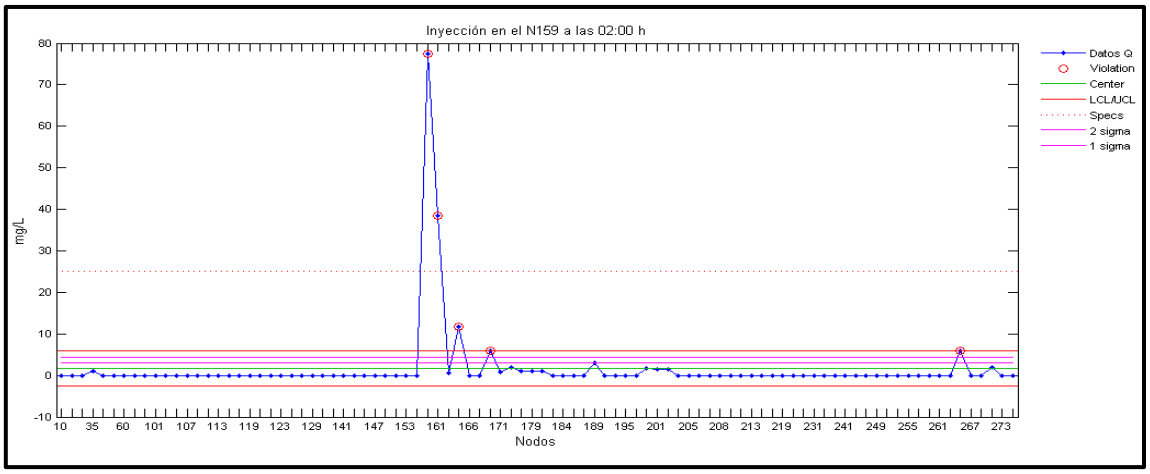

Figura 7.13. *Gráfico de control: Nodos afectados en el evento de contaminación del N159 a las 02:00 h con cierre de válvulas*

7.3.3. Evento de contaminación a las 12:00 h

Los resultados obtenidos para este evento de contaminación, con cierre de válvulas, son los que se muestran en la Figura 7.14 y en la Figura 7.15.

En el caso del gráfico de control de la evolución del contaminante en el tiempo, solo se detecta una alarma a las 14:00 h. Posteriormente las concentraciones se mantienen por debajo del *LCS*. También cabe notar, que el nivel máximo de concentración baja de 80 mg/L a 26 mg/L.

En referencia a los nodos, al igual que en los casos anteriores, se ve una gran disminución en el número de nodos con presencia del contaminante, ya que las concentraciones más altas se detectan solo en dos nodos, y sólo un nodo pasa el *LA*.

En la Tabla 7.13 y la Tabla 7.14, se observan los datos significativos observados en los gráficos de control para el mismo evento, según el estado de las válvulas.

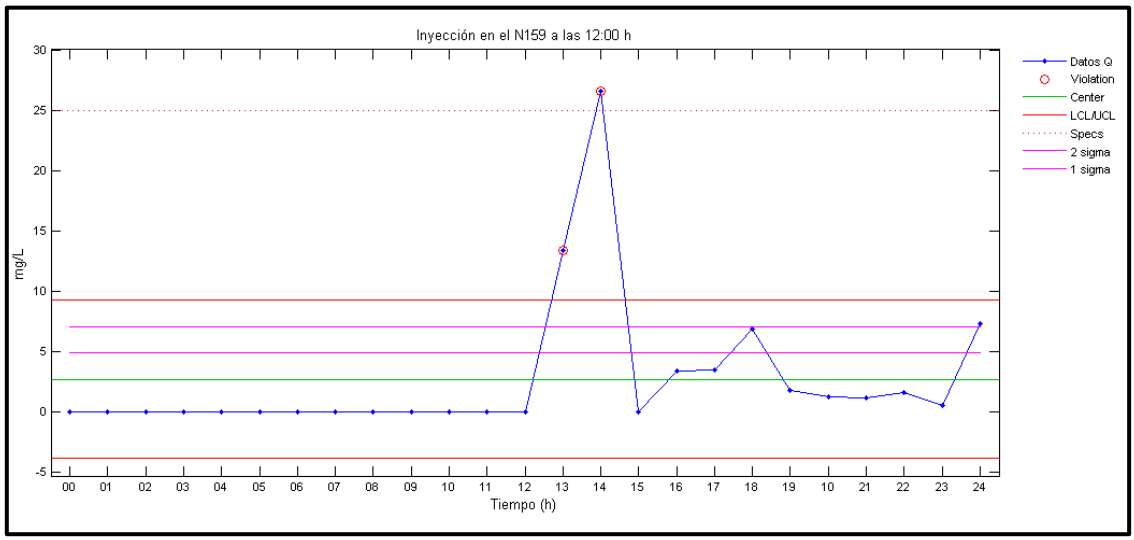

Figura 7.14. *Gráfico de control: Evolución del contaminante del evento de contaminación en el N159 a las 12:00h con cierre de válvulas*

Tabla 7.13. *Tabla de comparación para el evento de contaminación de las 12:00 h, con base en las horas de simulación*

Estado de las válvulas	Sin cierre	Con cierre
Hora de detección del contaminante	13:00	13:00
Horas que sobrepasan el *LA*	14:00	14:00
Horas de máxima concentración	18:00, 19:00, 20:00 y 21:00	13:00 y 14:00
Duración del evento	12 horas	3 horas
μ del evento de contaminación	19.7941	2.68254
σ del evento de contaminación	91.1246	20.9424

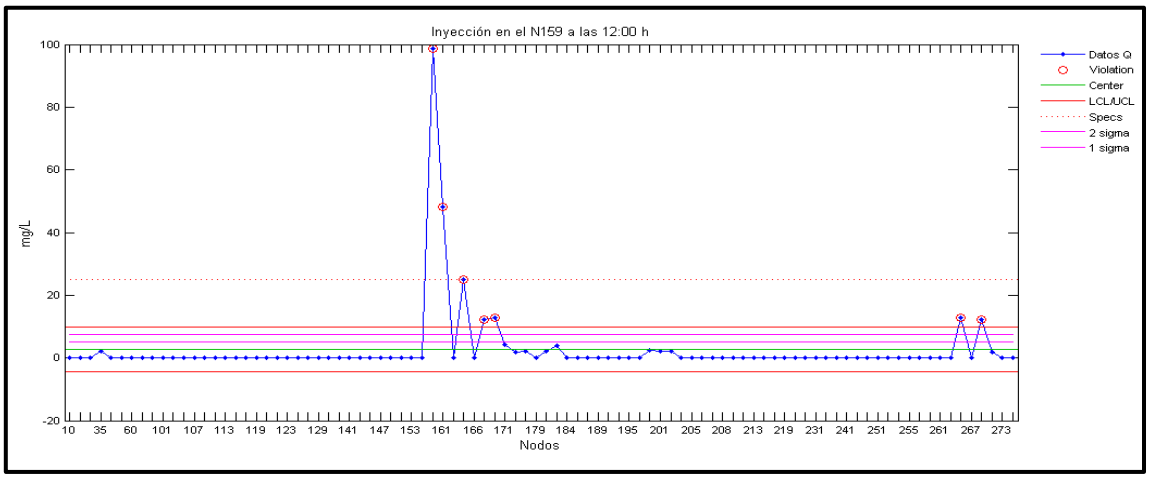

Figura 7.15. *Gráfico de control: Nodos afectados en el evento de contaminación del N159 a las 12:00 con cierre de válvulas*

Tabla 7.14. *Tabla de comparación para el evento de contaminación de las 12:00 h, con base en nodos afectados*

Estado de las válvulas	Sin cierre	Con cierre
Nodos que sobrepasan el *LA*	35, 164, 177, 179, 184, 185, 187, 201, 204, 205, 207, 267, 273, 275	159, 161, 164
Nodos con la máxima concentración	159, 161, 163, 167, 169, 171, 173, 181, 183, 189, 199, 265, 269, 271	159, 161, 164, 167, 169, 265, 269
Duración del evento	12 horas	3 horas
μ del evento de contaminación	19.7941	2.68254
σ del evento de contaminación	70.6117	11.7277

7.3.4. Evento de contaminación a las 13:00 h

Los gráficos de control obtenidos para el evento de contaminación de las 13:00 h, son los que se muestran en la Figura 7.16 y Figura 7.17. El primero, corresponde a los resultados de la evolución del contaminante a lo largo del período de simulación, y se puede observar que la primera alarma es a las 14:00 h y a las 15:00 h se pasa el *LA*. El gráfico demuestra que, en comparación con los resultados obtenidos en el apartado 7.2.4 de este mismo capítulo, se reduce el número de horas de la duración del evento, el nivel de concentración y el número de veces que se excede el *LA.* Esta comparación, se resume en la Tabla 7.15. En el segundo gráfico, los nodos en los que se detectaron altas concentraciones del contaminante también se redujeron y como se puede notar, solo en un grupo de nodos predomina el contaminante.

Tabla 7.15. *Tabla de comparación para el evento de contaminación de las 13:00 h, con base en las horas de simulación*

Estado de las válvulas	Sin cierre	Con cierre
Hora de detección del contaminante	14:00	14:00
Horas que sobrepasan el *LA*	15:00	15:00
Horas de máxima concentración	19:00, 20:00, 21:00 y 22:00	14:00 y 15:00
Duración del evento	11 horas	3 horas
μ del evento de contaminación	21.427	2.52742
σ del evento de contaminación	92.2941	19.2651

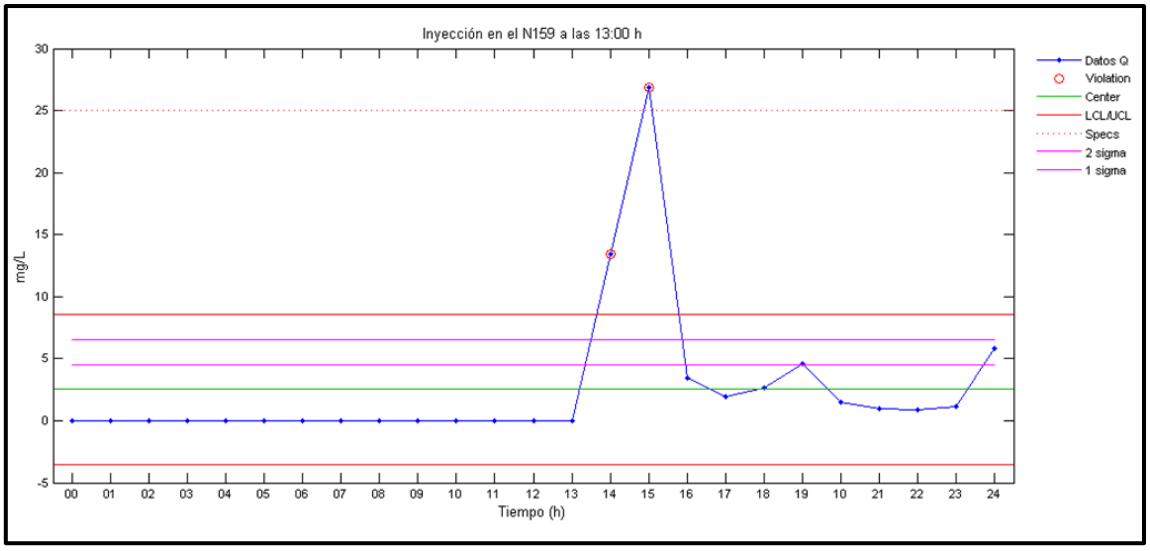

Figura 7.16. *Gráfico de control: Evolución del contaminante del evento de contaminación en el N159 a las 13:00h con cierre de válvulas*

Tabla 7.16. *Tabla de comparación para el evento de contaminación de las 13:00 h, con base en nodos afectados*

Estado de las válvulas	Sin cierre	Con cierre
Nodos que sobrepasan el *LA*	35, 177, 179, 181, 184, 185, 187, 193, 195, 199, 201, 267, 273, 275	159, 161
Nodos con la máxima concentración	159, 161, 163, 167, 169, 171, 173, 183, 189, 203, 265, 269, 271	159, 161, 163, 164, 169, 265
Duración del evento	11 horas	3 horas
μ del evento de contaminación	21.427	2.52742
σ del evento de contaminación	78.711	10.6123

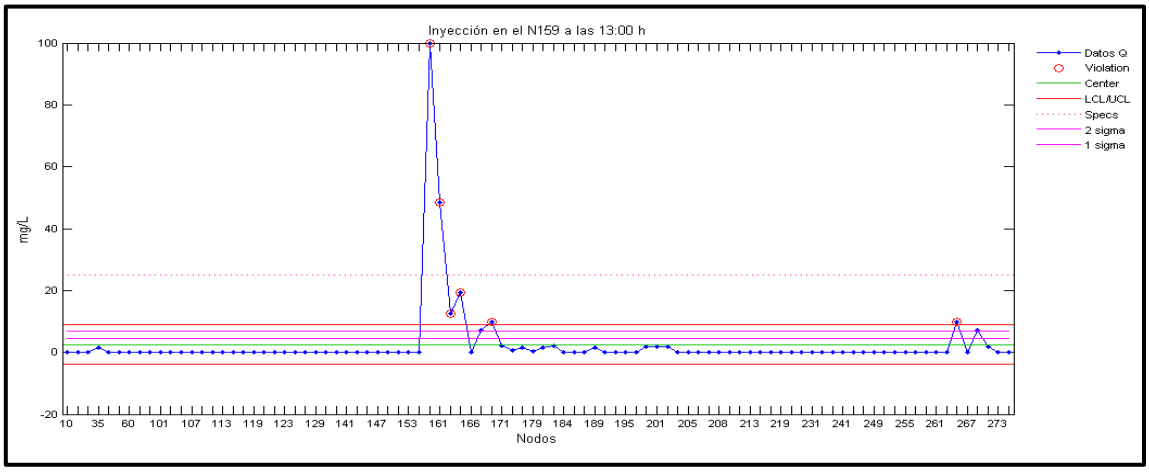

Figura 7.17. *Gráfico de control: Nodos afectados en el evento de contaminación del N159 a las 13:00 h con cierre de válvulas*

Por otro lado, con la finalidad de visualizar el efecto provocado por el cierre de válvulas se muestran los mapas de la red de distribución (Figura 7.18 y Figura 7.19) sin cierre de válvulas y con cierre de válvulas, respectivamente, para el evento de las 01:00 h. En ellos, se compara la propagación del contaminante en horas específicas, (02:00, 12:00, 13:00, 18:00, 22:00 y 24:00 horas). Se puede notar, que sin el cierre de las válvulas el contaminante sigue dispersándose hasta las 24:00 h. Mientras que con el cierre de válvulas, el contaminante desaparece a partir de las 17:00 h.

De la misma manera en la Figura 7.20 y Figura 7.21, se comparan los mapas de dispersión del contaminante del evento de las 12:00 h, en determinadas horas (14:00, 16:00, 18:00, 20:00, 22:00 y 24:00). Al igual que en el caso anterior, se observa que con el cierre de válvulas se disminuye la dispersión del contaminante en un período de tiempo menor.

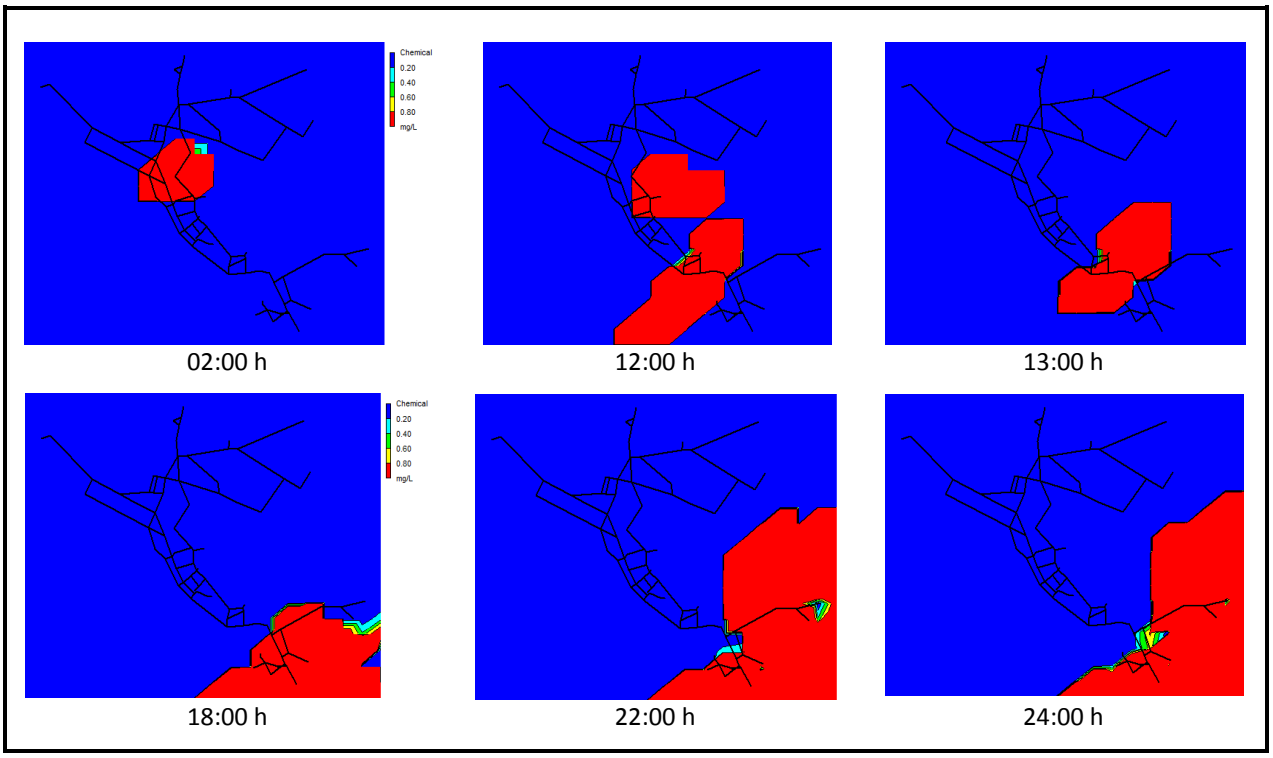

Figura 7.18. *Mapas de la dispersión del contaminante del evento de contaminación en el Nodo 159 a las 01:00h sin cierre de válvulas.*

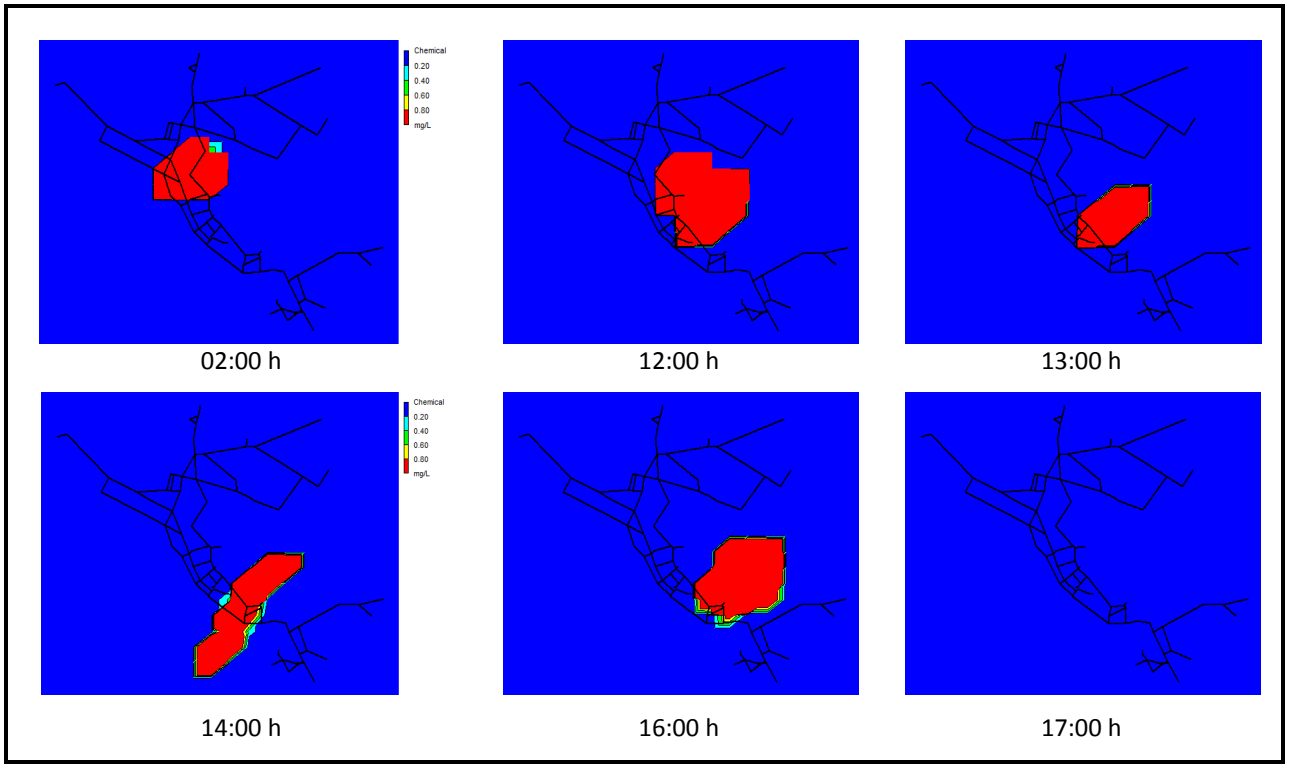

Figura 7.19. *Mapas de la dispersión del contaminante del evento de contaminación en el Nodo 159 a las 01:00h con cierre de válvulas*

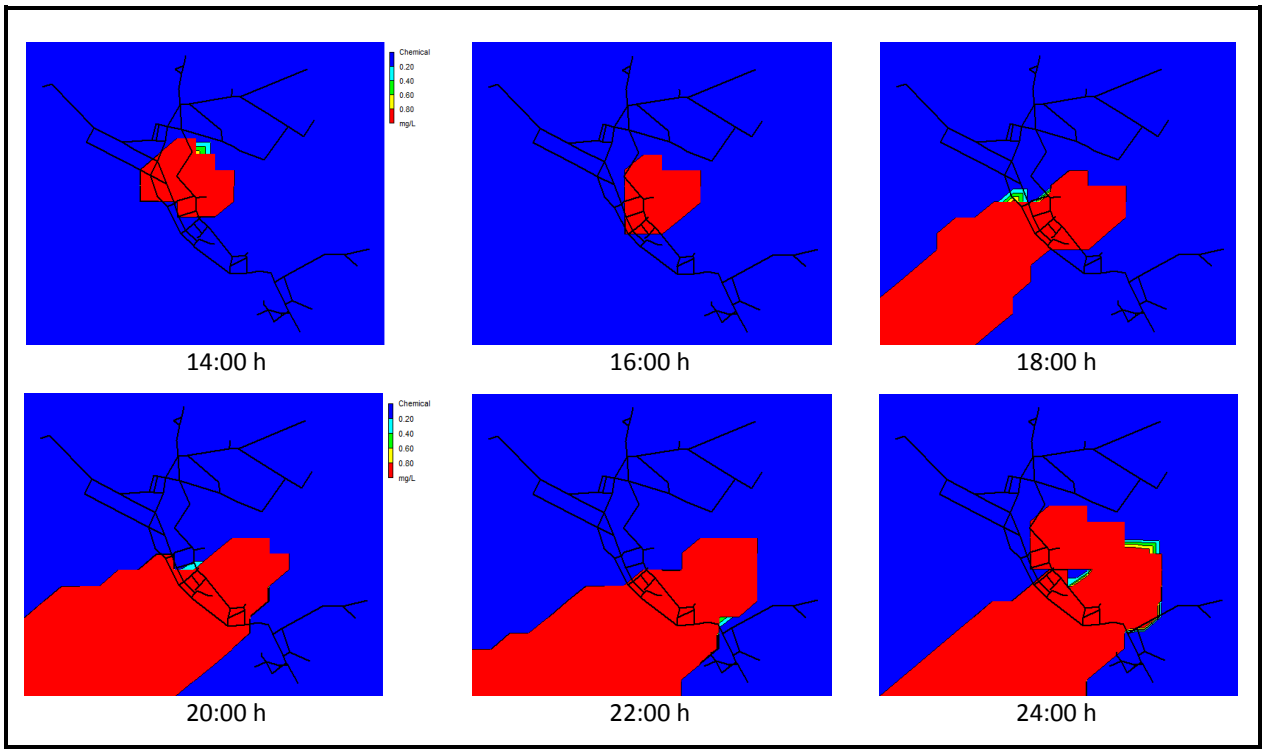

Figura 7.20. *Mapas de la dispersión del contaminante del evento de contaminación en el Nodo 159 a las 12:00h sin cierre de válvulas.*

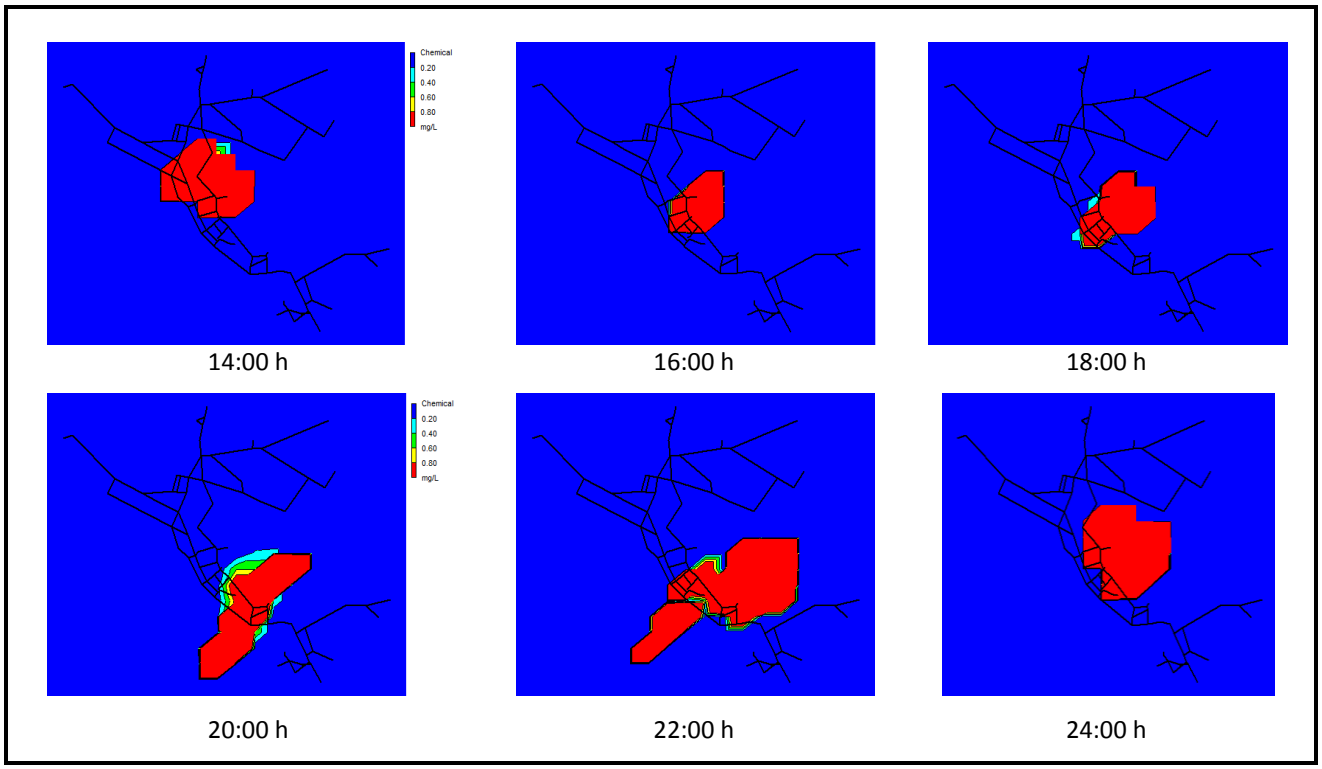

Figura 7.21. *Mapas de la dispersión del contaminante del evento de contaminación en el Nodo 159 a las 12:00h con cierre de válvulas*

7.4. RESUMEN DE RESULTADOS

Con la finalidad de tener una visión general de los resultados obtenidos para cada evento de contaminación, con y sin acción de mitigación (cierre de válvulas). A continuación, se presentan las tablas que resumen los datos más importantes observados en los gráficos de control.

7.4.1. Sin cierre de válvulas

Tabla 7.17. *Resumen de los datos significativos de los gráficos de control de los eventos de contaminación, por horas (sin cierre de válvulas).*

Hora del evento de contaminación	**01:00**	**02:00**	**12:00**	**13:00**
Hora de detección del contaminante	02:00	03:00	13:00	14:00
Horas en la que se sobrepasa el *LA*	06:00	07:00	14:00	15:00
Horas de máxima concentración	07:00, 09:00 y 10:00	08:00, 10:00 y 11:00	18:00, 19:00, 20:00 y 21:00	19:00, 20:00, 21:00 y 22:00
Duración del evento	9 horas	9 horas	12 horas	11 horas
μ del evento de contaminación	16.2783	15.8657	19.7941	21.427
σ del evento de contaminación	85.2953	82.5285	91.1246	92.2941

Tabla 7.18. *Resumen de los datos significativos de los gráficos de control, de los eventos de contaminación, por nodos, (sin cierre de válvulas).*

Hora del evento de contaminación	**01:00**	**02:00**	**12:00**	**13:00**
Hora de detección del contaminante	02:00	03:00	13:00	14:00
Nodos que sobrepasan el *LA*	163, 239, 241, 249, 265, 269	161, 163, 164, 239, 241, 249	35, 164, 177, 179, 184, 185, 187, 201, 204, 205, 207, 267, 273, 275	35, 177, 179, 181, 184, 185, 187, 193, 195, 199, 201, 267, 273, 275
Nodos con la máxima concentración	35, 159, 161, 164, 167, 169, 171, 173, 181, 199, 201, 203, 271, 273, 275	35, 159, 167, 169, 171, 173, 199, 201, 203, 265, 269, 271, 273, 275	159, 161, 163, 167, 169, 171, 173, 181, 183, 189, 199, 265, 269, 271	159, 161, 163, 167, 169, 171, 173, 183, 189, 203, 265, 269, 271
Duración del evento	9 horas	9 horas	12 horas	11 horas
μ del evento de contaminación	16.2783	15.8657	19.7941	21.427
σ del evento de contaminación	56.4715	55.004	70.6117	78.711

7.4.2. Con cierre de válvulas

Tabla 7.19. *Resumen de los datos significativos de los gráficos de control, de los eventos de contaminación, por horas (con cierre de válvulas).*

Hora del evento de contaminación	**01:00**	**02:00**	**12:00**	**13:00**
Hora de detección del contaminante	02:00	03:00	13:00	14:00
Horas en la que se sobrepasa el *LA*	ND	ND	14:00	15:00
Horas de máxima concentración	02:00 y 03:00	03:00 y 04:00	13:00 y 14:00	14:00 y 15:00
Duración del evento	3 horas	3 horas	3 horas	3 horas
μ del evento de contaminación	2.24816	1.69349	2.68254	2.52742
σ del evento de contaminación	18.0316	13.2958	20.9424	19.2651

Tabla 7.20. *Resumen de los datos significativos de los gráficos de control, de los eventos de contaminación, por nodos, (con cierre de válvulas).*

Hora del evento de contaminación	**01:00**	**02:00**	**12:00**	**13:00**
Hora de detección del contaminante	02:00	03:00	13:00	14:00
Nodos que sobrepasan el *LA*	159, 161, 164	159, 161	159, 161, 164	159, 161
Nodos con la máxima concentración	159, 161, 164, 169, 265	159, 161, 164, 169, 265	159, 161, 164, 167, 169, 265, 269	159, 161, 163, 164, 169, 265
Duración del evento	3 horas	3 horas	3 horas	3 horas
μ del evento de contaminación	2.24816	1.69349	2.68254	2.52742
σ del evento de contaminación	9.11826	6.9331	11.7277	10.6123

8. CONCLUSIONES

Si bien las técnicas de control estadístico de procesos originalmente han sido desarrolladas en procesos industriales para verificar la calidad de los productos y minimizar los posibles defectos en la producción, estas pueden ser aplicadas a otro tipo de eventos en los que se requiera detectar cambios o desajustes en una variable, siendo en este caso anomalías en la calidad del agua de una red de distribución.

El enfoque presentado permitió que, por medio de un gráfico de control, se detectara y observara la magnitud e intensidad de las variaciones debido a la intrusión del contaminante. Asimismo, fue posible saber acerca del funcionamiento del sistema durante y después de los eventos de contaminación.

Por otro lado, la propuesta de las acciones de mitigación confirmó que la combinación de los gráficos de control, tanto para determinar los nodos afectados, como para observar la evolución del contaminante a lo largo del período de simulación, permite determinar el tiempo, del cual se dispone, para efectuar acciones que mitiguen o eviten la mayor dispersión del contaminante a lo largo de la red.

8.1. LÍNEAS DE INVESTIGACIÓN (TRABAJOS FUTUROS)

Con base en el desarrollo y los resultados alcanzados en la tesis, se propone el seguimiento del tema con las siguientes líneas de investigación complementarias:

- Evaluar otras técnicas del *SPC* para poder comparar tiempos de detección, sensibilidad y la probabilidad de detección y así, poder establecer tanto la localización como el número de sensores adecuado para ese sistema de abastecimiento.

- Definición de una red de sensores con base en métodos heurísticos para resolver algoritmos de cubrimiento y localización de teoría de grafos, lo que permitirá una óptima ubicación de los recursos necesarios para el control de la calidad del agua dentro de la red de distribución.

- Definición de áreas de riesgo mediante grafos de regularización que señalarán la importancia relativa de cada nodo dentro de la red.

Por otro lado, debido a que el uso de un sistema de sensores involucra la participación significativa de capital y gastos operacionales, se requiere:

- Identificar los beneficios marginales por introducir sensores adicionales, como guía en el establecimiento del número apropiado de sensores para diferentes redes de distribución de agua, ya que cada red tiene características diferentes que la hacen única.

- Elaboración de estudios de vulnerabilidad y de planes para la gestión de emergencias, la implantación de medidas de seguridad, vigilancia y monitorización e instalaciones redundantes, bajo criterios económicos. Ya que, disponer de un sistema de distribución de agua seguro y fiable, implica una inversión considerable.

9. REFERENCIAS BIBLIOGRÁFICAS

Alzamora, F. y Ayala, H. (2006). "Optimal sensor location for detecting contamination events in water distribution systems using topological algorithms" Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Apostolakis, G. y Lemon, D., (2005). "A Screening Methodology for the identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism". Risk Analysis, Vol. 25, No. 2, pp. 361-376.

Baker III, G., (2003). "A Vulnerability Assessment Methodology for Critical Infrastructure Facilities". James Madison University.

Benneyan, J., (1998). "Use and interpretation of statistical quality control charts." International Journal for Quality in Health Care. Vol. 10, No. 1, pp. 69-73.

Bodou, R., (2006). "Évaluation de la vulnérabilité d'une ville face à son réseau d'eau potable: une aproche para conséquences". Maîtrise és sciences appliquées. École polytechnique de Montréal. Université de Montréal. Septiembre, 126. pp.

Burns, L.; Cooper, C.; Dobbins, D.; Edwards, J. y Lampe, L., (2004). "Security Analysis and response for water utilities". Chapter 20. Urban water supply handbook., McGraw-Hill, pp. 20.1-20.24.

Chastain Jr. J., (2004). "A heuristic Methodology for Locating Monitoring Stations to Detect Contamination Events in Potable Water Distribution Systems". Ph. D. Department of Environmental and Occupational Health College of Public Health University of South Florida. Octubre, 200 pp.

Chastain Jr., J., (2006). "Methodology for Locating Monitoring Stations to Detect Contamination in Potable Water Distribution Systems". Journal of Infrastructure Systems. Vol. 12, No. 4, Diciembre 1, pp. 252-259.

Clark, R. y Deininger, R., (2000). "Protecting the Nation´s Critical Infrastructure: The Vulnerability of U. S. Water Supply Systems". Journal of Contingencies and Crisis Management, Vol. 8, No. 2, Junio, pp. 73-80.

Clark, R.; Grayman, W.; Buchberger, S.; Lee y Hartman, D (2004). "Drinking water distribution systems: An overview". Chapter 4. Water Supply System Security. McGraw-Hill, pp. 4.1-4.49.

Coburn, A.; Spence, R. y Pomois, A., (1994). "Vulnerability and Risk Assessment". Second Edition, UNDP Disaster management training programe.

Doré, M., (2004). "Définitions et caractéristiques du risqué". Acétates du cours IND 6126. École Politechnique de Montréal: Départament de Mathématiques et de Génie Industriel.

Dorini, G.; Jonkergouw, P.; Kapelan, Z.; di Pierro, F.; Khu, S.; y Savic, D., (2006). "An efficient algorithm for sensor placement in water distribution systems." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Einarsson, S. y Rausand, M., (1998). "An Approach to Vulnerability Analyasis of Complex Industrial Systems". Risk Analysis, Vol. 18, No. 5, pp. 535-546.

Eliades, D. y Polycarpou, M., (2006) "Iterative deepening of Pareto solutions in water sensor Networks." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Ezell, B., (2007). "Infrastructure Vulnerability Assessment Model (I-VAM)". Risk Analysis, Vol. 27, No. 3, pp. 571-583.

Fallah, M. y Akhavan, S., (2009). "A new monitoring design for uni-variate statistical quality control charts". Information Sciences Vol. 180, pp. 1051-1059

Ghimire, S. y Barkdoll, B., (2006). "Heuristic method for the battle of the water network sensors: Demand-based approach." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Gleick, P., (2009). "Water Conflict Chronology". Pacific Institute for Studies in Development, Environment, and Security, disponible en http://www.worldwater.org/conflict.htm

Grayman, W.; Deininger, R.; Males, R. y Gullick R., (2004). "Source water early warning systems". Chapter 11. Water Supply System Security. McGraw-Hill, pp. 11.1-11.33.

Grigg, N., (2003). "Water Utility Security: Multiple Hazards and Multiple Barriers". Journal of Infrastructure Systems, Vol. 9, No. 2, June, pp 81-88.

Guan, J.; Aral, M.; Maslia, M. y Grayman, W.; (2006). "Optimization model and algorithms for design of water sensor placement in water distribution systems." Proc. 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Haestad, M.; Walski, T.; Chase, D.; Savic, D.; Grayman, W.; Backwith, S. y Koelle, E., (2003) "Advanced Water Distribution Modeling and Management", Haestad Press, Waterbury, CTUSA.

Haimes, Y., (2006). "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures". Risk Analysis Vol. 26, No. 2, pp. 293-296.

Haimes, Y.; Matalas, N.; Lambert, J.; Jackson, B.; y Fellows, J., (1998). "Redución Vulnerability of Water Supply Systems to Attack". Journal of Infrastructure Systems Vol. 4, No. 4, Diciembre, pp. 164-177.

Hasan, J.; Stanley S.; Deininger, R. (2004.). "Safeguarding The Security Of Public Water Supplies Using Early Warning Systems: A Brief Review". Journal of Contemporary Water Research and Education, No. 129 October, pp 27-33.

Huang, J.; McBean, E.; y James, W.; (2006). "Multiobjective optimization for monitoring sensor placement in water distribution systems." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Hudrey, S. y Krewski, D., (1995)."Is there a safe level of exposure to a carcinogen?". Environmental Science and Technology. Vol. 29, No. 8, 370 pp.

Krause, A., Leskovec, J.; Isovitsch, S.; Jianhua, X.; Guestrin, C.; VanBiresen, J.; Small, M. y Fischbeck, P., (2006). "Optimizing sensor placements in water distribution systems using submodular function maximization." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Lee, M., (2006). "Risk Assessment of Drinking Water Supply Failures in Canada". Master Thesis, University of Guelph, August, 116 pp.

Li, H., (2007). "Hierarchical Risk Assessment of Water Supply Systems".Ph. D. Department of Civil and Building Engineering Loughborough University. Marzo, 217 pp.

Matalas, N., (2005) "Acts of Nature and Potential Acts of Terrorists: Contrast Relative to Water Resource Systems" (Editorial). Journal of Water Resources Planning and Management, Vol. 131, No. 2, Marzo-Abril, pp. 79-80.

Mays, L., (2004). "Water Supply Security: An introduction". Chapter 1. Water Supply Systems Security. McGraw-Hill, pp. 1.1-1.12.

Moglia, M.; Burn, S.; Meddings, S., (2006). "Decision Support System for Water Pipeline Renewal Prioritisation". ITcon Vol. 11, Special Issue Decision Support Systems for Infrastructure Management, pp. 237-256, publicación electrónica <http://www.itcon.org>

Montgomery, D., (2004). "Control estadístico de la calidad". Tercera edición. Limusa Wiley, México, 823 pp.

Moteff, J.; Copeland, C. y Fischer, J., (2003). "Critical Infrastructures: What Makes an Infrastructure Critical?". Report for Congress. Congressional Research Service. The Library of Congress. Enero, 20 pp.

Munshi, D., (2003). "Pipelines Have Help Available to Safeguard Their SCADA Systems," Pipeline Gas J., disponible en: http://www.pipelineandgasjournal.com.

Murray, A. and Grubesic, T., (2007). "Critical Infrastructure. Reliability and Vulnerability. Advances in Spatial Science". Springer, Enero.

NESS, (2003) "Preventing Earthquake Disasters. The grand challenge in earthquake engineering". A research Agenda for the Network for Earthquake Engineering Simulation (NESS). Committee to Develop a Long-Term Research. Board on Infrastructure and the Constructed Environment Division on Engineering and Physical Sciences. National Research Council of the National Academies

O'Shea, K., (2003). "Cyber Attack Investigative Tools and Technologies". Institute for Security Technology Studies at Dartmouth College, Hanover, NH, disponible en: http://htcia_siliconvly.org/contacts.htm

Ostfeld, A.; Uber, J.; Salomons, E.; Berry; J.; Hart; W.; Phillips, C.; Watson, J.; Dorini, G.; Jonkergouw, P.; Kapeland, Z.; Di Pierro, F.; Khu, S.; Savic, D.; Eliades, D.; Polycarpou, M.; Ghimire, S.; Barkdoll, B.; Gueli, R.; Huang, J.; McBean, E.; James, W.; Krause, A.; Leskovec, J.; Isovitch, S.; Xu, J.; Guestrin, C.; VanBriesen, J.; Small, M.; Fischbeck, P.; Preis, A.; Propato, M.; Piller, O.; Trachtman, G.; Wu, Z. y Walski, T., (2008). "The Battle of the Water Sensor Networks (BWSN): A Design Challenge for Engineers and Algorithms". Journal of Water Resources Planning and Management. Vol. 134, Nº 6, November, pp 556-568.

Ostfeld, A., y Salomons, E., (2006). "Sensor network design proposal for the battle of the water sensor networks (BWSN)." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Ostfeld, A., y Salomons, E., (2004). "Optimal Layout of Early Warning Detection Stations for Water Distribution Systems Security". Journal of Water Resources Planning and Management, Vol. 130, No. 5, Septiembre, pp. 377-385.

Panguluri, S., Phillips, W. y Clark, R., (2004). "Cyber threats and IT/SCADA system vulnerability". Chapter 5, Water Supply Systems Security. McGraw-Hill, pp. 5.1-5.18.

Pérez-García, R.; Izquierdo, J.; Herrera, M.; Tavera, M.; Gutiérrez, J., (2008). "Aplicación de los sistemas de información y decisión en la predicción de escenarios de riesgo en sistemas de abastecimiento de agua". VIII Seminário Ibero-Americano sobre Sistemas de Abastecimiento e Drenagem (SEREA). "Alterações Climáticas e Gestão da Água e Energia em Sistemas de Abastecimiento e Drenagem". Lisboa, Portugal. Julio. Memoria de Congreso. 17 pp.

Pérez-García, R.; Izquierdo, J.; Herrera, y Gutiérrez, J., (2009). "La vulnerabilidad en los sistemas de abastecimiento de agua: prevención, alerta temprana y recuperación". IX Seminario Iberoamericano sobre Planificación, Proyecto y Operación de Sistemas de Abastecimiento de Agua (SEREA). Valencia, España, Noviembre. Memoria de Congreso.

Prat, A.; Grima, P.; Tort-Martorell, X. y Pozueta, L., (1997). "Métodos estadísticos. Control y mejora de la calidad". Ediciones de la Universidad Politécnica de Catalunya, SL. Barcelona, España. 300 p.

Preis, A., y Ostfeld, A., (2006). "Multiobjective sensor design for water distribution systems security." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Propato, M., y Piller, O., (2006). "Battle of the water sensor networks." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Qiao, J., (2005). "Security enhancement and consequence mitigation strategies for water infrastructure against physical destruction". Ph.D. Thesis, Purdue University, December, 158 pp.

Schneier, B., (1999). "Attack Trees: Modeling security threats" Dr. Dobb's J., disponible en: http://www.counterpane.com/attacktrees-ddj-ft.html.

Thomas, N., (2006). "Report for 2005RI34B: Risk Assessment Methods for Water Infrastructure Systems", Rhode Island Water Resources Center, University of Rhode Island, Kingston, RI. 22 pp.

Trachtman, G., (2006). "A 'strawman' common sense approach for water quality sensor site selection." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

US-EPA, (2010). http://www.epa.gov/nhsrc/water/teva.html#_epanet

Wang, W., Zhang, W. (2008). "Early defect identification: application of statistical process control methods". Journal of Quality in Maintenance Engineering. Vol. 14, No. 3. pp. 225-236.

Wu, Z. y Walski, T., (2006). "Multiobjective optimization of sensor placement in water distribution systems." Proc., 8th Annual Water Distribution System Analysis Symp., Cincinnati.

Ye, N., Vilbert, S., and Chen, Q., (2003). "Computer Intrusion Detection Through EWMA for Autocorrelated and Uncorrelated Data". IEEE Transactions on Reliability, Vol. 52, No. 1, March, pp75-82.