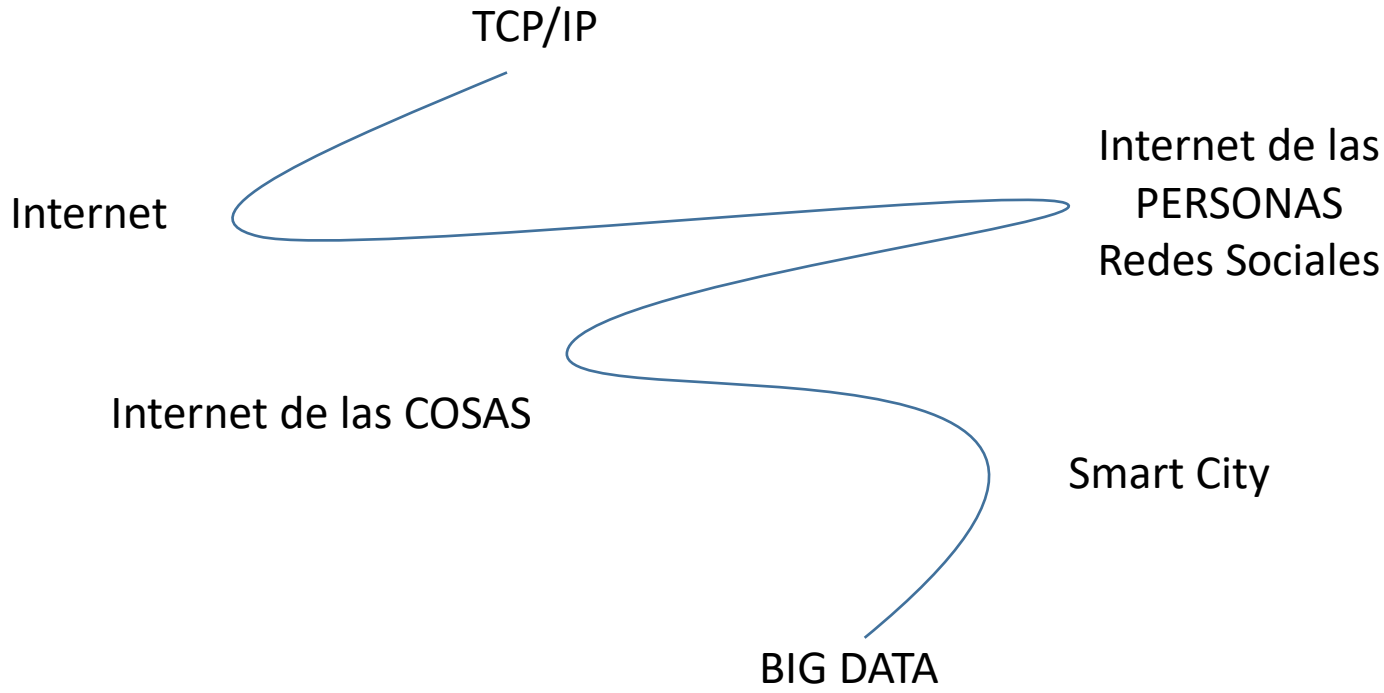
Seguridad Informatica I

Seguridad Logica

CONECTAR información

La evolución de conectar



Un repaso de la evolución

- El Inicio
- El Hoy
  - Redes inalámbricas
  - Internet masificada
  - Redes sociales
  - Que dicen las normativas

Algunos Temas de los que hablaremos

- Certificados digitales
- Firmas digitales
- Blockchain
- Criptomonedas
- Token
- Seguridad en una pymes
- IOT

La Internet…

Números que nos ponen en contexto

Internautas HOY!!!

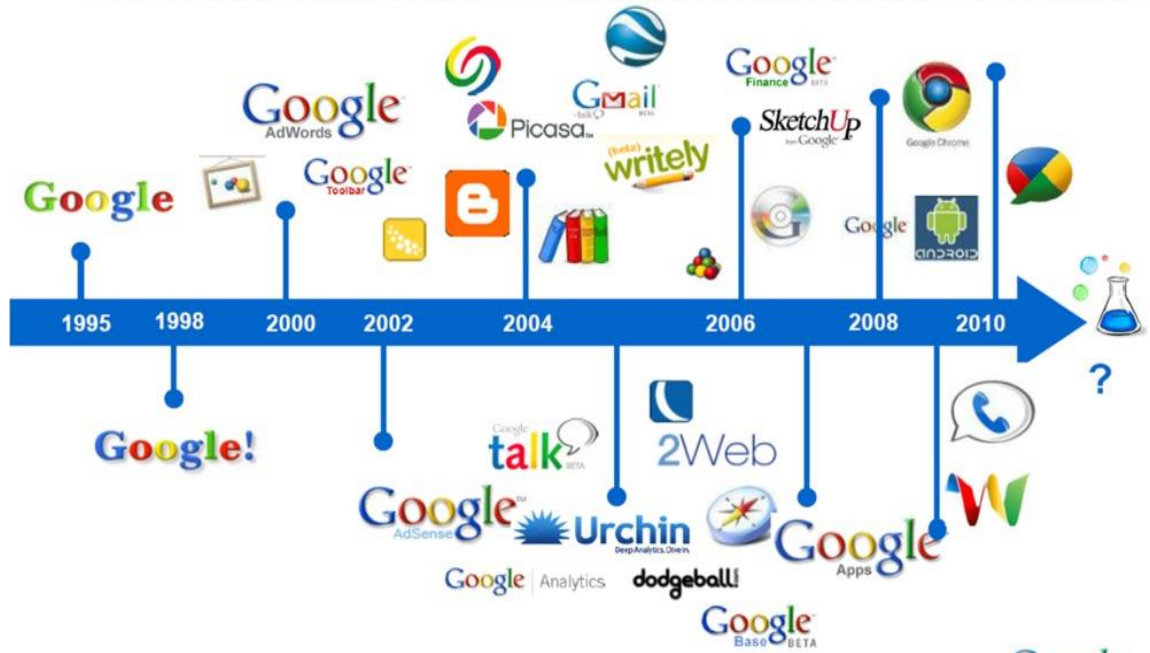
- Población Mundial 7.500 millones
- Internautas 3.600 millones

- Población LATAM 400 millones
- Internautas 242 millones

- Población Argentina 43 millones
- Internautas 30 millones

- Población Mendoza 1,7 millones
- Internautas 900.000

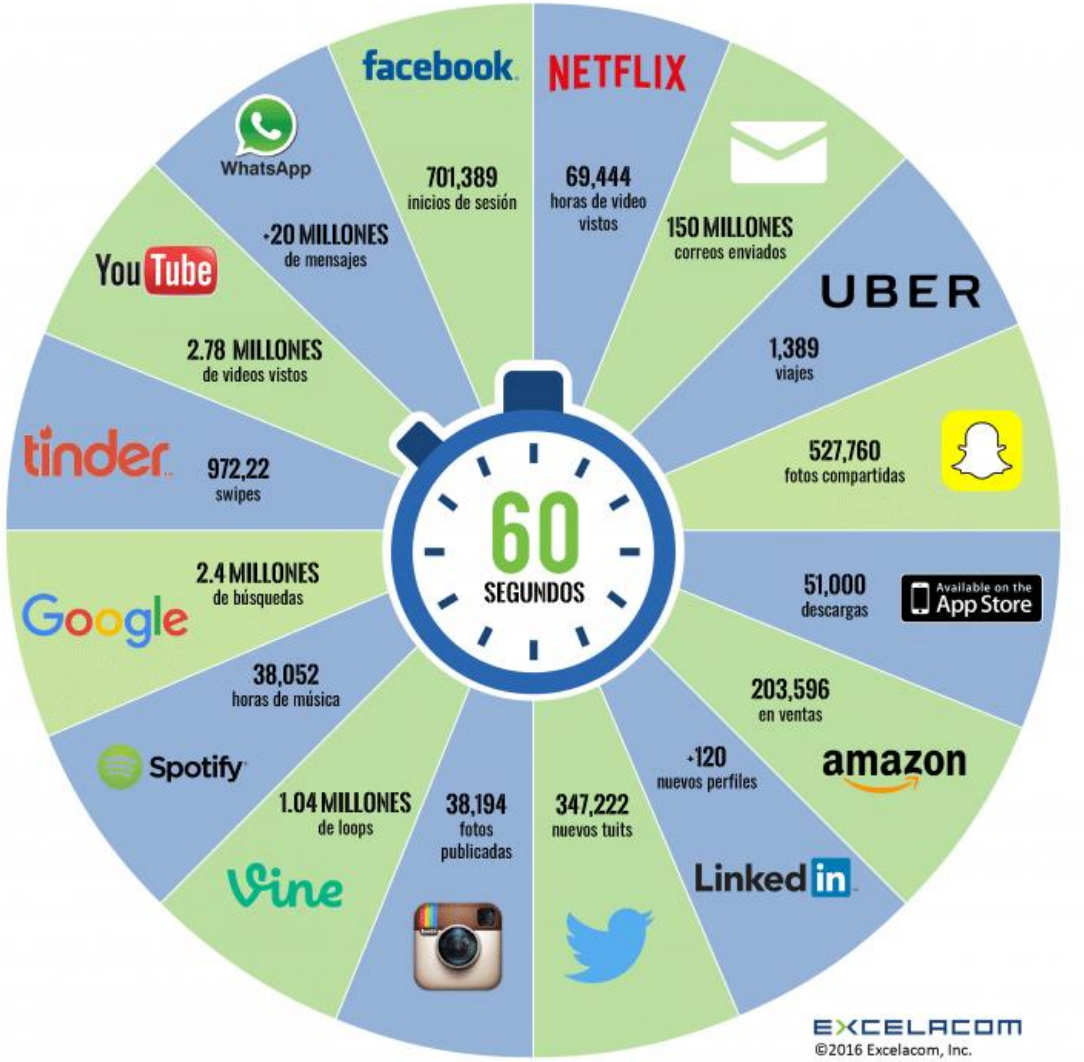
Google: Forced to innovate over the years



Google

La Internet…

Que pasa en internet en un minuto?



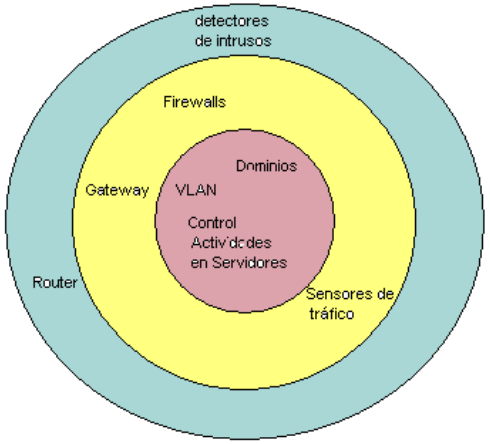
https://www.forbes.com.mx/lo-pasa-minuto-internet/

Cual es La computadora más segura?

Cloud Computing

¿Que es?

https://www.youtube.com/watch?v=WaxaOlnd_xE



Seguridad aplicada en capas

Que nos recomienda ISO 27001?

Que nos recomienda ISO 27001?

9.4 CONTROL DE ACCESO A LA RED

9.4.1 POLÍTICA DE UTILIZACIÓN DE LOS SERVICIOS DE RED

9.4.2 CAMINO FORZADO

9.4.3 AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

9.4.4 AUTENTICACIÓN DE NODOS

9.4.5 PROTECCIÓN DE LOS PUERTOS (PORTS) DE DIAGNOSTICO REMOTO

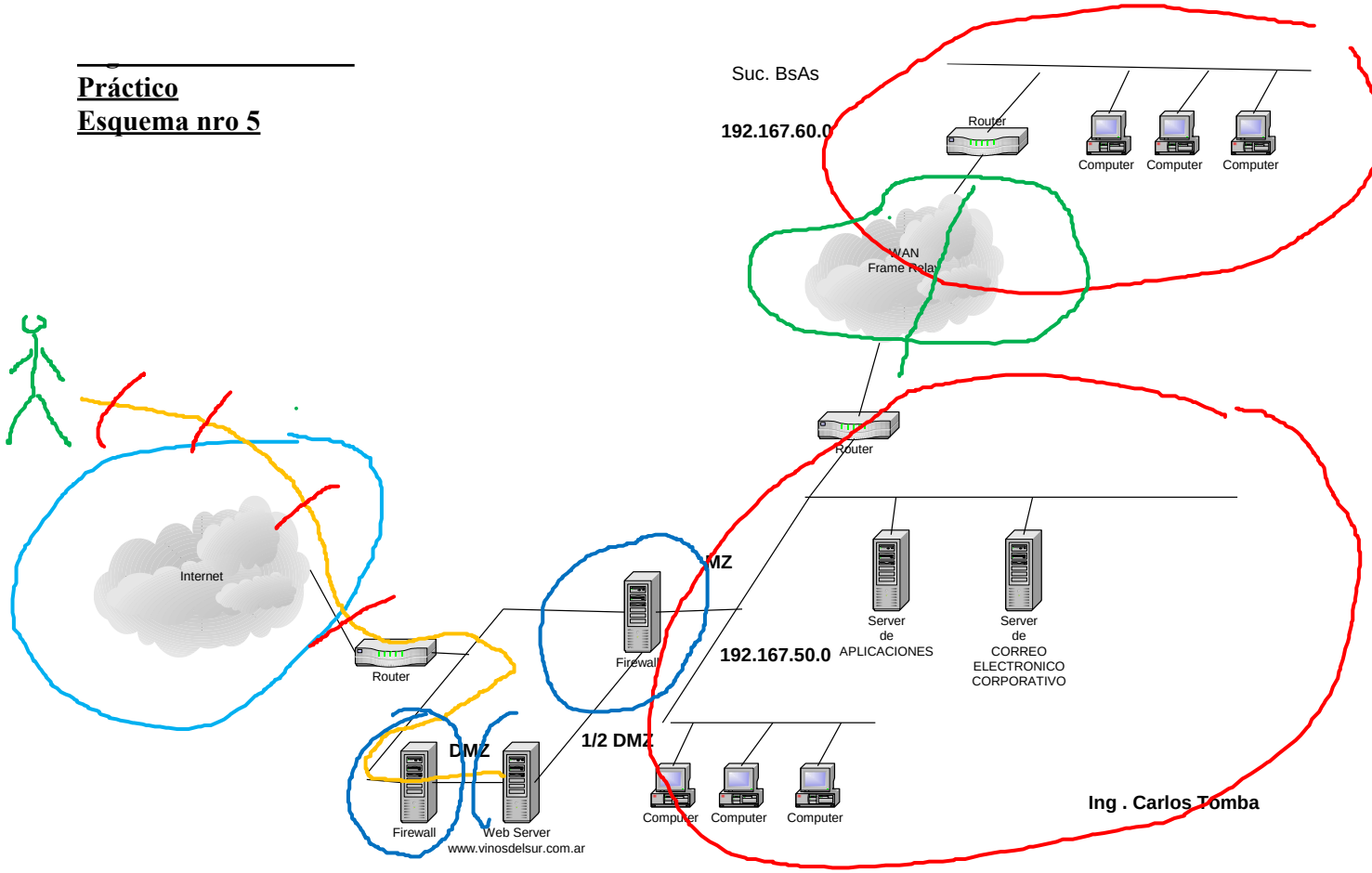
9.4.6 SUBDIVISIÓN DE REDES

9.4.7 CONTROL DE CONEXIÓN A LA RED

9.4.8 CONTROL DE RUTEO DE RED

9.4.9 SEGURIDAD DE LOS SERVICIOS DE RED

Publicando servicios en Internet



Proceso

Que nos recomienda ISO 27001 - 17799

- Vulnerabilidades
  - Disponibilidad
  - Confidencialidad
  - integridad
- Amenazas
- Contramedidas

Perimetro de seguridad

- Firewall
- WAF
- Antivirus
- IDS
- Antispam

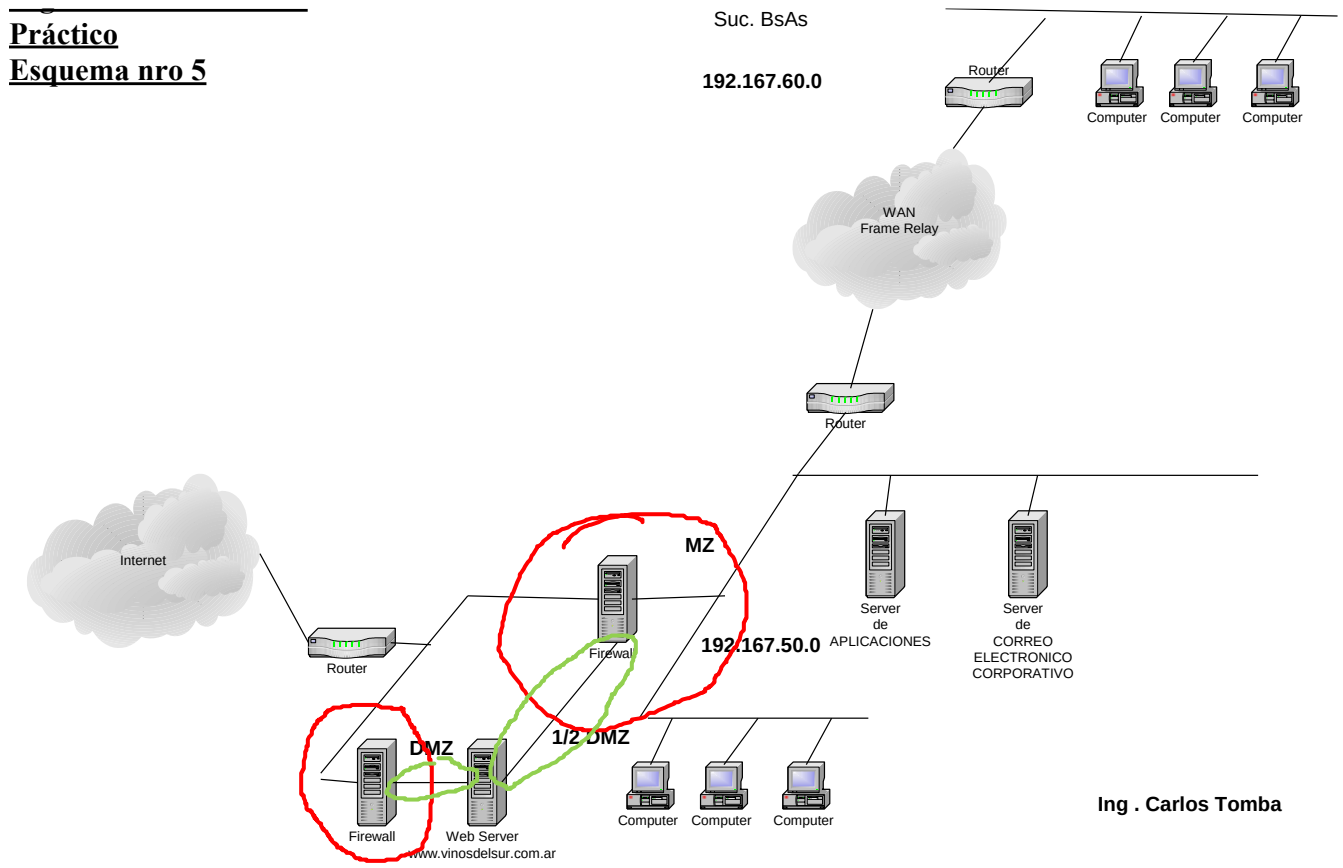
Analizando Un Caso Virus en el mail

- Como se propaga un virus en el correo mail coorporativos
- Sub división de redes
- Como es una regla de FW
- Como es una regla de NAT
- Contramedidas en contraposición

Perimetro de seguridad Firewall

- https://www.youtube.com/watch?v=7ytZ_s8n1WM
- Tipos de firewall
  - Hard
  - Soft
  - Según capas sobre las cuales trabaja
- Construyendo una regla
  - Polici
  - Nat

Publicando servicios en Internet



Proceso

Que nos recomienda ISO 27001 - 17799

- Vulnerabilidades
  - Disponibilidad
  - Confidencialidad
  - integridad
- Amenazas
- Contramedidas

HOY a que nos enfrentamos!!!! Tipos de amenazas

- Robo de Identidad
- Ingenieria social
- Ataque DoS
- Ataques a DNS
- Explotar puertos abiertos
- Virus
- Ransomware

- https://cybermap.kaspersky.com/es
- https://threatmap.checkpoint.com/

Veamos que esta pasando en el mundo ahora!!!

- https://cybermap.kaspersky.com/es
- https://threatmap.checkpoint.com/

Amenazas y sus Contramedidas

- https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos

Amenazas y sus Contramedidas

```
1-Cliente --------SYN-----> 2 Servidor
4-Cliente <-----SYN/ACK----  3 Servidor
5-Cliente --------ACK-----> 6 Servidor
```

Ataque DoS y Ddos

- https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio#Inundaci%C3%B3n_ICMP_(ICMP_Flood)

- **Smurf Attack**
  - Gran cantidad de solicitudes de eco ICMP a la dirección IP Broadcast
- **SYN Flood**

- **Ping Flood**
- **Ping de la muerte**
- **¿Cómo prevenir ataques DDoS?**

Amenazas y sus Contramedidas

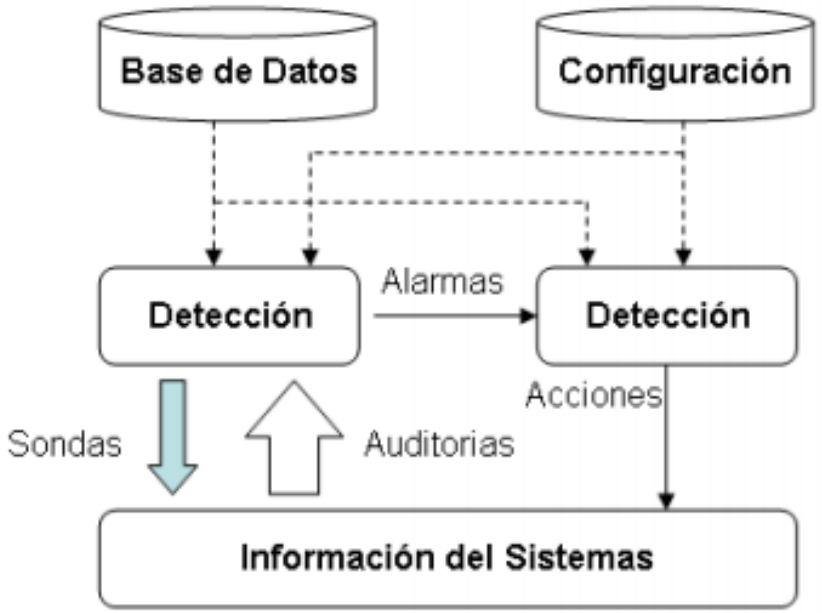
Escaneo de puertos

ARP Spoofing

- **Ataque de inundación MAC**
- **IP Spoofing**

IDS

- **Que es un IDS?**
- Un Sistema de Detección de Intrusos – IDS, (Intrusion Detection System, siglas en inglés); es un programa utilizado para analizar la detección de supuestos intrusos en la red o un computador, basado en sensores virtuales, permiten monitorear el tráfico de la red, permitiendo así evitar posibles ataques.
- El IDS, no solo analiza el tráfico de la red, sino su comportamiento y contenido.
- La cual es integrado por lo general a un Firewall. Estos IDS, poseen una base de datos de ataques, con “firmas”.



IDS
Tipos de IDS

- • HIDS.- IDS basados en Host, estos solo procesan determinadas actividades de
- los usuarios o computadoras. Ejemplos: Tripwire, SWATCH, LIDS RealSecure
- y NetIQ Vigilent.
- • NIDS.- IDS basados en Red, realizan sniffing en algún punto de la red, en
- busca de intrusos. Bien ubicados los NIDS en la red, puede ser una alternativa
- excelente para la prevención de los intrusos y un bajo impacto en la red al
- abarcar grandes redes. Ejemplos: SNORT, RealSecure, NFR y el IDS de
- CISCO.
- • DIDS.- Es parte del NIDS, solo que distribuido en varios lugares de la red, con
- un consolido en un solo banco de información.
- • IDS basados en Log, revisa los archivos de Logs en busca de posibles
- intrusos, se caracteriza por su precisión y completitud.

Analizando
Un Caso
Seguridad en Transacciones Electrónicas

Transacciones Electrónicas

- Autentificación de doble factor
- Certificados Dígitales
- Firma Dígital
- Blockchain
- Criptomonedas

Seguridad en Transacciones Electrónicas

🔒 Existen **cinco necesidades básicas** que un sistema debería poder garantizar en una transmisión por Internet:

- **Control de acceso**: sólo los usuarios autorizados deben poder acceder a las redes de comunicación y a la información contenida en las mismas.
- **Confidencialidad**: la información transmitida sólo debe poder leerse por aquel o aquellos a quién está dirigida.
- **Integridad**: la información transmitida debe de ser protegida contra manipulaciones no autorizadas.
- **Autentificación**: el emisor de la información debe de poder ser identificado.
- **No repudio**: el emisor debe de ser identificado de tal manera que no pueda negar la autoría de un mensaje o una transacción.

Link de la clase 8

- https://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n
- https://es.wikipedia.org/wiki/Firma_electr%C3%B3nica

PKI

- “Clave pública" o por su equivalente en inglés (Public Key Infrastructure o PKI).
- La normativa crea el marco regulatorio para el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional que no produzcan efectos jurídicos individuales en forma directa, otorgándole a esta nueva tecnología similares efectos que a la firma ológrafa.
- Decreto Nº 427 del 16 de Abril de 1998.

PKI como solución Estándar de seguridad
Descripción

- La tecnología PKI permite, mediante el cifrado **de la información electrónica**, que las comunicaciones y transacciones en Internet se lleven a cabo de una forma segura.
- El cifrado consiste en la **codificación de la información mediante algoritmos matemáticos** de forma que sólo pueda ser interpretada por aquel que posea la clave de decodificación correspondiente.
- Además, la tecnología PKI permite, **mediante la firma electrónica**, vincular un documento a su autor.

PKI como solución Estándar de seguridad
Componentes

- El entorno PKI se basa en tres componentes:
  - **Las claves públicas y privadas de cada usuario**
    - La base del sistema de certificación PKI son las claves públicas y privadas de cada usuario, que se generan mediante unos algoritmos matemáticos basados en números primos.
    - Cada pareja de claves es única.
    - Estas claves sirven para cifrar, descifrar, firmar y comprobar la información que se transmite.
    - Poseen la propiedad de que "lo que una llave cierra (cifrar) sólo lo puede abrir la otra (descifrar)".
  - **El certificado digital**
    - El elemento de Software firmado por una CA que determina la identidad del titular del certificado. (contiene registros con el nombre, NIF, etc.).
    - Un certificado está asociado a una persona, servidor o empresa.
    - Entre otros registros contiene la clave pública del titular del certificado.
  - **Las Autoridades de Certificación.** (CA's)
    - Son las instituciones encargadas de la emisión, revocación, y administración de los identificadores digitales. Son la tercera parte confiable (TTP) que asegura identidades en Internet.
    - Una CA puede a su vez crear Autoridades Certificadoras de Segundo Nivel (CAC's)
    - Una CAC proporciona las mismas funciones que una CA, pero en entornos cerrados
    - (dentro de una misma empresa o en las relaciones de ésta con terceros).

PKI como solución Estándar de seguridad
Utilidades y tipos de Certificados

- Los Certificados:
  - **Identifican** un usuario, servidor o empresa.
  - Permiten el **cifrado** de las comunicaciones (con las claves).
  - Permiten la **firma** un documento electrónico.
- Existen varios tipos de certificados según el protocolo de comunicaciones y la aplicación que se esté utilizando:
  - **Certificado personal:** documento de identificación de un usuario de Internet para navegar, comprar, enviar y recibir correo, firmar documentos electrónicos, etc. de forma segura.
  - **Certificado de servidor:** permite asegurar toda comunicación entre un navegador y un servidor web.
  - **Certificado para VPNs:** permite la comunicación segura, entre las empresas y sus empleados, clientes y proveedores, mediante la creación de redes privadas virtuales en el entorno abierto de internet.
  - **Certificado Servidor WAP:** permite asegurar toda comunicación entre un terminal móvil y un servidor WAP.
  - **Certificado para firmar código:** permite a una empresa firmar su software y distribuirlo de forma segura.

PKI como solución Estándar de seguridad

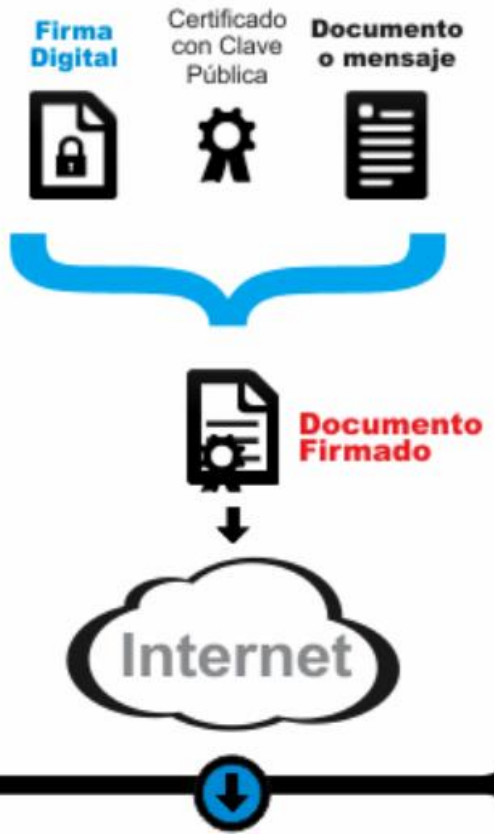
Mecanismo de Firma Electrónica

- **La firma electrónica tiene las siguientes etapas:**
  - 1ª Cuando el emisor crea un documento electrónico también crea, gracias a una aplicación de firma digital, un resumen con sus parámetros clave.
  - 2ª Este resumen lo cifra con su clave privada y lo adjunta al documento.
  - 3ª Cuando le llega al receptor, éste genera, con la misma aplicación de firma, otro resumen y con la clave pública del emisor descifra el resumen recibido.
  - 4ª Si ambos resúmenes son idénticos significa que el documento no ha sido alterado.

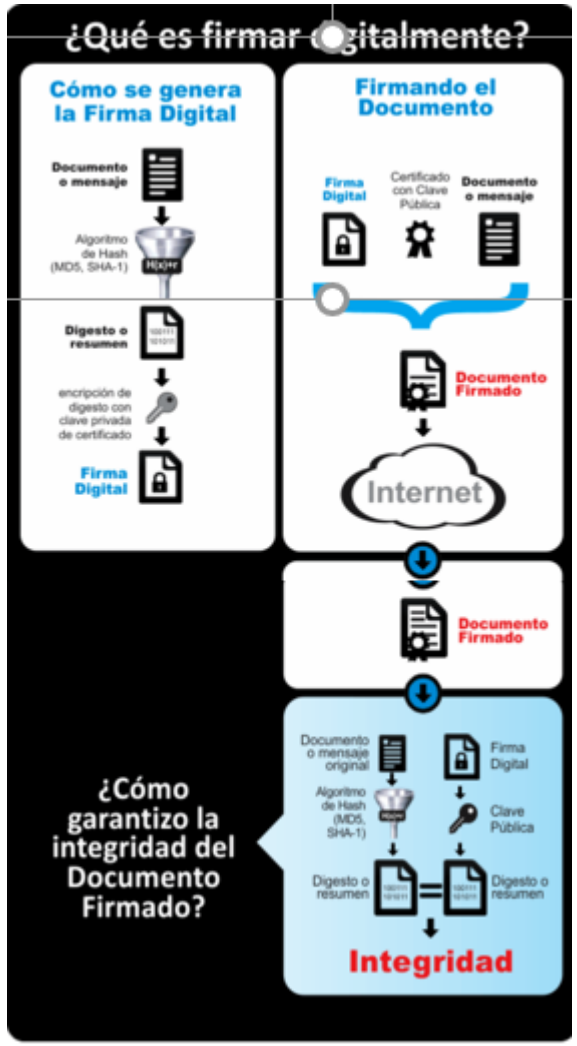
¿Qué es firmar digitalmente?

Cómo se genera la Firma Digital

Firmando el Documento



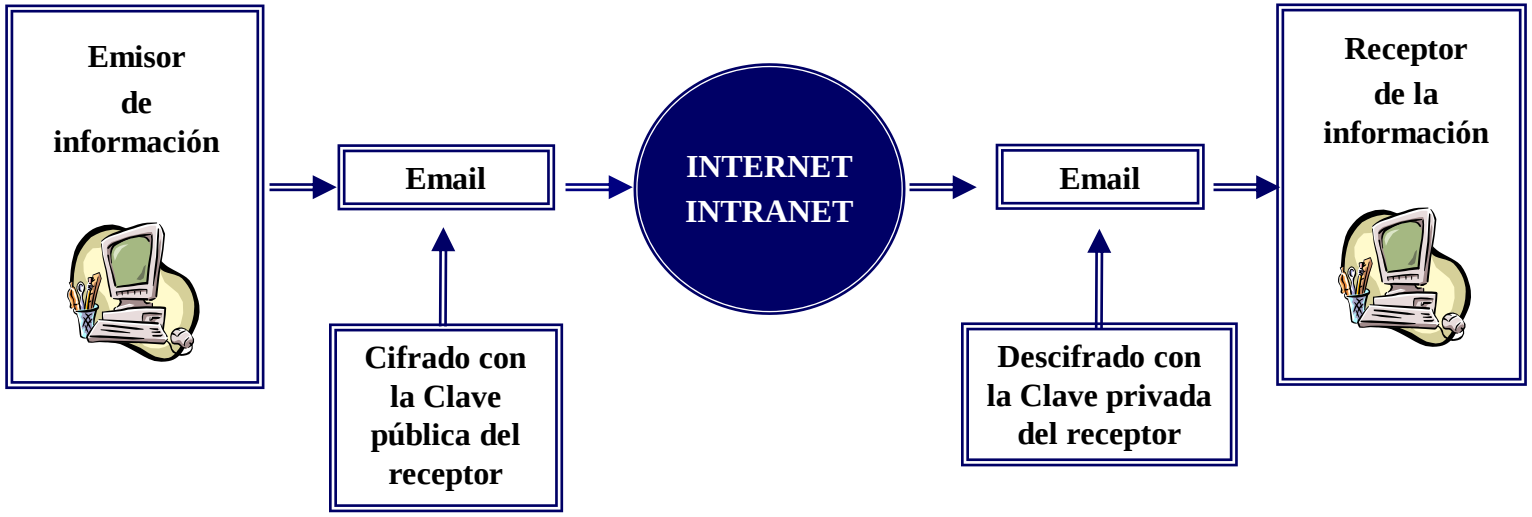
¿Cómo garantizo la integridad del Documento Firmado?


¿Qué es firmar digitalmente?
Cómo se genera la Firma Digital
Documento o mensaje
Algoritmo de Hash (MD5, SHA-1)
Digesto o resumen
encripción de digesto con clave privada de certificado
Firma Digital
Firmando el Documento
Firma Digital
Certificado con Clave Pública
Documento o mensaje
Documento Firmado
Internet
Documento Firmado
¿Cómo garantizo la integridad del Documento Firmado?
Documento o mensaje original
Algoritmo de Hash (MD5, SHA-1)
Digesto o resumen
Firma Digital
Clave Pública
Digesto o resumen
Integridad

PKI como solución Estándar de seguridad

Seguridad en email

- Cuando se envía un e-mail el programa de correo del emisor lo cifra con la clave pública del receptor (que es pública bien porque está en algún registro de la Autoridad de Certificación o bien porque el receptor se la ha enviado en un e-mail anterior).
- Cómo lo que se cifra con esa clave pública del receptor, sólo se puede descifrarse con su clave privada, la comunicación es absolutamente segura (CONFIDENCIALIDAD).
- Además el emisor puede firmar el mensaje y de esa forma asegurar su identidad. (AUTENTICACIÓN).



PKI como solución Estándar de seguridad

Ejemplos de Aplicaciones

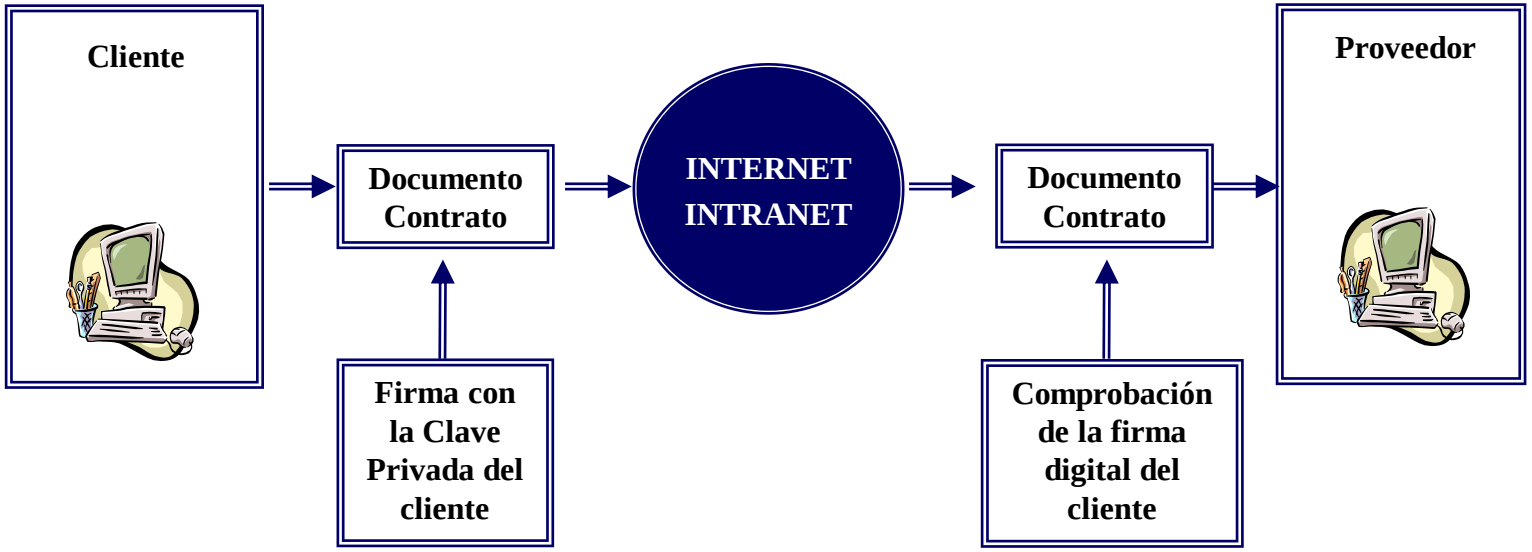
- **CONTRATOS ELECTRÓNICOS** online
- **BANCA ELECTRÓNICA** segura sin repudio.
- Transmisión de **INFORMACIÓN MEDICA CONFIDENCIAL**.
- Contratación de **POLIZAS DE SEGURO**.
- Cotratación de sistemas de **FINANCIACIÓN A PLAZOS**.
- **CONTROL DE ACCESO** en portales verticales.
- Conexión con **SISTEMAS DE FIDELIZACION**. Lotus Notes
- Sistemas de **BOLSA POR INTERNET** sin repudio.
- **AUTENTICACIÓN DE DOCUMENTOS** elaborados por empleados desplazados.
- Relaciones seguras entre miembros de **ENTORNOS B2B Y B2C**.
- **FE PUBLICA** electrónica (pendiente de regulación).
- Emisión de **FACTURAS ONLINE** (e-billing).

.NET consultores

PKI como solución Estándar de seguridad

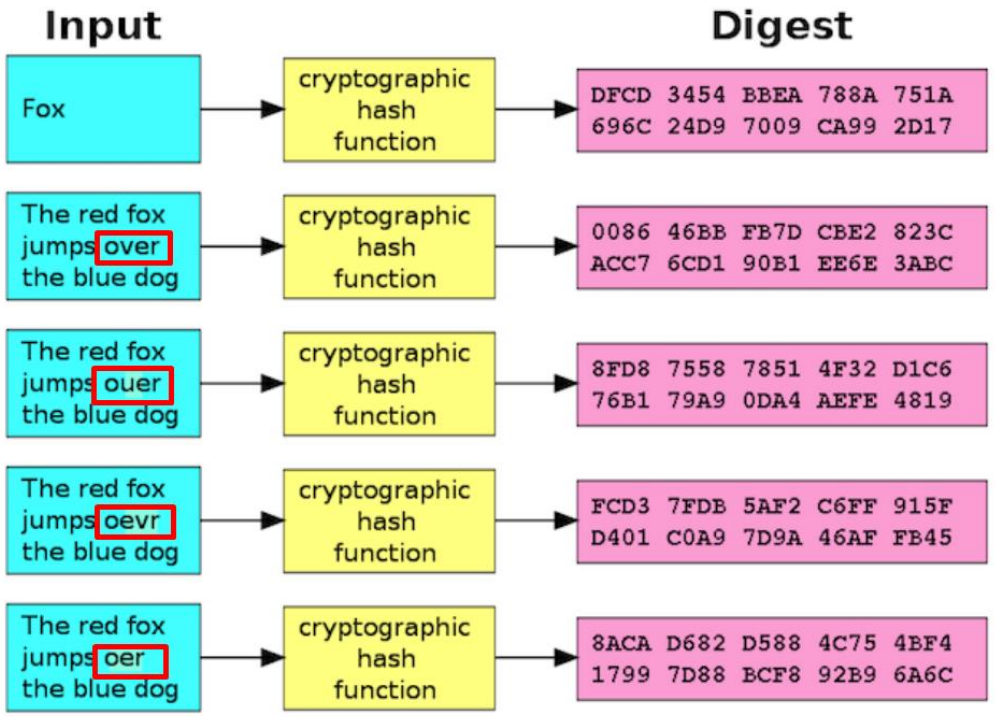
Contratación con Firma Electrónica

- En un entorno de comercio electrónico, en que dos entidades quieran llevar a cabo un acuerdo mediante un contrato, pueden utilizar la firma electrónica como mecanismo para autenticar sus identidades.



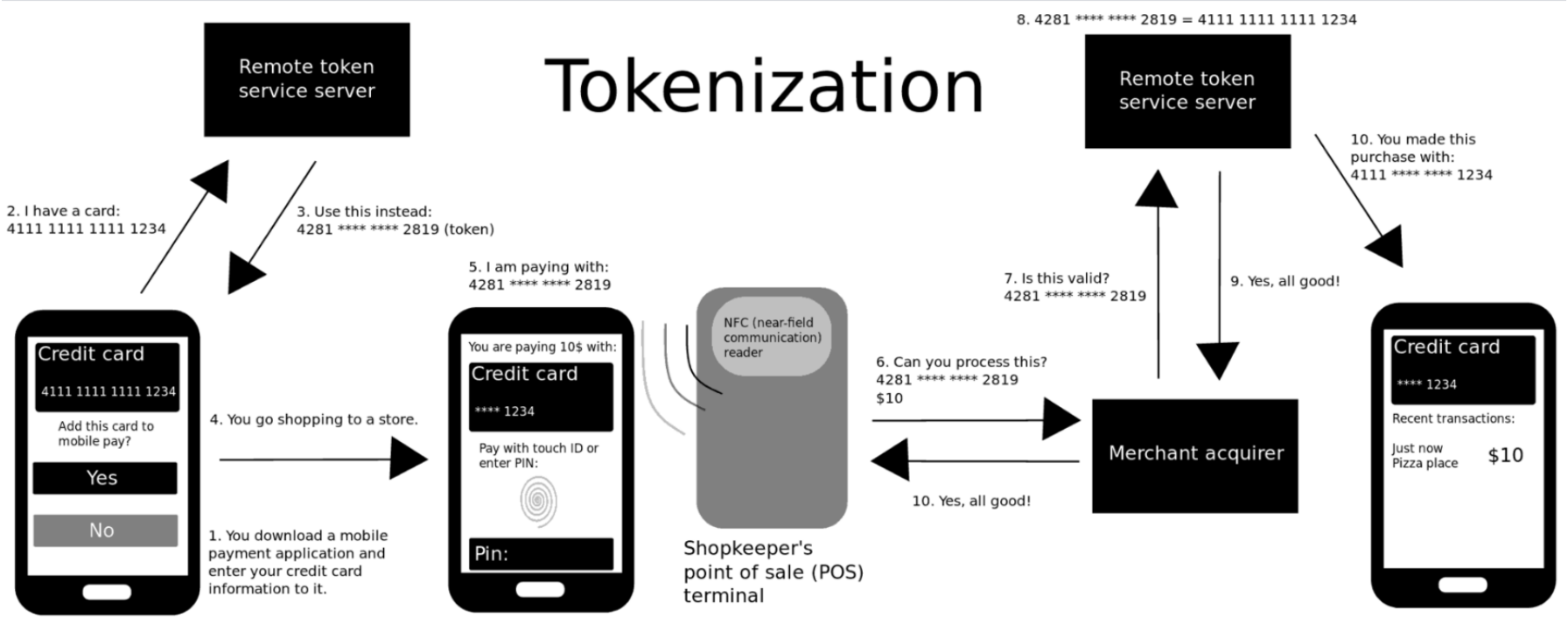
Codigo Hash

Que es un código Hash?



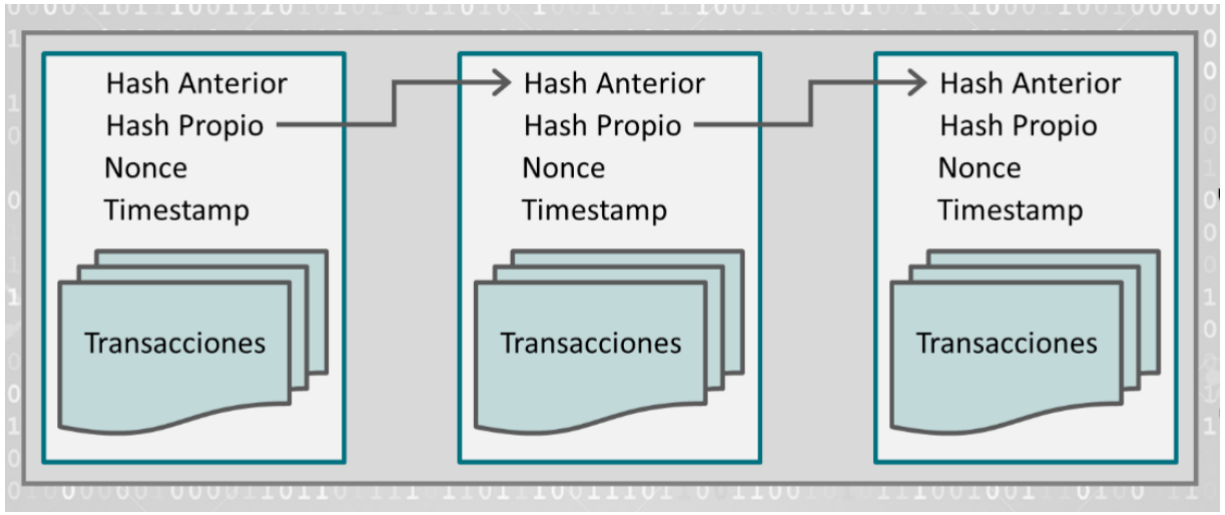
Token

[Que es un token?]



Blockchain

- https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado
- https://es.cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners



Desafios de la Seguridad Lógica
Conceptos claves

La Internet

- https://www.youtube.com/watch?v=i4RE6dBAjH4
- https://www.youtube.com/watch?v=31LE0bPLrhM

Google, Youtube, Redes Sociales

Internet de las cosas

- https://www.youtube.com/watch?v=VTs5y1QlEtk

Cloud Computing o la Nube

- https://www.youtube.com/watch?v=WaxaOlnd_xE
- https://www.youtube.com/watch?v=ao8MyWDHhsA
- Ddd
- La realidad virtual
- https://www.youtube.com/watch?v=OAPmn7POZ6Q
- https://www.youtube.com/watch?v=lX8-WOb5bBg
- https://www.youtube.com/watch?v=uYbsSj6t0V4

Nuevos Conceptos claves

Internet de las cosas

- https://www.youtube.com/watch?v=VTs5y1QlEtk
- La realidad virtual
- https://www.youtube.com/watch?v=OAPmn7POZ6Q
- https://www.youtube.com/watch?v=lX8-WOb5bBg
- https://www.youtube.com/watch?v=uYbsSj6t0V4

BigData

- https://www.youtube.com/watch?v=CcDCqW88uNY
- Un avión que vuela de una punta a otra de EEUU genera 240 Tbyte de datos
- Facebook 500Tbyte de datos en un día
- Bigdata en las redes sociales
- https://www.youtube.com/watch?v=yoSqojO2-CQ