

# Comerç segur a la xarxa internet (e-commerce)

**Remo Suppi**

Remo.Suppi@uab.es

Escola Universitaria  
d'Informàtica

Universitat Autònoma de  
Barcelona

Juliol 2002

## ¿Cómo se paga?

- La mayor parte de las compras se pagan con tarjeta de crédito
  - Facilitando directamente el número a través de un formulario seguro o a través de una cartera electrónica.
    - El usuario debe facilitar datos sobre su persona y sobre su entidad bancaria, de forma que las tiendas estén en condiciones de cobrarle aquellos productos que ha adquirido.
- Noticias diarias sobre jóvenes piratas que consiguen acceder a los servidores más seguros de autoridades y empresas de todo tipo y color
  - Panorama no muy favorable para creer en la seguridad del comercio electrónico.
  - Temor a facilitar datos personales o de la tarjeta de crédito en un formulario online son justificados

**Más simple**

## Introducción a la Seguridad

- Mecanismos de encriptación y codificación de la información son tan potentes y seguros que las probabilidades de que los datos así cifrados caigan en manos ajenas por robo es casi nula.
  - En la actualidad la mayoría de Sites-EC ofrecen garantías más que suficientes para una compra segura con todas las garantías.
    - Pago por canales seguros.
    - Garantizar la buena gestión en los pagos con tarjeta, con protección y encriptación para que la información no sea interceptada, y si lo es, no pueda ser descifrada.
    - Método más común: formulario seguro https://
    - Los monederos electrónicos, (2º más utilizado) (e-wallets).
      - El usuario transforma dinero físico en crédito y el sistema se encarga de reconocer y autorizar el pago.
      - La ventaja de este sistema es que el número de tarjeta de crédito nunca aparece en ninguna compra.
      - NO existe estándar claro y universal.
      - Recarga igual que los móviles.

3

## Comunicación segura a través de una red abierta

- La mayoría de las TIC basan su seguridad en la identificación de un nombre y una contraseña.
  - Este sistema es adecuado si se trata de una red cerrada
  - No garantiza la seguridad de los datos
- Agencia de Certificación Electrónica (ACE) emite certificados digitales X509v3 que cifran la información y garantizan:
  - **Autenticación:** identificando los participantes en las transacciones.
  - **Integridad:** asegura que la información no ha sido alterada durante la transmisión.
  - **Confidencialidad:** Cifra la información intercambiada.
  - **No Repudio:** establece constancia de quién ha intervenido en la transacción.
- El sistema de certificación se estructura en base a **dos clases** de certificados:
  - De servidor: autentifica al servidor frente al usuario pero no autentifica al puesto cliente.
  - De navegador: autentifica al cliente que se está conectando, con las funciones de firma y cifrado de los mensajes que envíe. Asimismo, permite el correo electrónico seguro entre usuarios o suscriptores de certificados.

4

## Comunicación segura a través de una red abierta

- **Ámbito de aplicación:** PC Banking, Tarjetas Inteligentes Correo Electrónico seguro.
  - Los certificados digitales: tecnología denominada de Clave Pública (PKI)
  - La autenticación de las de los individuos se realiza mediante firmas digitales que van incorporadas en el mensaje y que son únicas para cada individuo
  - El no repudio resulta del hecho de que cada persona es la única responsable de mantener su clave privada en la más absoluta confidencialidad
- **Sistema de certificación:** la "autoridad de registro" y la "autoridad de certificación"
  - RA: valida y registra las transacciones utilizando CD
  - CA: procesa, emite y garantiza los CD

## Seguridad en el comercio electrónico

- Imposibilidad de controlar todos los puntos por donde "pasan" las transacciones.
  - Desarrollo de sistemas "seguros" que permitan comprar sin peligro de posibles estafas.
  - Más utilizados SSL y SET.
  - Sistema de seguridad que implementan los navegadores:
    - Canales seguros de comunicación
      - canales seguros para el intercambio de datos entre el servidor y el cliente
    - Control de ejecución de código.
      - Previenen de ataques producidos por applets, controles y scripts dañinos.
  - Seguridad local:
    - Privacidad a los datos sensibles que almacenamos en nuestro ordenador (passwords, Nº tarjetas de crédito, etc.)
  - Secure Hypertext Transfer Protocol (S-HTTP), Secure Socket Layer (SSL), Private Communication Technology (PCT) y Secure Electronic Transaction (SET).

# SSL Secure Socket Layer

- Método más difundido
  - Gracias sobre todo al empeño que en esta tarea ha puesto su creador, Netscape.
  - Extendido: Apache y Microsoft Internet Information Server.
- Se sitúa entre la capa de transporte (TCP) y las aplicaciones, por encima del protocolo TCP/IP.
  - El sistema que utiliza SSL para lograr establecer una comunicación segura se basa en criptografía de clave pública, la cual utiliza algoritmos proporcionados por la empresa RSA.
  - Proceso de autenticación:
    - El cliente establece la conexión con el servidor enviándole un mensaje de bienvenida donde incluye su clave pública, el servidor le devuelve un ACK con su clave pública.
    - Una vez que el cliente recibe esta clave pública y confirma la información recibida, remite un mensaje al servidor codificando con la clave pública del mismo la llave que utilizarán durante toda la sesión SSL para codificar sus mensajes.
    - Una vez recibida esta por el servidor, éste le remite de vuelta dicha clave al cliente como último paso de la negociación, a partir de este momento tanto cliente como servidor comienzan la transmisión segura utilizando dicha llave para transmitir la información.

# SSL Secure Socket Layer

- La forma para determinar si el navegador ha logrado establecer esa conexión segura con el servidor es a través de una llave/candado entera que aparece en el Netscape Navigator, o bien un candado cerrado en el caso del Microsoft Internet Explorer.
  - Además también es posible adivinar si la conexión segura se está llevando a cabo observando si en la dirección URL, el "http://" ha sido sustituido por un https://.
- Debido a la popularización de los firewalls o cortafuegos entre la mayoría de las redes corporativas, en algunos casos era imposible establecer la seguridad aportada por el SSL.
- Solución: permitir que sea el firewall el que establezca la conexión SSL con el servidor remoto.
  - De esta manera la conexión sería segura de firewall para afuera, dejando la conexión entre éste y el cliente al descubierto, hecho que no tiene mayor importancia si el cliente está protegido detrás del firewall.

# SET Secure Electronic Transaction

- Sistema de pago seguro de más reciente creación.
  - Ha sido desarrollado por Netscape y Microsoft en colaboración con Visa y MasterCard.
    - Este sistema mejora el SSL añadiendo certificados digitales que relacionan al comprador y al vendedor con sus respectivos bancos, haciendo que la estafa sea casi imposible.
    - Al igual que el SSL, SET utiliza un sistema de clave pública/privada, la cual incluye codificación RSA.
    - El comprador utiliza su aplicación, llamada Wallet, para comprobar que el sitio del vendedor cumple el SET Mark si esto es así dicho programa le permitirá realizar la transacción.
  - Futuro y actualidad: criptografía de al menos 1024 Bytes, TSL, Internet (IPv6 ).

# Problemas generales sobre Seguridad Informática

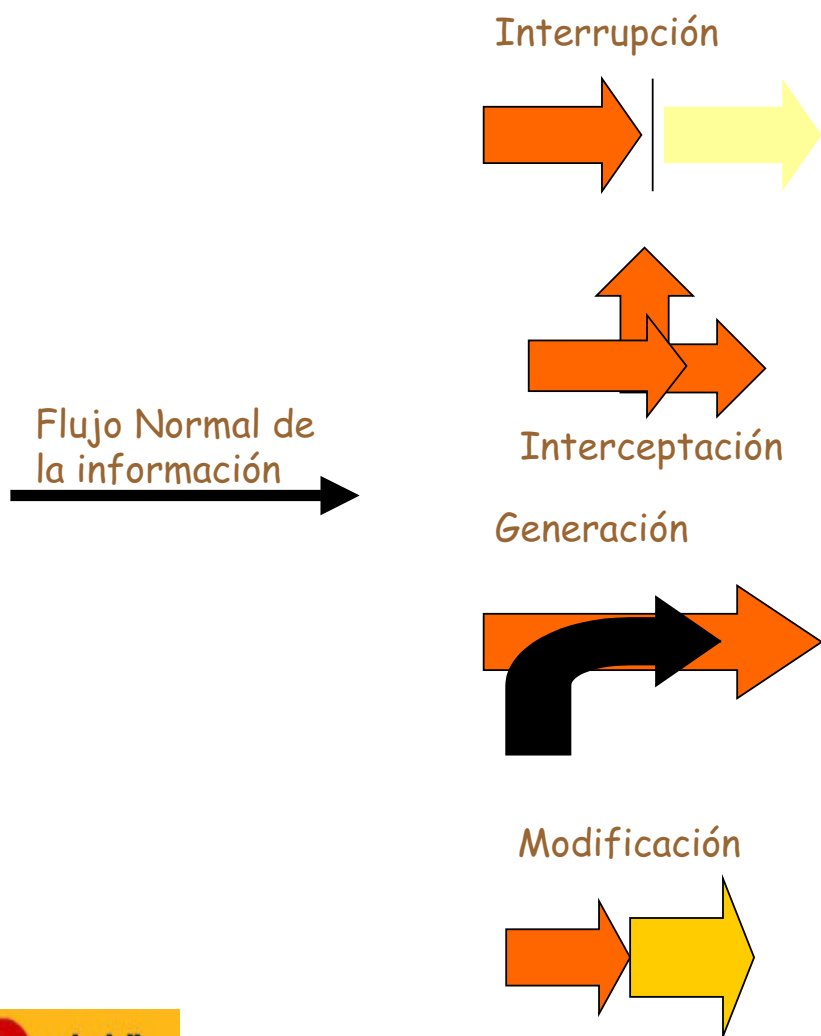
- Recomendaciones de la AUI (Asociación de Usuarios de Internet):
  - Utilizar siempre accesos seguros
  - No realizar compras en páginas no identificadas
  - Si se realizan compras a través de un servidor situado en el extranjero 'es como ir al extranjero y comprar algo', a efectos de reclamaciones posteriores y preguntar siempre si los portes y aranceles de los productos están incluidos en el precio.
  - Evitar 'a toda costa' cargar en el ordenador programas desconocidos y comprar siempre con tarjeta de crédito 'ya que pueden rechazarse los cargos durante un período de tres meses'.

## Amenazas a un sistema informático

•Existen cuatro tipo de amenazas según su características:

- Interrupción
- Interceptación
- Modificación
- Generación

# Problemas generales sobre Seguridad Informática



# Problemas generales sobre Seguridad Informática

## Amenazas de interrupción

- Existen daños y/o pérdida de información o el funcionamiento del sistema se ve afectado.
- Detección posible y en algunos casos inmediata.

### Problemas:

- Destrucción o desconfiguración del hardware
- Borrado de programas y/o datos
- Fallos en el sistema operativo

# Problemas generales sobre Seguridad Informática

## Amenazas de interceptación

1. Permite acceder al intruso a información no autorizada utilizando privilegios no adquiridos.
2. Si no es "in fraganti" la detección es difícil y si el intruso es hábil puede borrar su rastro impidiendo localizarlo.

Problemas:      Modificación de bases de datos  
                    Modificación de la configuración del hardware

## Amenazas de modificación

1. Permite el acceso sin autorización a un sistema para utilizarlo posteriormente generalmente en beneficio propio. La detección es similar al caso anterior.

Problemas:      Copias sin licencia de programas  
                    Captura de datos en líneas de comunicaciones



# Problemas generales sobre Seguridad Informática

## Amenazas de interceptación

1. Permite acceder al intruso a información no autorizada utilizando privilegios no adquiridos.
2. Si no es "in fraganti" la detección es difícil y si el intruso es hábil puede borrar su rastro impidiendo localizarlo.

Problemas:      Modificación de bases de datos  
                    Modificación de la configuración del hardware

## Amenazas de modificación

1. Permite el acceso sin autorización a un sistema para utilizarlo posteriormente generalmente en beneficio propio. La detección es similar al caso anterior.

Problemas:      Copias sin licencia de programas  
                    Captura de datos en líneas de comunicaciones



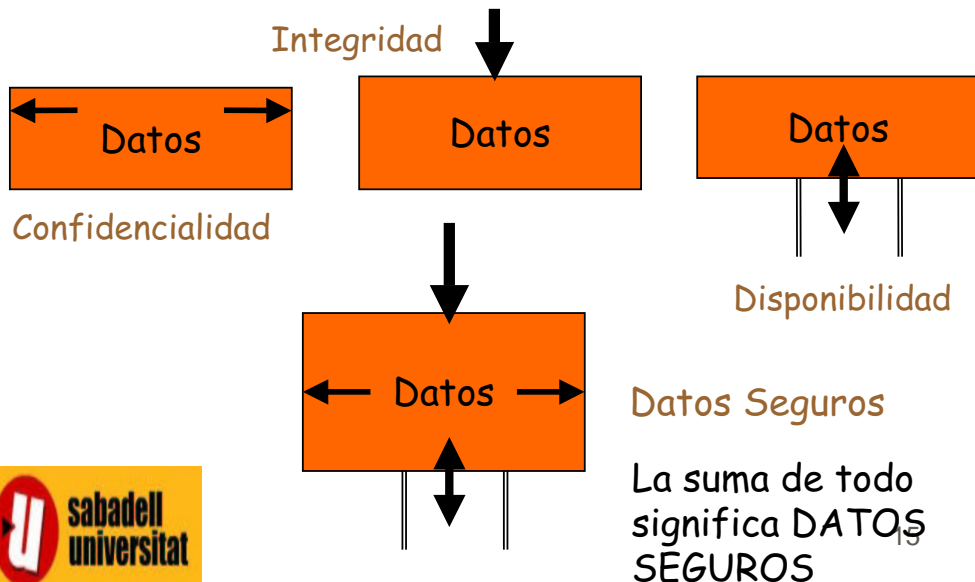
# Problemas generales sobre Seguridad Informática

## Amenazas de Generación

- o Creación de nuevos elementos dentro del sistema informático. La detección es como en los casos anteriores y conforman los llamados "Delitos de falsificación".

Problemas: Generar transacciones en una línea de comunicaciones como si fuera el cliente  
Añadir y/o modificar los registros en base de datos

Las flechas marcan donde y como se acceden a los Datos dentro del entorno donde se encuentran



# Elementos de la seguridad informática

## •Confidencialidad

-Los componentes del sistema son accesibles sólo por los usuarios autorizados.

## •Integridad

-Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

## •Disponibilidad

-Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

## •No Repudio

-Obliga a que la medida de seguridad esté siempre activa y el usuario no pueda desactivarla por comodidad o interés.

•Si se cumplen estas 4 condiciones diremos que los datos están protegidos y seguros.

# Encriptación

• Cambiar forma y sentido de la información para que otro individuo no pueda entenderla.

• SABADELL Universitat

• TBCBEFMM VMJFSTJUBU

• Clave para cifrar +1 letra, clave para descifrar -1 una letra .

• Gran cantidad de métodos (2a GM) por ejemplo matrices:

A B C

D a q f

E h e l

F t o i

Mensaje original: hola

Mensaje cifrado: AEBFCEAD

• Problemas de estos métodos: conocida la clave= método inservible. Necesidad de una metodología independiente de la clave.

• Esteganografía: ocultar la información dentro de otra mayor.

# Encriptación



• Los protocolos de encriptación modernos utilizan claves simétricas o asimétricas: DES (bancos), 3DES, IDEA, RCx, RSA, etc.

• Clave simétrica: se utiliza la misma clave para cifrar y descifrar. Problema como se transfiere la llave entre generador y receptor.

• Clave asimétrica: clave privada , clave pública: si cifro con la privada descifro con la pública o viceversa.

• Las claves públicas se encuentran en un servidor web seguro y utiliza la llave del destinatario para cifrar el mensaje. El destinatario utiliza la suya para descifrarlo.

• Asegurar la identidad: A envía un mensaje a B y hace:  $CP_rA + CP_uB$ , B hace:  $CP_rB$  y necesita la  $CP_uA$  del servidor seguro para descifrar el mensaje.

# Encriptación

- **Problemas:** Tiempo si el texto es muy grande.
  - Generalmente se utiliza clave simétrica para cifrar el texto (DES-IDEA) y clave asimétrica para cifrar esta clave.
- **Hash:** permite hacer un resumen de un texto generando un número muy grande de tamaño fijo tal que es imposible que dos textos diferentes tengan igual hash. Más conocidos MD5, SHA (firmas digitales)
- **Cómo funciona el PGP (Pretty Good Privacy):**
  - Mensaje de A a B
  - Hash al mensaje de A= 1234567890
  - Cifra 1234567890 con CPrA = Hcifrado
  - Usa clave simétrica y cifra: Hcifrado+Mensaje
  - Usa CPuB y encripta clave simétrica y envía todo a B
  - B usa CPrB obtiene la clave simétrica y con ello el mensaje y el Hcifrado.
  - Usa la CPuA para descifrar el Hash verificando que es B el que lo ha enviado, calcula el hash del texto y los compara.

• Si está bien, identidad garantizada, confidencialidad del mensaje de A y además evita el repudio.



# Aspectos legales

<http://civil.udg.es/normacivil/espanya.htm>

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
- Real Decreto 636/1993, por el que se regula el Sistema Arbitral de Consumo (BOE núm 121, de 21-05-1993)
- Ley 26/1984, de 19 de julio, General para la defensa de los consumidores y usuarios (BOE núms. 175 y 176, de 24-07-1984)
- Ley 34/1988, de 11 de noviembre de 1988, General de publicidad (BOE núm. 274, de 15-11-1988)
- Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de la contratación (BOE núm. 313, 31-12-1999)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

<http://civil.udg.es/normacivil/estatal/contract/LSSI.htm>



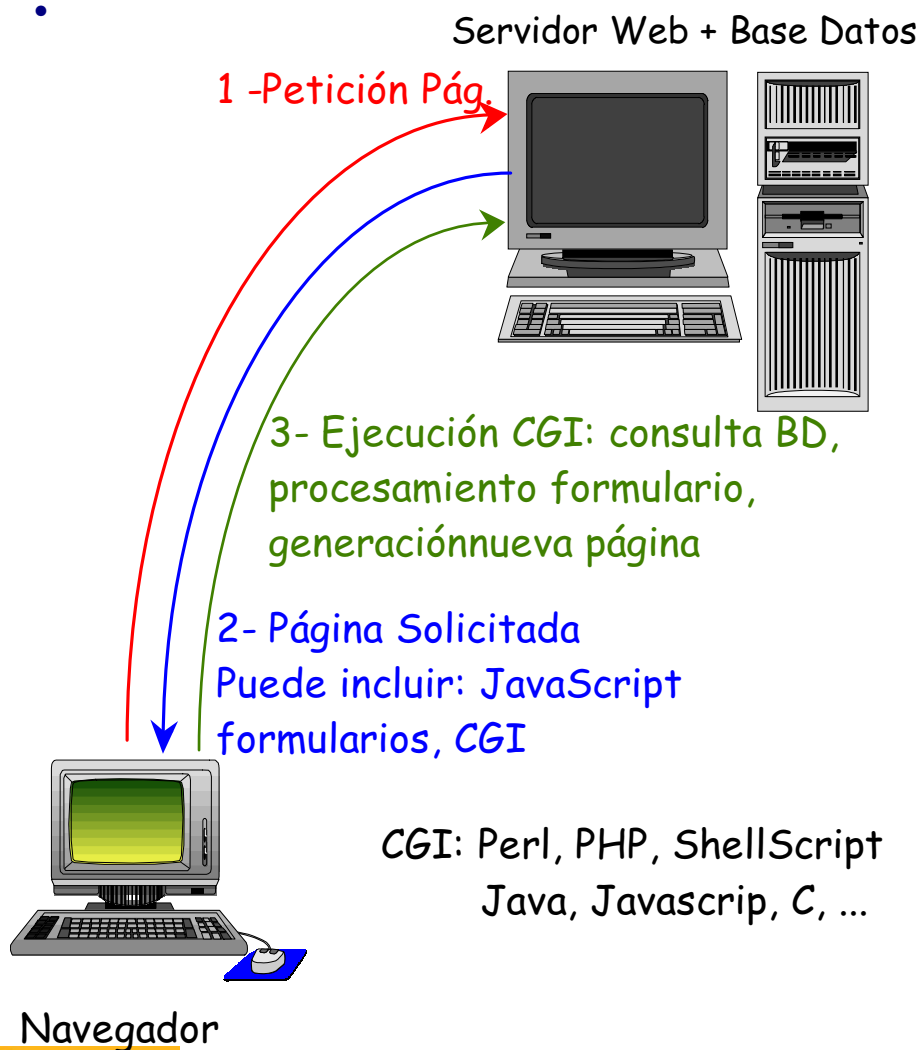
# Modos De Pago en CE

- **Pago:** forma de intercambio de bienes, imprescindible para nuestra supervivencia.
  - **Pagos en la red:** adecuados a l medio y a la virtualidad.
  - **Características:** simple, rápido, universal, trasladable (quien recibe lo pueda utilizar como moneda), céntimos €, valores grandes o pequeños, inviolable (seguridad e intimidad), seguro (de robo, o si lo hacen que no les sirva, o que si lo hacen servir no sea responsable), garantías de recibo, 1pago=1recibo, sin costes.
  - Nadie cumple con TODAS estas premisas, pero si hay variedad y métodos más adecuados a cada situación.
- **Tarjetas de Crédito o Débito:**
  - Método más utilizado. Comunicación SSL.
    - Peligro: datos en el vendedor en formato electrónico.
    - Es necesario conocer el vendedor, su localización física, etc.
- **TPV Virtual:** método más avanzado para la utilización de las tarjetas de crédito en Internet.
  - El vendedor no conoce los datos ya que son enviados en forma ilegible (encriptados) a la entidad bancaria.
  - El vendedor se ahorra problemas y el comprador dispone de un método eficiente, ágil y simple de pago.

# Modos De Pago en CE

- **Tarjetas chips:**
  - Es necesario hardware especial (lector) en el ordenador del cliente.
  - El cliente dispone de un tarjeta chip (La Caixa. Caixa de Catalunya) que se carga en un cajero.
  - La transacción es segura (https) y el importe se descuenta del crédito de la tarjeta.
  - No es Universal (Visa Chip)
- **Monedas electrónicas:**
  - Gran cantidad de tipos y estándares. Específicas para Internet. Garantía.
  - Sistema de crédito (cambio € por estas "monedas" y pago con ellas.
  - Aptas para pago de céntimos.
  - Necesitan casi todas la intalación de un programa para gestionar este dinero
    - **CYBERCASH** (<http://www.cybercash.com/>)
    - **MILLICENT**(<http://www.millicent.digital.com/>)
- **Otros:** PayBox, 906, SMS, etc.

# Arquitectura de un SITE CE



# Análisis de un SITE CE

- Necesidades básicas de un CE: Catálogo de Productos, Pedidos, Clientes, Tarifas y flujo de compra.
  - **Catálogo:** Estructura en capas o árbol
    - Gestión del catálogo (altas, bajas), búsquedas.
  - **Pedidos:** gestión y control de pedidos, pagos
    - Control de clientes, seguimiento, control de stock, administración y control de cuentas, logística.
  - **Tarifas:** gestión y control de precios, ofertas, promociones, etc.
  - **Control de flujo:**
    - **A: Identificación** (Nombre del usuario y passwd). Ir a B
    - **B: Acceso al catálogo:** por características o búsquedas. Inserción en el carrito de compra. Consulta info adicional. Ir a C
    - **C: Visualizar** el contenido del carrito y modificación de cantidades de producto. Ir a B: seguir comprando. Ir a D: tramitar.
    - **D: Tramitar pedido:** Resumen del pedido, datos adicionales, gastos de envío. Ir a E.
    - **E: Pedido Final:** Forma de pago, detalles, factura, clave del pedido, página de seguimiento.

# Análisis de un SITE CE

- **Aspectos diferenciadores:**
  - **Búsquedas:** por categorías, ofertas, promociones, palabras claves, ...
  - **Información:** pre-postventa, manuales de instrucciones, fichas técnicas, servicios de garantías, disponibilidad de productos, fechas aprox. de entrega, ...
  - **Gestión de la Base de datos:** actualización de productos e información relacionada, gestión de clientes y pedidos
  - **Logística:** Administración y control de pedidos (seguimiento).
  - **Administrativo:** gestión y control de pagos.
  - **Seguridad**
- **Elementos Adicionales (valor añadido):**
  - Puntos o cheques de regalo
  - Lista de distribución
  - Foros de discusión
  - Descuentos por cantidad
  - Información relacionada