La Tecnología al Servicio de la Defensa y la Seguridad Nacional

CASO DE USO: IBM ILOG RULES EN SISTEMAS DE GUERRA ELECTRÓNICA

15 Septiembre 2010

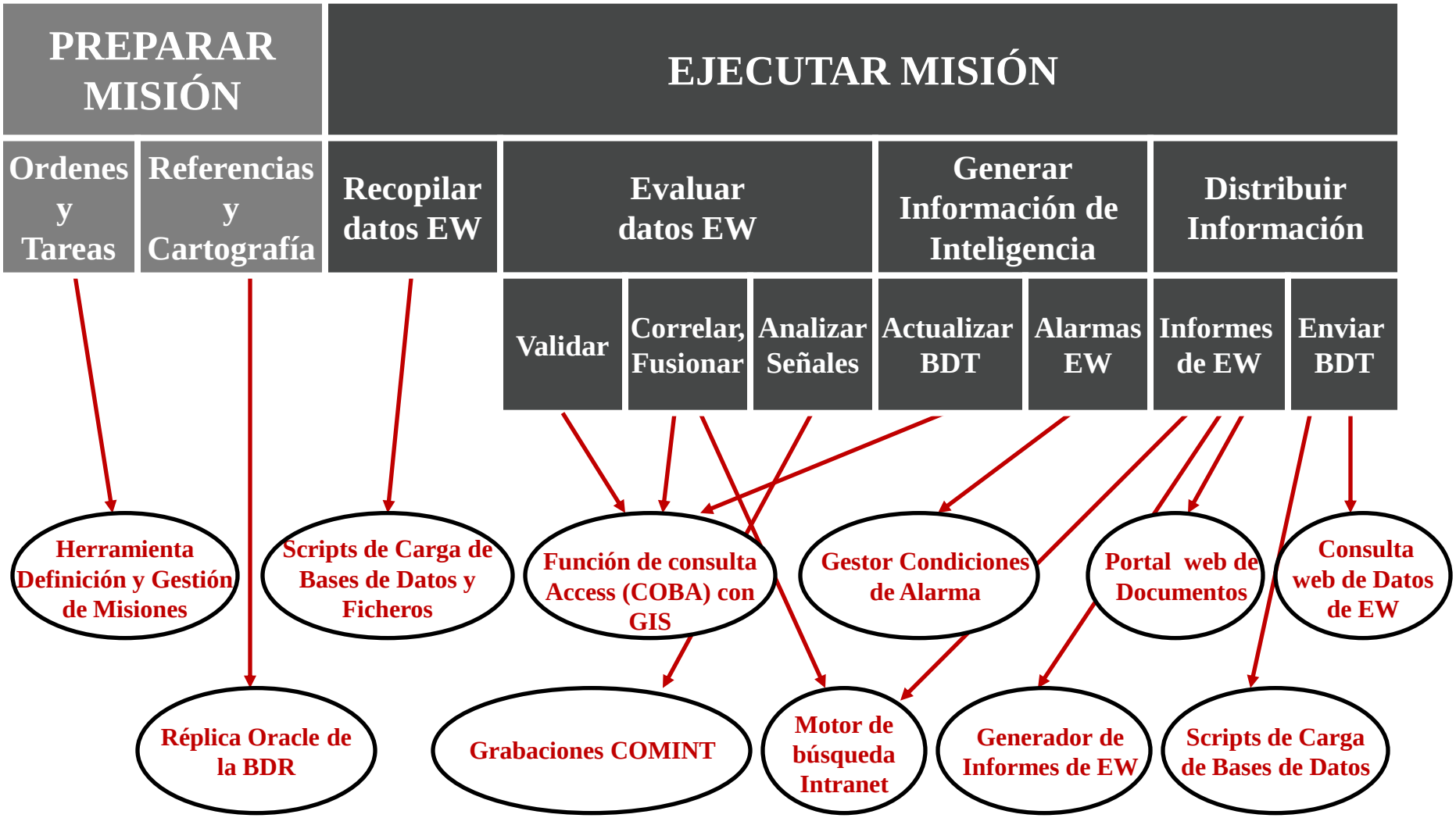
Manuel Pérez Cortés
Director General Defensa y Seguridad
GMV

INNOVATING SOLUTIONS

TRAYECTORIA DE GMV EN GUERRA ELECTRÓNICA

- Desde el año 2002 GMV ha integrado más de 10 nodos de procesamiento de datos de Guerra Electrónica para el Ministerio de Defensa
- Desde esa fecha un equipo de 20 ingenieros están dedicados al 100% al desarrollo e integración de este tipo de sistemas
- En global, estos nodos suponen más de 80 puestos de analista de inteligencia de señales

CONCEPTO DE EJECUCIÓN



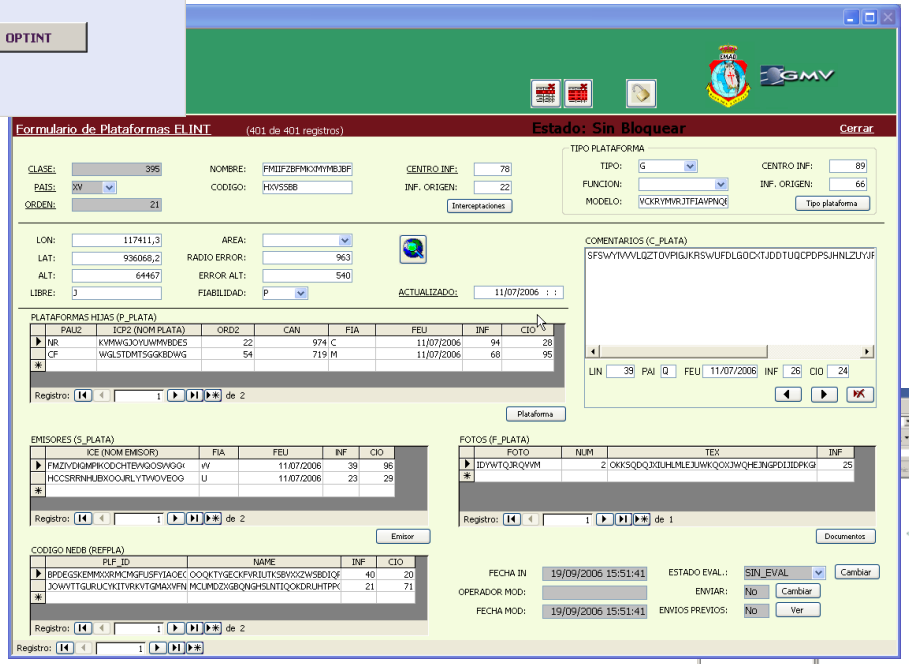
HERRAMIENTAS SW DESARROLLADAS

- Aplicaciones Desktop:
  - Análisis de datos de EW con presentación GIS (depuración, evaluación y correlación)
  - Digitalización de Señales
- Aplicaciones Web:
  - Gestión de bases de datos de EW (recopilación de datos, distribución de referencias, control de cambios)
  - Consulta a bases de datos de EW con presentación GIS
  - Portal de documentos
  - Motor de búsqueda en documentos y bases de datos
  - Generación de Informes a partir de plantillas tipo
  - Definición y Gestión de Misiones
  - Gestión de alarmas
  - Gestión de usuarios
- COTS de base
  - Gestor de bases de datos Oracle
  - Servidor de aplicaciones Oracle
  - GIS ESRI
  - Motor de reglas de negocio **IBM ILOG JRules**
  - Sistemas operativos Windows XP y Windows 2003 Server

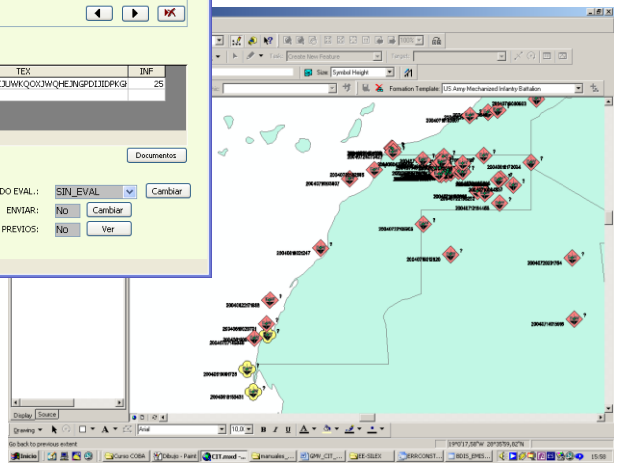
ANÁLISIS DE DATOS DE EW

Acceso por contraseña a BD para los distintos entornos: COMINT, ELINT, OPTINT.

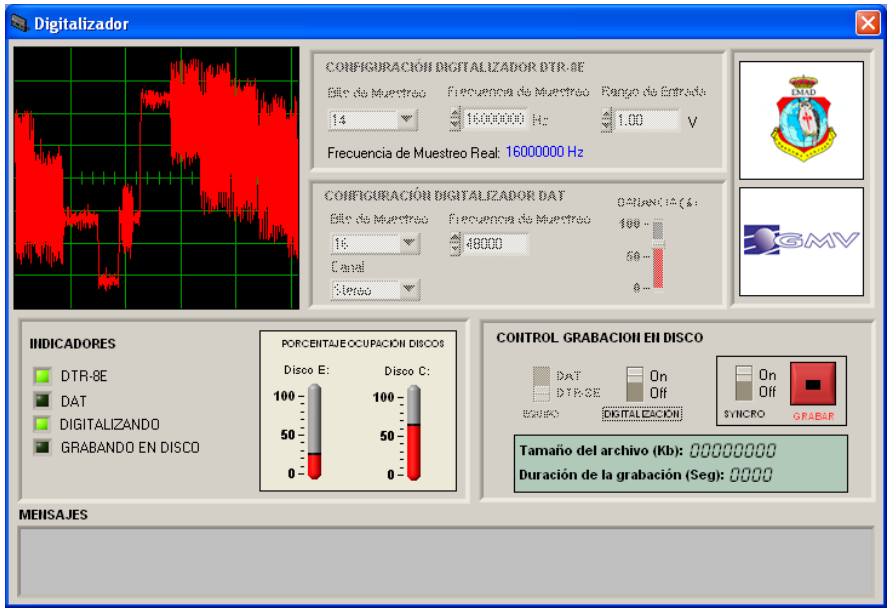
Formularios a medida de las necesidades de los usuarios



Representación cartográfica



DIGITALIZACIÓN DE SEÑALES



GESTOR DE CONDICIONES DE ALARMA

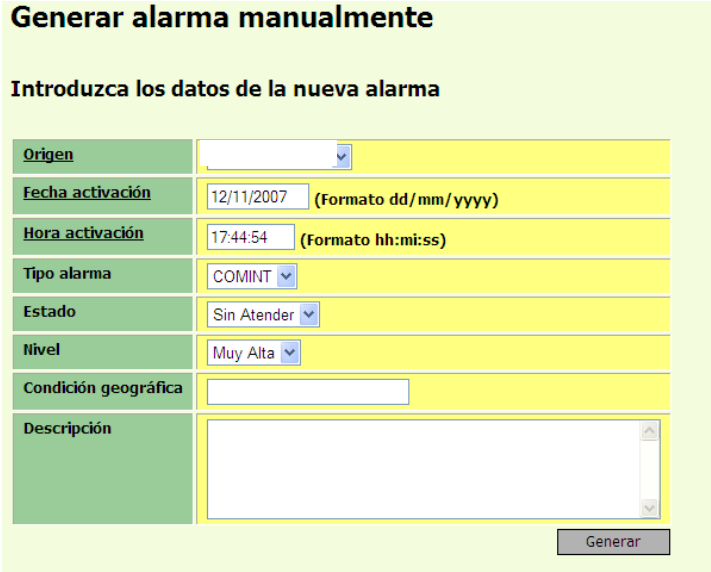
- Se ha desarrollado una serie de herramientas para el tratamiento de grandes volúmenes de información, con una metodología enfocada a un ciclo de obtención de inteligencia
- En los sistemas desarrollados por GMV de guerra electrónica se incluye un gestor de condiciones de alarmas que proporciona las siguientes capacidades:
  - Recepción de alarmas de otros subsistemas.
  - Detección de las condiciones de alarma mediante reglas aplicadas a los datos.
  - Comunicación y distribución de alarmas, tanto de forma automática, como de forma manual a petición del analista.
  - Registro de las alarmas.

MODOS DE DETECCIÓN DE CONDICIONES DE ALARMA

Están disponibles dos modos de detección de condiciones de alarma:

- ***Automático***, con software que aplicando **un juego de reglas** a las bases de datos, obtenga una serie de resultados, que a su vez puede realimentar el juego de reglas, pudiendo resultar el proceso en la activación de una alarma. **Para el modo de detección automática se usa IBM ILOG Jrules**
- ***Manualmente,*** detectada por el propio analista. En este caso una vez activada la alarma se guarda en la base de datos y se utilizan los procesos automáticos de comunicación y distribución de la alarma del mismo modo que en el sistema automático.

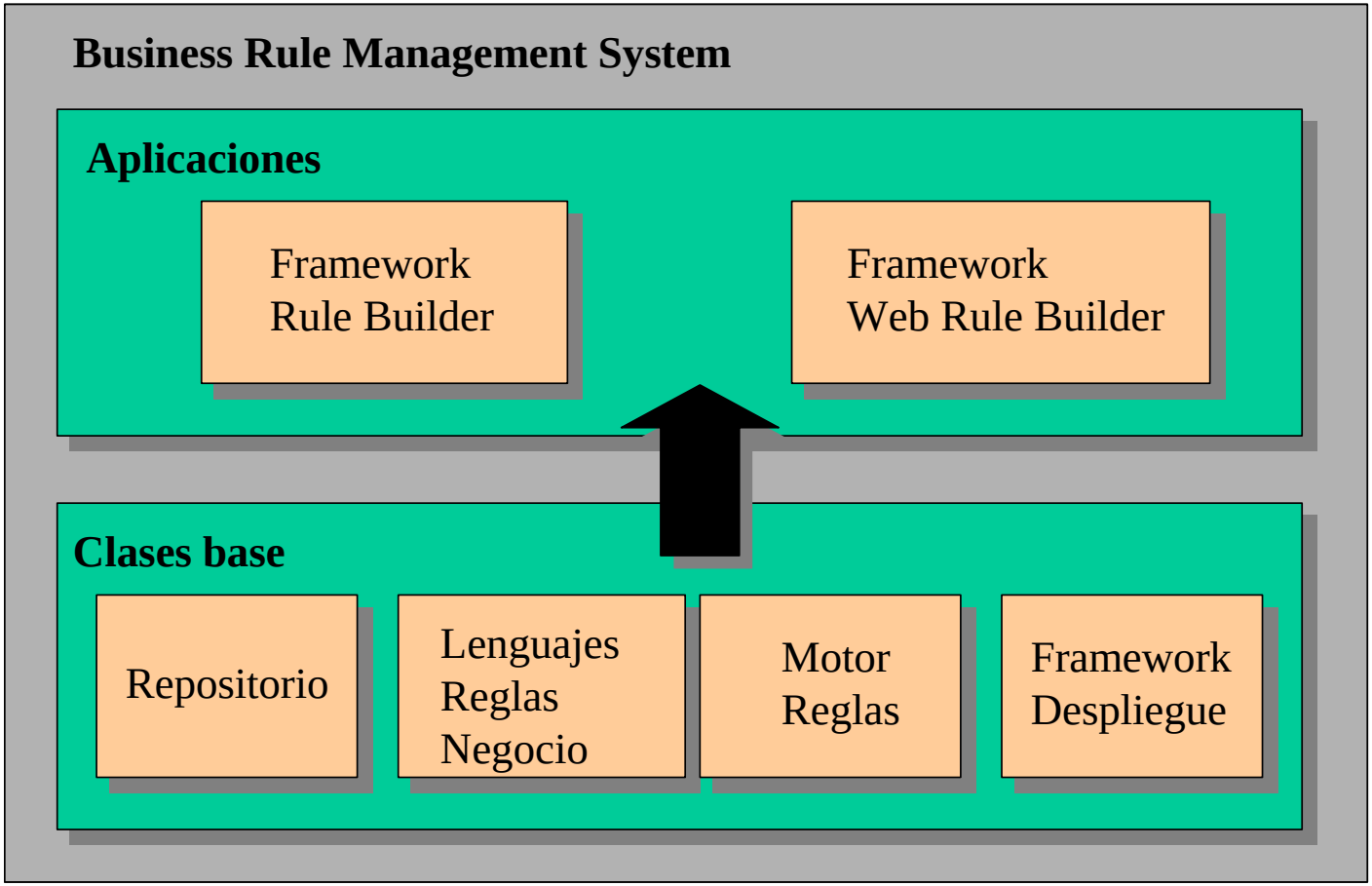
- Página de creación de alarma



ALARMAS CON ILOG JRULES

- Desarrollo de reglas para alarmas con ILOG JRULES.
  - Rule Builder
    - Interfaz gráfico y editores para desarrollar reglas
  - Repositorio de reglas
    - Almacena las reglas y sus datos asociados
    - Proporciona servicios para gestionarlo
  - Lenguajes
    - Se usan para escribir reglas
    - Pueden ser proporcionados por la herramienta o desarrollados por el usuario
      - Business Action Language (BAL)
      - Technical Rule Language (TRL)
      - ILOG Rule Language (IRL)

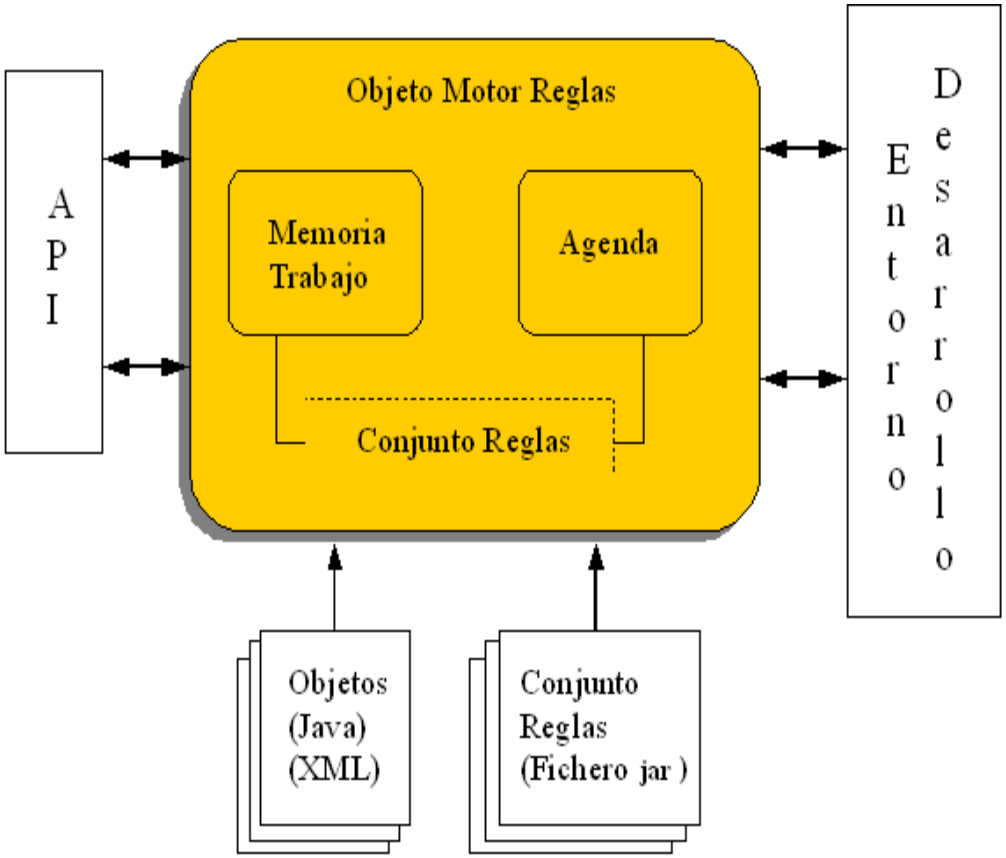
ARQUITECTURA DE ILOG JRULES



MOTOR DE REGLAS

- Conceptos clave y ejecución de reglas:

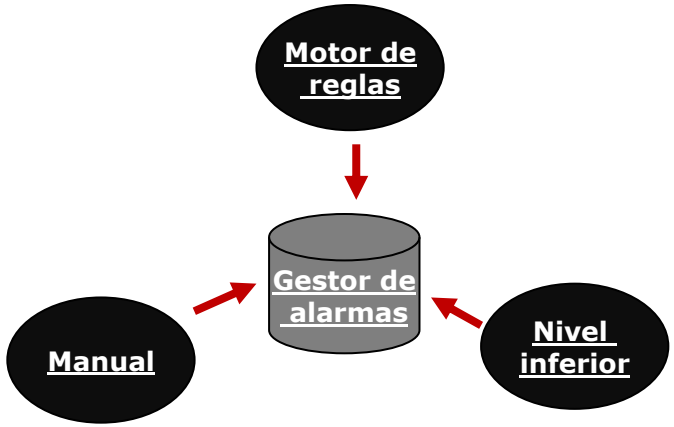
  "*Una regla es un trozo de lógica que tiene una parte de condiciones y una parte de acciones*"



- Componentes del motor:
  - **Objetos**. Sobre ellos actúan las reglas
  - **Memoria de trabajo (Working Memory).** Almacena los objetos
  - **Agenda**. Reglas a ejecutar
  - **Conjunto de reglas (RuleSet).** Las reglas de negocio
  - **API**. Existe un conjunto de llamadas disponibles para interactuar con el motor de reglas

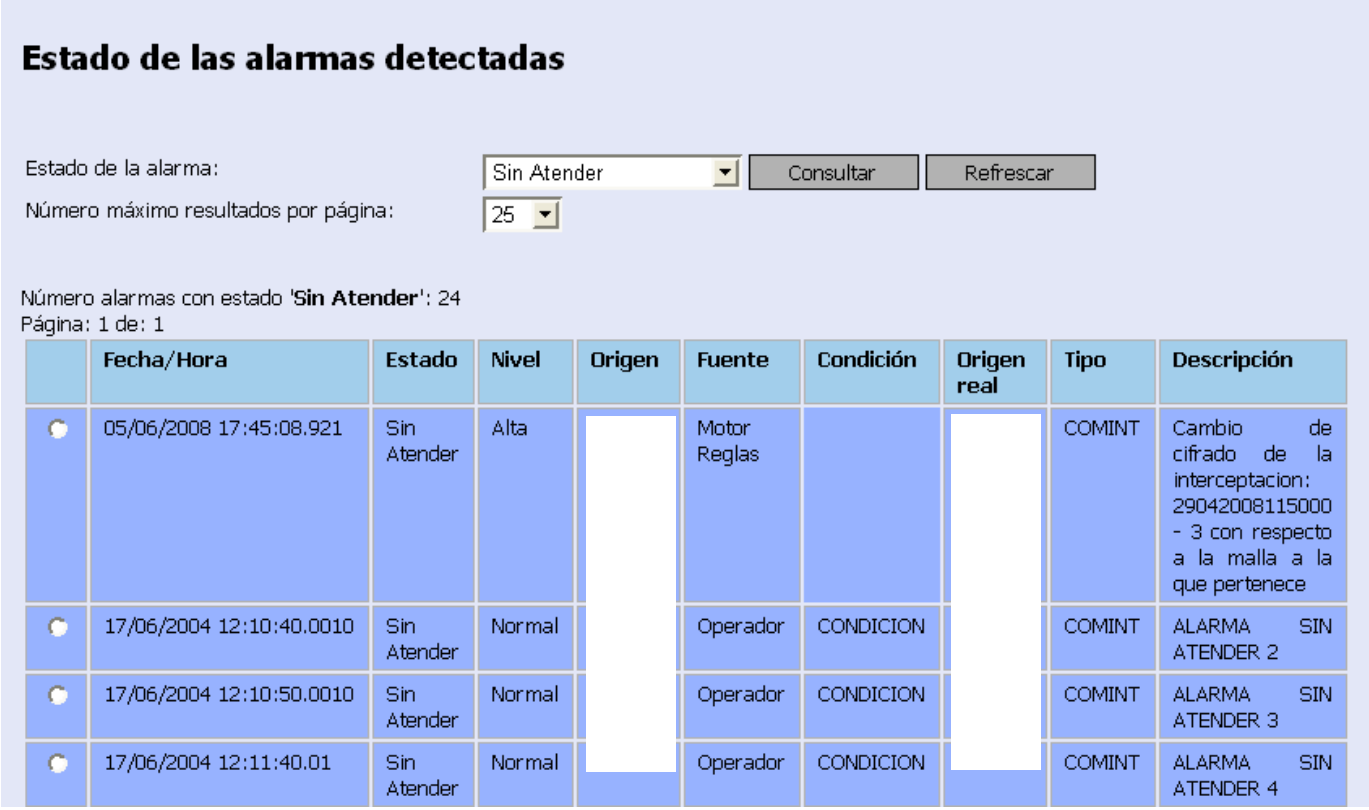
GESTIÓN DEL ESTADO DE LAS ALARMAS

- Sistema de gestión de alarmas con el que poder crear, gestionar y distribuir alarmas.
- Motor de reglas que realiza una búsqueda continua de alarmas.
  - Reglas
  - Bases de datos de EW
- Distribución organizada de forma jerárquica. De abajo hacia arriba.
- Como medio de distribución se utiliza el correo electrónico.
- Entrada de alarmas en el sistema:



GESTIÓN DEL ESTADO DE LAS ALARMAS

Página "***Estado de las alarmas***"



Estado de las alarmas detectadas

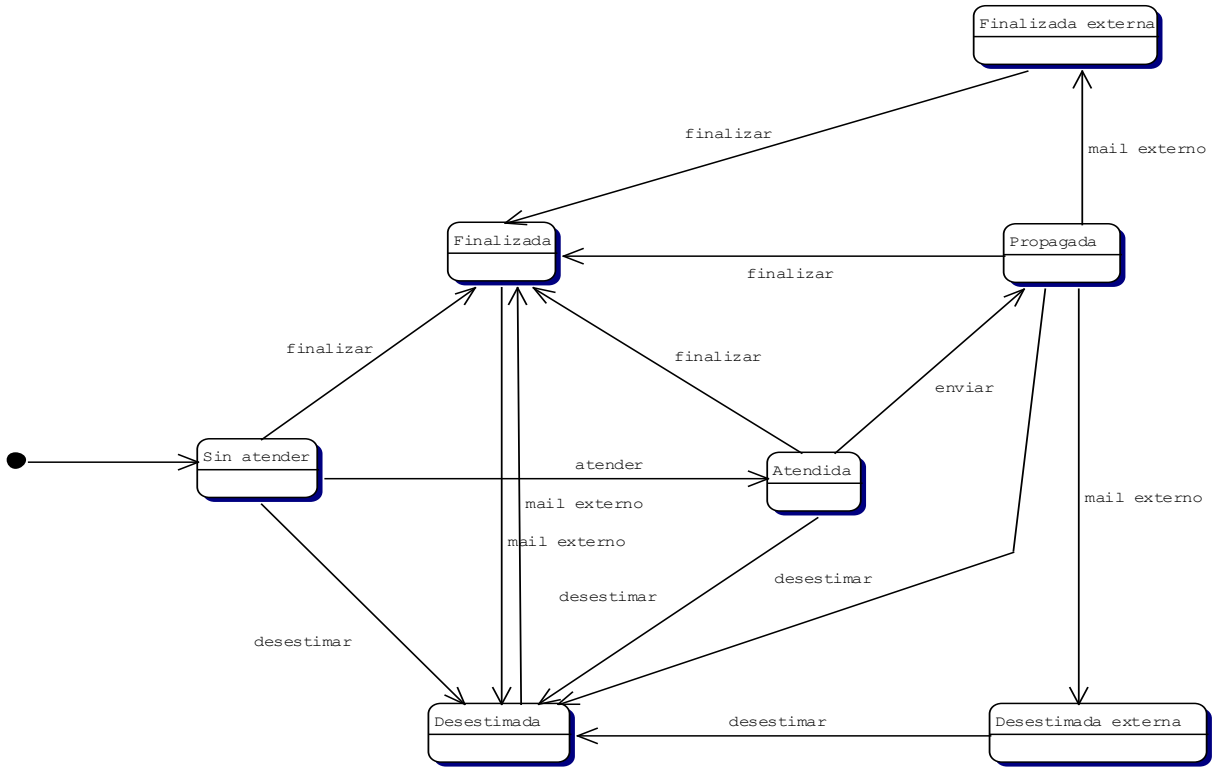
Estado de la alarma: Sin Atender | Consultar | Refrescar

Número máximo resultados por página: 25

Número alarmas con estado '**Sin Atender**': 24
Página: 1 de: 1

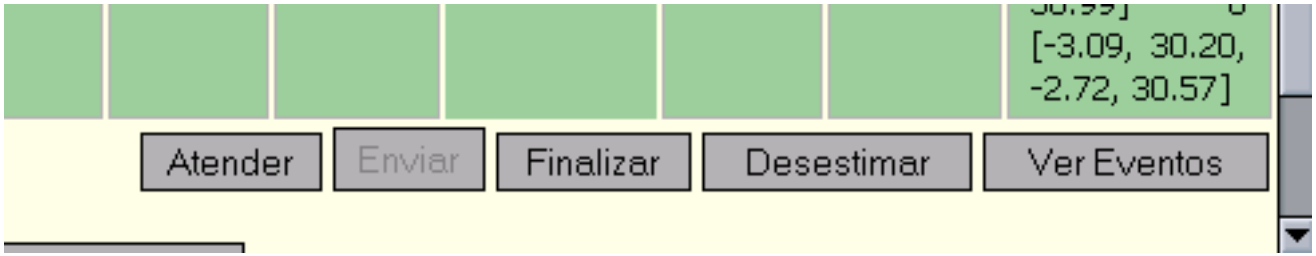
	Fecha/Hora	Estado	Nivel	Origen	Fuente	Condición	Origen real	Tipo	Descripción
○	05/06/2008 17:45:08.921	Sin Atender	Alta		Motor Reglas			COMINT	Cambio de cifrado de la interceptacion: 29042008115000 - 3 con respecto a la malla a la que pertenece
○	17/06/2004 12:10:40.0010	Sin Atender	Normal		Operador	CONDICION		COMINT	ALARMA SIN ATENDER 2
○	17/06/2004 12:10:50.0010	Sin Atender	Normal		Operador	CONDICION		COMINT	ALARMA SIN ATENDER 3
○	17/06/2004 12:11:40.01	Sin Atender	Normal		Operador	CONDICION		COMINT	ALARMA SIN ATENDER 4

GESTIÓN DEL ESTADO DE LAS ALARMAS



Posibles estados para las alarmas:

- **Sin Atender**. Estado inicial de las alarmas
- **Atendida**. Alarma atendida por un operador
- **Propagada**. Alarma enviada a un nivel superior o un(os) contacto(s)
- **Desestimada**. Alarma declarada falsa
- **Desestimada externa**. Desestimada por nivel superior
- **Finalizada**. Alarma concluida por operador o nivel superior
- **Finalizada externa**. Alarma concluida por nivel superior



VENTAJAS DE DISPONER DE UN MOTOR DE REGLAS

- Un motor de reglas permite crear una gramática propia adaptada a cada tipo de necesidad
  - El usuario escribe reglas en su gramática.
  - Crear la gramática exige programación, pero escribir reglas no, por lo que se pueden introducir nuevas reglas de forma inmediata en tiempo de ejecución.
- A medida que se detectan nuevas reglas el operador puede crearlas sin tener que recurrir a un programador y sin recompilar el sistema.
  - Se pone de manifiesto la ventaja de permitir evolucionar el sistema (nuevas reglas) sin necesidad de recompilar el sistema.
  - Permite crear sistema flexibles y escalables.
  - Es de resaltar que en aplicaciones en las que se manejan datos de carácter reservado la empresa desarrolladora no tiene visibilidad de las reglas que aplicará el analista/sistema.

CONCLUSIONES

- GMV viene utilizando las herramientas de ILOG desde hace más de 10 años, tanto par el ámbito de proyectos de guerra electrónica usando IBM ILOG JRules (JAVA), como para el campo espacial, pues en varios proyectos de Mission Planning para satélites se utiliza IBM ILOG Rules (C++) para aplicar las restricciones y optimizar la misión
- La experiencia es muy satisfactoria
  - en las posibilidades que ofrecen estas herramientas
  - en la integración con otra aplicaciones
  - y en el apoyo técnico
- En el caso de manejo de datos de carácter reservado el hecho de hacer uso de un gestor de reglas permite que la empresa desarrolladora de la aplicación no necesite tener visibilidad de las reglas que aplicará el analista o el sistema, lo que hace esta herramienta muy indicada en aplicaciones militares

