

# APLICACIÓN DE MINERÍA DE DATOS EN GERENCIAMIENTO DE ALARMAS- CASO DE ESTUDIO

Jenny Carolina Saldaña Cortes

Ing. Químico

Msc.en Economía

DBA -Doctor of Business Administration (Estudiante)

Bogotá D.C,

Colombiajenny.saldana@uexternado.edu.co

Jairo de Jesús Ramírez Mongui

Ingeniero de Automatización

Msc. Gerencia de Innovación (Estudiante)

Bogotá, Colombia

Jairo.ramirez01@est.uexternado.edu.co

**Resumen**—El objetivo de esta investigación es realizar un análisis descriptivo y por minería de datos de una crónica de eventos generada por un sistema de control para el gerenciamiento de alarmas mediante los lineamientos de la norma ANSI/ISA 18.2 usando herramientas analíticas de minería de Datos.

**Palabras clave** — Gerenciamiento de alarmas, minería de datos y crónica de eventos.

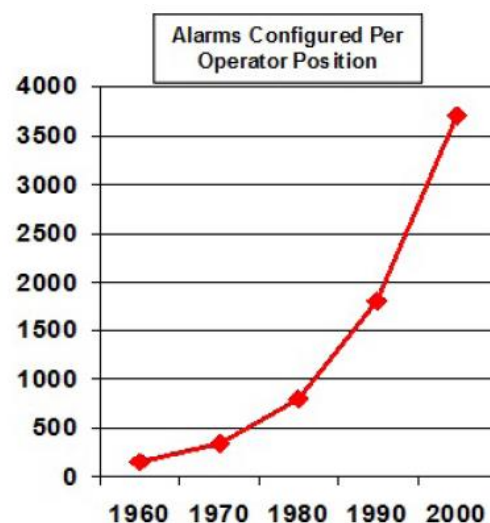
## I. INTRODUCCIÓN

El arribo de los sistemas de control, dispositivos inteligentes y el incremento de la capacidad de procesamiento de los computadores en el control y monitoreo de procesos industriales, ha desembocado en una generación de datos e información relevante para el desempeño eficiente de las operaciones en las plantas industriales; sin embargo para un completo entendimiento de esta información y de los fenómenos propios identificados dentro de la misma, es requerido la aplicación de herramientas como la minería de datos para la toma de decisiones y optimización de las operaciones citadas.

## II. DESCRIPCIÓN DEL PROBLEMA

Los grandes volúmenes de información que manejan los actuales sistemas de control hacen necesario de un análisis más detallado de los eventos iniciales para un correcto análisis de falla o peligros que se encuentren ocultos. La flexibilidad con la que cuentan los sistemas de control actuales para la configuración y administración de los sistemas de alarmas ha producido un incremento en el número de eventos y alarmas reportados al operador de la planta (Figura 1).

**Figura 1.** Crecimiento exponencial de las alarmas configuradas por operador



Fuente: (Hollifield, Alarm Management: The seven step approach for significant improvement, 2011)

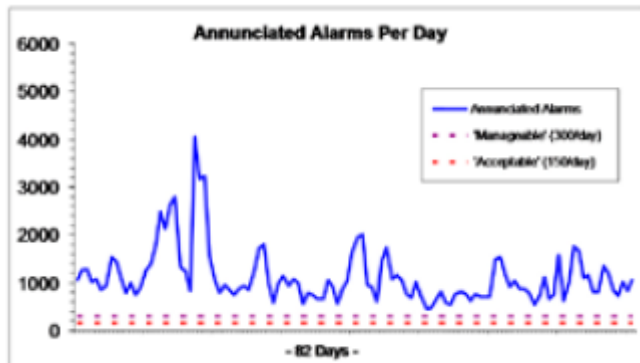
Adicional al incremento en las alarmas configuradas se tienen identificadas fallas operacionales las cuales comprometen la integridad de las operaciones (Hollender & Carsten, 2007)); dentro de estas se pueden resaltar:

- Alarmas permanentes durante largos periodos de tiempo (días o semanas).
- Reconocimiento masivo de alarmas sin investigación (Reconocimiento “Ciego”).
- Operadores que no valoran las alarmas como sistema de ayuda.
- Alarmas sonoras desactivadas para evitar una constante contaminación acústica.

Estos tipos de fallas operacionales combinado con la facilidad de configuración para alarmas y eventos de los

sistemas de control, desencadenan avalanchas de alarmas anunciadas en los cuartos de control que son de difícil manejo en la operación diaria (Figura 2).

**Figura 2.** Rata de alarmas día excedida



Fuente: (Hollifield & Habibi, *Alarm Management a comprehensive*, 2015)

Eventos catastróficos registrados por un mal manejo del gerenciamiento de alarmas se puede presentar con casos como (Marina, 2014):

- Central nuclear de three mile island (1979): Una serie de fallos y errores operaciones dieron como resultado una fuga de material radioactivo a la atmosfera.
- Plataforma petrolera Piper Alpha (1988): Una acumulación de errores y decisiones cuestionables dieron lugar a una fuga de gas que finalmente explosiono en una plataforma offshore. Esto causo un incendio catastrófico, 167 muertos y billones de dólares en daños
- Refinería Texaco en Milford Haven (1994): las inestabilidades y perturbaciones causadas en la planta por una fuerte tormenta eléctrica, dieron lugar a una combinación de fallos en los equipos, el sistema de control y la gestión, que terminaron cinco horas más tarde con una importante explosión. Como consecuencia 26 personas resultaron heridas y se produjeron daños por valor de 48 millones de libras.

### III. GERENCIAMIENTO DE ALARMAS Y MINERÍA DE DATOS

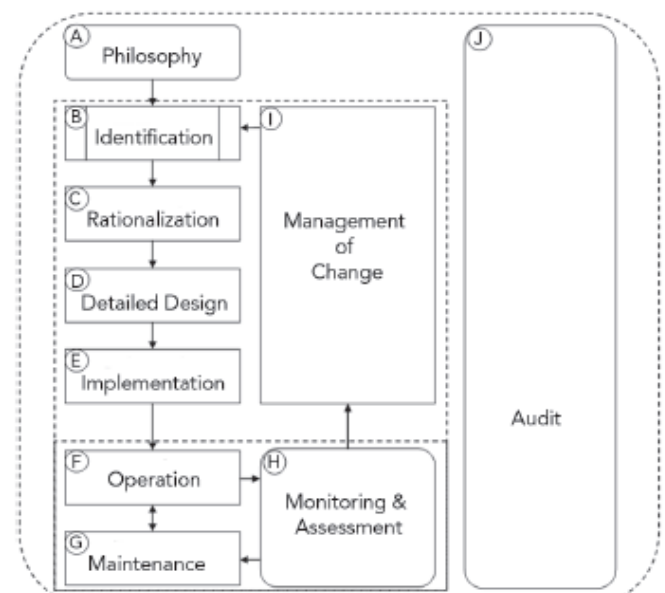
Diferentes organismos internacionales coordinaron la creación de la ANSI/ISA 18.2 la cual tiene como propósito:

*Direccionar el desarrollo, diseño, instalación y administración de sistemas de alarmas en procesos industriales* ( (International Society of Automation, 2009))

Esta norma busca orientar los esfuerzos del personal a cargo del manejo de los sistemas de control, operaciones y supervisores para un correcto análisis de eventos y prevenir el suceso de situaciones críticas en las plantas industriales.

El estándar ANSI/ISA 18.2 (Figura 3), lo componen las etapas: a) el desarrollo de la filosofía de alarmas, b) identificación de malos actores, c) Proceso de racionalización, d) diseño en detalle de la alarma, e) proceso de implementación, f) operación del sistema, g) procedimiento de mantenimiento, h) monitoreo y administración, i) administración de cambios y j) auditoria ( (International Society of Automation, 2009)).

**Figura 3.** Ciclo de vida del gerenciamiento de alarmas



Fuente: (Hollifield, *Understanding and applying the ANSI/ISA 18.2 Alarm Management standard*, 2010)

La norma plantea una identificación de métricas en la etapa de monitoreo y administración (H), para un seguimiento de la implementación de la norma (Gomez & Romero, 2011); sin embargo, la norma tiene una aplicación de la estadística descriptiva, donde solo se realiza una ponderación media de los eventos que se presentan en el sistema de alarmas y no contempla una relación causal dentro los eventos (Figura4 ).

**Figura4 . Indicadores clave de desempeño**

INDICADOR			VALOR		
Tasa promedio de alarmas anunciadas por operador			Una alarma desplegada en un periodo de 10 minutos en promedio. (1 alarma/10 min) promedio.		
Tasa pico promedio de alarmas anunciadas por operador			Menos de 10 alarmas en 10 minutos.		
Avalanchas de alarmas			Menos de 1% de los periodos de 10 minutos reportados.		
Alarmas repetitivas			0		
Alarmas espurias			0		
Alarmas antiguas			0		
DISTRIBUCIÓN DE PRIORIDADES:			PORCENTAJES:		
BAJA	MEDIA	ALTA	80%	15%	5%

Fuente: (Gomez & Romero, 2011)

## MINERÍA DE DATOS

La minería de datos o *Data Mining* es una técnica computacional de tratamiento de grandes volúmenes de información que busca identificar: patrones, perfiles y tendencias, por medio de la aplicación de relaciones estadísticas y sistemas expertos. El objetivo principal de esta técnica es dar soporte a las decisiones de negocio y aproximar un comportamiento futuro con los modelos generados (Pérez López & Satín González, 2007).

La minería de datos es una etapa dentro de la *extracción de conocimiento a partir de bases de datos (KDD)*, la cual es posterior a la depuración de los datos de diferentes sistemas (selección, pre procesamiento y transformación), una vez identificados los patrones en la etapa de minería de datos se obtiene el conocimiento propiamente dicho (Figura 4); En el caso de los análisis realizados para el gerenciamiento de alarmas las etapas de filtrado son más sencillas por ser generadas por

sistemas de control de forma automática y del tipo texto para su correspondiente análisis.

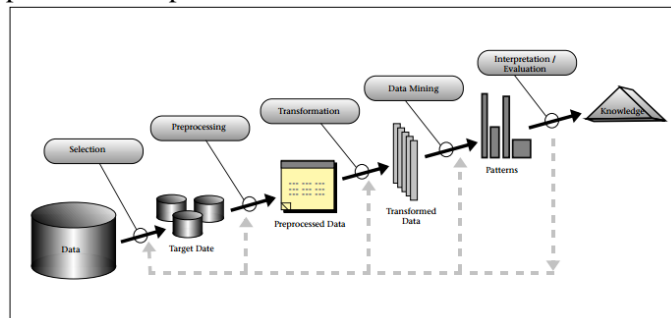
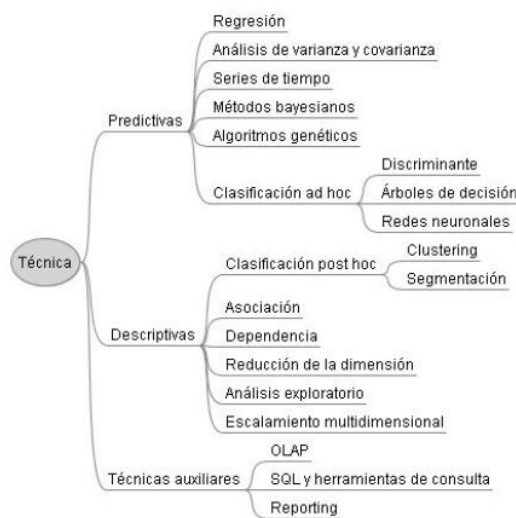


Figura 4 Resumen de pasos que componen el KDD

Fuente: (Fayyad, Piatetsky-Shapiro, & Smyth, 1996)

Las técnicas empleadas en la minería de datos pueden clasificarse entre herramientas predictivas, herramientas descriptivas (herramientas de descubrimiento de modelos, patrones e información no evidente) y auxiliares (herramientas de verificación); estas últimas principalmente para el reporte visual del usuario final (Figura 5).

**Figura 5. Clasificación de técnicas de la minería de datos**



Fuente: (Pérez López & Satín González, 2007)

Aunque la norma ANSI/ISA 18.2 establece dentro de sus métricas herramientas del tipo descriptivo (alarmas por minuto, picos de alarmas, porcentajes de alarmas anunciados en condiciones de lluvia de alarmas,

distribución por prioridad, entre otras), estas no tienen el mismo alcance cuantitativo de las herramientas descritas en la clasificación de técnicas de la minería de datos (Clustering/segmentación, escalamiento, reglas de asociación, análisis exploratorio y reducción de dimensión).

#### IV. IMPORTANCIA Y JUSTIFICACIÓN

A medida que las plantas industriales se hacen más grandes y complejas se requiere un sistema de alarmas cada vez más sofisticado para informar a los operadores de los posibles fallos. Con cientos de procesos diferentes ejecutándose simultáneamente, los operadores pueden verse obligados a responder en cualquier momento a varias alarmas, incluso en condiciones normales. Si la gestión no es eficiente, hasta el operador más diligente puede pasar por alto una alarma. Incluso es posible que se desactiven alarmas persistentes con consecuencias potencialmente catastróficas (Hollender & Carsten, 2007).

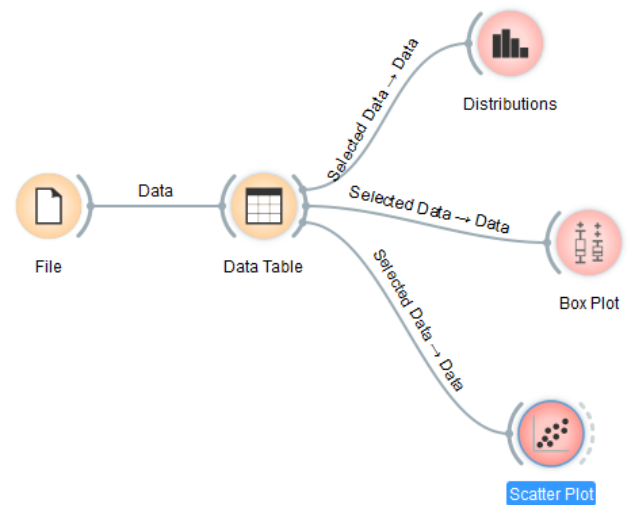
Por lo anterior se propone como objetivo general:

- Optimización del proceso de gerenciamiento de alarmas mediante la aplicación de la minería de datos para la detección de malos actores y generación de modelos predictivos.

#### V. ANÁLISIS DESCRIPTIVOS DE ALARMAS

Haciendo uso de la aplicación *orange canvas*<sup>1</sup> se realizará un análisis descriptivo y un análisis con correlación de los datos almacenados en una crónica de eventos característica de los sistemas de información en plantas industriales; El análisis descriptivo lo componen de las herramientas de visualización *Distributions* y *Box Plot*, y para el análisis de correlación cruzada se emplea la herramienta de visualización *Scatter Plot*. El flujo de trabajo en presentado de forma gráfica en la interface de operación de la aplicación lo que brinda un fácil entendimiento del tratamiento de la información (Figura 6).

**Figura 6.** Estructura de análisis para la crónica de eventos



*Fuente: Propia*

El análisis descriptivo se realizará por medio del despliegue visual de las alarmas dentro de cada *controlador*<sup>2</sup> y el despliegue de alarmas por *área de configuración*<sup>3</sup>. Estos dos análisis están encaminados a identificar concentraciones de alarmas en regiones físicas de la planta para definir alguna relación de causalidad por parte del personal de operación de la planta (Figura 7 y Figura 8).

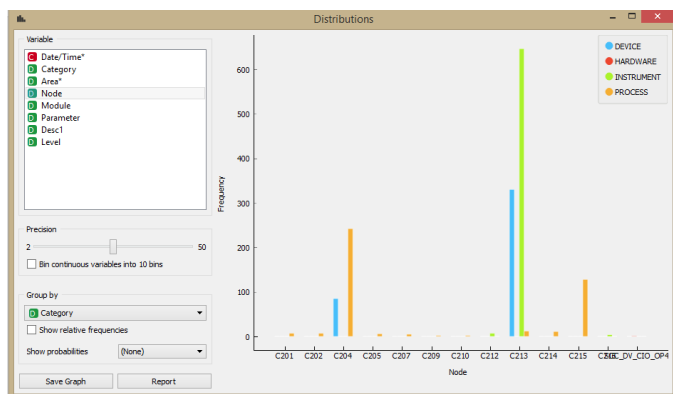
La distribución de alarmas por controlador (Figura 7), identifica un tipo dos tipos de alarmas reiterativas la cual por referencia de la norma 18.2 no debe ser considerada como alarmas sino como evento (*Instrument* y *Device*), el tipo de alarma de instrumentación y de dispositivo son eventos de la instrumentación inteligente los cuales dentro del proceso de gerenciamiento de alarmas debe ser rejerarquizada para evitar información inconsistente al personal de operación y posibles inundaciones de alarmas en el sistema de control.

<sup>1</sup> Software open source para la visualización y análisis de datos creado por universidad de Ljubljana.

<sup>2</sup> Dispositivo electrónico para la ejecución de las estrategias de control

<sup>3</sup> Agrupaciones de software que administran áreas físicas de la planta industrial

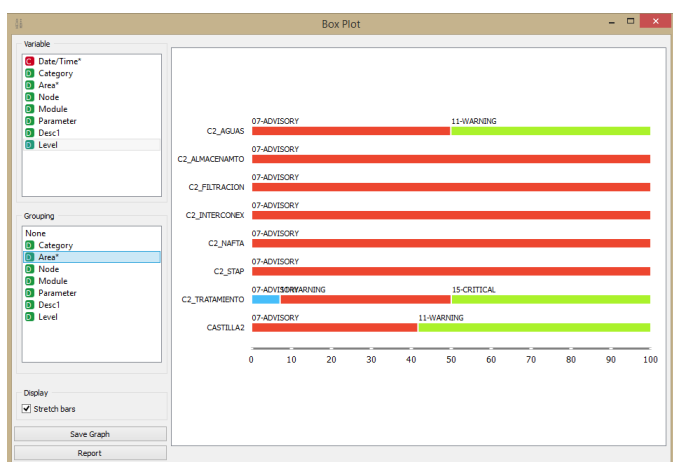
**Figura 7.** Distribución de alarmas por controlador



*Fuente: propia*

En el análisis descriptivo de alarmas por controlador también evidencia que las alarmas del tipo proceso (*Process*), son las que tienen un menor impacto dentro del reporte de la crónica de eventos, sin embargo, este tipo de alarmas son las que requieren mayor atención por parte del personal de operación haciendo que las alarmas presentadas como de primer nivel.

**Figura 9.** Distribución de alarmas por controlador



**Figura 8** Concentración de alarmas por área de configuración

*Fuente: propia*

En la distribución de concentración de alarmas por área de configuración (Figura 8), se evidencia que la concentración de alarmas críticas y de aviso en determinadas áreas de operación, Esto dentro de las

operaciones diarias de una planta industrial es normal debido principalmente al tipo de equipos y operaciones requeridas para cada etapa de tratamiento; sin embargo este distribución presenta una ayuda visual para determinar los mayores focos de atención en la operación diaria y de cómo estos pueden ser abordados en tareas de racionalización del gerenciamiento de alarmas (fase C).

Con los análisis anteriores se puede lograr una segmentación de los eventos de alarmas en la estación y una convalidación de los eventos registrados con las operaciones rutinarias de la planta; es importante identificar destacar que este análisis también arroja la presencia de *malos actores* al poder identificar alarmas mal configuradas y con fallas en la jerarquización debido a la presencia de los volúmenes de alarmas presentes en las gráficas.

La implementación de un análisis más detallado con la información suministrada por la crónica de eventos para una predicción del comportamiento de las variables críticas de operación expone la necesidad de herramientas de análisis más sofisticadas como las suministradas en la minería de datos.

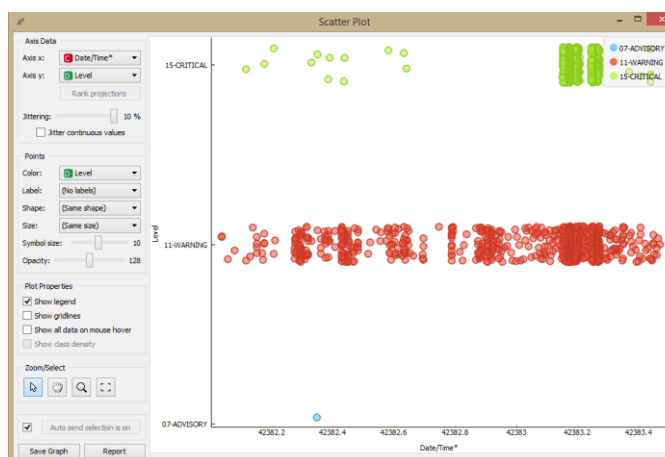
## VI. ANÁLISIS CON MINERÍA DE DATOS DE ALARMAS

Trabajos realizados de minería de datos para la detección de eventos buscan identificar anomalías tempranas del sistema, para ello cuentan con una metodología en la cual se tiene: a) análisis o entendimiento del negocio, b) análisis o entendimiento de los datos, c) preparación de los datos, d) modelado, e) evaluación de resultados, f) explotación o despliegue de resultados (Vallejo & Tenelanda, 2012); esto conlleva a que es necesario involucrar al personal de operaciones y de planta en las labores de gerenciamiento detallado de alarmas para su correcta interpretación.

Para el desarrollo del presente trabajo se realiza un análisis de correlaciones cruzadas dentro de la crónica de eventos las cuales pretenden identificar malos actores de configuración dentro del sistema de control que no sean de fácil percepción.



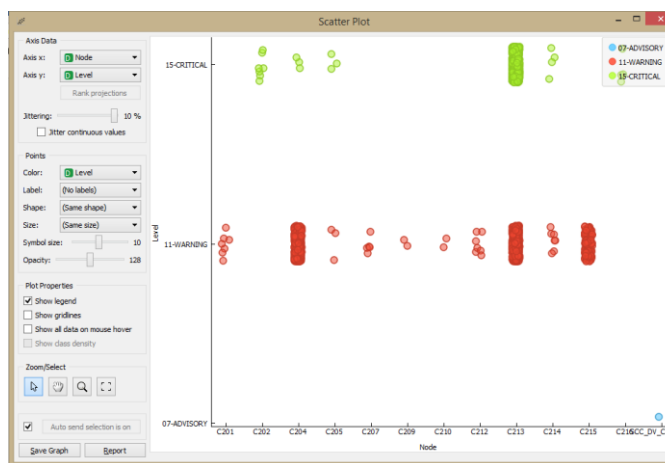
**Figura 9.** Distribución de alarmas por prioridad en el tiempo



*Fuente: Propia*

En un análisis de comportamiento de alarmas por prioridad vs tiempo (Figura 9), evidencia alarmas que se encuentran con límites muy cercanos entre los valores de aviso y crítico haciendo que se tenga disparos de eventos casi simultáneos. Los comportamientos esperados para las alarmas críticas son más cercanos a los presentados en la primera instancia donde su presencia no es regular, y donde en segunda instancia se ven correlacionados directamente con alarmas del tipo aviso.

**Figura 10** Distribución de alarmas por prioridad vs controlador



*Fuente: Propia*

Un segundo análisis donde se tenga la concentración de alarmas por prioridad vs controlador (Figura 10),

evidencia la presencia de eventos simultáneos de las alarmas críticas y las de aviso, evidenciando aún más las correlaciones existentes entre los límites de crítico y aviso de las áreas configuradas.

Los análisis anteriores nos presentan la oportunidad de la identificación de patrones dentro de la crónica de eventos los cuales puede ser usados como entradas para sistemas expertos los cuales pueden realizar reglas de filtrado para la disminución de información presentada al operador de la planta, con lo cual se pueda optimizar la forma de operación (Sánchez Gomez).

## CONCLUSIONES

- Los grandes volúmenes de información presentados en las crónicas de eventos de los sistemas de control precisan de análisis más detallados que permitan la identificación de fallos ocultos o de difícil percepción.
- Los análisis de correlación cruzada de las crónicas de eventos muestran la presencia de malos actores dentro de las crónicas de eventos analizadas. Es de precisar que no solo es requerido un proceso de gerenciamiento de alarmas sino de un proceso sistemático de las mismas para detección temprana de fallas.
- El análisis de posibles patrones de falla dentro de las crónicas de eventos crea la posibilidad de proyectar diferentes escenarios de operación para la planta industrial.
- Como tendencia para el análisis de grandes volúmenes de información es requerido herramientas que permitan el manejo de la misma, de una forma flexible y rápida como la presentada en el presente documento.

## VII. REFERENCIAS

- Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI magazine*, 37-54.
- Gomez , O., & Romero, G. (2011). Gestión de alarmas en plantas de proceso. *Boletín IIE*, 3-11.
- Hollender, M., & Carsten, B. (2007). Sistema inteligente de alarmas. *ABB*, 20-23.
- Hollifield, B. (2010). *Understanding and applying the ANSI/ISA 18.2 Alarm Management standard*. Houston: PAS.

- Hollifield, B. (2011). *Alarm Management: The seven step approach for significant improvement*. Houston: PAS.
- Hollifield, B., & Habibi, E. (2015). *Alarm Management a comprehe*. Houston: International Society of Automation - ISA.
- International Society of Automation. (2009). *ANSI/ISA 18.2-2009 Management of Alarm Systems for the process Insdustries*. North Carolina: International Society of Automation.
- Marina, G. (2014). *Gestión de alarmas en sistemas de control distribuido*. Barcelona: Universidad Politécnica de Cataluya.
- Pérez López, C., & Satín González, D. (2007). *Minería de datos: Técnicas y herramientas*. Madrid: Paraninfo.
- Sánchez Gomez, M. (s.f.). *Redes neuronales - aplicacion al procesamiento de alarmas*. Madrid: Universidad Carlos III.
- Vallejo, D., & Tenelanda, G. (2012). Minería de datos aplicada en la detección de intrusos. *USBMed*, 50-61.