



Proyecto "Etiquetado y Vigilancia del Mercado"

Propuesta de  
**DISEÑO DEL SISTEMA DE ALERTA RAPIDA**  
**PARA ALIMENTOS Y BEBIDAS INDUSTRIALIZADOS**  
**SARABI**  
V.3

**PROPUESTA FINAL**  
**11 de octubre de 2010**

---

**Consultor: Carlos Leño**

ALA-2005-17607  
Proyecto UE-CAN FAT  
Etiquetado y Vigilancia del Mercado

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

La presente propuesta ha sido elaborada en el marco del Proyecto “Facilidad de Cooperación UE-CAN para la Asistencia Técnica al Comercio (FAT)” y ha sido actualizada con base en los comentarios presentados por los Miembros del Comité Consultivo Regional del Proyecto Etiquetado y Vigilancia del Mercado durante y después de las reuniones por videoconferencia que tuvieron lugar en Lima, Quito, Bogotá, los días 26 de abril, 22 de julio y 30 de septiembre de 2010.

El contenido de la misma es responsabilidad exclusiva del Consultor y en ningún caso refleja los puntos de vista de la Comisión Europea y de la Secretaría General de la Comunidad Andina, ni del Proyecto FAT.

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

# INDICE

1	RESUMEN EJECUTIVO .....	6
2	SITUACION ACTUAL .....	7
2.1	Colombia .....	7
2.2	Ecuador.....	7
2.3	Perú.....	8
3	DESCRIPCION GENERAL .....	8
3.1	Contexto del producto .....	10
3.2	Perspectivas futuras del producto.....	12
3.3	Reglas y funciones del negocio .....	13
4	DESCRIPCION DETALLADA DE REQUERIMIENTOS .....	14
4.1	Actores .....	14
4.2	Requerimientos funcionales .....	15
	Diagramas de casos de uso.....	15
	Listado de casos de uso .....	21
	Detalle de casos de uso.....	22
	Prototipo de interfaz de usuario .....	29
4.3	Requerimientos No Funcionales .....	38
4.4	Modelo de clases .....	39
4.5	Modelo de datos .....	43
4.6	Diccionario de datos .....	48
5	REQUERIMIENTOS DE INTERFAZ .....	53
5.1	Interfaces de hardware .....	53
5.2	Interfaces de software.....	54
5.3	Interfaces de comunicación.....	54
6	RESTRICCIONES DE DISEÑO .....	54
6.1	Estrategia institucional .....	55
6.2	Sistema operativo .....	55
6.3	Lenguajes de software.....	55
6.4	Base de datos .....	56
7	REQUERIMIENTOS DE LICENCIA .....	56
8	ARQUITECTURA .....	57
8.1	Red .....	57
8.2	Aplicaciones .....	58
8.3	Servicios Web .....	59
8.4	Contexto del negocio.....	60
8.5	Entidades del negocio.....	62
8.6	Interoperabilidad de las aplicaciones .....	68
8.7	Formato del archivo XML con los datos del incidente .....	69
8.8	Integración y armonización de las entidades de base.....	70
9	SEGURIDAD Y BACKUP .....	71





## Proyecto "Etiquetado y Vigilancia del Mercado"

9.1	Seguridad.....	71
9.2	Fallos de energía y/o equipamiento.....	73
9.3	Back Up.....	73
9.4	Manejo de Excepciones.....	74
10	TAMAÑO Y PERFORMANCE.....	74
10.1	Requerimientos de capacidad.....	75
10.2	Evaluación de impacto .....	75
	Personal .....	75
	Logística .....	76
11	PRESUPUESTO .....	76
11.1	Servicios.....	76
11.2	Equipos.....	77





## Proyecto "Etiquetado y Vigilancia del Mercado"

### Glosario

ANVISA	Agência Nacional de Vigilância Sanitária ( <a href="http://portal.anvisa.gov.br">http://portal.anvisa.gov.br</a> )
CAE	Corporación Aduanera del Ecuador ( <a href="http://www.aduana.gov.ec/">http://www.aduana.gov.ec/</a> )
CAN	Comunidad Andina
CRUD	"Create, Read, Update, Delete" - Crear, Leer, Actualizar, Eliminar
DIGESA	Dirección General de Salud Ambiental ( <a href="http://www.digesa.minsa.gob.pe">http://www.digesa.minsa.gob.pe</a> )
IICA	Instituto Interamericano de Cooperación para la Agricultura ( <a href="http://www.iica.int">http://www.iica.int</a> )
INEN	Instituto Ecuatoriano de Normalización ( <a href="http://www.inen.gov.ec">http://www.inen.gov.ec</a> )
INHMT	Instituto Nacional de Higiene y Medicina Tropical ( <a href="http://www.inh.gov.ec">http://www.inh.gov.ec</a> )
INVIMA	Instituto Nacional de Vigilancia de Medicamentos y Alimentos ( <a href="http://web.invima.gov.co">http://web.invima.gov.co</a> )
OMC	Organización Mundial de Comercio ( <a href="http://www.wto.org">http://www.wto.org</a> )
OMS	Organización Mundial de Salud ( <a href="http://www.who.int">http://www.who.int</a> )
RASFF	"Rapid Alert System for Food and Feed" ( <a href="https://webgate.ec.europa.eu/rasff-window/portal">https://webgate.ec.europa.eu/rasff-window/portal</a> )
SANIPES	Servicio Nacional de Sanidad Pesquera ( <a href="http://www.itp.org.pe/desarrollo-sanipes.php">http://www.itp.org.pe/desarrollo-sanipes.php</a> )
SARABI	Sistema de Alerta Rápida para Alimentos y Bebidas Industrializados
SENASA	Servicio Nacional de Sanidad Agraria del Perú ( <a href="http://www.senasa.gob.pe">http://www.senasa.gob.pe</a> )
SGCAN	Secretaría General de la CAN ( <a href="http://www.comunidadandina.org">http://www.comunidadandina.org</a> )
SINAVA	Sistema Nacional de Vigilancia de Alimentos
SIRT	Sistema de Alerta al Exportar de la CAN ( <a href="http://secgen.comunidadandina.org/sirt">http://secgen.comunidadandina.org/sirt</a> )
SMBD	Sistema Manejador de Base de Datos
SQL	"Structured Query Language" – Lenguaje de acceso a datos en bases de datos relacionales
SSL	"Secure Sockets Layer" – Protocolo de traslado de datos en modo encriptado
TdR	Términos de Referencia
UE	Unión Europea
UML	"Unified Modeling Language" – Lenguaje estándar de modelación de sistemas
URL	"Uniform Resource Locator" – Dirección de un recurso en Internet
VPN	"Virtual Private Network" – Red Privada Virtual
WS	"Web Service" – Servicio Web
XML	"eXtended Markup Language" – Lenguaje estándar de traslado de datos





## Proyecto "Etiquetado y Vigilancia del Mercado"

# 1 RESUMEN EJECUTIVO

El sistema de información de alerta rápida – SARABI - aquí definido en este documento tiene dos alcances principales:

1. Proveer los Países Miembros de la CAN con un sistema de vigilancia de alimentos que garantice la seguridad de los mismos y permita establecer la “espiral de la calidad” fomentando la mejora continua.
2. Permitir integrar la información producida por los Países Miembros a nivel comunitario de la CAN, posibilitando análisis consolidados, contribuyendo para el proceso de armonización de procedimientos necesario para alcanzar el objetivo de promover el comercio intrasubregional.

En términos conceptuales el sistema consistirá en una aplicación nacional de gestión de incidentes relacionados con alimentos, en un sistema de notificaciones por correo electrónico y en una página Web accesible al público donde se podrá hacer consultas sobre los incidentes y denuncias de peligros. Cada país miembro será responsable por mantener su sistema de gestión de incidentes, y la SGCAN sería la responsable por el mantenimiento de la página Web. El traslado de información de las bases de datos nacionales a la base de datos de la SGCAN sería automático, por la Internet, y a través de programas ejecutados diariamente en batch o con recurso a automatismos de los propios sistemas manejadores de base de datos (en este caso, y en las base de datos nacionales, el SMBD elegido tendría que incluir esta funcionalidad).

Cada usuario del sistema de gestión de incidentes necesitará de una clave de acceso (Nombre de usuario y Contraseña) y tendrá un rol asociado que le dará acceso a un cierto número de procesos. Estos usuarios serán definidos por el administrador de la aplicación que, a su vez, debe ser nombrado por la autoridad competente en materia de vigilancia de alimentos. Si varias instituciones deben acceder al sistema, entonces el administrador de la aplicación deberá ser notificado por la autoridad competente de cuáles serán los usuarios que accederán al sistema y cual su rol en esto. Esta información podrá ser básica (Nombre, institución y rol) porque después el propio usuario podrá actualizarla y complementarla. Para cada rol podrán existir varios usuarios. Cada institución lo puede definir y tendrá de comunicarlo al administrador para que este proceda a su creación. El cambio de usuarios podrá ser manejado a nivel de la institución.

Para una flexibilidad e independencia más grande, el sistema ha sido diseñado de modo a que cada país pueda, en dado momento, modificar algunas especificaciones del sistema para adaptarlo a sus necesidades específicas. Sin embargo, lo que se pretende con este proyecto es fomentar la cooperación institucional de los Países Miembros de la CAN y mejorar el nivel de integración. En este sentido, sería más ventajoso si los cambios fueron discutidos a nivel comunitario y el propio desarrollo ejecutado, o con supervisión, por la SGCAN. Como aquí es propuesto un diseño del sistema, cada país puede tomar la libertad de empezar el desarrollo de la solución individualmente, pero ese no sería el camino más adecuado. Los Países Miembros de la CAN deberían ponerse de acuerdo e intentar arreglar medios de financiación conjuntos para que se desarrolle un solo sistema

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

y no tres o cuatro, que a su vez difícilmente estarían preparados para se comunicar mutuamente. Se ahorraría tiempo y presupuesto. Aunque, posteriormente, cada uno de los países pudiese quedar con la propiedad de los fuentes del sistema.

Como el sistema propuesto puede ser distribuido, y se prevé la posibilidad de que cada país pueda tomar el desarrollo de la solución individualmente, se definió una estructura de datos estándar mínima, en XML, para que esté siempre garantizado el traslado de información a la base de datos común a existir en la SGCAN. El formato de este archivo, la periodicidad de actualización, y las competencias procesales y técnicas de cada institución involucrada (puntos focales nacionales y la SGCAN) deberían ser establecidos en un instrumento legal de la CAN.

## 2 SITUACIÓN ACTUAL

La situación actual en materia de vigilancia de alimentos en los tres países diagnosticados y en materia de informatización de los procesos es muy débil.

Colombia está un poco más avanzada con la presencia de INVIMA en los puntos de entrada lo que no sucede en Ecuador y Perú, donde las autoridades responsables (INHMT y DIGESA, respectivamente) solo actúan en situaciones de alerta, emitidos del extranjero o por la aduana. Sin embargo, ninguna de las autoridades maneja un sistema informatizado que permita gestionar, de un modo integrado con las demás autoridades involucradas, los incidentes ocurridos.

### 2.1 COLOMBIA

En Colombia la responsabilidad de vigilancia de alimentos está asignada a dos entidades autónomas, aunque estén dependientes del mismo ministerio (Protección Social): El INVIMA y las Direcciones Regionales de Salud.

El INVIMA tiene la responsabilidad de vigilancia en frontera y en las plantas. Las direcciones de Salud en el mercado. No existe (todavía aunque esté planeado) ninguno sistema integrado de gestión de inspecciones y de incidentes. Se está manejando, como pilotaje, un sistema a nivel regional de Sudamérica que permite la emisión de alertas relacionados con salud pública, que ha sido desarrollado por ANVISA de Brasil. Sin embargo, los datos introducidos en este sistema son descriptivos, muy poco estructurados, y no permiten un adecuado análisis de información estadística.

### 2.2 ECUADOR

En Ecuador la responsabilidad de vigilancia de alimentos está repartida por el INH, el INEN, los Municipios y las direcciones regionales de salud. Teóricamente todas estas instituciones pueden hacer vigilancia en el mercado y en planta, y el INH en frontera.



## Proyecto "Etiquetado y Vigilancia del Mercado"

Con relación a sistemas de información para gestión de las tareas de vigilancia del mercado, no existe ninguna aplicación que permita la interoperabilidad de las diversas instituciones involucradas. La Cancillería está manejando un sistema de notificaciones que permite también registrar y notificar las instituciones nacionales los alertas emitidos por organizaciones internacionales (como la OMS) relativamente a alimentos, y de terceros países, los cuales han detectado algún tipo de problema con alimentos provenientes de Ecuador.

Está en preparación (fase final) un reglamento técnico que pretende cambiar el sistema tornándolo más ágil y eficiente. Todavía no se conoce detalladamente el alcance del reglamento en materia de sistema de información y de conectividad de las instituciones involucradas.

### 2.3 PERÚ

La autoridad responsable por la vigilancia de alimentos procesados, en frontera y en planta es DIGESA (Ministerio de Salud). Las municipalidades tienen la responsabilidad de la vigilancia en el mercado. Caso estas no lo hagan, por motivos técnicos o logísticos, las direcciones regionales de DIGESA pueden hacerlo. DIGESA también presta apoyo técnico a los municipios.

No existe ninguno sistema informático específicamente para vigilancia de alimentos ni ninguna red que conecte las diversas instituciones involucradas.

La ley de inocuidad de alimentos, que ya está aprobada (a la fecha no había sido notificado a la OMC), establece la COMPIAL como siendo la entidad responsable por todo relacionado con alimentos en Perú. Esta entidad es constituida por las instituciones involucradas en alimentos:

- DIGESA (Ministerio de Salud)
- SENASA (Ministerio de Agricultura)
- SANIPES (Ministerio de la Producción)

Esta nueva ley pretende fomentar y agilizar la vigilancia de los alimentos centrando los esfuerzos en el mercado, garantizando así al consumidor una seguridad más grande en los productos que consume.

## 3 DESCRIPCIÓN GENERAL

El sistema SARABI pretende agilizar el proceso de alertas sobre incidentes con alimentos entre los Países Miembros de la CAN, para permitir acciones más rápidas y evitar consecuencias más graves para los consumidores. Por otro lado, para que el sistema pueda funcionar plenamente a nivel de los alertas, será necesario que los países tengan sus propios sistemas de vigilancia de alimentos preparados e interconectados con esta red de alerta rápida.

El SARABI es constituido por cinco subsistemas:

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"





## Proyecto "Etiquetado y Vigilancia del Mercado"

1. El SINAVA
2. El sistema de notificaciones de alertas
3. El sistema de traslado de información
4. El sistema de inteligencia de negocio (BI)
5. El Portal de acceso a la base de datos de alertas

El SINAVA es el sistema nacional de vigilancia de alimentos, que el consultor entendió incluir en esta propuesta por su pertinencia. Sin un sistema de vigilancia nacional adecuadamente diseñado el sistema comunitario tendría éxito. Asimismo, aunque no estuviera previsto en los TdR, en este documento está planteado el diseño mínimo del sistema que permitirá a los países registrar todos los eventos relacionados con alimentos (Inspecciones, Incidentes, Seguimiento, Alertas).

El sistema de traslado de información es el canal de comunicaciones entre los Países Miembros de la red y entre estos y la SGCAN. Como la producción de la información será efectuada en el SINAVA de cada país miembro, después es necesario copiar esta información a nivel comunitario para que los consumidores (y otras entidades interesadas) puedan hacer búsquedas consolidadas de la información. Por otro lado, cuando un país emite un alerta sobre un dado incidente con alimentos, la información detallada del mismo es enviada, en formato estándar, a los demás socios de la red, evitando que estos la tengan que cargar manualmente en sus bases de datos nacionales. Las denuncias efectuadas a través del portal Web comunitario también serán enviadas al Punto Focal del respectivo país en un formato estándar que puede ser cargado automáticamente a la base de datos nacional.

El sistema de notificaciones funcionará por correo electrónico. Cada país miembro de la red tendrá de notificar a la SGCAN cual es la entidad nacional responsable por recibir las notificaciones, especificando los datos detallados, entre ellos la cuenta de e-mail.

El sistema de inteligencia de negocio es diseñado para funcionar a nivel comunitario (con información consolidada). Los países podrán fácilmente aprovechar este diseño y transponer sus funciones al nivel nacional. Una de las funciones principales de este sistema es la de alimentar el sistema de análisis de riesgo que eventualmente los países tengan en operación para programar sus inspecciones.

El portal de acceso a la base de datos de alertas tendrá información filtrada para mantener la confidencialidad necesaria que se requiere en este tipo de servicios. Asimismo, se evitará identificar nombres de empresas y de marcas en el registro de incidentes. El objetivo del sistema es de garantizar la seguridad de los alimentos y no de denuncia de incumplidores. Además que, para probar la culpabilidad de una entidad puede tardar tiempo, que no se tiene cuando las consecuencias de un incidente son muy graves y se tornan peores con el pasar de los días.

Para un mejor entendimiento del sistema, se hará un resumen de las principales funcionalidades:

- Definición de cada una de las entidades de base
- Programación de inspecciones

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"

- Registro del resultado de inspección
- Registro del resultado de los análisis solicitados
- Registro de incidentes – Alertas
- Envío de notificaciones a los socios
- Utilización de la partida arancelaria – NANDINA (8 dígitos)
- Análisis de información y estadísticas
- Consultas públicas a información consolidada y seleccionada
- Denuncias de consumidores a través del portal Web

### 3.1 CONTEXTO DEL PRODUCTO

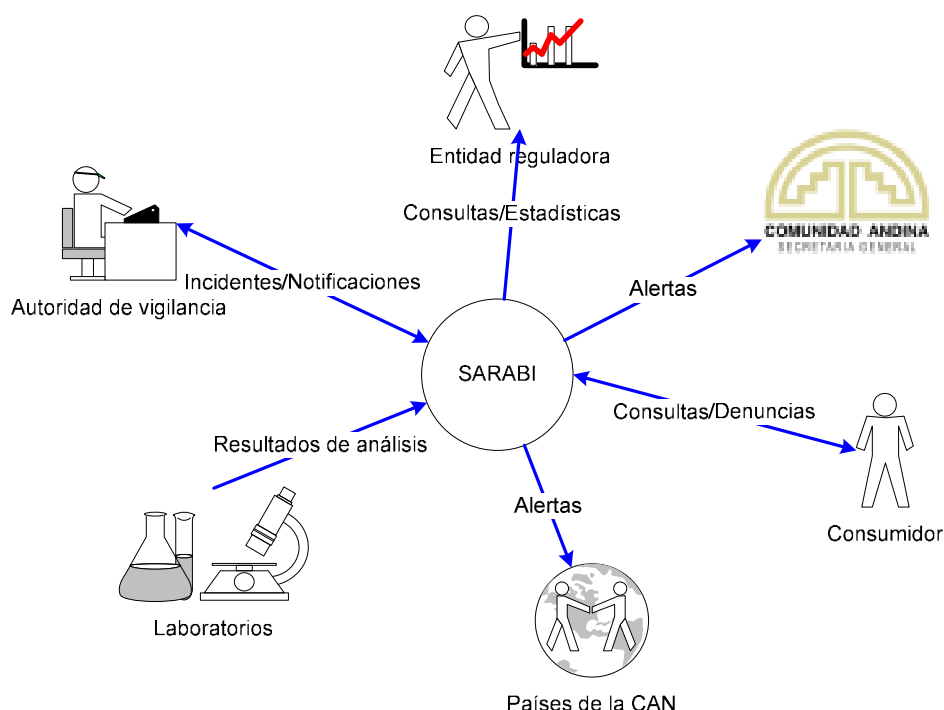


Figura 1 – Diagrama de contexto del sistema. Interacción con los beneficiarios.

El SARABI a través de sus aplicaciones distribuidas permitirá un fácil intercambio de informaciones entre las diversas entidades involucradas con el tema de alimentos. En la figura 1 se puede observar cuales son los beneficiarios del sistema y su modo de interactuar con el SARABI.

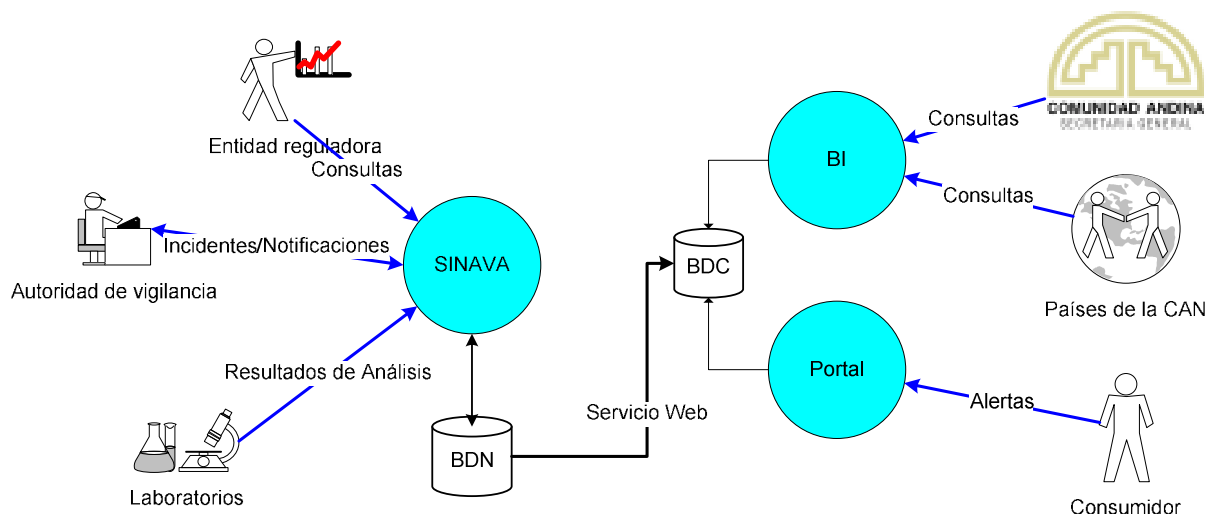


Figura 2 – Interacción de los diversos beneficiarios con las aplicaciones del SARABI.

El esquema de la figura 2, se puede observar, cuales las aplicaciones con las cuales cada actor interactúa. La aplicación BI solo se separó por una cuestión de claridad, en la práctica las consultas de ‘Inteligencia de negocio’ son integrantes de cada modulo respectivo. Sin embargo, los países, y mismo la SGCAN, se creen necesario, más adelante, pueden adquirir una aplicación específica para esta función.

Actualmente, debido a la cada vez más necesidad de consolidación de información que permita facilitar las decisiones operativas y estratégicas de los negocios, las aplicaciones de gestión deben disponer de “puertas” por donde exportar sus datos que puedan ser pertinentes en otros sistemas. De este modo, quedan más flexibles, más escalables y con más longevidad.

En el esquema de la figura 3 están representadas las aplicaciones del SARABI, el modo de comunicación entre ellas y el mundo exterior. La comunicación entre los SINAVAs, por una cuestión de independencia nacional es interactiva y, asimismo, la información es trasladada por correo electrónico. La comunicación con la SGCAN es automática y manejada por servicios Web existentes en los dos locales físicos (servidor nacional y de la SGCAN). La comunicación con aplicaciones externas al SARABI puede ser interactiva o automática. En esta propuesta solo se contempla la opción interactiva. Para la automática se tendría de evaluar cuales los datos existentes que podrían ser necesarios en otras aplicaciones y desarrollarse servicios Web que pudieran ser consumidos por esos sistemas externos.

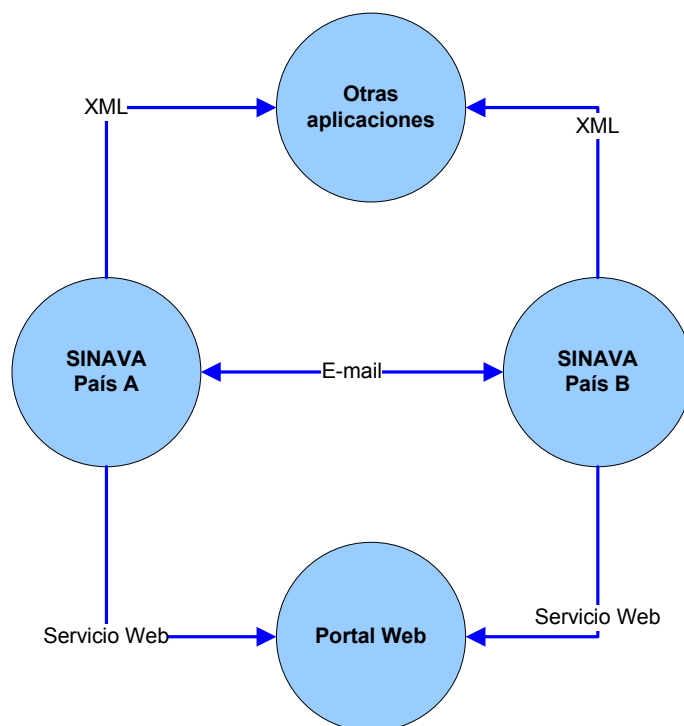


Figura 3 – Comunicación entre aplicaciones del SARABI y sistemas externos.

La información trasladada entre las aplicaciones es siempre en formato XML pero, por motivos de facilitación de la lectura del esquema, se indican los mecanismos de transporte de la información.

La comunicación entre los países es efectuada por e-mail en el cual es anexo un archivo XML que puede ser importado, por el país que recibe, a su aplicación SINAVA. Este procedimiento es interactivo, efectuado por un usuario, porque la decisión de hacer la importación es del país. Al revés, la comunicación con el portal Web es automática. Cada uno de los SINAVA ejecuta Servicios Web localmente que comunicaran con otro Servicio Web disponible en el servidor de la SGCAN que a su vez hará la actualización de la información en la base de datos central.

Para poder interactuar con otras aplicaciones, externas al SARABI, el SINAVA tendrá una función de exportación de datos, que podrá posteriormente ser desarrollada, que permitirá exportar alguna información (ver estructura del archivo en 8.6) de los alertas emitidos. El archivo generado estará en formato XML, lo cual tendrá de ser interpretado por las aplicaciones destino (de nuevo, si el sistema es idéntico este problema no se colocará).

### 3.2 PERSPECTIVAS FUTURAS DEL PRODUCTO

Las bases del presente proyecto tenían como objetivo la elaboración de una propuesta de diseño de un sistema de alerta rápida para alimentos y bebidas industrializados que pudiera ser manejado por todos los Países Miembros de la CAN. Sin embargo, debido al bajo nivel de utilización de herramientas informatizadas en la materia de vigilancia de alimentos, el consultor decidió incluir



## Proyecto "Etiquetado y Vigilancia del Mercado"

en el diseño la aplicación de gestión de los incidentes con este tipo de productos, denominada de SINAVA. Pero, como el diseño de esta aplicación ya está fuera del alcance del proyecto y por motivos de plazos, no es posible hacer el diseño completo de una aplicación con el alcance que esta debe tener. Asimismo, el diseño aquí incluido refleja las funcionalidades principales de esta aplicación. Pero, la inclusión futura en el SINAVA de los siguientes módulos facilitaría inmenso el proceso de control y análisis de los eventos:

1. Un módulo de análisis de riesgo para la programación de las inspecciones, que se basara en la información contenida en la base de datos, en datos históricos existentes a la fecha y en heurísticas definidas por los usuarios.
2. Un módulo de conectividad con los sistemas de comercio exterior (como la ventanilla única y el sistema de despacho aduanero) permitiría agilizar el proceso de evaluación de los envíos (importaciones y exportaciones) más problemáticos para alimentar también el sistema de análisis de riesgo y programar las inspecciones.
3. Un módulo de conectividad con otros sistemas de alerta relacionados con salud pública (alertas epidemiológicos y ambientales) también permitiría a las autoridades en cada materia tener una visión integrada de las ocurrencias.

El SARABI, en su globalidad, solo tendrá que adaptarse a los cambios usuales relacionados con la dinámica específica del tema. El SINAVA, sin embargo, y como parte integrante del SARABI, puede desarrollarse un poco más con el objetivo de obtener estadísticas más detalladas que posibiliten una mejora continua de los sistemas nacionales de análisis de riesgo en vigilancia de alimentos, y salud pública en general.

El diseño del sistema promueve la modularidad de las aplicaciones constituyentes para facilitar el mantenimiento y consecuente sostenibilidad del sistema. El modelo presentado puede ser implementado en dos (Interfaz y base de datos) o tres (Interfaz, reglas de negocio y base de datos) capas de software, siendo que para el sistema en causa las dos capas sean suficientes en términos de escalabilidad provocando también un mejor desempeño relativamente a la respuesta al usuario. El tiempo de procesamiento de cada instrucción es menos con las dos capas.

### 3.3 REGLAS Y FUNCIONES DEL NEGOCIO

En este punto se hace un resumen de las principales características del sistema con el objetivo de subrayar el alcance del SARABI:

1. Las autoridades de vigilancia pueden programar sus actividades de inspección a través del SINAVA en el módulo Inspección.
2. Se puede crear una base de datos de las empresas (plantas, importadores, distribuidores, etc.) que fueron sometidos a inspecciones.

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

3. Siempre que ocurra un incidente con alimentos este debe ser registrado en el modulo *Alerta* y conectado a la inspección correspondiente en el modulo *Inspección*.
4. Las denuncias pueden ser efectuadas por los siguientes medios: Teléfono, Web, e-mail, Presencial, Sobre, Fax. Las efectuadas por la Web pueden ser cargadas automáticamente a la base de datos a partir de un archivo XML. Las demás tendrán de ser cargadas por un funcionario de la autoridad.
5. El flujo del proceso de denuncia es el siguiente: Denuncia → Inspección → Incidente → Seguimiento. El proceso puede ser cambiado si el origen, al revés de una denuncia de consumidor, es una Programación basada en análisis de riesgo o un alerta internacional.
6. Al terminar el registro del alerta, el usuario tiene la opción de enviar inmediatamente, por correo electrónico, este alerta a todos los demás socios de la red, incluyendo la SGCAN. La estructura del correo está predefinida y este llevará como anexos el formulario, en formato XML generado automáticamente, e los demás documentos de soporte al registro del incidente, como son, por ejemplo, los resultados de los análisis.
7. Es posible sacar variadas estadísticas sobre la operatividad del sistema y la evolución de los diversos parámetros como, por ejemplo, los peligros asociados, el tipo y local de los incidentes, y las categorías de producto más afectadas.
8. La información que estará disponible libremente al público a partir del portal Web del SARABI no incorporará informaciones comerciales, como el nombre de las empresas ni las marcas.
9. Las búsquedas efectuadas en el portal Web pueden ser exportadas para un archivo en formato XLS (Excel) para permitir a los interesados más libertad en el tratamiento de la información presentada.
10. Los países podrán cargar al SINAVA los alertas emitidos a nivel internacional a sus productos para que puedan hacer el seguimiento de los mismos con el objetivo de averiguar la causa del incidente.

## 4 DESCRIPCIÓN DETALLADA DE REQUERIMIENTOS

### 4.1 ACTORES



## Proyecto "Etiquetado y Vigilancia del Mercado"

- **Administrador del sistema**

Encargado de la administración de los datos de base del sistema (usuarios, permisos, tablas de entidades técnicas, etc.).

- **Funcionario**

Funcionario que operará el SINAVA. Será el encargado de registrar las inspecciones, incidentes, emitir alertas y hacer consultas operativas y estadísticas.

- **Consumidor**

Este actor representa toda la población en general ya que sus roles son del dominio público. Podrá hacer búsquedas con varios parámetros en la base de datos central sobre los alertas emitidos por los Países Miembros, y hacer denuncias de incidentes con alimentos, a través del portal Web.

- **SARABI**

Se incluye este elemento automático para mejor modelizar las diversas acciones ejecutadas por el sistema. Todos los procesos generados automáticamente serán identificados por este actor (Generar archivo de traslado de los datos de alerta, enviar datos a la base de datos central, generar archivo XLS, etc.).

Como resumen, se pueden asumir los siguientes roles:

Administrador	Configuraciones de base; Entidades técnicas del sistema
Funcionario	Proceso operativo. Todas las funciones necesarias a la gestión diaria
SARABI	Procesos automáticos ejecutados por el sistema
Consumidor	Consultas y denuncias de incidentes con alimentos

## 4.2 REQUERIMIENTOS FUNCIONALES

### Diagramas de casos de uso

En los diagramas (y listado) de los casos de uso, cuando se refiere la palabra “Mantener” significa que el usuario puede ejecutar las operaciones CRUD (Leer, Crear, Actualizar y Eliminar). Sin embargo, estas operaciones están sujetas a los premisos asignados a cada Usuario en el programa “Mantener Permisos”. Los programas del módulo “Entidades de base” están por lógica asociados al rol Administrador. Sin embargo, este puede atribuir esas funciones a otros usuarios, que no hagan parte de este grupo.

La notificación utilizada sigue el estándar UML 2.0.





## Proyecto "Etiquetado y Vigilancia del Mercado"

### Entidades de base

Se consideran Entidades de base aquellas que sirven de modelación al negocio con el objetivo de darle más información estructurada y así se poder obtener estadísticas más amplias y detalladas. Estas entidades también sirven para facilitar el relleno de los formularios electrónicos por los usuarios ya que estos tienen acceso a las opciones disponibles en cada caso.

El diagrama siguiente enseña la interacción de los actores del sistema con los procesos que hacen parte de este módulo. Como estas entidades tienen muy poca, o ninguna, variación en el tiempo, son definidas inicialmente por el usuario administrador y cualquier cambio o adición también solo es posible se efectuado por este.

En el diagrama también se destacaron las entidades más importantes de este módulo:

- Categoría de productos
- Peligros asociados a los alimentos
- Usuarios
- Permisos

Entre las entidades no especificadas están:

- Partida arancelaria (NANDINA a 8 dígitos)
- País origen del incidente
- País donde el producto ha sido distribuido
- País que notificó
- Tipo de Producto (Alimento, Material de contacto)
- Clasificación de la Notificación (Alerta, Rechazo, Información, Noticia)
- Base de Notificación (Rechazo, Queja de consumidor, Brote de intoxicación alimentaria, Control oficial en el mercado, Control oficial posterior a una notificación internacional, Muestreo en frontera sin retención de la remesa, Autocontrol de la empresa)
- Autoridad Responsable – Datos institucionales, con indicación de las personas de contacto, de cada una de las entidades involucradas en la vigilancia de alimentos
- Tipo de autoridad (Mercado, Frontera, Planta) – identifica cuál el tipo de vigilancia que la entidad podrá ejecutar. Puede tener varias funciones
- Nacionalidad de la autoridad (Nacional, Extranjera, Comunitaria)
- Tipo de notificación (Alimento, Material de contacto) – identifica el rubro de la notificación.
- Base para la notificación – Acción de vigilancia que originó la notificación.
- Contra análisis – Si se efectuaron contra análisis.
- Local de las muestras
- Relación del producto con el producto notificado anteriormente en otra notificación enlazada – En el caso de que existan medidas sobre el producto.
- Estado de la distribución – En que estado se encuentra la distribución del producto.
- Tipo de riesgo (Salud humana, Salud animal, Ambiente)

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



- Legislación (Nacional, CAN, Estándar internacional)
- Medidas voluntarias – Posición del producto
- Medidas voluntarias - Destino
- Causa de la Inspección – Cuál la razón que originó la inspección.
- Medio de denuncia – Como fue efectuada la denuncia junto de la autoridad.

Estas entidades serán detalladas, más adelante, en el diccionario de datos.

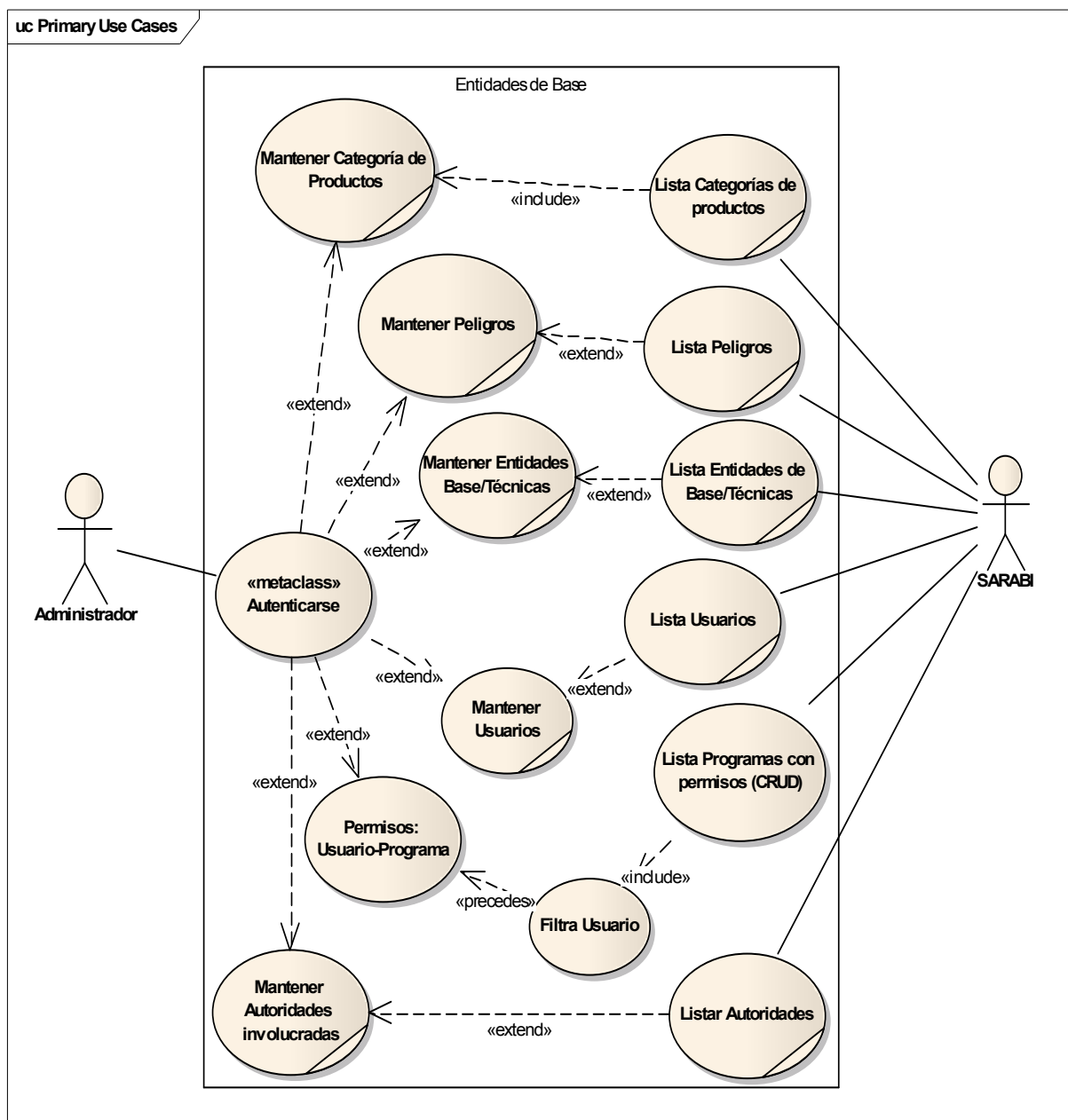


Figura 4 – Diagrama de casos de uso para definición de las entidades de base/técnicas del sistema.

Como se puede observar por el diagrama de casos de uso de la figura 4, la definición de estas entidades solo está disponible para un usuario administrador y que se haya autenticado al sistema. Aunque se pueda considerar la existencia de roles (administrador, funcionario), para una flexibilidad más grande en los accesos a los programas (permisos), el administrador debe definir los tipos de acción (leer, crear, editar, eliminar) que cada usuario podrá efectuar en cada programa disponible. Solo aparecerán en el menú del usuario los programas que tengan uno de los accesos posibles seleccionados.

Cada usuario tendrá una ficha de identificación de datos personales y institucionales y existirá la posibilidad de efectuar auditoria al sistema, para se conocer quién hizo lo qué, donde y cuando.

### Inspección

El modulo de inspección permitirá a los países hacer la gestión de las tareas relacionadas con la inspección de alimentos. Estas tareas consisten en:

- Registrar empresas
- Programar inspecciones versus empresa
- Consultar inspecciones (por empresa, producto, fecha, región).

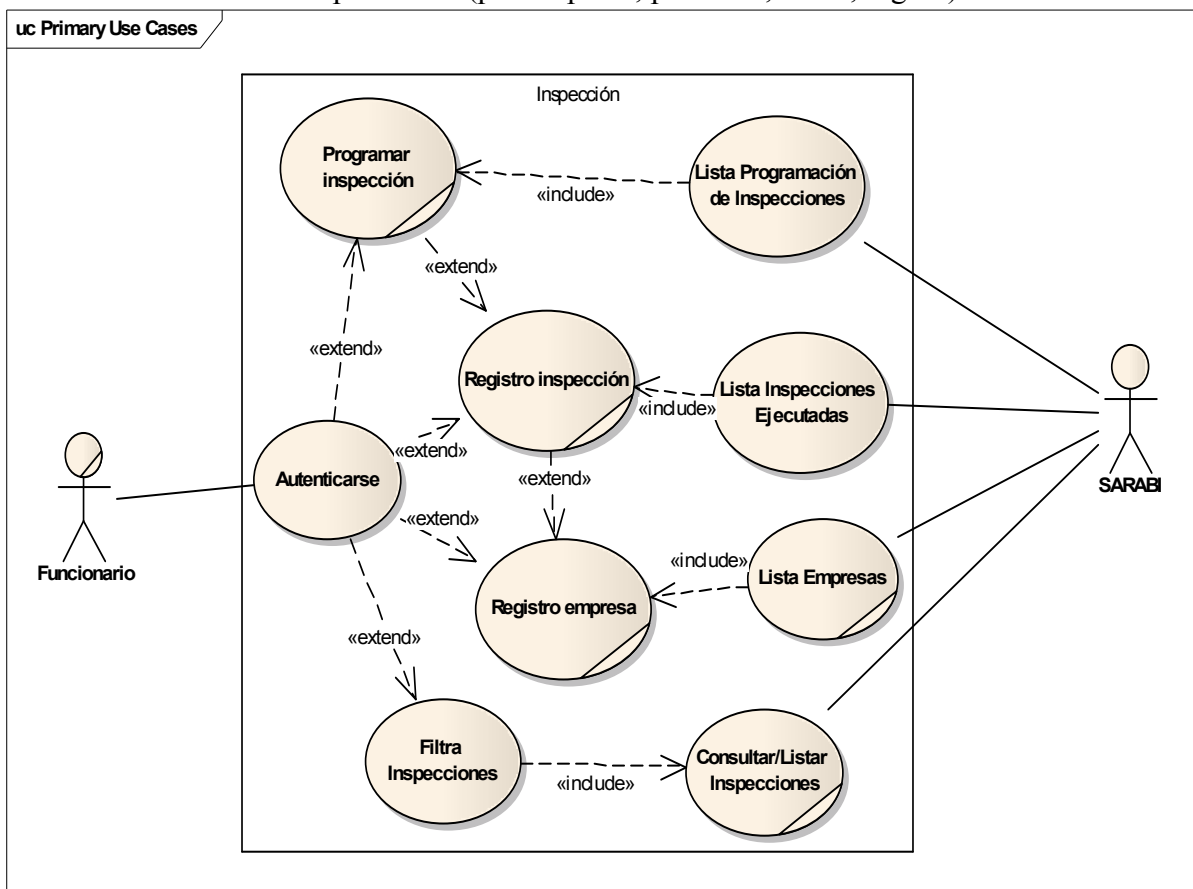


Figura 5 - Diagrama de casos de uso del módulo de Inspección.

El diagrama de la figura 5 esquematiza las actividades relacionadas con el modulo de inspección.

### Incidente

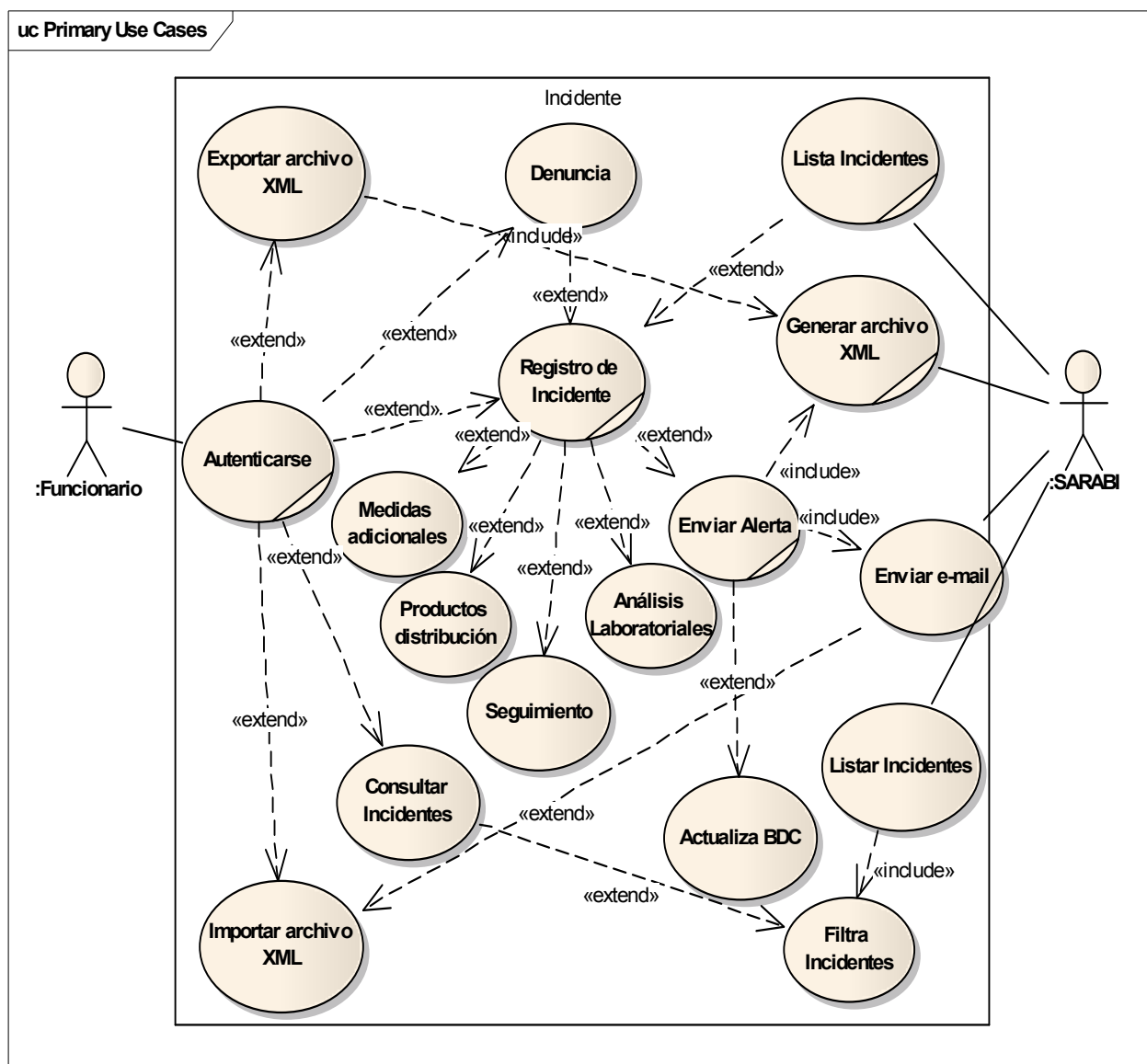


Figura 6 – Módulo de Incidentes y Alertas.

El modulo de gestión de incidentes posibilita a los países la creación de una base de datos detallada relativamente a los problemas encontrados con alimentos durante una inspección o por notificación de una entidad extranjera. Este módulo estará conectado con el modulo de Inspección para se mantener la trazabilidad y incluirá un sistema de notificación de alertas por correo electrónico, que agilizará el proceso de comunicación a las demás instituciones nacionales

involucradas, a sus socios comunitarios y, eventualmente, a las instituciones internacionales como la OMS.

El diagrama de la figura 6, esquematiza los casos de uso y los procedimientos involucrados incluidos en estos.

### Portal Web

El portal Web es la aplicación que permitirá a los consumidores de los países de la CAN hacer consultas libremente sobre los alertas emitidos por sus autoridades en vigilancia de alimentos. A partir de aquí también podrán interactuar con las autoridades haciendo denuncias de incidentes que eventualmente les hayan ocurrido.

La información enseñada en el portal estará tratada para no se mencionen el nombre de las empresas ni de las marcas garantizando la confidencialidad. Solo en último caso, en que la salud pública esté en riesgo de un brote muy grave, estas informaciones deberán ser proveídas.

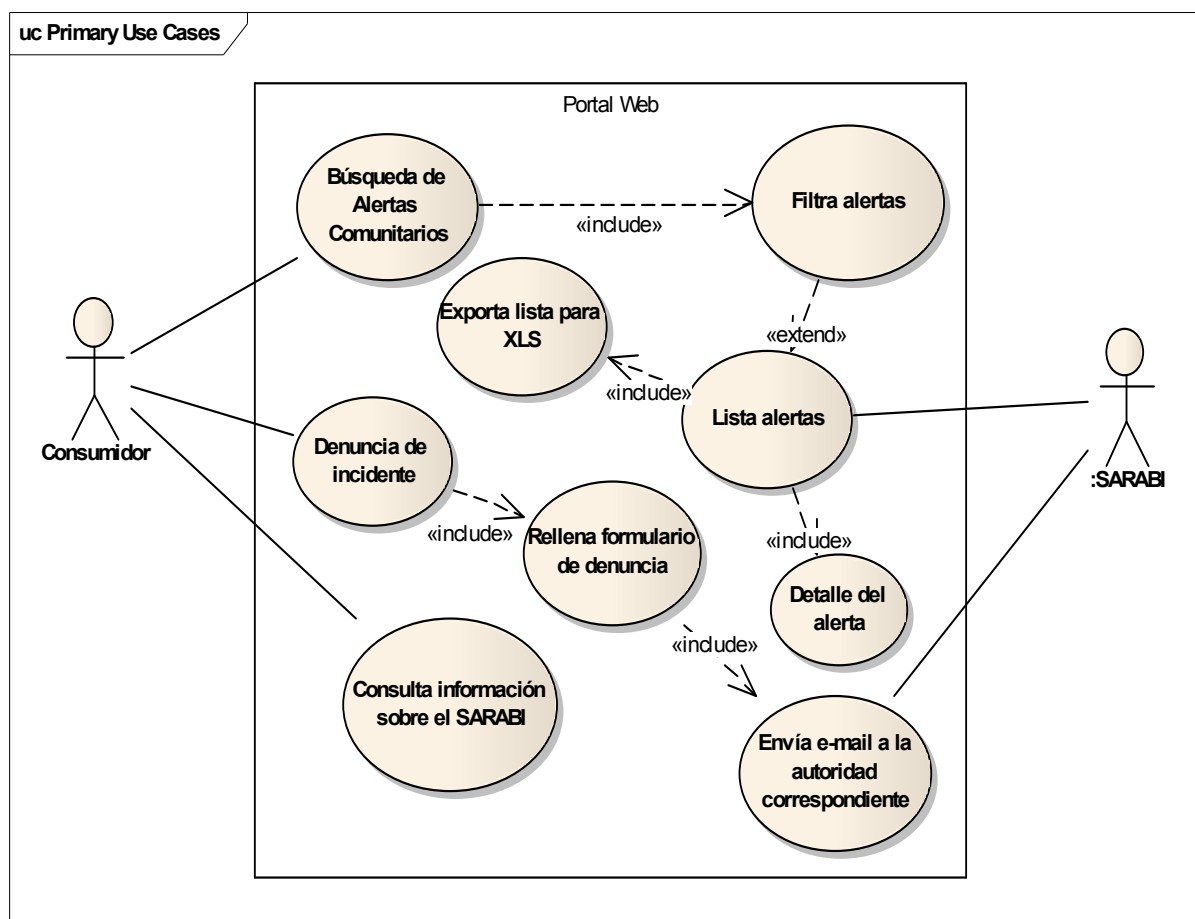


Figura 7 – Portal Web comunitario.



## Proyecto "Etiquetado y Vigilancia del Mercado"

Como se puede observar por la figura 7, el consumidor puede ejecutar tres tareas principales en el portal:

- Búsqueda de alertas;
- Denuncia de incidentes;
- Consulta de información sobre el funcionamiento del SARABI.

### Listado de casos de uso

#	Caso de uso	Rol	Módulo
1	Mantener entidades de base del sistema	Administrador	Entidades de base
2	Mantener categorías de productos	Administrador	Entidades de base
3	Mantener peligros asociados a los alimentos	Administrador	Entidades de base
4	Mantener Usuarios	Administrador	Entidades de base
5	Mantener permisos	Administrador	Entidades de base
6	Registro de empresa	Funcionario	Inspección
7	Programar Inspección	Funcionario	Inspección
8	Registro de Inspección	Funcionario	Inspección
9	Registro de Incidente	Funcionario	Incidente
10	Envío de alertas sobre incidentes a los socios	Funcionario	Incidente
11	Generar archivo de información de alerta en formato XML	SARABI	Incidente
12	Importar archivo XML de información de alerta	Funcionario	Incidente
13	Búsqueda de alertas en la base de datos	Consumidor	Portal
14	Generar archivo XLS (Excel) con datos de búsqueda	SARABI	Portal
15	Exportar datos de búsqueda para formato XLS	Consumidor	Portal
16	Registro de denuncias	Consumidor	Portal
17	Consulta de inspecciones	Funcionario	Inspección
18	Consulta de incidentes	Funcionario	Incidente
19	Registro de denuncias	Funcionario	Incidente

Los módulos indicados en la tabla anterior corresponderán a los **menús** en el sistema. Se salvaguarda el caso particular del *Portal* que es una aplicación independiente y que tendrá tres programas (páginas Web), además de la portada, ya descritos en el punto anterior:

- Búsqueda de notificaciones
- Denuncia de incidentes
- Información sobre el sistema



## Proyecto "Etiquetado y Vigilancia del Mercado"

### Detalle de casos de uso

Como norma en los diversos programas del sistema se hará aquí una descripción de las acciones típicas en cada entidad (conocidas como CRUD):

#### Crear

Siempre que se elige esta acción es abierta una página con los campos vacíos para que el usuario los pueda rellenar.

#### Editar

El usuario debe seleccionar una entidad del listado presentado y al seleccionar la opción 'Editar' se abrirá la página ya con los datos de la entidad cargados para que se puedan cambiar.

#### Eliminar

En el listado presentado al usuario, el usuario debe seleccionar la línea correspondiente al registro que pretende eliminar y pulsar el respectivo botón. Esta acción exige siempre una confirmación por parte del usuario para evitar equívocos.

#### Leer

Como en la opción 'Editar', es abierta la página con los datos del registro seleccionado en el listado pero el usuario no tendrá posibilidad de hacer cambios a los mismos.

Además de las acciones usuales descritas arriba, todos los casos de uso, exceptuando las consultas, tendrán el mismo modo de acceso, lo que facilitará también el conocimiento y manejo del sistema:

- Acceder al menú correspondiente;
- Seleccionar el programa respectivo;
- Presentar un listado con las instancias ya creadas y con los campos más relevantes de las mismas, ordenados por orden cronológica inversa, y con botones (o enlaces) con las acciones CRUD mencionadas.

Cuando se refiere abajo en las precondiciones que es necesario permiso para acceder al programa (lo que puede parecer redundante), se quiere realzar que esos casos de uso están normalmente disponibles a los usuarios administradores.

### Entidades de base

Todos los casos de uso de entidades de base y técnicas del sistema consisten en estructuras de información con código y descripción, así que la modelación de los mismos es idéntica.

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

Para estos tres casos de uso (las entidades de base del sistema son varias, solo se separaron las categorías y los peligros para realzar su relevancia) las acciones son las siguientes:

- Será enseñado un listado de las entidades ya creadas y existirán las opciones de Crear, Editar, Consultar, Eliminar e Imprimir (el listado). Cada una de estas acciones tiene el funcionamiento descrito arriba.

Precondiciones:

- Autenticación como administrador del sistema.
- La tabla de Tipos de Entidad deberá estar ya definida para el tipo que se pretende crear sus instancias.

### **Registro de Empresa**

Pasos:

1. Acceder al menú Inspección y seleccionar el programa 'Empresa';
2. Es presentado el listado con las empresas ya cargadas;
3. Se elije una de las acciones CRUD o imprimir el listado.

Precondiciones:

- Autenticación en el sistema.
- Tener los datos de la empresa (Razón social, Responsable, Categoría de producto con que trabaja, etc.)

### **Registro de Inspección**

Este caso de uso es utilizado en dos modos diferentes. Primero para programar las inspecciones y después para registrar los datos de la ejecución de la misma. Asimismo, los atributos obligatorios son diferentes en cada caso.

La inspección es el acto de vigilancia llevado a cabo por las autoridades responsables junto de las empresas que producen y/o comercializan productos alimentarios. Los locales típicos de inspección son en: Frontera, Mercado y Planta. La inspección puede tener origen en varios factores: Programación de análisis de riesgo, denuncia, seguimiento de incidente previo, alerta internacional.

Atributos obligatorios:

Programación:

- Fecha prevista

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"





## Proyecto "Etiquetado y Vigilancia del Mercado"

- Hora prevista
- Empresa
- Justificación
- Autoridad (automático – definido por el usuario que registra)

### Ejecución:

- Fecha real
- Hora real
- Datos de contacto del responsable
- Causa de la inspección (programación u otra)
- Informe – descripción detallada de la ocurrencia.

### Pasos:

1. Registro de la programación de la inspección (opcional);
2. Registro de la ejecución;
3. Impresión de los datos de la inspección;

### Precondiciones:

- Autenticación en el sistema;
- Empresa a inspeccionar ya creada en el 'Registro de Empresa'.

### Poscondiciones:

- Registro de análisis;
- Programación de nueva inspección.

## **Registro de Incidente**

El Incidente puede tener como causas las siguientes acciones:

- Inspección llevada a cabo por una autoridad de vigilancia;
- Notificación de alerta de un tercero país o institución internacional (e.j. OMS) sobre productos nacionales;
- Notificación de alerta de un tercero país o institución internacional sobre productos que pueden haber alcanzado, o alcanzar, el mercado nacional.

Un punto importante en el registro de Incidente es la indicación de los países (si conocidos) donde el producto ha sido distribuido. Esto ayuda los países que reciban la notificación a mejor identificar la urgencia de acciones de la misma.

### Pasos:

1. Rellenar formulario de Incidente con todos los campos indicados como obligatorios en el Diagrama Entidad-Relación ("Not Null");
2. Grabar el formulario;
3. Opcionalmente:

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"





## Proyecto "Etiquetado y Vigilancia del Mercado"

- a. Añadir documentos digitales relacionados con el incidente que sirvan para ayudar en su mitigación;
- b. Registrar ocurrencias de seguimiento del incidente;
- c. Indicar medidas adicionales para importación;
- d. Registrar datos de análisis efectuadas;
4. Elegir si pretende enviar notificación por correo electrónico. Si procede, entonces elegir si envía solo a las autoridades nacionales o también a las internacionales;
5. Opcionalmente, imprimir el formulario.

### Precondiciones:

- Autenticación al sistema;
- Definición de todas las entidades de base necesarias en el formulario de incidente;
- Servidor de SMTP configurado y probado.

### Poscondiciones:

- Enviar notificaciones automáticamente a las demás autoridades nacionales;
- Enviar notificaciones a los socios de la CAN si es un producto importado o que es exportado a esos países.

## **Registro de denuncias**

### Pasos:

1. Acceder al portal Web;
2. Elegir 'Denuncias';
3. Rellenar el formulario indicando un teléfono válido;
4. Grabar el formulario. Esta acción genera el envío de un correo electrónico al Punto Focal del país correspondiente.

### Precondiciones:

- Acceso a Internet;
- Navegador Web compatible (Internet Explorer 6, Firefox 2 o Chrome 4, como mínimo);
- Conocimiento básico de manejo de formularios Web.

### Poscondiciones:

- Si procede, conexión a un Incidente (solo para funcionarios).

## **Búsqueda de alertas en la base de datos**

### Parámetros de búsqueda:

- País incidente;

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

- País origen del producto;
- Categoría de Producto;
- Período (Fecha inicial y final);
- Peligro;
- Tipo de alerta (notificación).

### Pasos:

1. Acceder al portal Web;
2. Elegir 'Búsquedas de alertas';
3. Seleccionar los parámetros de consulta que pretende para filtrar la información;
4. Pulsar el botón 'Buscar';
5. Es presentado un listado con los alertas que coinciden con el filtro utilizado;
6. Pulsando sobre el código del alerta se puede acceder al detalle de la misma;
7. Opcionalmente, puede imprimir y/o exportar la información a un archivo XLS (Excel)

### Precondiciones:

- Acceso a Internet;
- Navegador Web compatible (Internet Explorer 6, Firefox 2 o Chrome 4, como mínimo);
- Conocimiento básico de manejo de formularios Web.

## **Consulta de incidentes**

### Parámetros de búsqueda:

- Período;
- Autoridad;
- Departamento (región)
- Categoría de producto
- Peligro
- Local de vigilancia

### Pasos:

1. Acceder al programa de Consultas en el Menú Incidentes;
2. Seleccionar los parámetros de búsqueda pretendidos;
3. Pulsar el botón Consultar;
4. Es presentado el listado de los incidentes que pueden ser, opcionalmente, impresos.

### Precondiciones:

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

- Autenticación en el sistema;
- Permiso de acceso al programa.

### **Consulta de inspecciones**

Parámetros de búsqueda:

- Período;
- Autoridad;
- Departamento (región)
- Categoría de producto

Pasos:

1. Acceder al programa de Consultas en el Menú Inspecciones;
2. Seleccionar los parámetros de búsqueda pretendidos;
3. Pulsar el botón Consultar;
4. Es presentado el listado de las inspecciones que pueden ser, opcionalmente, impresas.

Precondiciones:

- Autenticación en el sistema;
- Permiso de acceso al programa.

### **Generar archivo de información de alerta en formato XML**

Este caso de uso es despaletado por el caso de uso 'Registro de Incidente' en la opción de envío de notificación. Sin embargo también puede ser generado separadamente.

Pasos:

1. Acceder al programa de Incidentes;
2. Seleccionar el Incidente respectivo y pulsar el botón (enlace) 'Editar';
3. En la página que es abierta con el detalle del incidente, seleccionar 'Enviar notificación';
4. El archivo es generado automáticamente y guardado en la carpeta 'Docs' (con la notación: INCIDENTE\_+ el ID del incidente en el nombre del archivo) del servidor que deberá poder ser configurada en la aplicación;
5. El usuario tendrá de poder acceder a la carpeta para leer el archivo.

Precondiciones:

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

- Autenticación en el sistema;
- Permiso de acceso al programa;
- Permiso de acceso al servidor y a la carpeta 'Docs'

### **Importar archivo de información de alerta**

Pasos:

1. Acceder al menú Incidentes y seleccionar el programa 'Importar archivo de alerta';
2. En el campo de selección de archivos, elegir el archivo XML que ha sido generado en la opción de envío de notificaciones, en el programa 'Registro de incidente';
3. Pulsar 'Importar';
4. Acceder al programa 'Registro de Incidente';
5. Analizar en el listado presentado si el nuevo alerta ha sido añadido;
6. Seleccionar el nuevo incidente y elegir la opción CRUD pretendida (en este caso la acción 'Crear' no hace sentido).

Precondiciones:

- Autenticación en el sistema;
- Permiso de acceso al programa;

### **Exportar datos de búsqueda para formato XLS**

Permite al usuario exportar la información visualizada en pantalla para un archivo XLS. Esta posibilidad permite al usuario la libertad de tratamiento de los datos segundo varios criterios a su elección.

Pasos:

1. Ejecutar el caso de uso 'Búsqueda de alertas en la base de datos';
2. Pulsar el botón (enlace) 'Exportar XLS' en la página con el listado de los alertas;
3. Elegir la carpeta donde grabar el archivo en la computadora personal.

Precondiciones:

- Acceso a Internet;
- Navegador Web compatible (Internet Explorer 6, Firefox 2 o Chrome 4, como mínimo);
- Conocimiento básico de manejo de formularios Web;
- Disponer de software que permita leer (y/o manejar) archivos XLS (e.g. Excel).

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

### **Mantener permisos**

Pasos:

1. Acceder al programa 'Permisos';
2. Elegir el usuario para el cuál se pretende visualizar o manejar los permisos de acceso a los programas;
3. Seleccionar las acciones CRUD, identificadas por 'CheckBoxes' en cada uno de los programas que el usuario debe poder ejecutar;
4. Grabar las definiciones.

Precondiciones:

- Autenticación como Administrador.
- Usuario ya creado en el sistema.

### **Mantener Usuarios**

Pasos:

1. Acceder al programa Usuarios;
2. Seleccionar del listado el usuario a Consultar/Editar/Desactivar, o pulsar el botón Crear para añadir un nuevo usuario, o seleccionar imprimir el listado de usuarios.
3. En el formulario de edición de los atributos del usuario, rellenar todos los campos presentados.
4. La Contraseña no es enseñada en modo de Consulta y Edición. Para cambiarla es necesario introducirla dos veces. Al grabar es enviado un correo electrónico a la cuenta definida en el sistema con la indicación de la Contraseña y Nombre de usuario.

Precondiciones:

- Autenticación en el sistema;
- Cada usuario puede mantener su cuenta;
- El administrador puede cambiar los datos y es el único que podrá crear nuevos usuarios (a menos que en el programa Permisos sea asignado otro usuario).

### **Prototipo de interfaz de usuario**

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

Para el interfaz con el usuario se debe considerar la regla de mantener los menús de navegación en la aplicación horizontalmente en el encabezamiento de todas las páginas de la aplicación SINAVA. De este modo queda más espacio para presentación de la información en formato de planilla, lo que torna la aplicación más ergonómica, no siendo necesario utilizar definiciones de pantalla muy grandes con el consecuente tamaño de letra muy pequeño (la aplicación debe estar preparada para funcionar con una resolución de pantalla de 1024x768 píxel).

Todas las páginas con listados de procesos o entidades deben tener un botón para que el usuario pueda imprimir la información presentada.

Las páginas que no tienen ninguna señal de navegación son las presentadas cuando se elige el programa en el menú. Por coherencia, estas páginas enseñan un listado de las instancias de la entidad respectiva con botones que ejecutan las acciones CRUD.

El botón 'Cancelar' indicado en las páginas ejecuta la acción de volver a la página anterior. Caso la palabra 'Volver' sea más adecuada (en función de la experiencia en la región) se debe utilizar.

### SINAVA

Para se acceder al SINAVA es necesario poseer una cuenta que debe ser creada por el administrador nacional del sistema. Los usuarios están conectados con sus instituciones y siempre que es necesario indicar la 'Autoridad' el sistema selecciona automáticamente la institución conectada al usuario.

La portada de entrada del SINAVA presenta inmediatamente los últimos 5 (cinco) incidentes registrados y las próximas 5 inspecciones programadas. Pulsando sobre el código de cada una se puede acceder al detalle.

Como se puede observar en la Figura 8, todas las páginas deben contener el menú de navegación para cualquier una de las demás, facilitando la utilización al usuario.



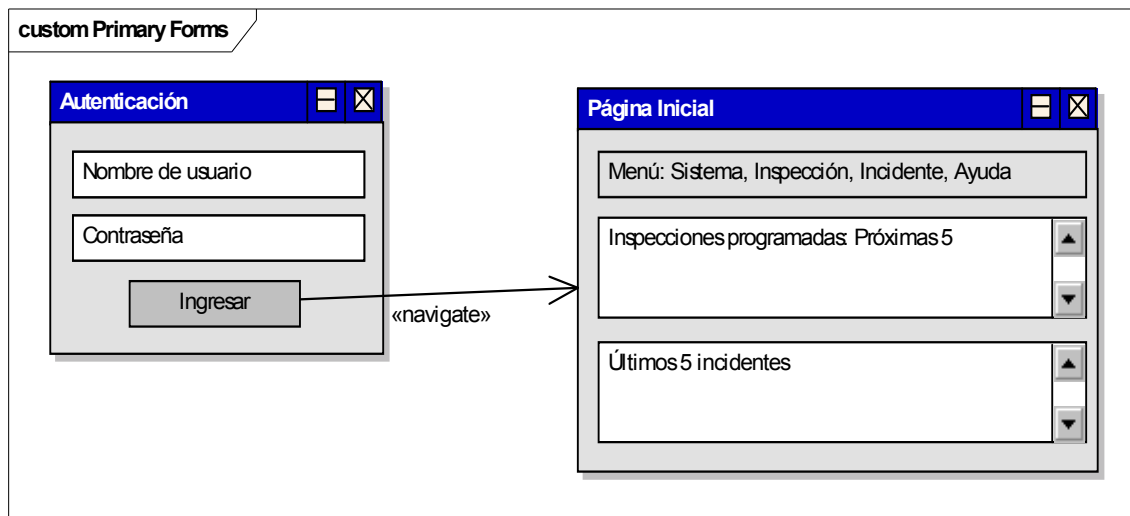


Figura 8 – Página de autenticación y de entrada en la aplicación SINAVA.

Para facilitar el manejo de las entidades con objetivos estadísticos, se diseñó un pequeño módulo, llamado Entidades de Base, que evitará modificaciones de código fuente de los programas y de la estructura de la base de datos en el futuro, caso sea necesario añadir o modificar algo. La Figura 9 enseña las tres páginas necesarias para manejar estas entidades.

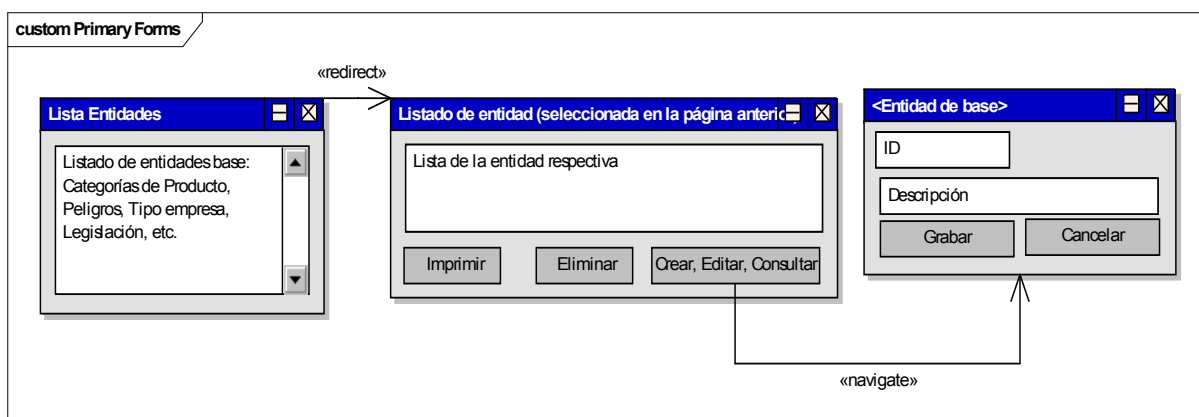


Figura 9 – Tipos e instancias de las Entidades de base.

La gestión de usuarios está simplificada. Después de crear la cuenta se debe indicar cuales son los programas a los cuales el nuevo usuario puede acceder. Este procedimiento debe ser ejecutado por un usuario administrador. La figura 10 representa el estilo de las páginas para este caso de uso.

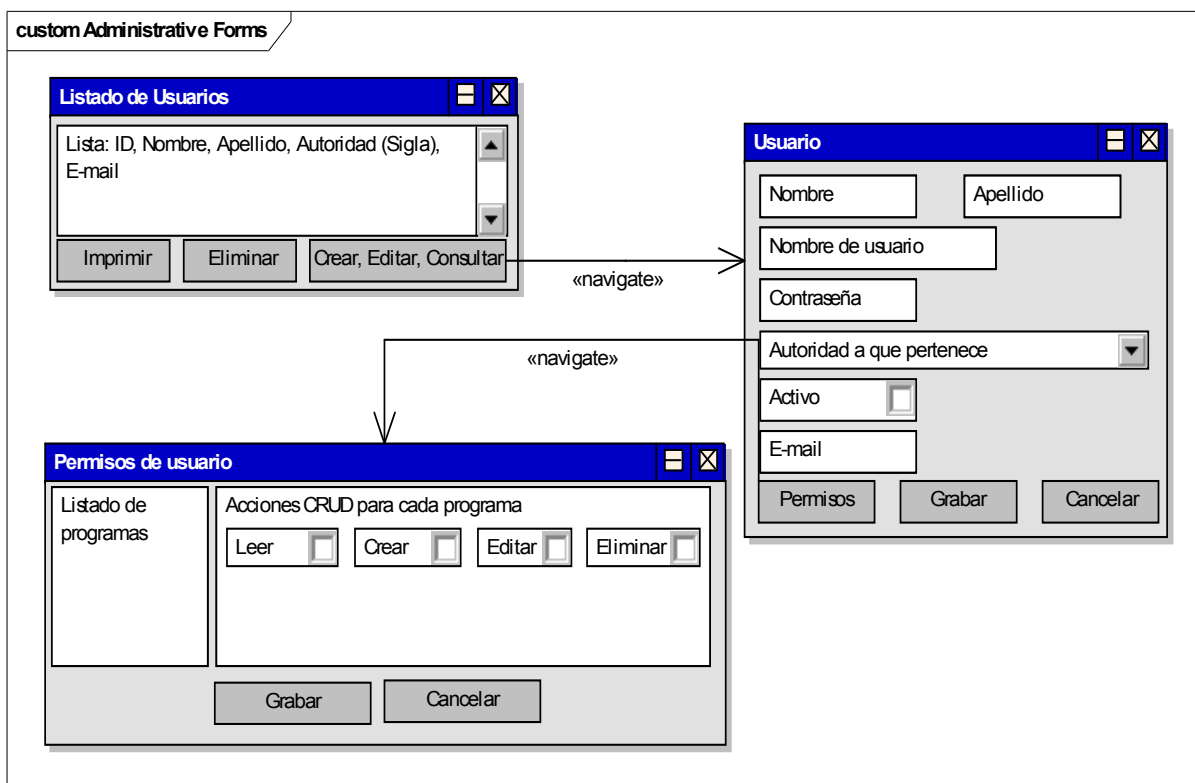


Figura 10 – Configuración de usuarios.

El proceso de registro de incidentes y notificación de alertas es el central de todo este sistema y todos los demás sirven de apoyo, o son consecuencia, de este. Al ingresar al programa es enseñado, como en los demás, un listado ordenado por orden decreciente de la fecha de incidente, que es posible filtrar por periodo, categoría de producto y región. En esta página aparecen os botones con las cuatro operaciones CRUD más la de imprimir el listado enseñado en la pantalla. Para se acceder al detalle, es necesario pulsar sobre el botón, que puede estar en forma de enlace, en la línea respectiva. Si el usuario tiene permiso de Edición para ese programa puede hacer cambios, sino, solo podrá consultar (si también tiene permiso para eso). Para insertar un nuevo incidente basta tan solo pulsar el botón Crear y aparecerá el formulario respectivo en blanco, con los campos automáticos rellenados (autoridad a la cual el usuario está conectado, país notificante al cuál la autoridad pertenece, fecha, etc.). Dentro del formulario de incidente el usuario puede añadir documentos digitales e indicar los países (si conoce) donde el producto ha sido distribuido. Después de confirmar todos los datos y grabar le es preguntado si quiere enviar notificaciones a las demás entidades y socios comunitarios. En esta página se puede elegir esa información y hacer las notificaciones. La figura 11 representa todo este proceso.



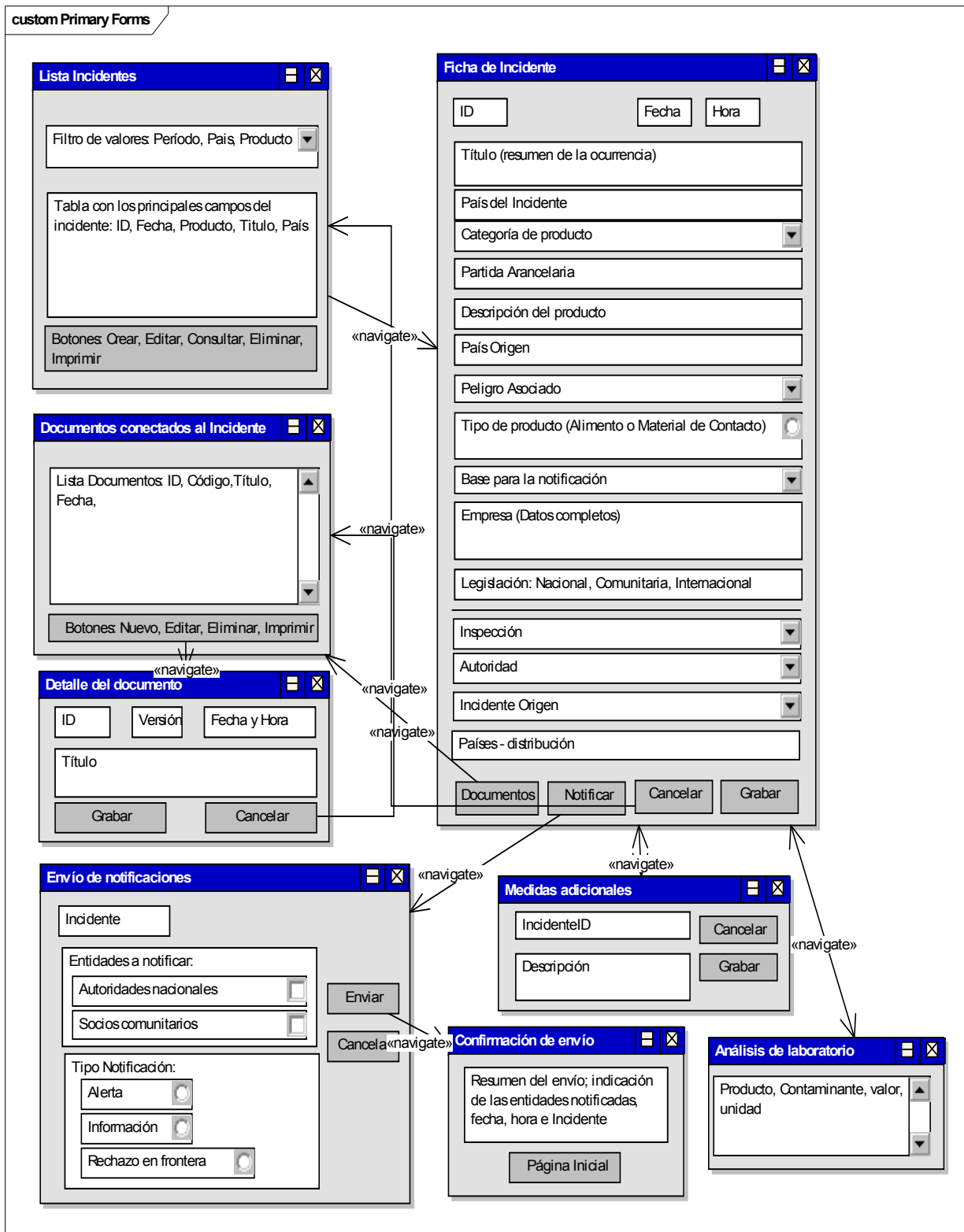


Figura 11 – Proceso de registro de incidentes.

El proceso de inspección no era parte integrante de los TdR de esta consultoría por ser un proceso puramente nacional pero, como ya fue referenciado antes, este proceso es fundamental para tener la trazabilidad completa de los productos y proveer a las autoridades involucradas con un sistema de gestión eficaz.

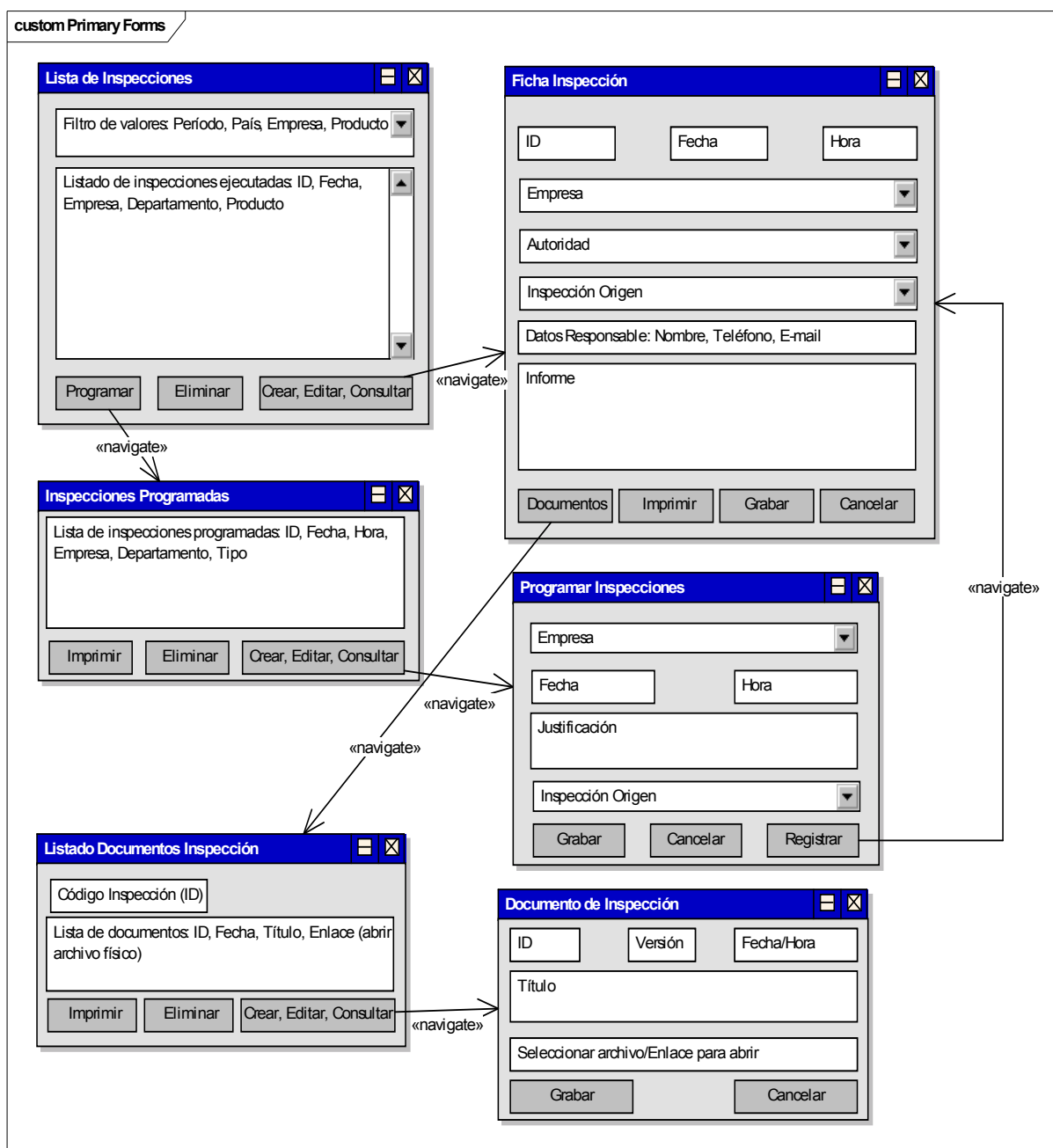
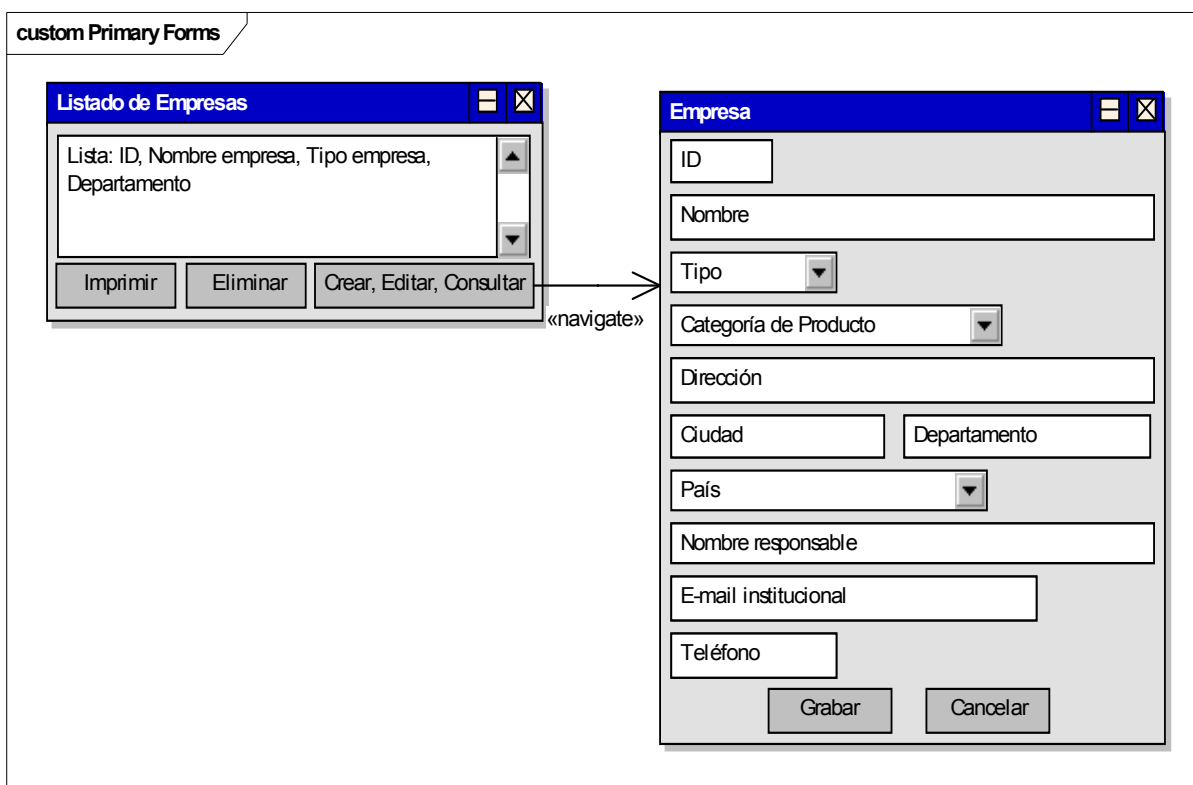


Figura 12 – Proceso de inspección.

La figura 12 representa este proceso que puede ser ejecutado a dos tiempos. Primero programando la inspección, y después registrando el informe de la misma. Una inspección puede o no dar origen a un incidente. Asimismo, en la ficha de Incidente existe un campo, no obligatorio porque es posible registrar incidentes sin inspección, donde es posible indicar la inspección que le ha dado origen.

Como en el proceso de Incidente, también es posible aquí añadir documento digitales relacionados con la inspección, incluyendo los documentos de análisis de laboratorio (en el registro de incidente los análisis de laboratorio están estructurados en una tabla para facilitar su búsqueda y presentación al público), para que se tenga todo en un solo local y sea más fácil acceder a la información.



The screenshot displays two windows within a 'custom Primary Forms' container. The 'Listado de Empresas' window on the left shows a list of companies with columns for ID, Name, Type, and Department. It includes buttons for 'Imprimir', 'Eliminar', and 'Crear, Editar, Consultar'. The 'Empresa' window on the right is a form for entering company details, including fields for ID, Name, Type, Product Category, Address, City, Department, Country, Responsible Name, Institutional Email, and Phone. It also has 'Grabar' and 'Cancelar' buttons. An arrow labeled '«navigate»' indicates the flow from the list window to the form window.

Figura 13 – Ficha de empresa.

Para que el proceso de inspección esté completo es necesario mantener una base de datos de las empresas a las cuales se hará o hizo inspecciones. Este registro ayudará también en la trazabilidad de los incidentes ya que pueden ser detectados en la empresa distribuidora pero tener origen en el fabricante o productor (se considera al Productor como la empresa que cultiva productos naturales y al Fabricante lo que vende productos procesados). La figura 13 muestra un ejemplo de cómo puede ser diseñada la página con la ficha de empresa.

Los usuarios que manejarán el SINAVA pertenecen a instituciones nacionales que son clasificadas como Autoridades en alimentos y que ejecutan un rol en el sistema. Los roles identificados son lo

de regulación y vigilancia, siendo que esta última puede ser ejecutada en Frontera, Mercado o Planta. Asimismo, es necesario mantener una ficha de autoridad en el sistema con los datos institucionales para que estas se puedan comunicar también entre si. La figura 14 enseña un ejemplo de páginas para la ficha de autoridad.

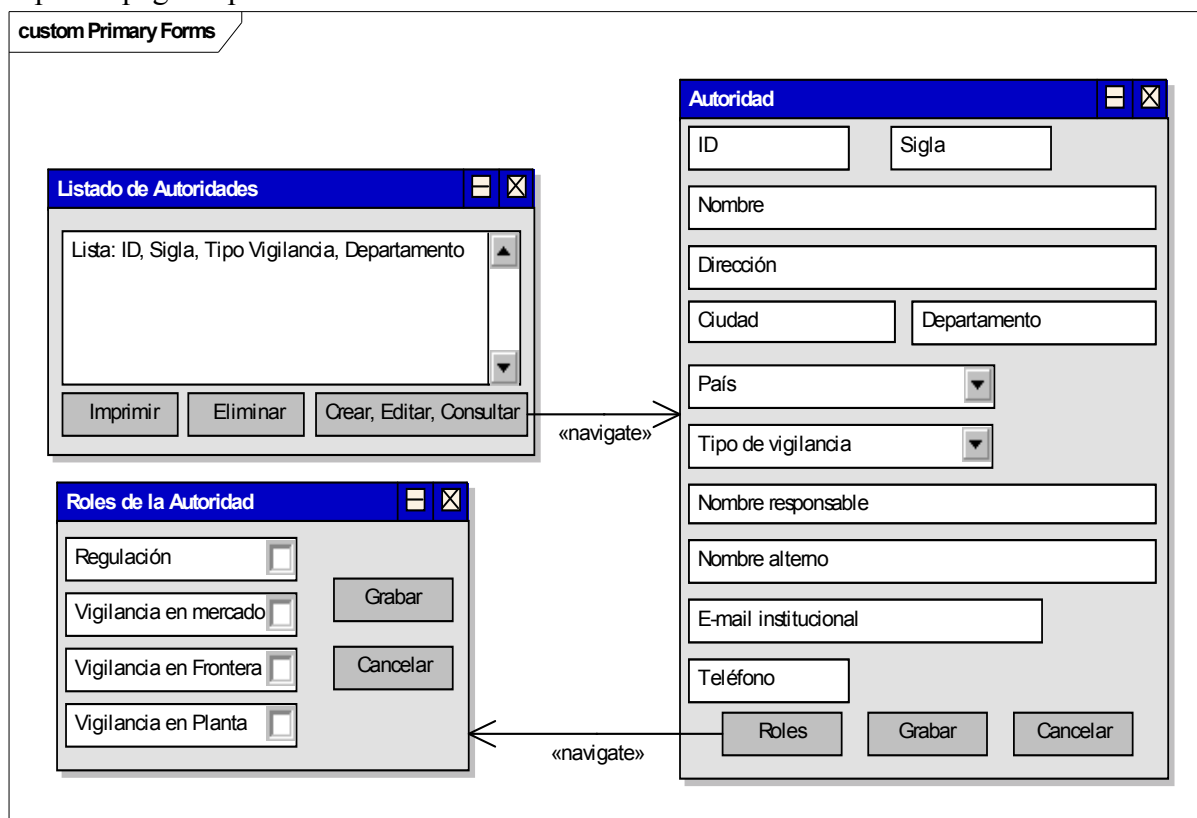


Figura 14 – Ficha de Autoridad.

### Portal Web Comunitario

En el diseño propuesto, y como lo solicitado en los TdR, se prevé que la ventana al público sea común para toda la red, por lo que, lógicamente, tendría que estar soportada por la SGCAN. Sin embargo, a partir del mismo diseño, los países pueden desarrollar sus ventanas nacionales. El portal Web comunitario permite a los consumidores la consulta de alertas (incidentes) existentes con alimentos en la Comunidad Andina, hacer comparaciones, y otros análisis estadísticos. Las búsquedas efectuadas pueden ser exportadas a formato XLS (Excel) para que los consumidores (u otros usuarios con interés en el tema) puedan tratar la información a su manera.

El portal debe ser muy sencillo, con la información necesaria y suficiente al consumidor. En la figura 15 se muestra un ejemplo de las páginas del portal donde se puede observar que el menú de navegación es parte integrante de todas.

La página de Información debe funcionar como ayuda al consumidor para que entienda fácilmente el alcance del sistema y cómo se puede utilizar. Aquí también debe estar explícito el procedimiento para hacer una denuncia, especialmente los datos mínimos a proveer, como:

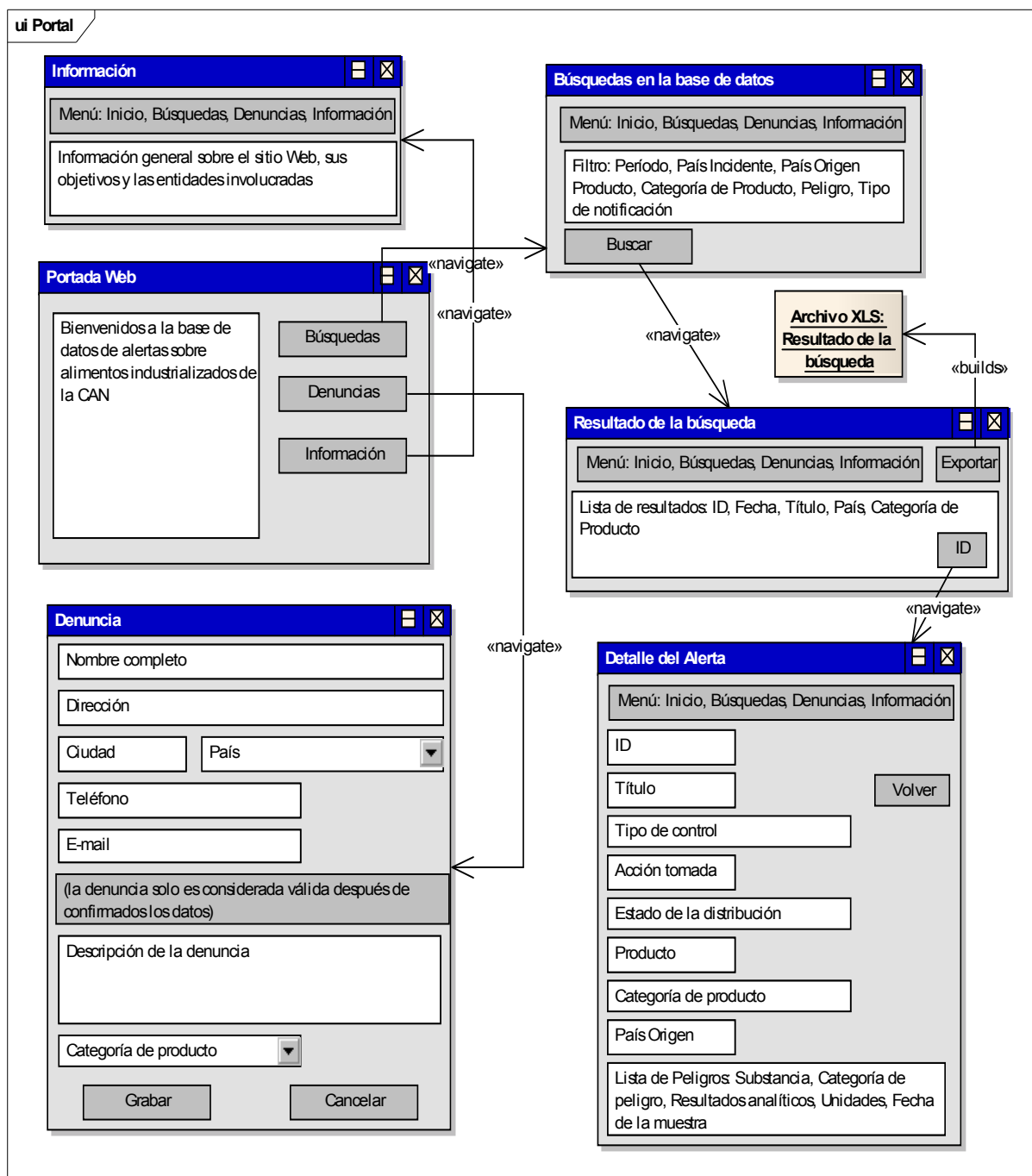


Figura 15 – Portal Web

Datos personales:



## Proyecto "Etiquetado y Vigilancia del Mercado"

- Nombre completo
- Teléfono (la denuncia solo es válida después de que el consumidor haya sido contactado telefónicamente)
- e-mail
- Dirección completa
- DNI
- Fecha nacimiento

Datos de la empresa:

- Nombre de la empresa donde ocurrió/compró el producto en causa
- Dirección completa
- Tipo empresa: Supermercado, restaurante, mercado, etc.
- Categoría de producto ( a elegir de una lista)
- Producto (descripción detallada)

Observaciones (descripción detallada del incidente)

### 4.3 REQUERIMIENTOS NO FUNCIONALES

#### Del producto

Usabilidad:

**RN-1.** El sistema debe estar preparado para ser operado a través del ratón y teclado.

**RN-2.** Las pantallas serán desarrolladas para entorno Web, con resolución de pantalla de 800 x 600 o superior.

**RN-3.** Todas las pantallas deben tener un modo de cancelar la operación en curso.

**RN-4.** Todas las búsquedas o consultas deben estar paginadas (botones primero, último, siguiente y anterior).

**RN-5.** Verificar/validar límites de campos y tipos de datos de las pantallas en relación al modelo de datos.

**RN-6.** Las pantallas podrán ser accedidas por medio de menús dentro del sistema.

Confiabilidad:

**RN-7.** Deberá existir consistencia de los datos a los fines de que los mismos sean ciertos evitando totalmente violaciones de integridad.

**RN-8.** Disponibilidad: el portal Web debe tener una disponibilidad muy cercana a los 100%. La aplicación SINAVA debe estar disponible en el horario laboral, contando con las posibles horas extra. Se debe reservar la madrugada para hacer las copias de seguridad y el final del

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

día laboral para el posible mantenimiento de los servidores y otros dispositivos de red.

### Performance:

**RN-9.** El sistema deberá liberar a todos los recursos de memoria al momento de cerrar una ventana y finalizar una funcionalidad.

**RN-10.** Ninguna página extra consultas/estadísticas debe tardar más que 3 segundos a abrirse completamente.

### Soportabilidad:

**RN-11.** El control de integridad de datos se hará del lado de la capa de datos (a nivel de la base de datos utilizando las claves foráneas). Los mensajes de error serán capturados por la aplicación y serán visualizados al usuario final.

**RN-12.** Se deberá mantener una convención de nombres y nomenclaturas que facilite el entendimiento de los diversos componentes del sistema sin causar ambigüedad.

### Documentación:

**RN-13.** La implementación deberá ser acompañada por un manual de usuario en línea y una manual de pase-a-producción. El manual técnico de la base de datos, con su versión final (caso se hagan cambios al diseño aquí propuesto) también deberá ser proveído.

### Del ambiente

#### Ético:

El sistema busca beneficiar al mayor número de consumidores garantizando la seguridad de los alimentos en la medida que facilita la gestión de la información y de las operaciones de las autoridades responsables por la vigilancia de alimentos.

#### Legales:

El sistema no puede ir contra las leyes y reglamentaciones de la función pública de cada uno de los países en los cuales será implementado.

## 4.4 MODELO DE CLASES

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

En este modelo de clases se estableció una clase única con todas las entidades de base y técnicas del sistema, las cuales son definidas tan solo por dos atributos: código y asignación. Esta aproximación provee una flexibilidad, y escalabilidad, más grande al sistema al permitir crear nuevas entidades, y sus instancias, sin necesidad de modificar el código de los programas. Las demás clases identificadas son las siguientes:

- Empresa
- Inspección
- Incidente
- Notificación
- Autoridad
- Denuncia
- Entidad Base
- País
- Usuario
- Programa
- Menú
- Auditoría

En el diagrama de clases se puede observar que no están indicados los Métodos usuales que la mayoría de las clases implementan: **Leer, Crear, Actualizar y Eliminar**, más conocidos como CRUD. Todos estos métodos (menos el crear que lleva todos los atributos) llevan como parámetro el ID de la instancia de la clase. Hay dos clases que, por su lógica, no implementan el método Actualizar y Eliminar – *Auditoría y Notificación*.

Todas las clases son identificadas unívocamente a través de su ID (atributo de identidad único por instancia). Este atributo es secuencial y se incrementa automáticamente.

Algunas clases tienen atributos para trazabilidad de sus instancias como la Fecha de Creación, Fecha de Cambio y el Usuario. El usuario y la fecha de cambio son actualizados siempre que hay una modificación del registro.

En la figura 16 se enseña el modelo de clases general para todo el SARABI. Aunque este esté separado en dos aplicaciones (SINAVA y Portal Web Comunitario) el diseño presentado sirve también para una implementación centralizada de todo el sistema. Es decir, se puede elegir una única ubicación (de servidores) y los países accederían a través de la Internet. Cualquiera una de las opciones no tienen implicaciones para el usuario ya que el modo de manejar el sistema es exactamente igual. La ventaja sería los costos (más bajos) de implementación y sostenibilidad.





Por otro lado, los países pueden aprovechar el modelo presentado para implementar sus páginas Web de consulta de incidentes a nivel nacional.

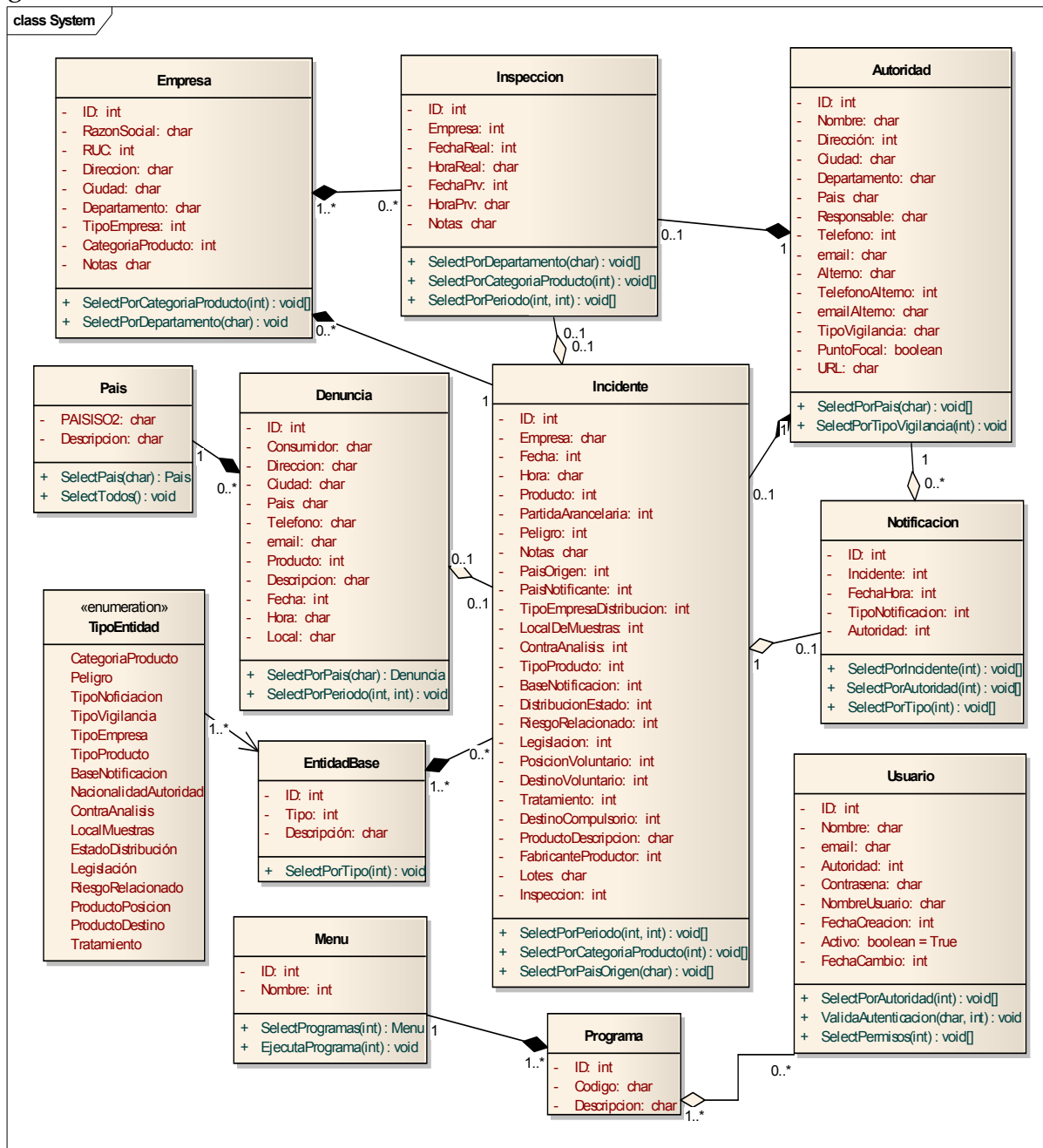


Figura 16 – Diagrama de Clases.

Empresa



## Proyecto "Etiquetado y Vigilancia del Mercado"

Representa las empresas sobre las cuales son ejecutadas las inspecciones o fue notificado un Incidente con alimentos. Si es una empresa extranjera, no debe ser definida. Esta quedará solo en el registro de incidente.

### Inspección

Permite modelar todas las acciones relacionadas con las inspecciones sobre alimentos. Aquí es posible programar y registrar los informes de inspección.

### Incidente

Estructura todos los eventos relacionados con problemas con alimentos, tanto a nivel nacional como a nivel internacional. Los incidentes a nivel nacional pueden tener varias fuentes: Frontera, Mercado, Planta, Denuncia, y pueden estar o no relacionados con una inspección.

### Notificación

Todos los incidentes detectados deben ser notificados a las demás entidades nacionales involucradas, y a los socios comunitarios si procede. En esta notificación sigue un archivo con los datos del incidente para que pueda ser importado a los sistemas de información de los demás socios de la CAN. Para permitir la trazabilidad de los incidentes, es posible enlazar las notificaciones con los respectivos incidentes. Asimismo, en las notificaciones de seguimiento se identificará la notificación anterior y se añadirá solo la información nueva.

### Autoridad

Representa todas las entidades, nacionales e internacionales, que tienen un rol, activo o pasivo, en el sistema. Las autoridades son las responsables, cada una en su rol, de programar y registrar las inspecciones, registrar los incidentes, consecuentes o no a una inspección, y emitir las notificaciones, cuando proceda, a las demás entidades involucradas y a los socios comunitarios.

### Denuncia

Caracteriza las denuncias y/o quejas efectuadas por los consumidores a través del sitio Web oficial, denominado Portal Web, que se ubicará en la SGCAN. La denuncia nunca podrá ser anónima. Asimismo, el consumidor que pretenda hacer una denuncia por esta vía deberá proveer, además de otros datos personales, un número de teléfono válido para ser contactado posteriormente.

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

### País

Representa todos los países del mundo que serán identificados por el código ISO de dos caracteres. Permitirá evaluar el origen de los incidentes, notificaciones y nacionalidad de las autoridades.

### Usuario

Caracteriza completamente todos los usuarios del sistema, su rol y accesos a los diversos programas. Existirán dos tipos de usuario que necesitarán de una cuenta para acceder al sistema (Administrador y Funcionario), y otro (Consumidor) que podrá acceder libremente sin autenticación. La diferencia entre el Administrador y el Funcionario está en los niveles de acceso predefinidos. El Administrador tendrá acceso total a todos los programas del sistema y el Funcionario tan solo a los de exploración diaria (Inspecciones, Incidentes, Notificaciones). Sin embargo, el Administrador puede atribuir a un Funcionario permisos de acceso a los demás programas. EL único programa que deberá ser accesible solo por el Administrador es el de Permisos.

### Programa

Caracteriza todos los programas del sistema. Permite adicionar fácilmente otros programas al sistema. Un programa representa un proceso en el sistema. Es una unidad funcional lógica para el usuario que le permite una facilidad de utilización muy grande.

### Menú (subclase de programa)

Permite estructurar los programas de un modo lógico facilitando el acceso a los mismos. Estarán directamente relacionados con los módulos del sistema:

- Administración
- Entidades de base
- Inspección
- Incidente

## 4.5 MODELO DE DATOS

Aquí se enseñan los modelos de datos de las dos aplicaciones que pueden funcionar de modo deslocalizado:

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"

- SINAVA – Sistema de gestión de vigilancia nacional.
  - Inspección
  - Incidente
- Portal Web Comunitario – Páginas de información, búsquedas y denuncias sobre incidentes.

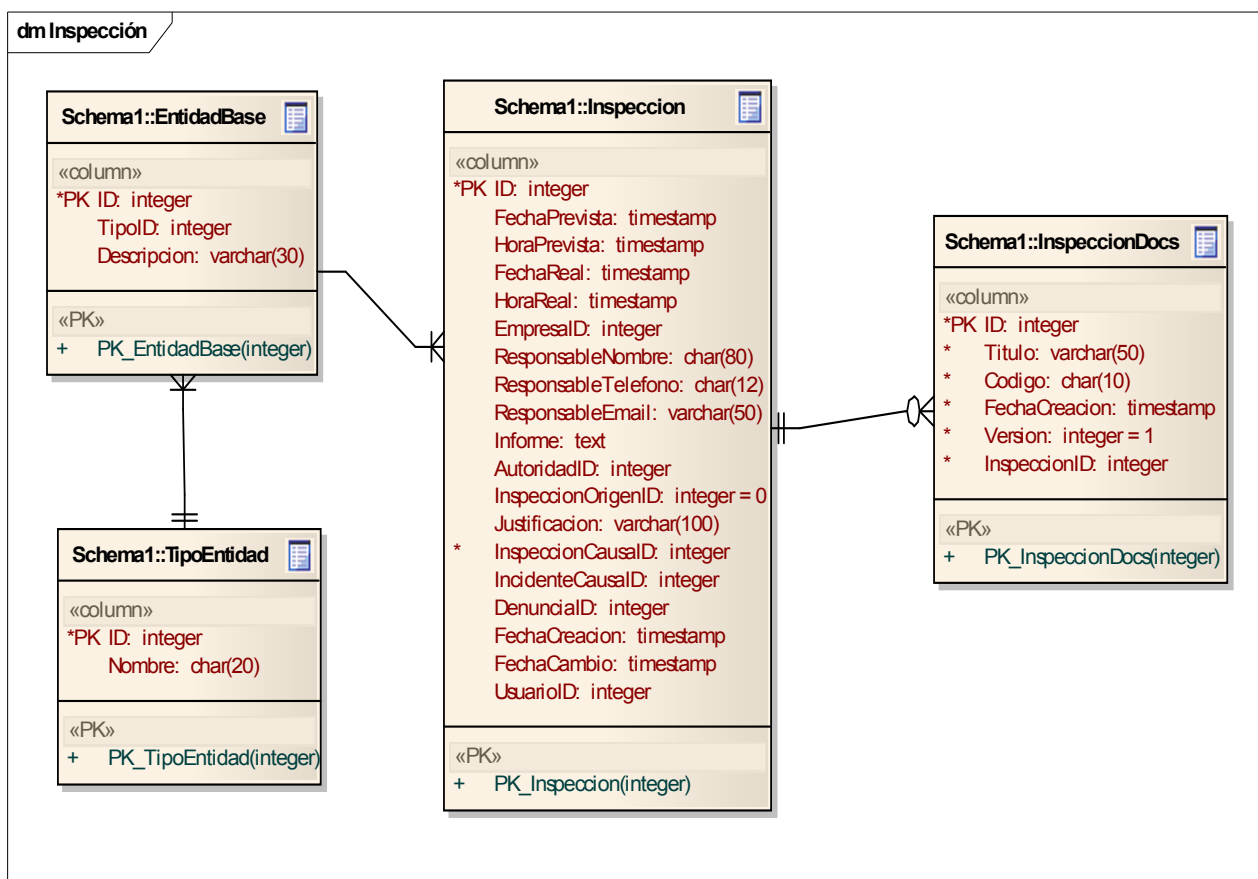


Figura 17 – Diagrama ER del módulo de Inspección.

La figura 17 enseña el modelo de datos de las tablas de soporte a las Entidades básicas del sistema y del módulo de Inspección. El módulo de Entidades de Base fue diseñado para ser flexible y escalable. La definición de estas entidades tiene como objetivo principal detallar las características de una determinada entidad del sistema. Como los sistemas son dinámicos, con el manejo del mismo y con los cambios naturales del entorno, puede ser necesario agregar otros parámetros de análisis. Con este modelo, estos parámetros pueden ser añadidos sin que sea necesario hacer cambios en la base de datos, facilitando de este modo el proceso de despliegue del software actualizado con las nuevas funcionalidades. Un nuevo parámetro es modelado como un 'Tipo de entidad' y sus instancias como 'Entidades de base'.

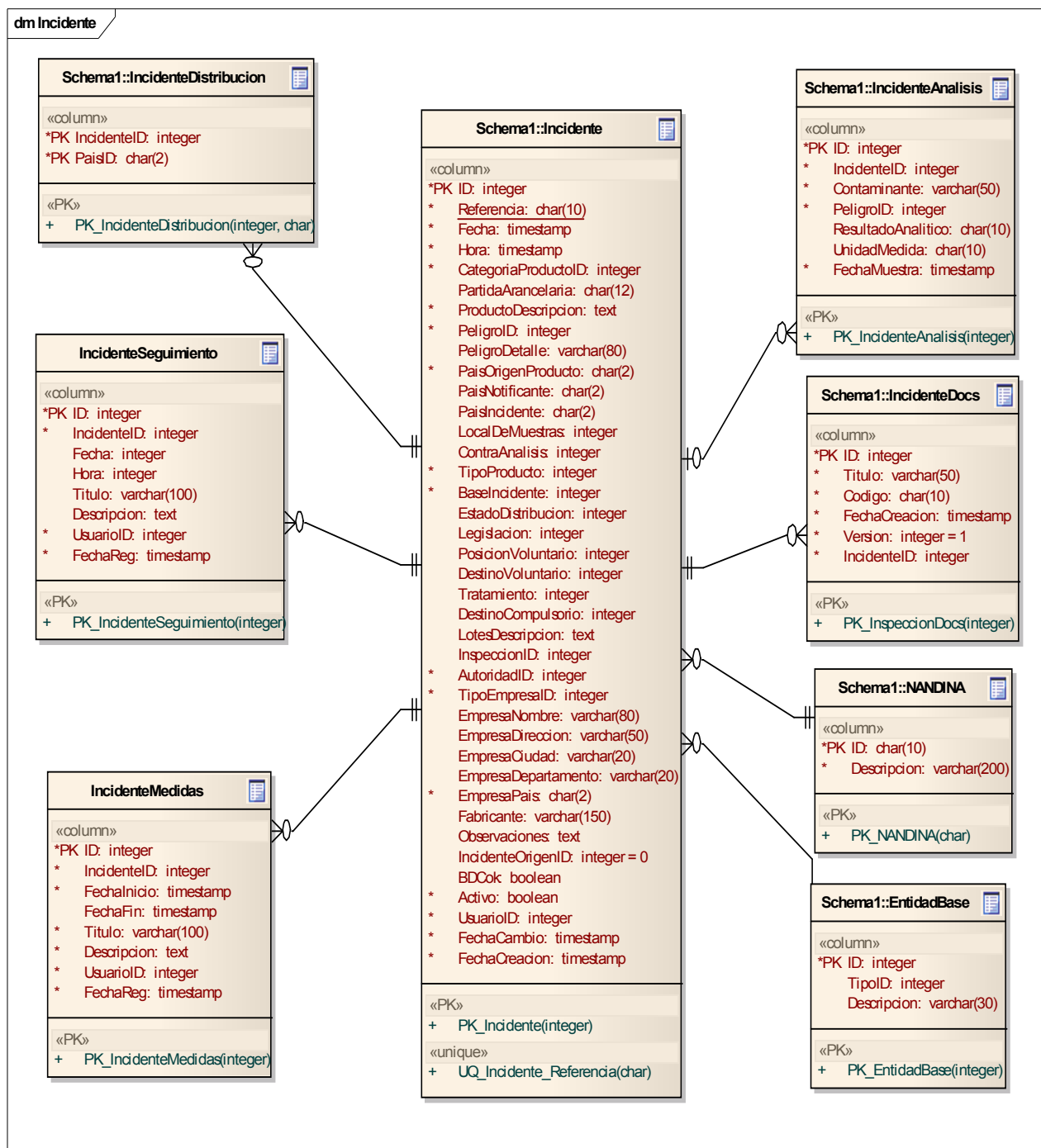


Figura 18 – Diagrama ER del módulo de Incidente.

El diagrama de la figura anterior representa el modelo de datos del módulo de registro de Incidentes. Los Incidentes pueden ser divididos en dos tipos: nacionales e internacionales. Los nacionales deben tener como origen una Inspección. A través del diagrama se puede observar que el Incidente incorpora una serie atributos modelados



## Proyecto "Etiquetado y Vigilancia del Mercado"

como entidades de base y que se debe indicar la partida arancelaria (NANDINA) del producto(s) involucrado(s). Opcionalmente, el Incidente puede también tener atributos adicionales para su mejor caracterización como:

- Documentos pertinentes a la evaluación.
- Registro de los análisis de laboratorio.
- Medidas de control adicionales a implementar para el país/producto.
- Seguimiento del incidente (descripción de ocurrencias siguientes que puedan estar conectadas con el incidente).
- Países donde el producto ha sido distribuido.

Los dos diagramas ER presentados corresponden a una misma base de datos. Su separación lógica tuvo el objetivo de aclarar el entendimiento de la estructura. Esta base de datos es la de soporte a la aplicación SINAVA. La aplicación SINAVA también incorpora el módulo de denuncias que solo está caracterizado en el diagrama del Portal Web (por se considerar que este es el medio más sencillo de efectuar una denuncia). Juntando los dos diagramas anteriores con el siguiente del Portal Web podemos construir una base de datos única para todo el SARABI. Este modelo puede ser utilizado en el caso de que se haga un sistema totalmente centralizado físicamente (situación más económica y sencilla) en la SGCAN (por ejemplo). Para el usuario, esta solución sería transparente ya que el único atributo que cambiaría sería la dirección Web (URL) de acceso a la aplicación. Esta solución ya está probada y a funcionar en la CAN con el sistema SIRT de alerta de Reglamentos Técnicos. La solución centralizada tiene dos puntos que se pueden considerar en contra:

1. La implementación necesita de una decisión de la CAN, lo que debido a la no participación de Bolivia en el proyecto puede incurrir en retrasos que otros países no quieren admitir;
2. La información del SINAVA estaría alojada en servidores extra-nacionales lo que puede no ser admisible para algunos países debido a sus estrategias de e-Gobierno.

### Portal Web Comunitario

Como se ha referenciado antes, en la figura 17 está representado el modelo centralizado del sistema, con una sola base de datos porque, efectivamente, se puede elegir esta solución. Aunque esta solución sea la que tiene los costos técnicos más bajos es la que tiene los políticos más elevados. Para la implementación de esta solución centralizada sería necesario que la CAN sacara una decisión que diera soporte legal al SARABI. Por experiencia, el consultor sabe que este proceso puede tardar tiempo que algunos países no quieren perder para proceder a la implementación del sistema de alerta rápida aquí propuesto.







## Proyecto "Etiquetado y Vigilancia del Mercado"

Para que las dos soluciones puedan ser utilizadas y los Países Miembros elegir entre una de ellas, es aquí enseñado el modelo de datos de la BDC a ser utilizado en el caso de un sistema SARABI distribuido, en que cada país tendría la base de datos completa con el modelo de la figura 17 y la SGCAN la BDC con el modelo enseñado en la figura 18.

En el modelo de la figura 18 solo están representadas las entidades necesarias al funcionamiento del Portal Web comunitario caso se opte por la solución distribuida (cada país con su base de datos del SINAVA). En este caso será necesaria una coordinación más eficiente entre los países ya que las entidades de base/técnicas son compartidas por todos los miembros de la red. Es decir, si es necesario hacer una actualización a estas entidades, todos los países se deben poner de acuerdo. En la situación centralizada esto también es válido, solo que si un país actualizaría una entidad esta se quedaba inmediatamente disponible para los demás. En el caso distribuido, como los países tienen la potestad sobre sus bases de datos, pueden crear libremente sus datos. Sin embargo, si se pretende una eficiente comunicación entre los sistemas, disminuyendo la intervención humana, es fundamental que todos los SINAVA utilicen el mismo "lenguaje", para que se pueda trasladar información automáticamente.

En el modelo centralizado, para evitar que los países crearan entidades libremente, y como estas tendrían implicaciones con sus socios, este procedimiento tendría de ser coordinado por un usuario de la SGCAN, nombrado como administrador técnico del sistema. Este usuario estaría pendiente de las resoluciones tomadas por un comité comunitario responsable por decidir sobre los aspectos funcionales del SARABI.









Proyecto "Etiquetado y Vigilancia del Mercado"

	<i>programadas.</i>
<b>Campo</b>	<b>Descripción</b>
TipoEmpresaID	Llave extranjera de la tabla EntidadBase. Las opciones están indicadas en la sección Enumerados más abajo.
CategoriaProductoID	Llave extranjera de la tabla EntidadBase. Permite indicar la categoría de alimentos con que la empresa trabaja.
Responsable	Nombre de la persona de contacto en la empresa.
Email	Correo electrónico del responsable.
Telefono	Teléfono del responsable.

<b>EntidadBase</b>	<i>Entidades de base y técnicas del sistema. Permiten una flexibilidad más grande en la definición de las instancias de los atributos necesarios para efectos estadísticos, al evitar la necesidad de programación informática.</i>
<b>Campo</b>	<b>Descripción</b>
TipoID	Llave extranjera de la tabla TipoEntidad. Identifica cada una de las entidades existentes en el sistema.
Descripción	Descripción de la entidad que será visible al usuario en las cajas de selección.

<b>Inspeccion</b>	<i>Registro de las programaciones y ejecuciones de inspección en materia de vigilancia de alimentos.</i>
<b>Campo</b>	<b>Descripción</b>
FechaPrevista	Fecha programada para la inspección.
HoraPrevista	Hora programada para la inspección.
FechaReal	Fecha real de la inspección. Puede no ser coincidente con la prevista.
Hora Real	Hora real de la inspección. También puede no ser coincidente con la prevista.
EmpresaID	Llave extranjera. Identifica la empresa que será inspeccionada.
Responsable: nombre, telefono, email	Datos de contacto de la persona responsable en la empresa por la inspección.
Informe	Texto de descripción de la inspección. Si existe un modelo predefinido se debe copiar el texto y pegarlo aquí.
UsuarioID	Último usuario que actualizó el registro de inspección en el sistema.
AutoridadID	Identificación de la autoridad que hará/hizo la inspección.
InspeccionOrigenID	Si la inspección es derivada de otra previa se debe indicar cuál para mantener la trazabilidad.
DenunciaID	Si la causa de la inspección es debida a una denuncia se debe indicar cuál.
Justificacion	Campo opcional que permite indicar los criterios que causaron la programación de la Inspección (normalmente los utilizados en el sistema de análisis de riesgo).



Proyecto "Etiquetado y Vigilancia del Mercado"

InspeccionCausaID	Entidad de base que permite caracterizar las causas de la inspección (Programación, Denuncia, Seguimiento de incidente previo, Solicitud de Registro Sanitario, Alerta internacional).
IncidenteCausaID	Si la causa de la inspección es el 'Seguimiento de incidente previo' se debe indicar aquí cuál.

<b>Autoridad</b>	<i>Ficha institucional de las autoridades, nacionales e internacionales, involucradas con el tema.</i>
<b>Campo</b>	<b>Descripción</b>
Alterno	Nombre de la persona co-responsable por el sistema en la Autoridad.
Sigla	Código abreviado del nombre de la institución que será utilizado en las consultas e informes.

<b>RolAutoridad</b>	<i>Indicación de los diversos roles que una autoridad puede poseer.</i>
<b>Campo</b>	<b>Descripción</b>
TipoVigilanciaID	Llave extranjera de la tabla EntidadBase. Una autoridad puede ejercer varios roles en el sistema en materia de vigilancia.

<b>InspeccionDocs</b>	<i>Documentos digitales conectados con la inspección.</i>
<b>Campo</b>	<b>Descripción</b>
Titulo	Título del documento que permita identificar su contenido fácilmente.
Codigo	Código del documento físico que será guardado en el sistema de archivos. Este código es atribuido automáticamente por el sistema basado en la fecha y hora para evitar duplicados. <ID inspección>+ +<código automático>
Version	Versión del documento. El sistema puede guardar varias versiones del mismo documento. La última es la que será siempre presentada al usuario. La versión es generada automáticamente cuando se elige un documento ya guardado para actualizarlo.

<b>Notificacion</b>	<i>Siempre que es registrado un incidente el usuario puede elegir enviar una notificación a las demás autoridades involucradas y a sus socios comunitarios.</i>
<b>Campo</b>	<b>Descripción</b>
TipoNotificacionID	Llave extranjera de la tabla EntidadBase. El tipo de notificación permite alertar las entidades notificadas del local del incidente y la acción a tomar.
AutoridadDestinoID	Identifica las autoridades que recibieran las notificaciones.
IncidenteID	Incidente notificado

<b>Incidente</b>	<i>Registro de todos los incidentes ocurridos con alimentos.</i>
------------------	--



Proyecto "Etiquetado y Vigilancia del Mercado"

Campo	Descripción
Fecha	Fecha del incidente
Hora	Hora del incidente
CategoriaProductoID	Categoría de Producto del alimento sobre el cuál se registró el incidente.
PartidaArancelaria	Partida de la NANDINA a 8 dígitos que permite identificar más detalladamente el producto del incidente.
ProductoDescripción	Posibilita una descripción detallada sobre el producto(s) para mejor identificación, en caso que exista una mala ubicación de la Partida Arancelaria.
PeligroID	Llave extranjera de la tabla EntidadBase. Identificación del peligro (contaminante) que constituye el incidente.
PeligroDetalle	Descripción más detallada del tipo de peligro asociado para una mejor identificación.
PaisOrigenProducto	Código del país de donde vino el producto.
PaisNotificante	Código del país que notificó el incidente (puede haber ocurrido afuera del país).
PaisDelIncidente	Código del país donde ocurrió el incidente.
TipoEmpresaDistribucionID	Identifica el ramo de actividad de la empresa responsable por el incidente.
LocalDeMuestras	Local donde fueron tomadas las muestras.
ContraAnálisis	Indica si hubo contraanálisis y de qué tipo.
TipoProducto	Alimento o material de contacto.
BaseNotificacion	Cuál fue el procedimiento que originó el incidente.
EstadoDistribucion	Pretende indicar dónde el producto ha sido distribuido el producto y principalmente si alcanzó a los consumidores para se proceder a su retiro.
Legislación	Indica si la legislación es nacional, comunitaria o internacional.
PosicionVoluntario	Posición del producto en cuanto a medidas voluntarias.
DestinoVoluntario	Destino del producto en cuanto a medidas voluntarias.
Tratamiento	Si la empresa lo elige, puede hacer un tratamiento opcional al producto para que los niveles de contaminación sean admisibles.
DestinoCompulsorio	En caso de que la empresa no asuma la responsabilidad sobre el producto las autoridades podrán tomar medidas compulsorias sobre el producto.
LotesDescripción	Detalle sobre los lotes identificados como no conformes.
Inspeccionad	Si el incidente es resultado de una inspección se debe indicar aquí cuál.
AutoridadID	Autoridad responsable por el registro del incidente.
Empresa: Nombre, Direccion, Ciudad, Departamento, País	Datos de la empresa responsable por los productos no conformes. Si el incidente es derivado de una inspección estos datos deben ser importados de la tabla <i>Empresa</i> .
Observaciones	Cualquier comentario adicional o nota que se pretenda registrar



Proyecto "Etiquetado y Vigilancia del Mercado"

	sobre el incidente que no esté en los demás campos.
IncidenteOrigenID	Si es un seguimiento, se deberá indicar cuál el incidente original.
BDCok	Indica si el incidente ha sido actualizado correctamente en la BDC

<b>IncidenteAnálisis</b>	<i>Resultados de los análisis que dan sostenibilidad al registro del incidente y su notificación.</i>
<b>Campo</b>	<b>Descripción</b>
Contaminante	Campo descriptivo de la sustancia (contaminante)
PeligroID	Llave extranjera de las entidades de base – Categoría de Peligro
ResultadoAnalítico	Valores de los niveles de contaminación que pueden ser comparados con la legislación para validar la razonabilidad del alerta.
UnidadMedida	Indica las unidades de medida utilizadas para los valores del resultado Analítico.
FechaMuestra	Fecha en que las muestras fueran tomadas.

<b>IncidenteDocs</b>	<i>Documentos conectados con el incidente. Igual que InspeccionDocs.</i>
----------------------	--

<b>IncidenteMedidas</b>	<i>Registro de los análisis de laboratorio que soportan el registro de incidente.</i>
<b>Campo</b>	<b>Descripción</b>
FechaInicio	Indicación del incidente.
FechaFin	Indicación del contaminante detectado (a elegir de la tabla de entidades de base).
Título	Causa de la medida
Descripción	Descripción detallada de las medidas a implementar.
UsuarioID	Último usuario a cambiar el registro.
FechaReg	Fecha de registro de la medida.

<b>IncidenteSeguimiento</b>	<i>Siempre que ocurre un incidente se puede hacer un seguimiento del mismo en función de su pertinencia.</i>
<b>Campo</b>	<b>Descripción</b>
Fecha	Fecha de la ocurrencia.
Hora	Hora de la ocurrencia.
Título	Título explicativo.
Descripción	Descripción más detallada.
UsuarioID	Usuario que registró la ocurrencia.
FechaReg	Fecha de registro de la ocurrencia.

<b>IncidenteDistribución</b>	<i>Países donde los productos referenciados en el incidente han sido distribuidos.</i>
<b>Campo</b>	<b>Descripción</b>
IncidenteID	Indicación del incidente.



## Proyecto "Etiquetado y Vigilancia del Mercado"

PaisID	Indicación del país.
--------	----------------------

<b>Usuario</b>	<i>Ficha personal de los usuarios no anónimos del sistema.</i>
<b>Campo</b>	<b>Descripción</b>
NombreUsuario	Palabra única que sirve como identificación del usuario en el acceso al sistema.
AutoridadID	Institución a que pertenece el usuario.
Activo	Indica si el usuario está activo, esto es, si puede acceder al sistema. Debido a la trazabilidad de usuarios no es permitido eliminar estos del sistema para mantener la integridad de los datos.

<b>Permiso</b>	<i>Define que acciones cada usuario puede realizar en cada programa.</i>
<b>Campo</b>	<b>Descripción</b>
Leer	Solo puede consultar. No puede actualizar información.
Crear	Puede crear nuevos registros en el programa.
Actualizar	Puede actualizar la información ya existente.
Eliminar	Puede eliminar registros de ese programa.

<b>Auditoria</b>	<i>Permite analizar las acciones llevadas a cabo por los usuarios en el sistema para se identificar posibles causas de errores.</i>
<b>Campo</b>	<b>Descripción</b>
FechaHora	Fecha y hora de la acción.
Accion	Identificación de la acción ejecutada por el usuario en el programa, como por ejemplo, una llamada a una función.

<b>Denuncia</b>	<i>Denuncias y quejas que pueden ser enviadas por los consumidores a través del portal Web.</i>
<b>Campo</b>	<b>Descripción</b>
NombreConsumidor	Nombre de la persona que hace la denuncia.
ProductoDescripcion	Detalle sobre el producto.
Descripcion	Descripción detallada de la ocurrencia, indicando el establecimiento donde ocurrió el incidente (o se compró el producto).
FechaCreacion	Fecha y hora del registro en el sistema (automático).

## 5 REQUERIMIENTOS DE INTERFAZ

### 5.1 INTERFACES DE HARDWARE

El sistema debe estar preparado para interactuar con distintas plataformas de hardware, de acuerdo a las necesidades del negocio. En esta materia se aconseja a los países/instituciones a que elijan tecnología abierta para que el sistema no quede “pegado” a una dada arquitectura de hardware.



## Proyecto "Etiquetado y Vigilancia del Mercado"

Hoy día, la mayoría de las arquitecturas de hardware, adecuadas a estos tipos de sistema, son interoperables porque se basan en los estándares del mercado.

### 5.2 INTERFACES DE SOFTWARE

No está prevista ninguna interacción con otras aplicaciones. El SARABI tendrá una función de exportación de datos que podrá ser aprovechada por otros sistemas a los cuales la información producida por este pueda ser útil.

### 5.3 INTERFACES DE COMUNICACIÓN

El sistema será constituido por dos aplicaciones, el SINAVA y el portal Web, siendo que el SINAVA tendrá varias instancias. Tantas cuantas los países que harán parte de la red. Existirán comunicaciones entre la base de datos del SINAVA y la base de datos central (consolidada) y entre las bases de datos de cada instancia del SINAVA. La primera de modo automático (servicios Web), la segunda en modo interactivo (usuario).

## 6 RESTRICCIONES DE DISEÑO

En este capítulo tan solo se abarcará la tecnología necesaria a nivel de servidores ya que para los equipos clientes solo se exigirá la existencia de un browser (navegador Web) relativamente actualizado: Internet Explorer 6, Firefox 2, Safari, Opera, Chrome. Exceptuando el Internet Explorer, los demás son gratuitos por lo que no constituye un problema.

En los puntos siguientes se indican las diversas tecnologías existentes y son indicadas aquellas que el consultor considera que corresponden a las necesidades del presente sistema. Cualquiera de las opciones permitirá alcanzar un buen resultado. Sin embargo, el consultor considera que debe transmitir su opinión, basada en su experiencia y en el conocimiento detallado del entorno específico de los países donde se hará la implementación, aunque esta no se constituya como una restricción a la utilización de cualquier otra tecnología. Asimismo, se propone utilizar una tecnología totalmente asiente en herramientas Microsoft:

Sistema operativo:	Windows Server 2003
Entorno de desarrollo:	Visual Studio 2008
Lenguaje de programación:	ASP.NET
Framework .NET	3.5
Servidor Web:	IIS 6.0
SMBD:	SQL Server 2005

Las versiones de las diversas herramientas presentadas son consideradas las mínimas.

La decisión se basa en las siguientes características:





## Proyecto "Etiquetado y Vigilancia del Mercado"

1. Aunque el sistema operativo exija licenciamiento, su costo es relativamente bajo.
2. Es el sistema operativo más utilizado en los países (95% del mercado) y por eso existen más técnicos cualificados y, consecuentemente, con costos más bajos.
3. Es de muy fácil manejo, por lo que no exige técnicos superiores para ejecutar tareas básicas como copias de seguridad, configuración de periféricos y otras tareas de administración.
4. El entorno de desarrollo Visual Studio 2008 es el más productivo de todos y tiene funciones que optimizan la programación de la persistencia de datos cuando se utiliza específicamente el SMBD SQL Server y, además, tiene versiones gratuitas (el Express).
5. El lenguaje ASP.NET tiene una comunidad de desarrolladores muy vasta en la región, muy buenos sitios Web de ayuda, y muchos objetos preconstruidos que posibilitan una grande productividad en la programación.
6. El servidor Web IIS es muy fácil de configurar y garantiza los niveles de seguridad necesarios a este tipo de aplicación.

### 6.1 ESTRATEGIA INSTITUCIONAL

La primera decisión en la implementación de cualquier sistema informático es la tecnología que está directamente conectada con la opción a nivel más macro de los sistemas utilizados a nivel institucional (o mismo gubernamental). Aquí tenemos dos opciones: sistemas propietarios con costos de licencia de utilización, y sistemas de código abierto, sin licenciamiento pero, que pueden tener costos de mantenimiento.

Para el tipo de sistema que se está diseñando, no siendo de carácter crítico en términos de disponibilidad y seguridad de información, existen muy buenas opciones en los dos tipos de tecnología.

### 6.2 SISTEMA OPERATIVO

En función de la estrategia tecnológica elegida se puede restringir inmediatamente el sistema operativo. Si la opción es por Código Abierto solo hay un sistema posible – Linux (dentro de este existen varias opciones). Si es por una solución propietaria, se puede elegir entre los varios Unix y Ms-Windows Server.

### 6.3 LENGUAJES DE SOFTWARE

Para un sistema como el planteado se aconseja a elegir entre 3 lenguajes (versiones mínimas indicadas):

- PHP 5.3
- Java – Jdk 1.5
- ASP.NET 2.0

La estructura de las aplicaciones debe ser modular y utilizar dos capas de software: Interfaz con el usuario y persistencia de datos. En aplicaciones más grandes, distribuidas y complejas, se



## Proyecto "Etiquetado y Vigilancia del Mercado"

aconseja la existencia de una tercera capa con las reglas de negocio que garantiza más flexibilidad en la escalabilidad del negocio. En el SARABI esta capa no se justifica porque, además de su pequeña dimensión, disminuiría la respuesta del sistema (el sistema queda más lento).

### 6.4 BASE DE DATOS

En función del lenguaje elegido también pueden existir más ventajas en utilizar un sistema manejador de base de datos (SMBD) u otro, debido a las ofertas existentes en el mercado en términos de plataformas de programación informática:

- Para el PHP el SMBD más adecuado sería el MySQL. Hay varios productos en el mercado que garantizan una buena productividad de desarrollo. Sin embargo, estos productos pueden ya no ser tan productivos en la fase de mantenimiento caso sea necesario hacer cambios profundos en el código de los programas.
- Para el Java existen muchas opciones (Eclipse, NetBeans, etc.) y su portabilidad le permite ser utilizado con cualquier SMBD, pero la suite de Oracle es la que garantiza una mayor productividad.
- El ASP.NET, a través del IDE Visual Studio .NET 2010, saca más provecho del Ms-SQL Server.

Como nota final, se realza de nuevo que la opción por la tecnología se debe basar en una estrategia más amplia de la institución o gobierno. Las notas aquí planteadas por el consultor solo pretenden ayudar en la elección de la misma en caso de dudas. Por otro lado, y como el SARABI es un sistema comunitario, los países tendrían ventajas si eligen la misma tecnología pues eso podría permitir una implementación común lo que disminuiría bastante el tiempo y el costo de la misma, además de se aprovechar la experiencia mutua de los usuarios y técnicos de informática.

## 7 REQUERIMIENTOS DE LICENCIA

Para la implementación del sistema segundo el diseño propuesto en este documento no requiere la adquisición de licencias, además de las del sistema operativo (si la decisión caer sobre un sistema propietario, como el Microsoft Windows o Solaris) y de otro “middleware” eventualmente necesario para ampliar las características de seguridad y backup.

Si la opción es la de utilizar las herramientas de desarrollo y de manejo de base de datos de Microsoft (como sugerido), las versiones disponibles gratuitamente son suficientes para un desarrollo y mantenimiento productivo y de calidad.

Las bases de esta consultoría están orientadas para una implementación comunitaria del sistema aquí diseñado que sería coordinado por la SGCAN. La visión del consultor es que este es el camino más ventajoso para todos los países. Sin embargo, la propuesta de diseño aquí planteada puede ser aprovechada por los países para implementaciones a nivel nacional, en el caso de que no se alcancen acuerdos a nivel comunitario.

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"





## Proyecto "Etiquetado y Vigilancia del Mercado"

Un punto importante a tener en cuenta es que los países tendrán todas las ventajas en que la aplicación desarrollada también tenga un mantenimiento compartido. Es decir, todos los cambios posteriores a la fase de implementación, deberán ser acordados entre los socios de la red. La idea subyacente a este proyecto es que se consiga dar continuidad a este diseño en otro proyecto de cooperación a nivel regional de la CAN. Asimismo, la propiedad de las fuentes sería de la SGCAN, pudiendo los países utilizar los mismos libremente. Sin embargo, para sacar el máximo de provecho del sistema con el mínimo costo, sería conveniente que los eventuales cambios que los países puedan necesitar, derivados de su utilización, fueran concertados con todos los socios. De otro modo, el sistema se fragmentará inevitablemente en tantas aplicaciones cuantos los Países Miembros de la red.

## 8 ARQUITECTURA

### 8.1 RED

El SARABI será una red informática que constituya un sistema de aplicaciones de gestión de vigilancia de alimentos distribuidas. Cada país que hará parte de la red SARABI necesitará de por lo menos dos servidores (uno de aplicaciones/Web y otro de base de datos) que servirán de soporte a la aplicación SINAVA y su respectiva base de datos nacional.

Se prevé que la comunicación entre las diversas aplicaciones se haga por Internet, utilizando servicios Web y correo electrónico. La comunicación se basa tan solo en la información sobre el alerta de incidente.

Al nivel nacional, se prevé que las distintas autoridades de vigilancia tengan sus direcciones regionales también a funcionar con el sistema SINAVA y también a través de la Internet (podría ser a través de una VPN). En este caso se sugiere la utilización de SSL (https) para las comunicaciones al servidor Web, para encriptación de los datos transmitidos por la red pública (Internet).



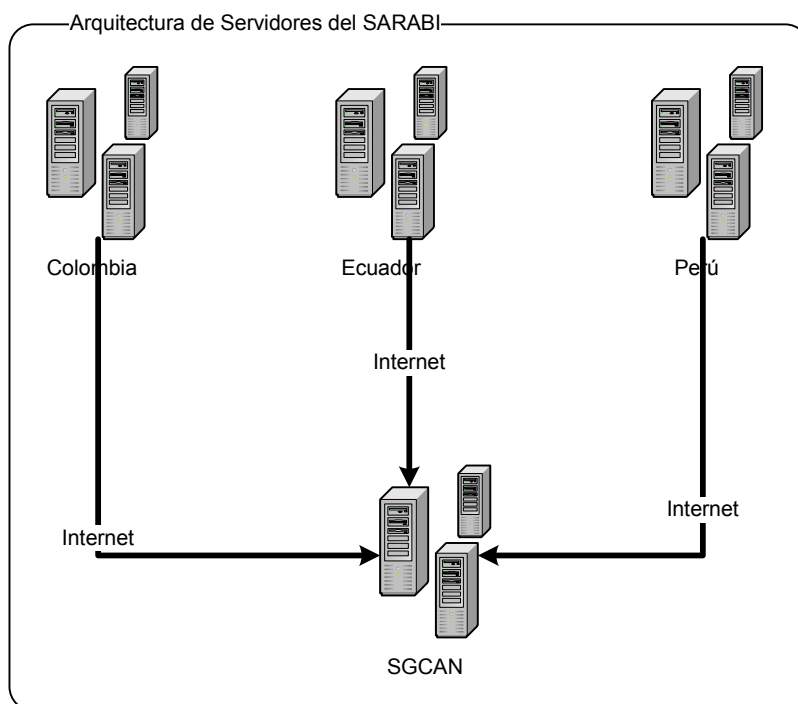


Figura 20 – Modelo de interconexiones entre los diversos servidores que harán parte del SARABI. Todos los países que fueren ingresando (como Bolivia por ejemplo) a la red tendrán la misma configuración.

## 8.2 APLICACIONES

La aplicación SINAVA es donde las autoridades nacionales gestionaran sus actividades de vigilancia de alimentos. Programaran y registraran sus inspecciones, los incidentes con alimentos, enviarán alertas a sus socios de la red y sacaran estadísticas operativas. Solo podrán acceder a esta aplicación usuarios autorizados. Aunque la aplicación sea igual para todos los países, cada uno tendrá total independencia en su manejo y gestión. Salvaguardando la interoperabilidad con la base de datos central (BDC) a existir en la SGCAN donde se podrán elaborar estadísticas consolidadas comunitarias. Para esto, y para que los países puedan cargar automáticamente a sus bases de datos la información de las alertas enviadas por sus socios, las Entidades de base deberán ser comunes a todos. Los países deben consensuar un catálogo donde estén referenciadas todas las instancias de las entidades de base a utilizar en el SARABI y después definirlas en sus sistemas nacionales. La ventaja de utilizar la BDC es que se podría definir estas entidades a nivel central y después los países las importaban automáticamente a sus bases de datos nacionales. Cualquier necesidad de adición o cambio de una de estas entidades por parte de uno de los países debe ser comunicado a los demás socios de la red, y también consensuado. Sin embargo, esto tipo de entidades, después de consensuados inicialmente (como ya están propuestas en este documento), tienen una probabilidad muy baja de necesitar de algún cambio. Lo más probable es que 99% de ellas se mantengan inalterables por varios años.

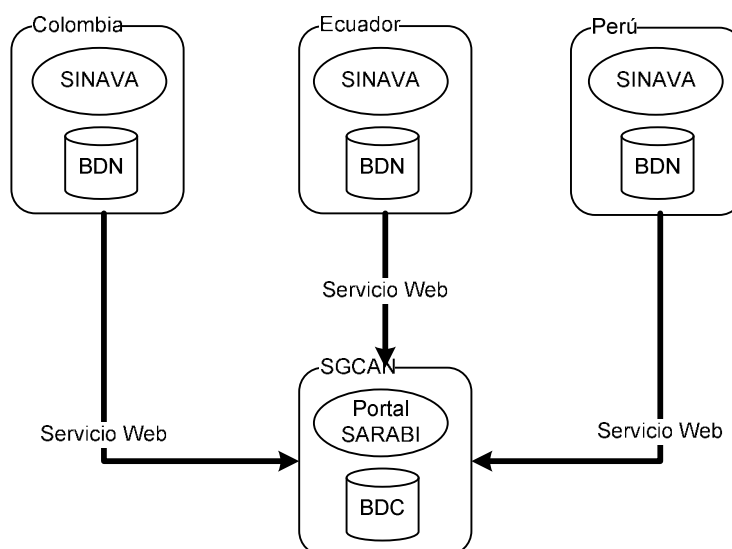


Figura 21 – Arquitectura conceptual de aplicaciones del SARABI.

En la figura 21 se puede observar que el SARABI es constituido por dos aplicaciones (SINAVA y Portal SARABI) y por dos estructuras de bases de datos distintas (BDN – Base de Datos Nacional y BDC – Base de datos central). Existirán tantas BDN cuantos los países que participaren en la red y cada uno de los países, tendrá de exportar sus datos a la BDC que existirá en la SGCAN, sobre la cual el Portal Web del SARABI trabajará.

### 8.3 SERVICIOS WEB

Del SINAVA hará parte también un Servicio Web que será responsable por trasladar la información nacional a la base de datos común a existir en la SGCAN. Este servicio Web llamará otro disponible en el servidor de la SGCAN que será el responsable por la actualización de la información en la BDC. Para garantizar la actualización de los datos (que las tablas de incidentes de las dos bases de datos están sincronizadas) existirán mecanismos de los dos lados que indicarán si una transacción ha finalizado con éxito.

Flujo del proceso de actualización de la BDC:

1. El SINAVA actualiza la BDN
2. Llama el WS local EnvíaDatosBDC que envía los datos referenciados en el archivo XML, y a su vez llamará el WS ActualizaDatosBDC, localizado en el servidor Web central, el cuál recibe como parámetros los campos indicados en el archivo XML del punto 8.7, y envía de vuelta al WS EnvíaDatosBDC la indicación del estado de ejecución de la transacción a través de un atributo booleano TRANSOK;
3. El WS ActualizaDatosBDC controla la existencia de errores en la actualización de datos en la BDC;



## Proyecto "Etiquetado y Vigilancia del Mercado"

4. Caso exista un error, el WS ActualizaDatosBDC actualiza el atributo TRANSOK = FALSE. Caso contrario lo envía como TRUE.
5. El WS EnviaDatosBDC cuando recibe el parámetro TRANSOK actualiza el campo correspondiente (BDCok) en la tabla Incidente con su valor.
6. Todos los registros con el atributo BDCok = FALSE en la tabla de Incidente serán sacados nuevamente por un programa ejecutado automáticamente y periódicamente (todos los días en la madrugada – 1h00, por ejemplo) que llama el WS EnviaDatosBDC e inicia nuevamente el proceso de actualización.
7. Adicionalmente existirá un log que grabará los errores ocurridos en el sistema (tanto a nivel del SINAVA como del Portal Web) para mejor identificar sus causas.

Los usuarios del sistema, después de enviar una notificación deberán confirmar enseguida si la BDC ha sido actualizada, haciendo una búsqueda en el portal Web, para se identificar más rápidamente algún tipo de error que pueda estar surgiendo. Muchas veces los errores son debidos a cambios en las políticas de seguridad de los servidores y routers y no a las aplicaciones.

### 8.4 CONTEXTO DEL NEGOCIO

#### Estrategia

Las autoridades de vigilancia y asociaciones de consumidores de los Países Miembros de la CAN han subrayado la necesidad de implementar un sistema de alerta rápida para alimentos y bebidas industrializados a nivel comunitario, similar al Sistema RASFF existente en Europa pero adaptado a las necesidades específicas de la subregión.

Se hizo una gira por los países participantes en este proyecto FAT entre finales de Abril e inicio de Mayo, donde, además de capacitar y promover el concepto de vigilancia de alimentos en talleres especializados, se analizó el estado actual de la actividad de vigilancia de alimentos en cada uno de los países y se entrevistó a las partes involucradas con el tema (públicas, privadas y beneficiarios).

Del análisis efectuado se concluyó que además de un sistema comunitario de alerta rápida, los países necesitaban, y requerían, un sistema nacional que les permitiera reaccionar rápidamente y efectuar la trazabilidad completa de los incidentes. Asimismo, el sistema propuesto tiene una arquitectura distribuida donde cada país tendrá la propiedad de sus sistemas de vigilancia y alerta rápida pero, con la obligación de cumplir con el traslado de los datos a la base de datos común que será propiedad de la SGCAN. Para esto, los estándares de comunicación de datos, aquí definidos, solo podrán ser cambiados con el acuerdo de todos los países participantes de la red de alerta.

El sistema propuesto necesita de medidas de validación comunitarias para garantizar la calidad y la integridad de las notificaciones emitidas por los Países Miembros para evitar que los consumidores tengan acceso, a través de la búsqueda en la página Web comunitaria, a informaciones equivocadas o fuera de contexto. Esto sería una tarea apropiada a un comité que pudiera existir a nivel central en la SGCAN. Sin embargo, no es una condición necesaria al funcionamiento del





## Proyecto "Etiquetado y Vigilancia del Mercado"

sistema. Es mejor tener un sistema con algunos desperfectos (que se conocen y se sabe que se pueden ir solucionando) do que no tener ninguno. Pero, es necesario poner en la página Web de búsqueda de notificaciones un mensaje para alertar los consumidores de este hecho. Algunas de las situaciones que pueden acontecer por falta de esta validación central son las siguientes:

- Información imprecisa.
- Insuficiente evidencia de riesgo directo o indirecto para la salud del consumidor.
- Niveles encontrados debajo del límite permitido.
- Los niveles no suponen un riesgo para la salud pública.
- La notificación no contiene información suficiente para una evaluación apropiada.
- La notificación no está actualizada.
- La notificación está fuera del ámbito del SARABI.
- Los límites legales indicados no se aplican a los niveles indicados.
- Los resultados analíticos obtenidos son inválidos.

El problema puede ser más grave si es una notificación de un país miembro sobre un alimento importado de otro país miembro. No existiendo un procedimiento definido para arbitrar el incidente, puede ser más complicado solucionarlo.

Todo esto sería más fácil de analizar y solucionar si la legislación sobre alimentos estuviera armonizada entre los Países Miembros.

La propuesta de diseño puede ser implementada a nivel nacional por los países en una primera fase y después a nivel comunitario, con los debidos acuerdos, sin necesidad de cambio en el software.

### Beneficiarios

Los beneficiarios directos del sistema serán las autoridades nacionales y comunitarias (comité de la CAN responsable por inocuidad de los alimentos) responsables por la vigilancia de alimentos y, como consecuencia de una vigilancia más efectiva, los consumidores.

Indirectamente tendremos las autoridades reguladoras que pasarán a disponer de una base de datos de incidentes con alimentos que podrá ser utilizada para mejor adaptar los reglamentos a la realidad, contribuyendo para mejorar también la seguridad de los alimentos. Los funcionarios de las autoridades de vigilancia podrán ser considerados beneficiarios indirectos ya que con el sistema en funcionamiento tendrán los procesos más organizados y las responsabilidades más aclaradas, ya que todas las actividades relacionadas estarán definidas por rol y sus instancias deberán estar registradas, siendo posible efectuar la trazabilidad de cada proceso.

### Topología

En términos de hardware, para cada aplicación y para cada país, será necesario un servidor Web/aplicaciones y otro de base de datos. Cada una de las aplicaciones debe ser desarrollada teniendo en cuenta que todos los comandos SQL deberán estar definidos en el propio motor de

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

base de datos (sistema manejador de base de datos SMBD), utilizando los “Stored-procedures” y “Triggers” existentes en el SMBD. Este tipo de arquitectura, además de aumentar el desempeño provee una flexibilidad más grande al sistema. Por otro lado, si es necesario corregir algún comando de SQL u optimizarlo (con el crecimiento de la información tornase necesario) no es necesario cambiar el código fuente de la aplicación y, como tal, tampoco compilar, ampliando así también la productividad del mantenimiento.

### Servidores

El sistema SARABI, si es instalado en todos los Países Miembros, necesitará, como mínimo aconsejable, de dos servidores por país participante de la red más dos en la SGCAN, donde uno funcionará como servidor Web y de aplicaciones y otro como servidor de base de datos. De este modo se garantiza un más elevado nivel de seguridad a la información ya que el servidor de base de datos no estará expuesto a la Internet.

### Distribución de las aplicaciones en los servidores

El SARABI será constituido por dos aplicaciones Web. Una para gestión de las actividades de vigilancia, a ser manejada y mantenida por los países que se adherirán a la red, y otra que funcionará sobre la base de datos común, permitirá hacer consultas sobre la información consolidada, y que estaría instalada en los servidores de la SGCAN. Esta última aplicación en una primera fase podría ser solo para efectuar consultas públicas y denuncias, disponible a los consumidores.

## 8.5 ENTIDADES DEL NEGOCIO

Las entidades que estarán involucradas con el sistema se pueden distinguir entre las siguientes:

- Entidades reguladoras;
- Entidades de vigilancia en frontera;
- Entidades de vigilancia en el mercado;
- Entidades de vigilancia en las plantas de fabricación;
- Consumidores.

Las entidades reguladoras también podrán tener competencias de vigilancia. De otro modo, su rol en el sistema sería tan solo de consulta de incidentes y estadísticas.

También podrá existir una sola entidad con todas las competencias de vigilancia. Asimismo, el sistema debe permitir hacer la conexión entre la entidad y el rol en términos de vigilancia.

Las entidades mencionadas arriba son las llamadas Actores del sistema. Sus usuarios se clasificarán del siguiente modo y rol:

### *Actores*

- Gerente



## Proyecto "Etiquetado y Vigilancia del Mercado"

- Funcionario
- Consumidor

Y podrán ejecutar los siguientes macro-procesos:

- Definición de entidades de base del sistema
- Registro y mantenimiento de incidentes
- Notificación de incidente a las demás autoridades nacionales
- Notificación de incidente a las autoridades de terceros países
- Registro y mantenimiento de inspecciones
- Registro de denuncias
- Búsqueda publica de alertas

### *Entidades Técnicas/Base del sistema*

- Categoría de productos
- Partida arancelaria (NANDINA a 8 dígitos)
- Peligro asociado
- País origen del incidente
- País donde el producto ha sido distribuido
- País que notificó
- Tipo de producto (Alimento, Material de contacto)
- Clasificación de la notificación (Alerta, Rechazo, Información, Noticia)
- Base de notificación (Rechazo, Queja de consumidor, Envenenamiento, Control oficial, etc.). Ver RASFF
- Usuario
- Autoridad
- Tipo de autoridad (Mercado, frontera, planta)
- Nacionalidad de la autoridad (Nacional, Extranjera, Comunitaria)
- Causa de la inspección
- Medio de denuncia

### *Descripción de las instancias de las entidades técnicas/base*

#### Tipo de producto

- Alimento
- Material de contacto con alimento

#### Base para la notificación

- Control oficial en el mercado

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"





## Proyecto "Etiquetado y Vigilancia del Mercado"

- Control efectuado a seguir a una notificación internacional
- Control efectuado a seguir a una notificación SARABI
- Brote de envenenamiento por comida
- Autocontrol de una empresa
- Queja de un consumidor

### Categoría del peligro

- Micro-organismos patogénicos (potencialmente)
- Adulteración
- Alérgenos
- Malo o insuficiente control
- Biocontaminantes (otros)
- Biotoxinas (otros)
- Contaminación química (otro)
- Composición
- Aditivos alimentarios
- Cuerpos raros
- OMG / Alimentos nuevos
- Metales pesados
- Contaminantes industriales (otros)
- Etiquetado inexistente/incompleto/incorrecto
- Migración
- Micotoxinas
- Aspectos organolépticos
- Envase defectuoso / incorrecto
- Infestación de parásito
- Residuos de pesticidas
- Radiación
- TSEs (Encefalopatía Espongiforme Transmisible)

Las instancias que tienen la indicación de '(otros)' significa que es necesario agregar más información en el campo 'Otros/Descripción de peligro' del formulario. Atributo 'PeligroDetalle' de la tabla Incidente.

### Contra análisis

- Ninguna
- En curso
- Confirmada
- No confirmada

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"





## Proyecto "Etiquetado y Vigilancia del Mercado"

### Local de las Muestras

- Despachante
- Detallista
- Minorista
- Mayorista
- Importador
- Fabricante
- Punto de entrada
- Productor

### Categoría de producto

- Bebidas alcohólicas (no vino)
- Moluscos bivalvos y productos relacionados
- Cefalópodos y productos relacionados
- Cereales y productos de panadería
- Cacao, cacao preparado, café y té
- Productos de confitería
- Crustáceos y productos relacionados
- Alimentos dietéticos, fortificados y suplementos alimentarios
- Aceites y grasas
- Pescado y productos relacionados
- Materiales de contacto con alimentos
- Frutas y vegetales
- Hierbas y especias
- Miel y mermeladas
- Carnes y productos cárnicos (no pollo)
- Leche y lácteos
- Bebidas no alcohólicas
- Nueces, productos derivados y semillas
- Pollo y derivados
- Platos preparados y aperitivos
- Sopas, caldos y salsas

### Relación del producto con el producto notificado previamente en una notificación enlazada

- Lotes adicionales
- Variedad distinta
- Ingrediente
- Producto procesado
- Insumo

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDALUZA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

### *Riesgo / Medidas*

#### Estado de la Distribución

- Distribución en el mercado (posible)
- Distribución restringida al país notificante
- Información sobre distribución no disponible (todavía)
- Sin distribución
- Sin stock
- Producto ya consumido
- Fecha de mejor consumo ultrapasada
- Fecha de utilización ultrapasada

#### Legislación

- Nacional
- Comunitaria (CAN)
- Estándar internacional

#### Medidas voluntarias

Posición (Producto a ser):

- Retirado de los consumidores
- Reenviado al despachante
- Sacado del mercado

Destino (Producto a ser):

- Destruído
- Re-etiquetado

Tratamiento físico:

- Tratamiento con ácido
- Blanqueamiento
- Congelación
- Tratamiento por calor
- Clasificado

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDALUZA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

### Medidas compulsorias

Destino (Producto a ser):

- Destruído
- Retenido
- Incautado
- Re-etiquetado

### Trazabilidad

Unidad de medida

- Unidad
- Kg
- Ton
- l
- m3

### País

(Importar tabla ISO-2 de países)

### Tipo de empresa

- Exportador
- Fabricante
- Productor
- Intermediario / Distribuidor

### Distribución

#### Empresa

- Fabricante
- Productor

#### Tipo empresa distribución:

- Despachante
- Importador
- Minorista
- Mayorista

### Causa de inspección

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

- Programación basada en análisis de riesgo
- Programación basada en la solicitud de Registro Sanitario
- Denuncia de consumidor
- Alerta internacional
- Seguimiento de Incidente previo

### Medio de denuncia

- Web
- Sobre
- Teléfono
- Presencial
- Fax

## 8.6 INTEROPERABILIDAD DE LAS APLICACIONES

El SARABI es constituido por la aplicación SINAVA (multiplicada por el número de países de la red) y por el portal Web comunitario. Como es un sistema distribuido, es necesario trasladar información entre las diversas aplicaciones de un modo rápido, eficaz y que garantice la integridad de los datos.

La información que es necesario pasar entre los sistemas es la que se refiere a las alertas de incidentes con alimentos. Para esto se propone dos métodos, uno interactivo, en que el usuario elige importar/exportar la información, y otro automático.

### **Interactivo**

El método interactivo es utilizado en las notificaciones internacionales a los socios comunitarios. Esto porque cada país tiene la potestad para elegir en cargar o no a sus sistemas la alerta recibida. Esta podrá no tener interés por diversos motivos, como la no comercialización del producto en el mercado nacional.

En este caso el usuario del país notificante, al elegir enviar la alerta, su SINAVA nacional genera un archivo XML y lo anexa automáticamente al correo electrónico de la alerta. El usuario del país que recibe la alerta, si cree pertinente, elige en su SINAVA la opción de 'Importar alerta' y selecciona el archivo añadido al correo electrónico.

En el esquema de la figura 22 los círculos representan procesos automáticos realizados por el sistema sin intervención del usuario, y los formularios procesos interactivos realizados por un usuario.



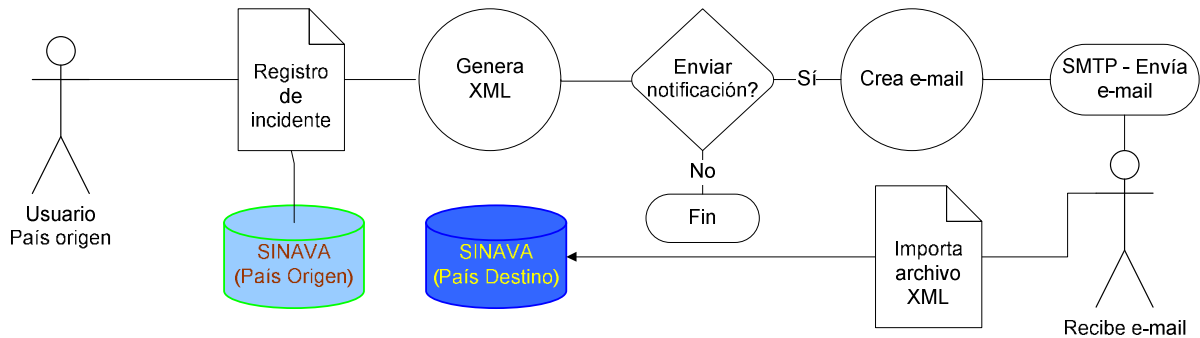


Figura 22 – Flujo de datos en la actualización interactiva.

### Automático

Este método utiliza servicios Web para trasladar la información entre los diversos SINAVAs y la base de datos central la que servirá de soporte de información al portal Web. Se pretende que la información sea trasladada en tiempo real, asimismo, existirá un WS en el SINAVA que llamará (enviará la información de la alerta) otro WS en el portal que, a su vez, actualizará la información en la base de datos central. Para garantizar la integridad de la transacción, esta solo terminará después de que el WS del portal conteste que ya procedió correctamente a la actualización.

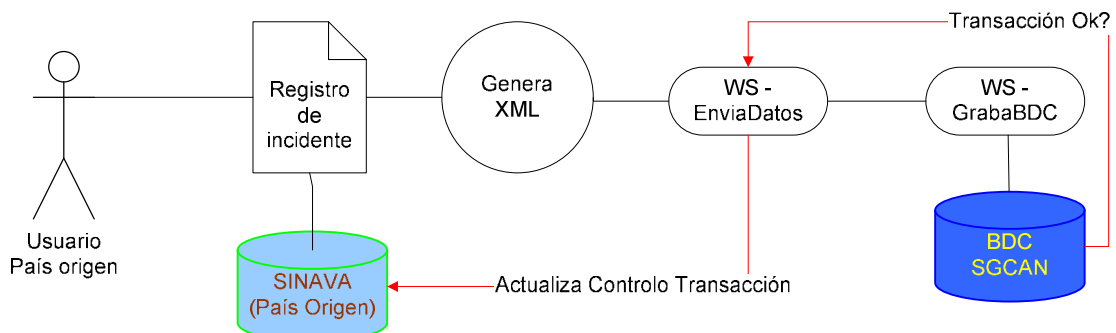


Figura 23 – Secuencia de acciones en el proceso de actualización de la base de datos central.

## 8.7 FORMATO DEL ARCHIVO XML CON LOS DATOS DEL INCIDENTE

```
<Document>
  <Row>
    <Titulo></Titulo>
    <FechaIncidente></FechaIncidente>
    <CategoriaProducto></CategoriaProducto>
    <ProdcutoDescripcion></ProdcutoDescripcion>
    <Partida></Partida>
    <Peligro></Peligro>
    <PaisOrigen></PaisOrigen>
```



## Proyecto "Etiquetado y Vigilancia del Mercado"

```
<PaisNotificante></PaisNotificante>
<PaisIncidente></PaisIncidente>
<LocalMuestras></LocalMuestras>
<ContraAnálisis></ContraAnálisis>
<TipoProducto></TipoProducto>
<BaseIncidente></BaseIncidente>
<EstadoDistribucion></EstadoDistribucion>
<Legislacion></Legislacion>
<PosicionVoluntario></PosicionVoluntario>
<DestinoVoluntario></DestinoVoluntario>
<Tratamiento></Tratamiento>
<DestinoCompulsorio></DestinoCompulsorio>
<LotesDescripcion></LotesDescripcion>
<EmpresaNombre></EmpresaNombre>
<EmpresaDireccion></EmpresaDireccion>
<EmpresaCiudad></EmpresaCiudad>
<EmpresaDepartamento></EmpresaDepartamento>
<EmpresaPais></EmpresaPais>
<Observaciones></Observaciones>
</Row>
</Document>
```

El tipo y tamaño de los campos está definido en el modelo de datos en la tabla incidente.

El programa de importación de este archivo debe añadir los restantes atributos necesarios a la tabla 'Incidente'. Atribuir un ID local, asociar la autoridad del usuario que está ejecutando la operación, y las fechas de trazabilidad. Se asume que esta importación es ejecutada por la autoridad nombrada como Punto Focal (de contacto) del sistema SARABI.

### 8.8 INTEGRACIÓN Y ARMONIZACIÓN DE LAS ENTIDADES DE BASE

Para que los sistemas puedan trasladar información entre sí de un modo automático o semi-automático es necesario que manejen las mismas entidades de base, para que los códigos pasados de un sistema al de otro país tengan el mismo significado. Esto exige un poco de coordinación entre los países y la SGCAN. En la primera versión, las instancias de las entidades son las que se plantean en este documento. Estas instancias fueron basadas en la experiencia europea en la materia, que ya lleva 30 (treinta) años, y por eso tienen la sostenibilidad de una grande experiencia en su manejo. Asimismo, no es previsible que estas entidades necesiten de permanentes actualizaciones lo que tornaría el proceso más pesado de coordinar. Los eventuales cambios serán puntuales y no se prevé que su aprobación por los diversos miembros de la red sea demorada o mismo complicada.

Esta armonización de entidades puede ser efectuada de dos maneras:

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

1. Los países aprueban los cambios, la codificación y después cada uno tiene la responsabilidad de actualizar la información en sus bases de datos nacionales.
2. Después de la aprobación de los cambios o actualizaciones la SGCAN actualiza la base de datos central y los sistemas nacionales de los países son actualizados a través de servicios Web.

Cualquiera de los procesos puede funcionar pero, el primero, debido a que la actualización se multiplica por el número de países, la probabilidad de existencia de errores de integridad también es incrementada. Asimismo, el primero tiene la ventaja de no necesitar de intervención por parte de la SGCAN, y el segundo tiene la ventaja de garantizar la integridad de los datos y la perfecta armonización de las entidades en los sistemas nacionales.

## 9 SEGURIDAD Y BACKUP

### 9.1 SEGURIDAD

#### Ataques a la información

Podemos clasificar los inconvenientes a nivel de seguridad en el siguiente modo:

1. Acceso a información no autorizada;
2. Cambio de información, lo que puede generar inconvenientes a los afectados;
3. Daño a la integridad de los datos;
4. Daño al software aplicativo y de base, lo que puede generar la falla del sistema y el envío de información no autorizada (normalmente causada por virus);
5. Sobrecarga de los sistemas que imposibilitan su operación ("Denial of Service");
6. Falsa identidad. El usuario no es quien dice ser.

Hay varios métodos de ataque para cada uno de los inconvenientes listados y hay también varios niveles de protección para cada uno. Hoy, la mayoría de los ataques exitosos se deben a la ingenuidad de los usuarios y a la displicencia en la configuración de la política de seguridad en las instituciones.

Es un hecho que la mayor parte de los ataques informáticos son efectuados por colaboradores internos de las instituciones. Asimismo, la política de seguridad de la institución debe tener eso en cuenta, siendo estricta en la atribución de permisos a sus usuarios. Esta política está directamente relacionada con la configuración del sistema operativo, de software propio de seguridad (antivirus, IDS/IPS) y con el hardware propio que eleva el nivel de seguridad, como es el caso de los routers.

Algunos de los inconvenientes listados arriba pueden ser causados también por fallas en las aplicaciones que posibilitan acceder a información sobre las cuentas de los sistemas con más privilegios. Para limitar estos tipos de ataques, el SARABI debe ser implementado con las siguientes reglas:

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

- Conexión segura al servidor a través de SSL (Secure Socket Layer) proveída con https (solo para la aplicación SINAVA porque es la que necesita autenticación);
- Autenticación de usuarios (que accederán a través de la Internet) mediante:
  - Nombre de usuario;
  - Contraseña;
- Permisos limitados de acceso a los recursos: ningún usuario de las aplicaciones tendrá rol de administrador de los equipos ni tampoco podrá consultar archivos en el sistema de archivos.
- Separación lógica de las aplicaciones – en el router se puede indicar cuales las aplicaciones accesibles a través de la Web.
- El servidor de base de datos estará separado físicamente del servidor de aplicaciones y Web.
- El acceso de las aplicaciones del SARABI a la base de datos será efectuado a través de un usuario con privilegios limitados en las tablas de administración de sistema.
- Las URLs Web utilizan parámetros encriptadas, evitando que los usuarios tengan acceso a información particular del sistema.
- La capa de persistencia de datos es independiente. No existen cláusulas de SQL en el código de los formularios.

### SQL Inyección

Uno de los ataques más comunes a las aplicaciones es a través del llamado SQL Inyección donde el atacante intenta sacar información de la base de datos que le pueda dar acceso a la misma con más privilegios a través de los formularios de las aplicaciones. Para limitar este tipo de ataques, las aplicaciones tienen implementado las siguientes funciones:

- Las contraseñas de los usuarios están encriptadas en la base de datos imposibilitando el acceso a cuentas de administración. Si se lograra ultrapasar la primera barrera de descubrir cuál es la tabla de usuarios y cuales sus campos, no se podría descubrir la contraseña.
- El usuario de las aplicaciones tendrá privilegios limitados en el acceso a las Bases de datos. Asimismo, no será capaz de poner la integridad de la base de datos en peligro.
- Los usuarios Web solo tendrán privilegios para Insertar, Seleccionar y Actualizar información en las tablas asociadas a los formularios de los trámites. Las demás tablas solo tendrán privilegios de Selección.
- Las bases de datos son instaladas con una cuenta con los privilegios mínimos necesarios a su ejecución.
- Todos los datos introducidos son validados. Por ejemplo, un nombre no podrá contener caracteres especiales (tipo # \$ % ' " ).

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"





## Proyecto "Etiquetado y Vigilancia del Mercado"

- Los mensajes de error están controlados y no muestran información sobre la estructura de las base de datos.

### “Denial of Service”

Como se ha referenciado en los tipos de ataque, algunos de ellos tienen el objetivo de dañar o mismo interrumpir el servicio prestado por los servidores.

Estos tipos de ataque son, también, en su mayoría ejecutados por colaboradores internos de la institución con acceso a la red. Asimismo, la propia institución es la responsable por definir su política de seguridad. La mayoría de las estrategias utilizadas en estos ataques son eliminadas con la utilización de Software y Hardware actualizado. Respecto al Hardware, la seguridad proporcionada está directamente relacionada con el precio de los equipos, y en este particular los Router.

La utilización de software específico de IPS (Intruder Protection System) o IDS (Intruder Detection System) ayuda en la seguridad. Este software de código abierto - <http://www.snort.org> - ejecuta las dos funciones, lo que puede ser una buena opción.

Los ataques de afuera solo serán posibles a través de la ejecución de programas instalados a través de virus. Asimismo, tener un antivirus actualizado y una política de instalación de programas estricta es fundamental para evitarlo.

## 9.2 FALLOS DE ENERGÍA Y/O EQUIPAMIENTO

Para estos tipos de fallos, las soluciones siempre involucran la necesidad de presupuesto para la adquisición de equipos específicos para este tipo de protección y en función del nivel de servicio que se pretende proveer. Para un servicio al cliente de 24 horas x 365 días sería necesario tener una infraestructura de hardware con configuración “Cluster”. Sin embargo, para el tipo de servicio que será prestado, es perfectamente admisible tener tiempos de baja de los servidores durante la madrugada y los fines de semana. Como mínimo, se considera la existencia de:

- Utilización de la configuración RAID 5 en los servidores.
- Utilización de unidades UPS por servidor con, por lo menos, 15 minutos de soporte de energía, y con limitadores de picos de energía eléctrica.

## 9.3 BACK UP

Las copias de seguridad están pendientes del nivel de servicio que se quiere prestar al cliente (ciudadano o funcionario). Para un nivel de servicio de 24 horas x 365 días, será



## Proyecto "Etiquetado y Vigilancia del Mercado"

necesario ejecutar la copia 'en carga' (o en 'caliente') lo que provoca una disminución del desempeño del servidor en ese periodo, que inicialmente no será mayor a los 15 minutos. Sin embargo, con el crecimiento del volumen de información puede ser necesario recurrir a backups incrementales para que estos tarden menos tiempo (mucho menos).

Una posible programación de los backups incrementales puede ser la siguiente:

Diariamente (sábado a viernes):

1. El primero a la hora de almuerzo;
2. El segundo en la madrugada.

Semanalmente (sábado en la madrugada):

1. Backup completo de las bases de datos.

Inicialmente, esta programación puede ser implementada siendo todos los backups completos. Se deberá monitorear regularmente el tiempo de los backups para evaluar la necesidad de pasar a backups incrementales (estos son también más costosos).

Dentro de las opciones existentes para almacenar el backup, se encuentra la Cinta magnética que es un método muy efectivo. Mientras el espacio en disco duro no sea crítico se puede efectuar el backup para disco, con tal que no esté en la misma máquina y que luego se pase a otro dispositivo (Cinta, CD o DVD) semanalmente.

### 9.4 MANEJO DE EXCEPCIONES

En caso de que el sistema presente alguna anomalía, el usuario administrador deberá verificar el correcto funcionamiento del motor de base de datos, del servidor de aplicaciones. En caso de presentarse algún problema con lo anteriormente descrito, deberá contactarse con personal técnico para que pueda resolver dichos problemas.

La gestión de errores debería ser de la siguiente forma:

- Se personalizarán los errores que pueden surgir por la intervención del usuario, definiendo mensajes claros para el mismo.
- El resto de errores se capturarán y se mostrará un mensaje estándar para todos los errores posibles.

En ninguno de los casos se deberá mostrar errores de la base de datos directamente al usuario final.

## 10 TAMAÑO Y PERFORMANCE

Como se ha podido observar en el punto referente a la arquitectura del sistema SARABI, existirán dos aplicaciones autónomas pero comunicables. Una es el sistema de gestión de las entidades oficiales de vigilancia de alimentos, y la otra la página Web que permitirá al consumidor consultar

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

directamente en la base de datos compartida de la CAN los incidentes ocurridos con alimentos en los Países Miembros y participantes del sistema.

### 10.1 REQUERIMIENTOS DE CAPACIDAD

El SARABI es un sistema que será manejado por los funcionarios de las instituciones responsables por la vigilancia de alimentos, y solo contendrá registro de las ocurrencias (incidentes) relacionadas con este tipo de productos. Como se sabe, al revés de otros sistemas, lo que se espera de este sistema es que con el tiempo el número de incidentes disminuya. Asimismo, no se espera un crecimiento exponencial, y continuo, del volumen de información. Como los sistemas de vigilancia se están implementando todavía en los países, en los primeros tiempos de utilización se espera que el número de incidentes crezca debido al volumen más grande de inspecciones que se hará. Sin embargo, aunque el número de inspecciones tiendan a aumentar el número de incidentes tenderán a disminuir por consecuencia del mejor cumplimiento de la legislación por parte de los operadores económicos, alcanzando así uno de los objetivos principales del sistema.

### 10.2 EVALUACIÓN DE IMPACTO

El análisis de impacto incide sobre algunos aspectos del entorno en que el sistema será implementado:

1. Personal que manejará el sistema;
2. Logística (instalaciones, infraestructura de comunicaciones, hardware) ;
3. Mantenimiento (recursos-humanos).

#### Personal

El impacto en el personal que manejará el sistema será considerado mínimo visto que se asume que estos funcionarios ya están acostumbrados al manejo de soluciones informatizadas por lo que fue analizado en la misión de campo. Asimismo, acciones de capacitación de dos días y la definición de los usuarios en cada rol del sistema, serán suficientes.

La resistencia al cambio que normalmente acontece en este tipo de implementaciones no será tan notoria debido al carácter innovador del sistema, principalmente porque el tema de vigilancia es, todavía, embrionario. No será el cambio de un proceso pero sí la implementación de un nuevo. En los casos en que el proceso ya está definido y/o implementado, las ventajas acrecentadas por el sistema no dejan argumentos para su no utilización.

Como lo referenciado en el punto anterior, no se espera que el crecimiento de la información a guardar sea muy elevado debido a las características específicas del sistema que solo será manejado por las entidades oficiales y que tiene como función la gestión de los incidentes ocurridos con alimentos. Por otro lado, el sistema no será altamente concurrente, con un elevado número de usuarios simultáneos accediendo a los diversos programas.

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"



## Proyecto "Etiquetado y Vigilancia del Mercado"

### Logística

En términos de logística, del diagnóstico previo elaborado, no se prevé la necesidad de grandes inversiones, tanto a nivel nacional como comunitario. Como ya referenciado, el sistema no representa una actividad crítica, que necesita de una disponibilidad a 100% (24 horas x 365 días) y no es de un manejo intensivo ni concurrente. Pero, se debe subrayar, que la elección del tipo de tecnología/arquitectura determinará la necesidad o no de nuevos recursos servidores y clientes.

La arquitectura del sistema presupone que cada país deba tener por lo menos dos servidores (uno Web y de aplicaciones y otro de base de datos) con capacidad para abarcar el SINAVA y la respectiva infraestructura de seguridad, backup, comunicaciones y climatización. La SGCAN también necesita de por lo menos los mismos dos servidores y condiciones para hospedar la base de datos central y el portal Web. Como el portal Web es de acceso público, necesita de configuraciones de seguridad más estrictas.

Al nivel del cliente, las instituciones necesitan que cada usuario tenga acceso a la Internet (o VPN) a través de una computadora que ejecute por lo menos el navegador Web Internet Explorer 6.0 (y las versiones de sus competidores equivalentes ya referenciadas arriba), con una resolución de pantalla de 1024x768 píxel, con memoria RAM de 512 MB (dependiente de la tecnología a utilizar) y un procesador con la velocidad de por lo menos 1GHz.

## 11 PRESUPUESTO

En este capítulo se estima el tiempo necesario para la implementación completa del sistema y un costo referencial para un consultor senior. La cifra referencial es de €850,00/día de trabajo. Esta cifra ya incluye todos los gastos necesarios (viajes, viáticos, costos administrativos).

### 11.1 SERVICIOS

Un proyecto de software estándar tiene las siguientes fases:

1. Análisis
2. Diseño
3. Programación informática
4. Pruebas
5. Despliegue (Instalación y Configuración)
6. Capacitación
7. Apoyo a la implementación (sistema en producción)

En este proyecto se realizaron las dos primeras fases: análisis y diseño. Quedan en falta las restantes, para las cuales se hará una estimativa de duración.

#	Actividad	Duración (mes)
---	-----------	----------------



Proyecto "Etiquetado y Vigilancia del Mercado"

1	Programación informática	4,00
2	Pruebas 1° nivel	0,50
3	Instalación y configuración, de aplicaciones y servidores	1,00
4	Capacitación de usuarios	1,00
5	Apoyo a la implementación ya con el sistema en producción	1,00
	<b>TOTAL:</b>	<b>7,50</b>

N° mes	N° días de trabajo	Costo (€850/día)
7,5	165	140.250,00

Las actividades 1, 2 y 5 son fijas. Es decir, que no están pendientes de la arquitectura elegida para la implementación. Las demás están estimadas para que se realicen en cuatro locales distintos (Colombia, Ecuador, Perú y la SGCAN).

## 11.2 EQUIPOS

Para la solución descentralizada, en que cada país tendrá su aplicación SINAVA y el Portal Web estará alojado en la SGCAN se necesitarían dos servidores, con sistemas de RAID y Backup para cada uno de los locales (Colombia, Ecuador, Perú y la SGCAN). Además, serán necesarios los equipos de red como Firewalls, Switchs y Modems.

El sistema no es muy competitivo en términos de usuarios/transacciones por lo que los equipos y el software de base y de seguridad, necesitarán de un presupuesto más accesible.

<b>Equipo</b>	<b>Cantidad (n° locales)</b>	<b>Precio unitario (€)</b>	<b>Monto Total</b>
Servidor Web y Aplicaciones	4	3000	12000
Servidor de base de datos	4	3000	12000
Firewall	4	1000	4000
Switch (8 puertos)	4	1000	4000
Rack de 19 " acondicionado con UPS y Aire (Ventilacion)	4	10000	40000
		<b>TOTAL:</b>	<b>72.000,00</b>

Los precios indicados son meramente indicativos, contemplan el software de base (sistema operativo, manejador de base de datos, servicios de red, seguridad y backup) y fueron estimados basados en las características necesarias a un buen desempeño del sistema.

No se han considerado los equipos Modem porque estos suelen ser ofrecidos por el ISP y su valor no es significativo. Tampoco se consideró la instalación del cableado.



### Proyecto "Etiquetado y Vigilancia del Mercado"

Los costos indicados son los iniciales. Los equipos pueden ser adquiridos ya con la asistencia técnica incluida para un número de años indicado en el contrato. También será necesario incluir el costo de un técnico (por local físico de los servidores) calificado para la asistencia inmediata a los usuarios, con conocimientos del sistema manejador de base de datos, del sistema operativo y de los demás componentes de software incluidos en el sistema.

Los costos indicados para los equipos son para instalaciones completamente nuevas. Sin embargo, cada uno de los países, y la SGCAN, puede ya disponer de servidores y respectivo software, funcionando actualmente abajo de su capacidad, donde el sistema pueda ser instalado.

---

Con el apoyo de:



COMISIÓN  
EUROPEA

COMUNIDAD  
ANDINA



PROYECTO DE COOPERACIÓN UE - CAN  
"Facilidad de Asistencia Técnica al Comercio"