— Ejemplar en Castellano (*) —

Aurrera !

Boletín Divulgativo de Nuevas Tecnologías en Informática y Telecomunicaciones

Publicado por el Gabinete Tecnológico de la DIT

Nº 14

Junio de 2004

Enviad vuestras sugerencias a: aurrera@ej-gv.es

ÍNDICE

Tal y como se os avanzaba en el Boletín anterior, el Gobierno Vasco (a través del Departamento de Ordenación del Territorio y Medio Ambiente) está dando los pasos necesarios para implantar un **GIS Corporativo**. En este sentido, y con el objeto de completar esa información, hemos dedicado en esta ocasión las primeras páginas de nuestro ejemplar a detallar cuales son sus antecedentes, cuales son las ventajas y objetivos del nuevo sistema, aplicaciones que se están desarrollando, así como su alineación con las directrices marcadas por el PIT2003-2005.

Por otra parte, el segundo tema hace una breve introducción a las soluciones denominadas "**Sistemas de Información para la Dirección**" y que lleva por título "Cuadros de Mando". Básicamente, estos sistemas permiten a los Altos Cargos de las entidades pedir datos a los sistemas de información corporativos, analizar los resultados y en base a ellos **tomar una decisión** y actuar. Todo ello, mediante interfaces totalmente amigables y sin la necesidad de depender del especialista informático correspondiente. Asimismo, a lo largo del artículo se hace un breve análisis de la evolución sufrida por estas herramientas (y sus siglas) desde los años 60 hasta nuestros días.

Por último, tal y como habréis comprobado, y dado el interés del tema seleccionado (los ataques informáticos), en esta ocasión se ha ampliado el apartado Alboan. Es cierto que en ocasiones anteriores ya se han analizado los distintos tipos de virus existentes, su funcionamiento, así como las tácticas usadas por los hackers; sin embargo, en esta ocasión el artículo se centra en los **métodos y soluciones defensivas** implementadas en los Sistemas de Información del Gobierno que nos evitan desagradables y molestas sorpresas en nuestro puesto de trabajo.

(*) Los ejemplares en Castellano y Euskera están disponibles en la web "Jakina".

GIS Corporativo

Desde 1989 se han llevado a cabo diversas iniciativas para la implantación de un Sistema de Información Geográfica[1] de ámbito general en el Gobierno Vasco.

DICCIONARIO

[1] GIS: Un Sistema de Información Geográfica (también conocido como SIG) es un sistema informático capaz de realizar una gestión completa de datos geográficos y de información alfanumérica asociada.

Para complementar la información publicada en este artículo podéis consultar el Boletín AURRERA Nº 13 (mes de marzo) en su página 2.

ANTECEDENTES

En 1989 se elaboró el denominado "Plan de Sistemas de Información Territorial", el cual permitió detectar las necesidades de los departamentos para la gestión de la información territorial y al mismo tiempo se definieron las acciones a realizar. Dichas acciones o tareas quedaron divididas en tres grandes grupos:

➢ **Acciones de infraestructura:**

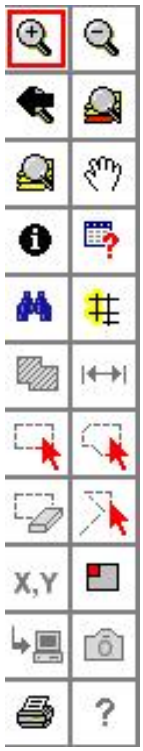
- Implantación de la Estructura Organizativa
- Definición y Adquisición de la Arquitectura
- Definición de los Procedimientos Operativos: manuales de normativa y procedimiento
- Desarrollo de la Cartografía Base: componentes elementales

➢ **Acciones a corto plazo:**

- Migración de los sistemas existentes
- Desarrollo de los Sistemas Prioritarios
- Desarrollo de la Cartografía Base: componentes específicos

➢ **Acciones a largo plazo:**

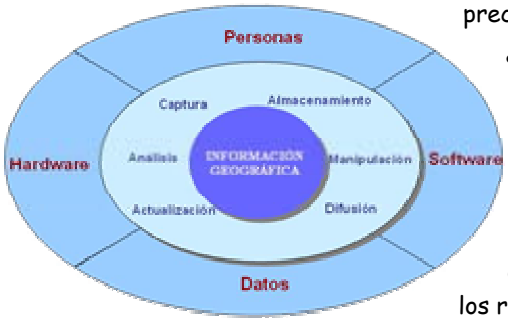
- Desarrollo de los subsistemas departamentales
- Desarrollo de la Cartografía Base: resto de componentes



En 1990 se acometen las primeras acciones de infraestructura ya definidas, se define la estructura organizativa para la realización del proyecto, se adquiere la infraestructura y se elaboran los manuales de normativa y procedimientos.

Asimismo, durante la **década de los 90**, se actualiza la información territorial de base:

- Cartografía Digital
- Ortofotos
- Red de vértices geodésicos
- Red de nivelación de alta precisión
- Adaptación de la cartografía a modelo SIG



A pesar de la labor y entusiasmo inicial, el plan definido no obtuvo los resultados esperados. Varias fueron las razones que impidieron evolucionar favorablemente al proyecto, entre las que cabe destacar la rigidez de la herramienta

seleccionada, la priorización de la parte alfanumérica de las aplicaciones frente a la gráfica y que el planteamiento inicial se hizo a largo plazo.

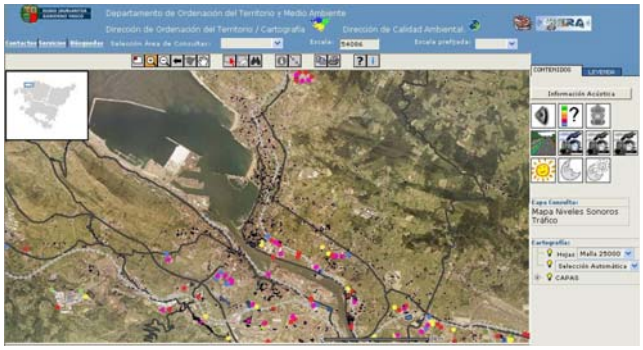
Debido a ese parón, a finales de los años 90 los responsables del proyecto decidieron reactivar nuevamente el plan. Como consecuencia de ello, uno de los primeros pasos dados consistió en abordar las tareas necesarias para adaptar el GIS al año 2000 y, asimismo se definió una nueva estrategia basada en realizar acciones de Infraestructura junto con **pequeños proyectos a corto plazo**. A partir del **año 2000** se han realizado las tareas que se indican a continuación:

- Actualización de la Información Territorial
- Informe de Análisis de la Situación Actual y Necesidades
- Prototipo del SIG cartográfico medioambiental
- Selección de la arquitectura tecnológica
- Implantación de la infraestructura de servidores
- Desarrollo de la Web Cartográfica
- Mapa de Ruidos de la CAPV
- Funcionalidad SIG para otras aplicaciones (Inventario de puntos de vertido, mapa sanitario)
- Organización de jornadas divulgativas y seminarios de SIG

GIS CORPORATIVO

Como definición podemos decir que un Sistema de Información Geográfica Corporativo es simplemente una colección de hardware, software, datos y personas que colaboran eficazmente en la captura, almacenamiento, actualización, manipulación, análisis y difusión de todas las formas de información geográfica.

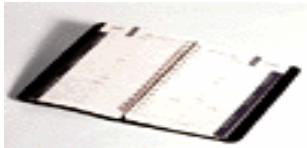
Un GIS Corporativo aporta la capacidad de almacenamiento de toda la información territorial y las herramientas para la gestión de la misma. Éste no implica un cambio en la



forma de trabajar de los diferentes Departamentos y Organismos Autónomos, sino que aumenta sus posibilidades.

[ver cuadro "Ventajas"]

Al mismo tiempo, se define una plataforma de Software GIS Corporativa, con el fin de mejorar el soporte a los usuarios. Al mismo tiempo los desarrollos GIS comparten



Funcionalidades

El GIS Corporativo proveerá una serie de funcionalidades de explotación de la información geográfica como pueden ser:

- Visor
- Catálogo
- Búsqueda
- Geolocalización
- Consulta
- Impresión
- Descarga
- Edición
- Importación masiva ...

VENTAJAS:

Un Sistema de Información Geográfica (GIS) aporta las siguientes ventajas:

- ✓ Representación más fiel del mundo real
- ✓ Mantenimiento de la integridad de los datos
- ✓ Gran número de reglas topológicas para utilizar
- ✓ Flexibilidad de geometrías (Puntos, Líneas y Polígonos pueden formar parte de una topología)
- ✓ La edición multiusuario
- ✓ Herramientas de edición de topologías
- ✓ Optimización. Herramientas de validación selectiva
- ✓ Herramientas de seguimiento y corrección de errores

un país en marcha

EUSKO JAURLARITZA GOBIERNO VASCO

componentes, abaratando considerablemente los costes y facilitando el mantenimiento global de las aplicaciones. Los nuevos desarrollos personalizados disponen desde un inicio de un gran número de funciones aportadas por el GIS Corporativo.

El GIS Corporativo facilita especialmente la **compartición** de información entre los distintos departamentos y su **difusión** a nivel interno (interdepartamental) y externo (hacia los ciudadanos).

<< El 75% de la información es susceptible de ser georreferenciada >>

Objetivos

El GIS Corporativo constituye una **aplicación horizontal** integrada dentro de la plataforma de aplicaciones definida en el Plan de Informática y Telecomunicaciones 2003-2005.

En definitiva, los objetivos de este GIS Corporativo se encuadran perfectamente dentro de las líneas establecidas para la Administración electrónica.

[ver cuadro "PIT2003-2005"]

Ventajas

El nuevo GIS Corporativo permitirá disponer en todo momento de Información no duplicada (accesible en base a los distintos perfiles de usuario creados), facilitará una Mejor comunicación interdepartamental, permitirá a todos los departamentos un Ahorro significativo en costes de desarrollo propios (ya que serán necesarias Menos Conversiones y Adaptaciones, quedando registrada toda la Documentación sobre la información almacenada). Asimismo se proporcionará un Mejor Soporte y mantenimiento al usuario del GIS (permitiendo a este una Mayor productividad en sus tareas).

Por último y como consecuencia de todo lo anterior se logrará una Mejor imagen Corporativa.

Compromisos

Desde el punto de vista de los departamentos indicar que, por un lado, cada departamento aportará información para la creación de la base de datos territorial común y, por otro lado, cada uno de ellos será responsable del mantenimiento de su información y decidirá quién puede consultarla. De forma similar a la gestión de contenidos en portales web.

Para conseguir un mantenimiento lo más eficaz posible ésta se realizará de acuerdo a procedimientos comunes a todos los departamentos y se

APLICACIONES ACTUALES

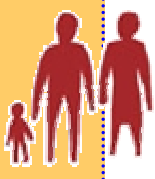
- ✓ Web Cartográfica
- ✓ Mapa de Ruidos de la CAPV
- ✓ Udalplan
- ✓ Prototipo de Medio Ambiente

PIT 2003-2005

El Plan de Informática y Telecomunicaciones 2003-2005 pretende alcanzar a través de este tipo de soluciones una ADMINISTRACIÓN ...

... orientada al ciudadano:

- ➢ Puesta a disposición del ciudadano de la información geográfica de la Administración
- ➢ Accesibilidad, disponibilidad y eficacia
- ➢ Oferta de servicios orientada al ciudadano



... interconectada:

- ➢ Canal de Comunicación entre Administraciones: Gobierno Vasco, Diputaciones y Ayuntamientos

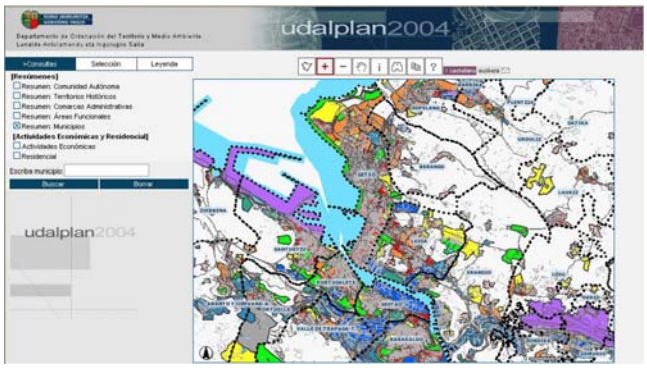
... integrada:

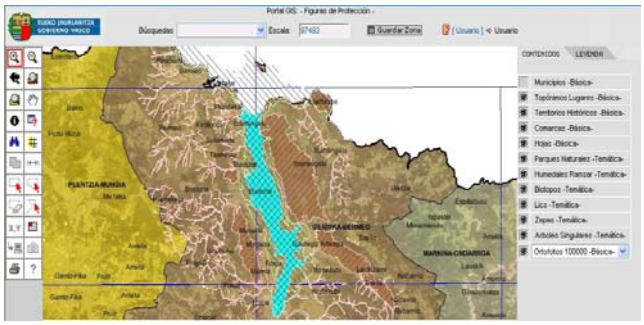
- ➢ Garantía de Coherencia en la información
- ➢ Herramientas comunes de decisión
- ➢ Imagen corporativa de la Administración en Internet

... eficiente y de calidad:

- ➢ Mejora de la gestión administrativa
- ➢ Reducción de costes
- ➢ Modernización del servicio
- ➢ Aumento de la calidad

almacenará siguiendo normas comunes que permitirá a todos compartir el mismo lenguaje. Por todo ello, la información se documentará para





hacer posible su compartición y difusión.

La información en el GIS Corporativo

La información del GIS Corporativo se almacenará en un repositorio centralizado y de acuerdo a un modelo de datos que:

- Evita duplicidades
- Permite diferentes vistas de la información a diferentes usuarios
- Permite la integración con información alfanumérica

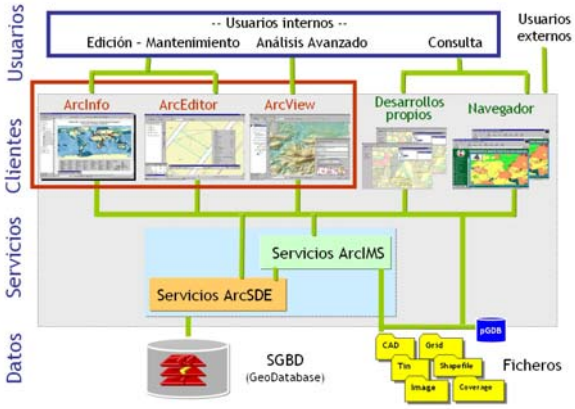
Para facilitar la compartición de toda la información, ésta se documentará mediante el uso de metadatos[(2)]. De esta forma el GIS Corporativo se convertirá en una potente herramienta de intercambio de información útil.

La información se generará y mantendrá de acuerdo a procedimientos que establecerán los flujos de trabajo y se regirán por normas comunes que permitan a todos los propietarios compartir el mismo lenguaje.

Accesos al GIS Corporativo

En función de las necesidades del usuario, el GIS Corporativo ofrecerá diferentes herramientas de acceso.

1. **Herramienta Cliente Web:** A través del navegador, sin necesidad de instalar ningún producto en la máquina local todos los usuarios del Gobierno Vasco podrán consultar la información almacenada en el GIS Corporativo. Los usuarios externos (los ciudadanos) también podrán disponer a través de Internet de las funcionalidades de consulta de esta herramienta.
2. **Herramienta Cliente Avanzada:** Ésta permitirá realizar consultas a las capas del GIS Corporativo, editar ficheros GIS y guardarlos en local, leer directamente de ficheros, etc.
3. **Herramientas Clientes ArcGIS:** Los usuarios con requerimientos mayores dispondrán de herramientas cliente de ArcGIS de la empresa ESRI. ArcView para consultas y análisis avanzados, y ArcEditor y ArcInfo para la edición y mantenimiento de la información.



DICCIONARIO

(2) Metadatos: Son los datos sobre los datos. Los metadatos dan respuesta al problema de conocer qué información hay, dónde está ubicada y en qué estado se encuentra. En definitiva **describen** los propios datos almacenados.

un país en marcha

EUSKO JAURLARITZA GOBIERNO VASCO

CUADROS de MANDO

Hoy en día, la información que llega a los altos cargos es excesiva: informes inmensos y no integrados entre si, que hacen que se reciban tantas informaciones distintas como fuentes puedan existir. La mayoría de las veces esta información es sectorial, no corporativa. Son informes reales, del momento actual, pero sin una visión de futuro, o sea, estratégicos. La información no está personalizada para cada usuario.

DICCIONARIO

(3) **CMI o BSC** (Cuadro de Mando Integral - Balanced Scorecard)

DSS (Decision Support System - Sistema de Soporte de Decisiones)

EIS o SIE (Executive Information System - Sistema de Información Ejecutiva)

MIS (Sistemas de Información Gerencial - Management Information Systems)

Algunos analistas definen los DSS como "un proceso de datos interactivo y un sistema de **representación visual** (gráfico) que es usado para ayudar en el proceso de toma de decisiones y debe reunir estas características:

- Ser sencillo para que lo pueda usar el que debe tomar las decisiones.
- Debe mostrar la información en formato y terminología conocida.
- Debe ser selectivo en su provisión de información (evitando abrumar al usuario)."

Los denominados "**Sistemas de Información para la Dirección**" tienen como principal objetivo poner a disposición de los directivos la mayor cantidad de información, hechos y circunstancias sobre su actividad, para ayudar a la toma de decisiones, a la gestión eficaz, el alineamiento estratégico de los recursos y la asignación de responsabilidades.

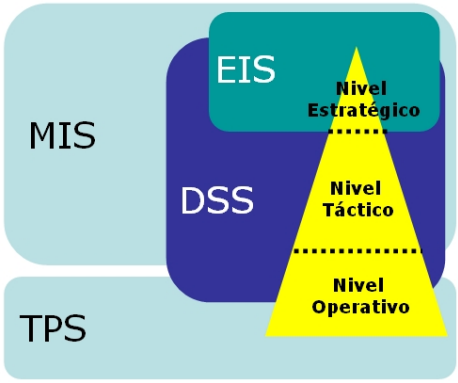
Estos sistemas se encuentran agrupados bajo siglas como CMI, DSS, EIS, ... (3)

LOS DSS Y LOS EIS

El objetivo principal de estos sistemas es la complementación de las capacidades de decisión del ser humano, valiéndose de la potencia de los ordenadores actuales para el procesamiento de datos.

Las características básicas de estos sistemas las podemos resumir en:

- Son simples y fáciles de utilizar por el usuario final.
- Permiten interactuar de forma amigable y en tiempo real.



- Apoyan el proceso de toma de decisiones estructuradas y no estructuradas.

[ver cuadro "**Decisiones**"]

- Pueden emplearse por usuarios de diferentes áreas.
- El usuario puede desarrollar sus propios modelos de decisión sin la participación de informáticos.
- Son capaces de acceder a la BD Corporativa(4) e interactuar con sistemas externos.
- Suelen ser intensivos en cálculos y escasos en entradas y salidas de información. Así, por ejemplo, un modelo de planificación financiera (sistema de información tradicional) requiere poca información de entrada, genera poca información de salida pero

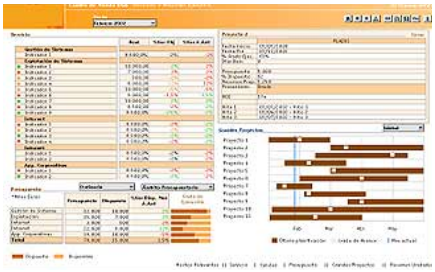
Las **DECISIONES** pueden ser:

- **Estructuradas (repetitivas o programadas).**
  - Se toman en niveles intermedios.
  - Son predecibles.
  - Su impacto afecta primordialmente a las operaciones cotidianas.
- **No estructuradas (no repetitivas o no programadas).**
  - Se presenta en los niveles más altos de la organización.
  - Considerable grado de incertidumbre.
  - Su elemento relevante es la imposibilidad de predecir el tipo y escenario de la decisión.

puede realizar muchos cálculos durante su proceso.

SUS PILARES BÁSICOS

Una parte fundamental de estos sistemas es su facilidad para explorar la información a través de **Gráficas de Alta Calidad** y reportes que se diseñan y obtienen en intervalos cortos de tiempo. El apoyo de los gráficos es fundamental para estos sistemas puesto que éstos agilizan la visualización de la información y por lo tanto, la velocidad con que se toman las decisiones.



Otro aspecto fundamental es la **Modelización**, que consiste en el "tratamiento" o filtrado al que debemos someter los datos brutos, para obtener de esta forma la información relevante que nos interese.

IMPLANTACIÓN

Si bien, la fase de implantación es abordada habitualmente con altas expectativas de éxito, muchos desarrollos terminan fracasando, debido, principalmente, a las **barreras** tecnológicas, organizacionales, psicológicas y educacionales que nos encontraremos.

En este sentido, indicar que aproximadamente el **75%** del éxito en la implantación debe atribuirse a estrategia, procesos, organización, personas y cultura y únicamente un **25%** al software.

[ver cuadro "Factores de éxito"]

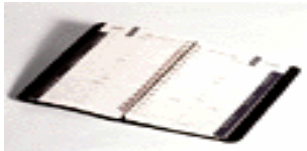
LA INFORMACIÓN YA EXISTE

Muchos de los datos que ofrecen los EIS, ya se encuentran disponibles tanto en los DSS y como en los Sistemas de Procesamiento Transaccional (TPS), aunque no está de forma integrada, ni tampoco en un formato a medida de las necesidades de los altos cargos.

En definitiva, se rentabiliza la información que **ya posee la propia corporación**, estructurándola, y permitiendo un control diario de los datos, y en consecuencia, mejorar y acelerar el proceso de toma de decisiones. Toda esta información es normalmente almacenada en los llamados Datawarehouse Corporativos (DW).

EL DATA WAREHOUSE

Un DW se basa en un repositorio de información, tanto detallada como resumida, que proviene de datos



DICCIONARIO

(4) BD CORPORATIVAS. Es la base de datos que integra toda la información de la compañía, la cual pueden consultar los diferentes usuarios para construir y utilizar herramientas para la toma de decisiones.

FACTORES de ÉXITO

- **Compromiso** de la Alta Dirección y apoyo operativo del usuario.
- Identificación clara de los **Requerimientos** del usuario.
- Debe ser capaz de agregar y extraer datos confiables desde medios internos y externos.
- Debe dar acceso a datos críticos y actualizados cuando se requieran.
- Los tiempos de respuesta deben ser cortos, para no "perder" el tiempo.
- Las interfaces deben ser **amigables**.
- Considerar la implantación como algo Corporativo y no algo del Dpto. de S.I.
- Ser realistas a la hora de establecer las **expectativas**.
- **Formar** e informar a los usuarios afectados por el cambio.
- Los sistemas deben adaptarse a la estrategia y no a la inversa.

residentes en BD operacionales y de otras fuentes externas.

Todos los datos del almacén reciben un "tratamiento" previo que garantiza la homogeneidad, la calidad y su orientación hacia el negocio.

La información albergada en un DW se caracteriza básicamente por ser un conjunto de datos:

<< Estos sistemas deben facilitar un soporte preciso y objetivo que minimice el riesgo en la toma de decisiones. >>

- **Temático**: Los datos están almacenados por temas, a diferencia de los sistemas operacionales en donde los datos están agrupados según las aplicaciones que los utilizan.
- **Integrado**: Todos los datos almacenados están integrados. Las BD operacionales orientadas hacia las aplicaciones fueron creadas sin pensar

en su integración, por lo que un mismo tipo de dato puede ser expresado de distinta manera en dos BD operacionales distintas.

- **No volátil**: Únicamente hay dos tipos de operaciones: la carga de los datos procedentes de los entornos operacionales (carga inicial y carga periódica) y la consulta de los mismos. La actualización de datos no forma parte de la operativa normal de un DW.
- **Histórico**: Las BD operacionales contienen los valores actuales de los datos. Un DW no es más que una serie de instantáneas en el tiempo tomadas periódicamente. Además, los datos almacenados en un DW permanecen en él más tiempo que en una BD operacional.

BUSINESS INTELLIGENCE

Las herramientas que facilitan el acceso a los DW, y su posterior explotación, son las denominadas Business Intelligence o BI.

Los sistemas BI son sistemas que recogen información de los sistemas utilizados en todos los departamentos de una organización (incluidos los sistemas ERP), organizándolos, y procesándolos de modo que sirvan a los ejecutivos de una empresa en la toma de decisiones.

Para construir sistemas BI es necesario utilizar técnicas de Data Warehousing, las que permiten preparar y almacenar los datos de forma adecuada para su posterior análisis con tecnologías analíticas

EVOLUCIÓN HISTÓRICA

Años 60: Esta época se caracterizó por los Informes **Batch** donde la información era difícil de encontrar y analizar, poco flexible y se necesitaba reprogramar cada petición o consulta.

Años 70: Nacen los primeros Sistemas de Información Gerencial (**MIS**) que se encargaban de realizar estadísticas a partir de BD centralizadas. Estos sistemas no cumplieron las expectativas que despertaron al dar una respuesta parcial y poco ágil a las necesidades de los directivos; su gran handicap era que no estaban integradas con otras herramientas Corporativas.

Años 80: Gracias a las interfaces gráficas, surgieron los programas **EIS** con el fin de suministrar a los ejecutivos información MIS integrada, combinada y unificada.

Años 90: Surgen conceptos como **Datawarehouse** y herramientas OLAP.

Año 2000: Se popularizan las Herramientas de **Minería de Datos** y Simulación.

GDSS

GDSS (Sistema de Soporte para la Toma de Decisiones de Grupo - Group Decision Support Systems)

Cubren la participación de un grupo de personas durante la toma de decisiones en ambientes de anonimato y consenso, permitiendo decisiones simultaneas.

Para ello es necesario introducir capacidades de comunicación y distribución de información (votaciones, foros, etc.)

El gran inconveniente es que la responsabilidad al tomar una decisión, puede diluirse.

Paquetes que se usan para apoyar decisiones en grupo: PLEXSYS, Colab (Xerox), Shell GDSS, DECAID (Decision Aids for Groups), LADN: (Local Area Decision Network), SMU: (Southern Methodist University), APL (Xerox), DELAWARE, ...

especializadas.

El procesamiento de estos datos (agrupamientos, asociaciones, secuenciamiento, reconocimiento de patrones, simulaciones, clasificaciones, etc.) se realiza con herramientas de "Datamining" o minería de datos.

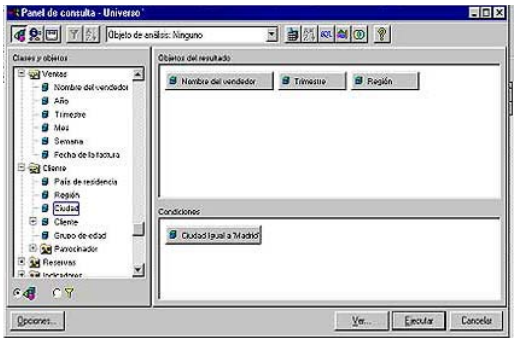
En estas herramientas se hace uso de técnicas como los árboles de decisión, métodos estadísticos, redes neuronales, lógica difusa, algoritmos genéticos, sistemas basados en el conocimiento, sistemas expertos y algoritmos matemáticos entre otros.

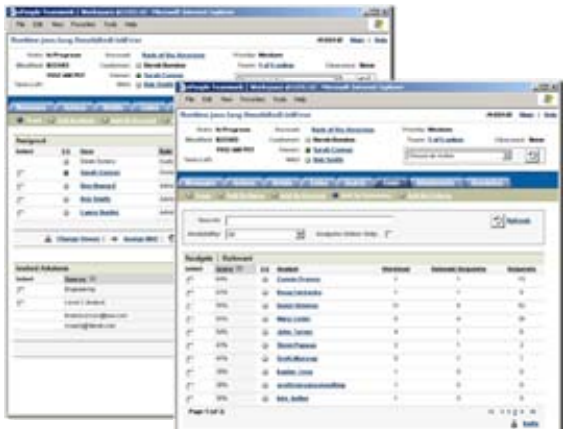
CONCLUSIONES

Un sistema que ayude a tomar decisiones correctas (o en determinado momento a no tomarlas), es sin duda alguna una de las mejores herramientas con la que cuentan actualmente los Altos Cargos.

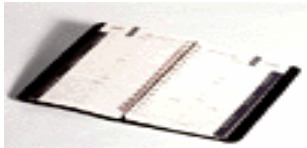
Estos sistemas facilitan de tal manera las tareas cotidianas que es cuestión de pedir datos, analizarlos y actuar.

De todas formas, estos sistemas por si mismos no solucionan problemas, ya que solo apoyan el proceso de la toma de decisiones mediante la generación y evaluación sistemática de diferentes alternativas o escenarios de decisión. Por ello, la responsabilidad final de tomar una decisión y de realizarla es de los administradores, no del DSS o del EIS. Estos sistemas únicamente deben facilitar un soporte preciso y objetivo que minimice el riesgo en la toma de decisiones.





Lista de algunos productos y de sus vendedores	
Herramientas EIS/BSC * Business Objetcs (Customer Intelligence, ...) * Computer Associates (CleverPath Forest & Trees) * Hyperion (Performance Scorecard) * Information Builders (WebFocus BSC) * MicroStrategy (Desktop y Web) * MIS (MIS onVision) * Oracle (Discoverer) * SAS (Strategic Performance Management) * Systar Software (Business Bridge) * Vincle (Board M.I.T.) * ...	**Herramientas de Query/Reporting y Análisis** * Altitude Software (uCI 2000 Plus) * Bertelsmann Direct (BD Mercury, Geocode ...) * BG&S (Applix iTM1 y Panorama Nova View e-BI) * Brio Software (Brio Performance Suite) * Business Objetcs (Web Intelligence, Infoview ...) * Cartesis Ibérica (Magnitude, Safran, Skover y Carat) * Computer Associates (CleverPath Reporter, ...) * Cognos (Finance y Analytic Applications) * Hyperion (Hyperion Essbase OLAP Server, …) * Information Builders (WebFocus Reporting Server) * J.D. Edwards (J.D. Edwards Business Intelligence) * Longview (Khalix) * MicroStrategy (Intelligence Server, Desktop y Web) * MIS (MIS onVision) * Optima Finance (Frango Consolidación y Advisor) * Oracle (Oracle 9i Reports) * Sagent (Sagent Solution) * SAS (Enterprise Guide y Enterprise Reporter) * SPSS (Showcase Strategy) * Sybase (Adaptive Server IQ, eBusiness ...) * Systar Software (Business Bridge) * Teradata (Teradata CRM) * Vincle (Board M.I.T.) * ...
Herramientas de Datamining * Computer Associates (CleverPath Predictive) * IBM (Intelligent Miner) * MicroStrategy (MicroStrategy Desktop) * MIS (MIS Delta Miner) * Oracle (Data Mining Darwin) * SAS (Enterprise Miner y Text Miner) * SPSS (Clementine) * Teradata (Warehouse Miner) * ...	



PIT 2003-2005

Según se concluye en el actual **"Plan de Informática y Telecomunicaciones 2003-2005"** del Gobierno Vasco << En el área de los Sistemas de Información (...) se trabaja en la línea de potenciar los sistemas basados en Datawarehouse, Datamining, Decision Support Systems (DSS) y Executive Information System (EIS), para poder disponer de indicadores de gestión a nivel corporativo. >>

un país en marcha

EUSKO JAURLARITZA GOBIERNO VASCO

ALBOAN: EJIE

LOS VIRUS Y ATAQUES INFORMÁTICOS.

CADA VEZ MÁS SOFISTICADOS

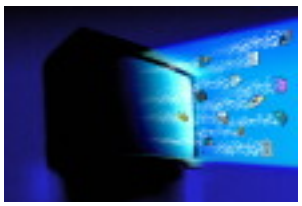
Recientemente se han cumplido 20 años de la aparición de los **virus informáticos** y de toda la inseguridad, molestias y gastos multimillonarios que tales códigos causan a particulares y empresas.

Muchos usuarios domésticos aún no están al tanto de las amenazas a la seguridad en Internet, o no conocen del todo cómo pueden establecer una buena protección para garantizar la seguridad de sus ordenadores o redes. En numerosos casos, los portátiles o las PDAs están directamente conectadas al módem ADSL, sin ninguna capa de seguridad, por lo que se convierten en objetivos privilegiados para los **hackers**, autores de virus y remitentes de spam (correo no solicitado ni deseado).

<< En numerosos casos, los portátiles o las PDAs están directamente conectadas al módem ADSL, sin ninguna capa de seguridad. >>

En muchos de estos casos estos virus consiguen instalar puertas traseras con la intención de recoger información de **contraseñas**, tarjetas de crédito, etc.

En estos momentos, las *vulnerabilidades de software* (fallo o hueco de seguridad detectado en algún programa o sistema informático que puede ser utilizado por virus o por hackers para entrar en los sistemas de forma no autorizada) se está utilizando como una de las principales vías de propagación de virus (Blaster, Nachi, Sasser, son algunos ejemplos). Estos virus han conseguido en un tiempo muy corto extender epidemias que están consiguiendo ocasionar graves daños a grandes organizaciones en todo el mundo. Normalmente, cuando se detecta una vulnerabilidad, la compañía fabricante del software afectado publica el parche necesario para corregirla. El problema se presenta cuando algún usuario malicioso tiene conocimiento de dicho problema y rápidamente desarrolla un "**exploit**" (programa diseñado para aprovecharlo) antes de que los usuarios actualicen sus sistemas. Este exploit, entre otros usos, puede ser incorporado a un código con intención de causar daño (virus, por ejemplo).



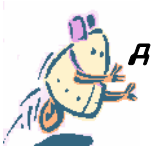
Hay que destacar también el modo de funcionamiento de muchos nuevos tipos de virus enviados por correo electrónico, habitualmente en correos que se consideran spam, en los que se colocan como falsos remitentes de esos correos a personas del entorno (dominio de correo) del usuario que lo recibe. En estos casos es mayor si cabe la confusión, dado que los supuestos remitentes reciben avisos de programas antivirus indicándoles que están enviando virus a otros usuarios conocidos cuando eso no es cierto en la mayoría de los casos. Esto puede ocurrir en estos momentos por dos razones: suscripciones de los usuarios en páginas web y listas de correo de dudosa reputación, y el "buen trabajo" realizado por nuevos programas creados para rastrear Internet en busca de esas direcciones de correo. *Es importante igualmente* ***no contestar*** *en muchos casos a correos no deseados ni siquiera para supuestamente anular una suscripción, porque desde ese momento se considera esa lista como "viva".*

En cuanto a otro tipo de ataques, como tema más importante en estos momentos hay que hablar del "**phising**" (estafas por e-mail). Estos ataques se producen cuando los que envían spams, haciéndose pasar por **bancos**, entidades de tarjetas de crédito u otras compañías muy conocidas, envían e-mails masivos instando a los receptores a actualizar su información bancaria en páginas web falsas que parecen legítimas. Microsoft publicó un parche urgente de Internet Explorer a primeros de Febrero de este año que solventaba este problema, pero el alto índice de afectados evidencia que éste no es muy conocido por los usuarios. Sin ir más lejos en el tiempo, a finales del mes pasado se ha hecho público un caso que ha afectado a clientes de Banco Pastor. *En estos casos, es muy importante* ***no entrar nunca*** *en este tipo de webs a través de enlaces que nos envíen por correo electrónico.*

LOS PROGRAMAS ANTIVIRUS TAMBIÉN EVOLUCIONAN

Las empresas antivirus están incorporado últimamente mejoras a sus productos añadiendo funcionalidades que controlan otro tipo de amenazas que han surgido en los últimos tiempos: software espía (con anti-**spyware**), virus de **mensajería** instantánea (en Messenger, etc.), marcadores web (con anti-**dialers**), ataques por la red (con **firewalls**).

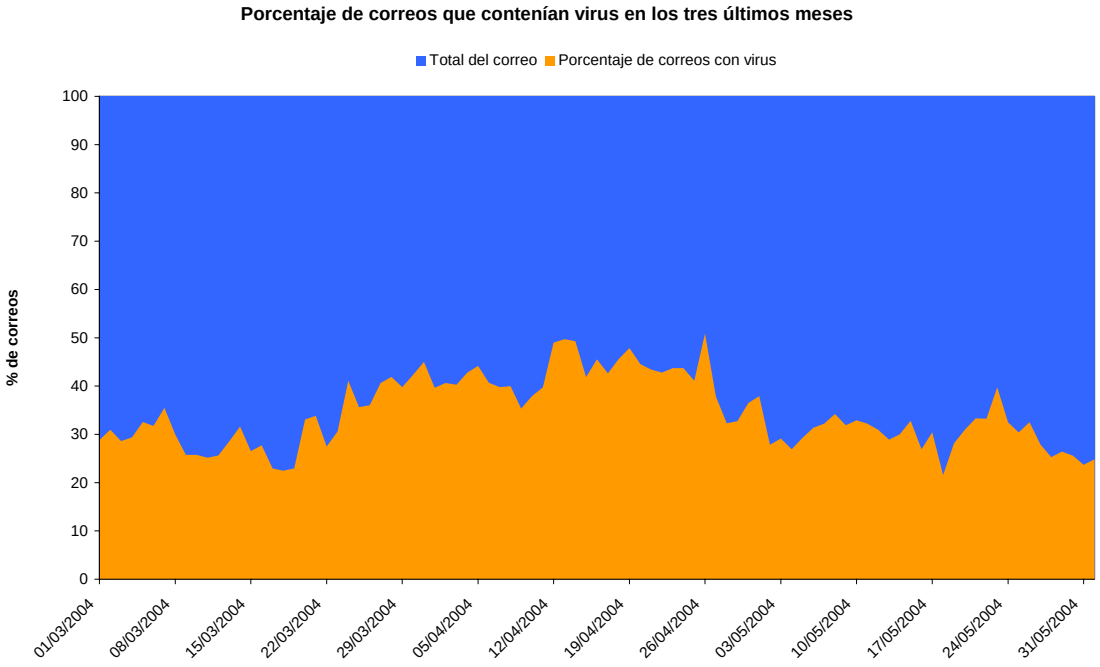
La finalidad del software espía o *spyware* (programas informáticos que se instalan sin permiso del usuario para registrar sus movimientos), es registrar los hábitos del internauta (por ejemplo con respecto a páginas visitadas y tiempo que pasa en cada una de ellas), una valiosa información que luego puede usarse para marear al consumidor con anuncios de publicidad a la medida. Los más dañinos son capaces de capturar lo que el usuario teclea, incluso nombres de usuario y **contraseñas**. Este software suele ser más complejo que los virus informáticos y además se renueva constantemente. Por no hablar de su omnipresencia, sobre todo en los programas de intercambio de ficheros: según la empresa de seguridad TruSecure, un 45% de los archivos descargados a través del popular servicio de intercambio de archivos Kazaa están infectados con virus o *spyware*.



Por su parte, los virus que llegan a través de productos de mensajería instantánea o aplicaciones P2P (compartición de archivos como Kazaa…) y la instalación sin conocimiento por el usuario de marcadores de telefóno o *dialers* que se conectan a líneas de pago (806…etc.) se están convirtiendo en el máximo problema de usuarios de tipo doméstico, que no están acostumbrados a tener ese tipo de incidencias en sus conexiones de trabajo debido a **políticas estrictas de seguridad** en las empresas.

EL CASO DEL GOBIERNO VASCO, GESTIONADO POR EJIE

Ante las últimas epidemias hemos asistido en informativos al caso de numerosas grandes empresas, gobiernos e instituciones afectadas, en algunos casos ante lo que pudiera parecer desidia de sus responsables informáticos.



un país
en marcha

EUSKO JAURLARITZA
GOBIERNO VASCO

Desde EJIE no podemos dejar ser muy cautos por aquello de "cuando las barbas de tu vecino veas cortar…", pero hasta ahora por lo menos nos hemos mantenido fuera del alcance de estos ataques.

En estos momentos en EJIE tenemos varias soluciones que intentan evitar que los temidos virus lleguen hasta los puestos de los usuarios vía correo electrónico; los virus tienen que pasar por **tres filtros diferentes** en los servidores de correo externo, más los propios de los servidores de correo interno, más los antivirus de los puestos de los usuarios. Es fundamental que estos antivirus estén siempre actualizados a la última versión, por lo que se realiza una comprobación **cada 30 minutos** con la casa proveedora y, en caso de haber actualización, ésta se instala de forma inmediata en los servidores de correo, y se comienza a distribuir a todos los equipos de la red.

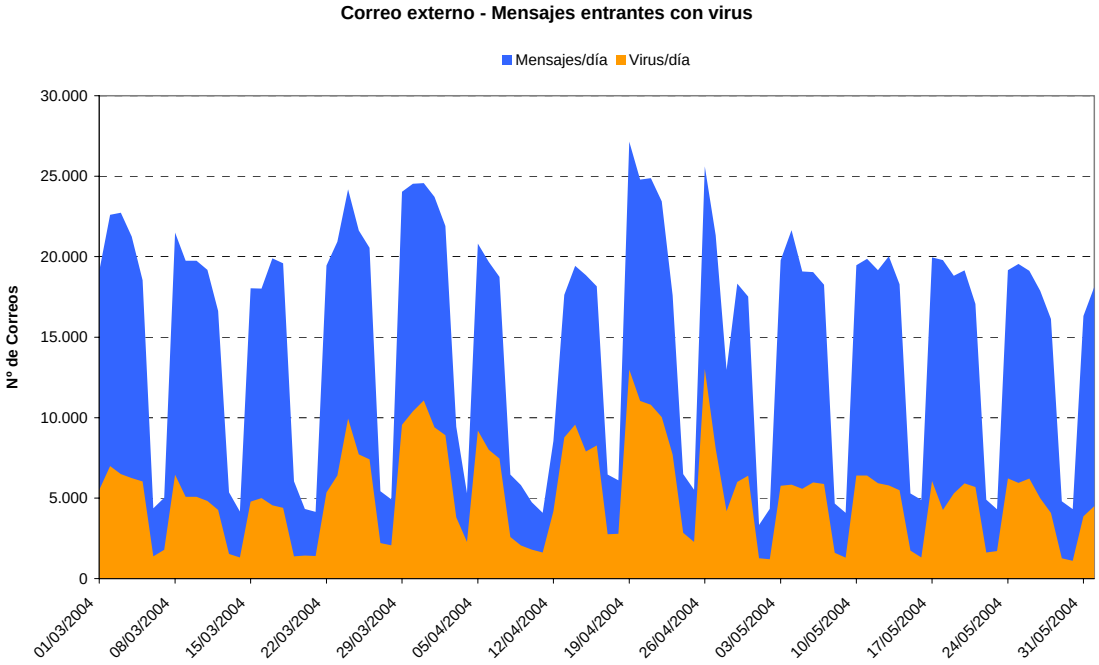
<< En el caso del Gobierno Vasco los virus tienen que pasar por tres filtros diferentes en los servidores de correo externo. >>

Últimamente se están probando nuevos productos que hagan más complicado que "nos toque" a nosotros, comprobando ya no sólo el correo electrónico o los archivos que se escriben en los servidores y los equipos de los usuarios, sino que analicen todo tipo de tráfico (datos) que llega desde el exterior; o herramientas que nos informan sobre qué equipos no están cumpliendo los requisitos necesarios en cuanto a actualizaciones de parches, etc.

Es fundamental en todo caso la **colaboración y concienciación de los usuarios**, principales afectados cuando este tipo de problemas les impiden desarrollar su trabajo, estando atentos a la actualización de su equipo (parches, antivirus, etc.). Los usuarios deben ser exigentes en este sentido y solicitar ayuda ante la mínima duda en cuanto al estado de esa herramienta de trabajo, porque eso redundará indudablemente en su beneficio. Por su parte, los Departamentos y Organismos Autónomos deberían considerar como propia la tarea de asegurarse de que el software antivirus y parches de seguridad están en perfectas condiciones en todos los equipos de su departamento.

DATOS QUE OBLIGAN A ESTAR "ENCIMA"

En los gráficos se puede apreciar el volumen real de mensajes, que provenientes de Internet llegaron al Gobierno Vasco en los últimos tres meses, y la proporción y número de ellos que contenían virus. Estos mensajes, obviamente, **nunca llegaron a los usuarios**, pero denota el efecto en coste y riesgo que suponen en nuestro entorno. Además en una escala temporal más larga, se podría apreciar la **tendencia creciente de ataques**, no sólo en cuanto a volumen, sino también en cuanto a sofisticación y rapidez de propagación.



Se puede observar que en algunos momentos han llegado a ser superiores al 50% de correos recibidos.

En el otro gráfico se puede observar que diariamente se pueden estar limpiando o eliminando entre 5.000 y 10.000 correos con virus, llegando a picos de 13.000 en un día.

Para conocer otras técnicas utilizadas por los hackers podéis consultar el artículo "**Ingeniería Social**" del Boletín AURRERA Nº 13 (marzo 2004)