Inter-Parliamentary Union
For democracy. For everyone.

THE NATIONAL ASSEMBLY OF
THE REPUBLIC OF KOREA

World e-Parliament Conference 2014

8 - 10 May 2014 // National Assembly of the Republic of Korea // Seoul

LA SEGURIDAD DEL SISTEMA INFORMÁTICO

Congreso de los Diputados de España

Javier de Andrés Blasco
Director del Centro de TIC

ÍNDICE

World e-Parliament Conference 2009. (noviembre, Washington D.C.)

Ponencia.- *Infraestructura y seguridad: las políticas y sus implicaciones en el ámbito legislativo*

- "Libro Naranja" del Ministerio de Defensa de EEUU
  Editado en 1985, detallaba muy bien los requisitos que debe cumplir un sistema para evaluar su nivel de seguridad. (D1; C1, C2; B1, B2, B3; A1)

- Costes de la seguridad

- Seguridad de la información almacenada y de la que está en movimiento

- *"Un **sistema completamente seguro** es aquel que se encuentra sin conexión a red, apagado, desenchufado y metido dentro de una caja fuerte inexpugnable cuya combinación sólo conoce una persona que se murió el año pasado"*

Referencias

Foro Parlamentario sobre la configuración de la Sociedad de la Información. Mayo 2011, Ginebra
Naciones Unidas, Unión Interparlamentaria, Unión Internacional de Telecomunicaciones

El triple reto de la ciberseguridad: información, ciudadanos e infraestructura

Ponencia.- *Garantizar la seguridad de infraestructuras esenciales*

- Legislación española. (Real Decreto 3/2010, de 8 de enero). La ley no sólo aconseja, la ley obliga a la Administración española a proteger sus sistemas informáticos…

- Garantizar la seguridad de infraestructuras esenciales es cada vez más costoso
  - . Máquinas
  - . Recursos humanos (hacking ético, …)
  - . Redes sociales

Momento actual

SE CUMPLEN LAS PREVISIONES

- Desarrollo tecnológico que permite:
  - Mejorar las defensas
  - Proporcionar más y mejores herramientas a los atacantes

- Grupos de extorsión perfectamente organizados y con una gran capacidad técnica y económica

- Campo de actuación a nivel global

- Crecimiento exponencial en la utilización de las TIC facilita:
  - Comunicación de los atacantes
  - Definición de objetivos comunes
  - Puesta en común de la capacidad de proceso

Legislación española

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
http://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330

En aplicación de lo dispuesto en la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (art. 42)
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352

- El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información.

- Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

LEGISLACIÓN ESPAÑOLA TENIDA EN CUENTA EN LA ELABORACIÓN DEL REAL DECRETO

Ley 15/1999 de Protección de Datos de Carácter Personal
http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico
http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

Ley 59/2003 de Firma Electrónica
http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399

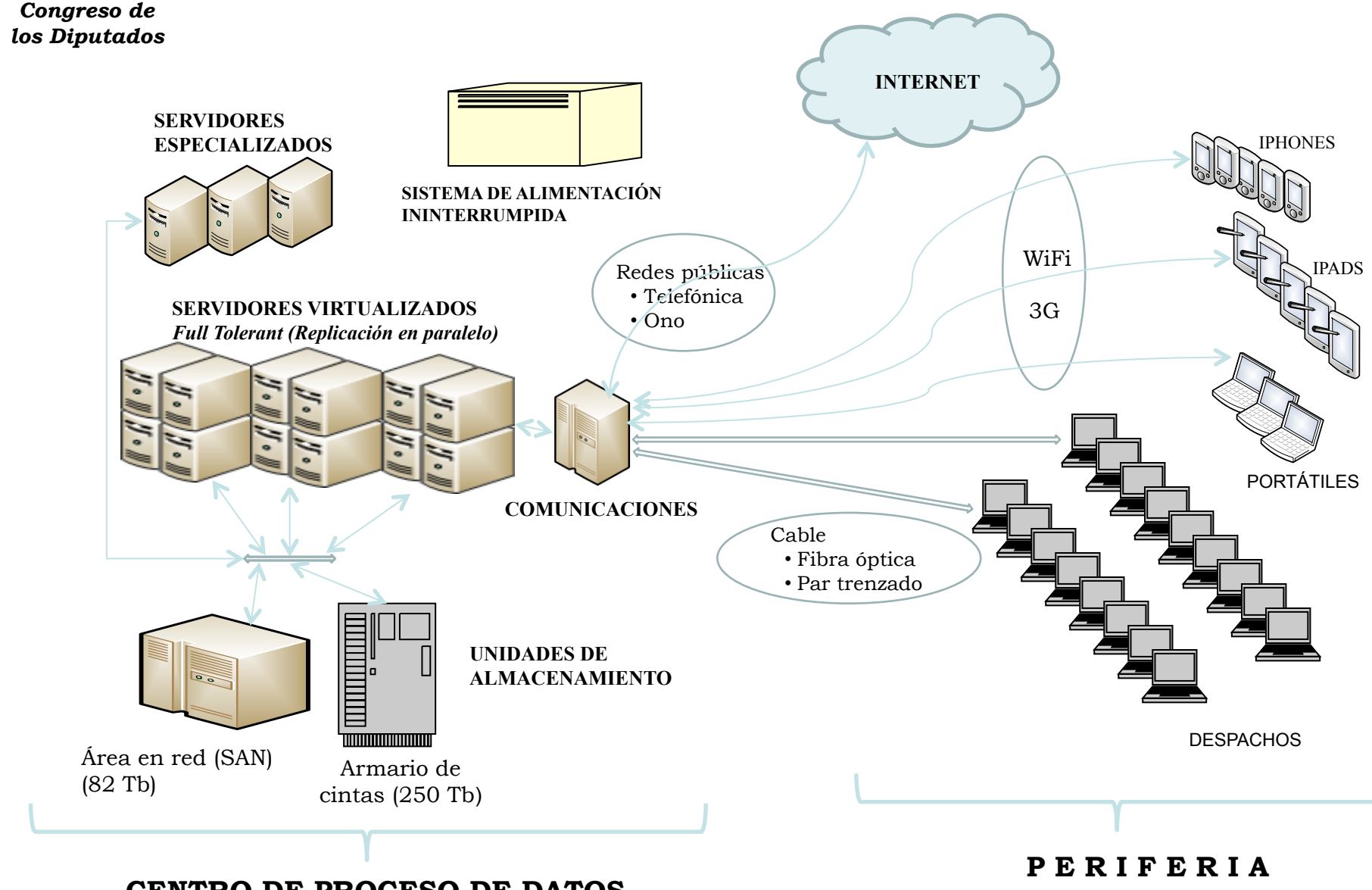
Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352

Ley 37/2007 sobre reutilización de la información del Sector Público
https://www.boe.es/buscar/doc.php?id=BOE-A-2007-19814

SISTEMA INFORMÁTICO

Esquema básico de la infraestructura

Lo que hay que proteger

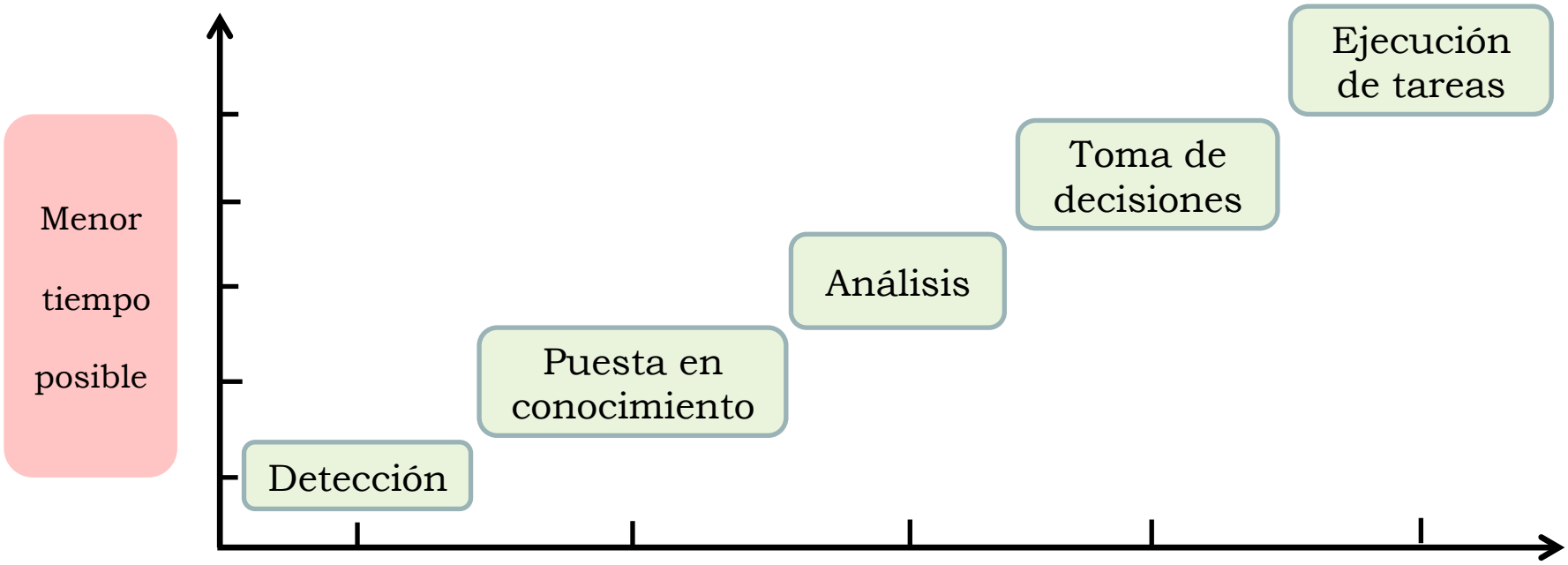


Congreso de los Diputados

PRINCIPIOS BÁSICOS

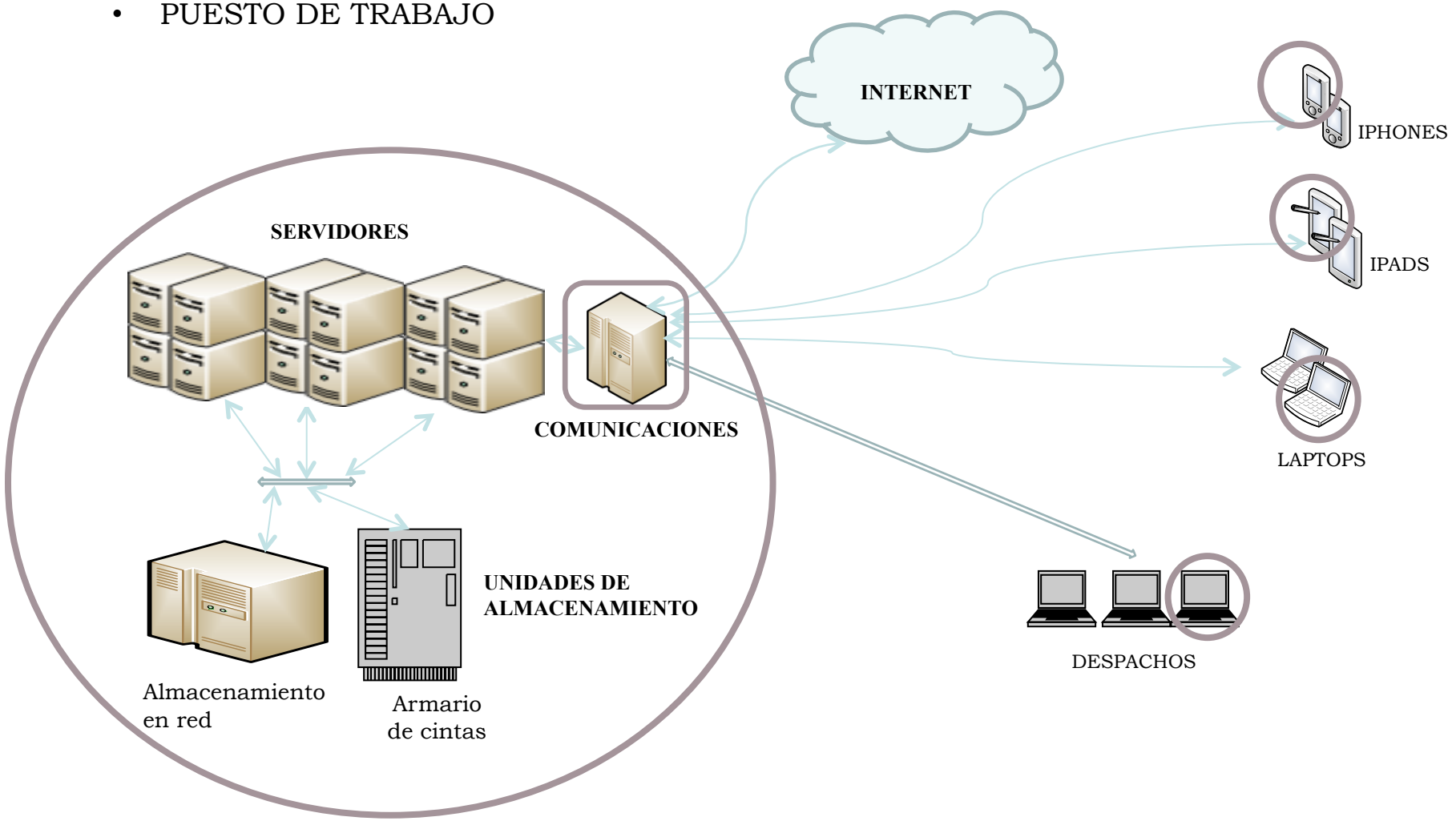
PREVENCIÓN → DETECCIÓN → RESPUESTA → RECUPERACIÓN

PROTOCOLO DE ACTUACIÓN

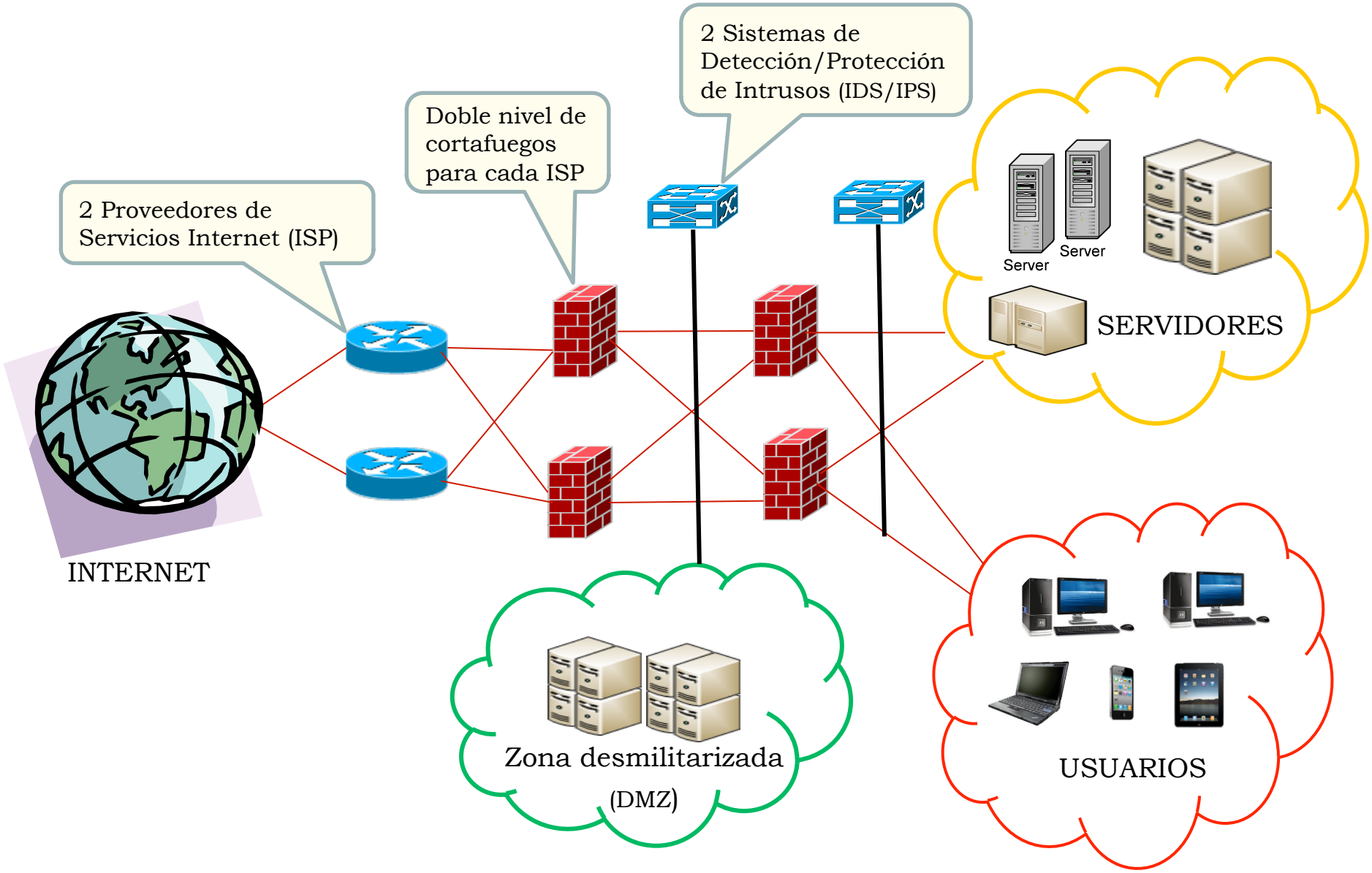


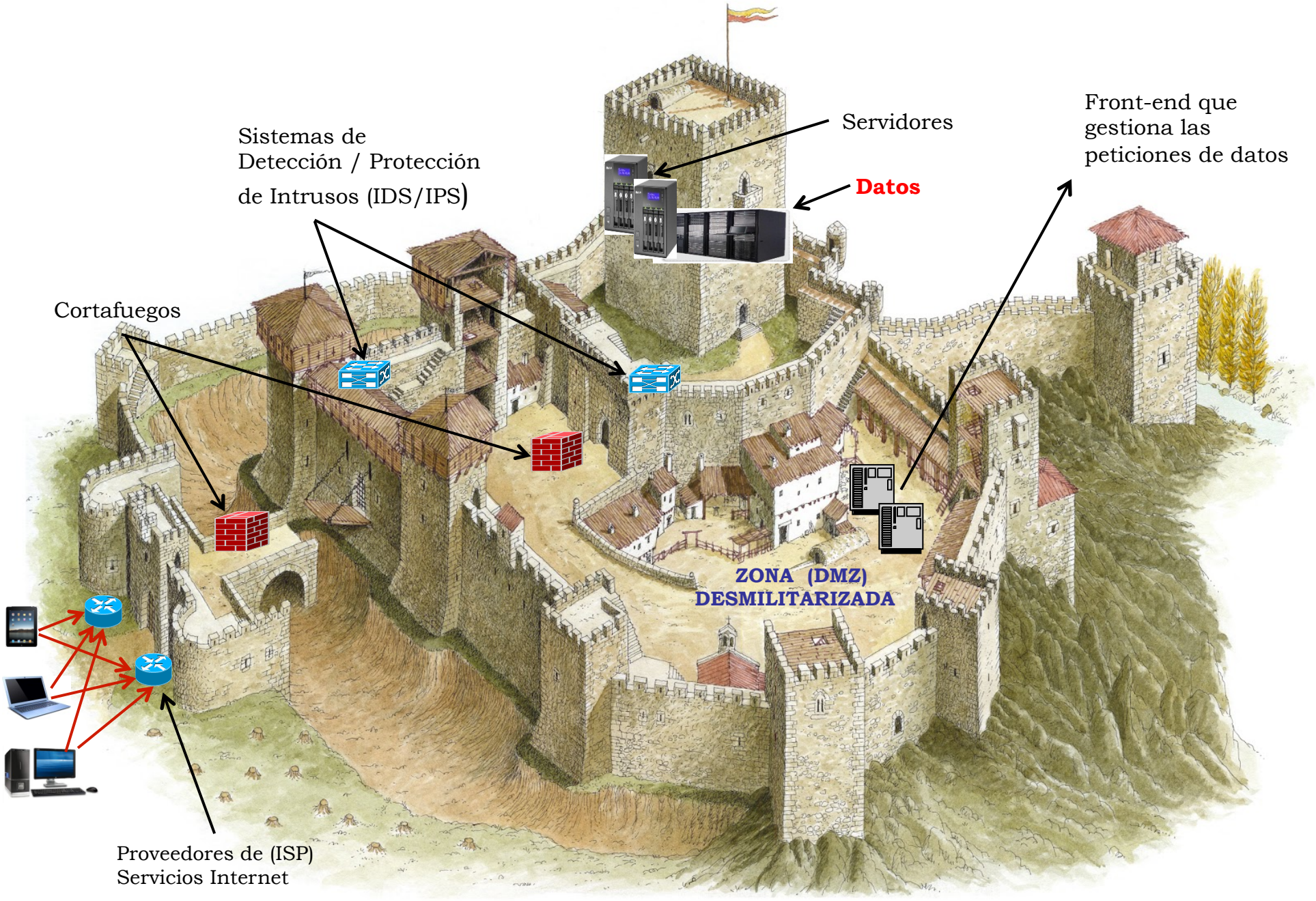
DOBLE NIVEL DE PROTECCIÓN

- PERIMETRAL
- PUESTO DE TRABAJO

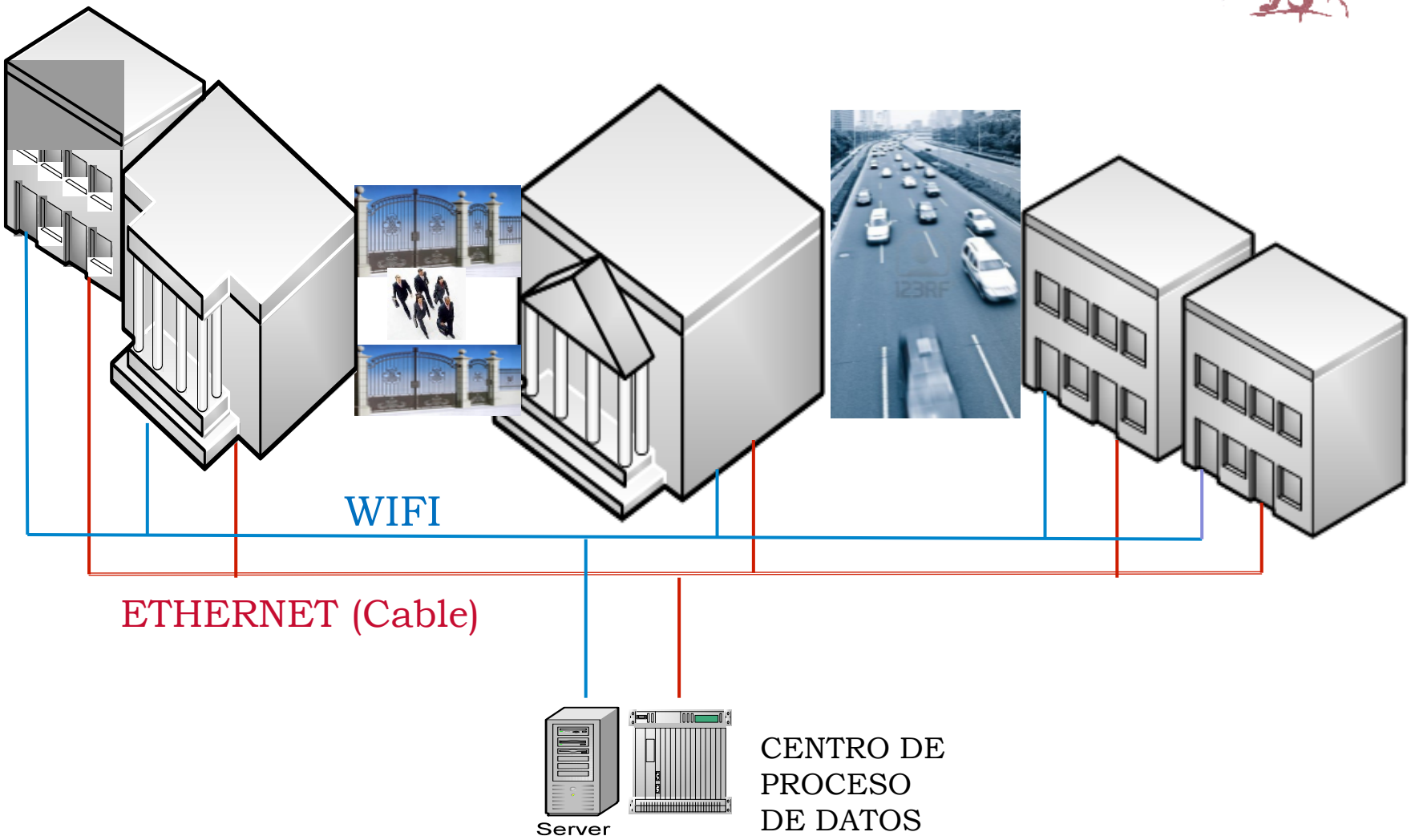


Infraestructura de seguridad




Sistemas de
Detección / Protección
de Intrusos (IDS/IPS)
Servidores
Datos
Front-end que
gestiona las
peticiones de datos
Cortafuegos
ZONA (DMZ)
DESMILITARIZADA
Proveedores de (ISP)
Servicios Internet

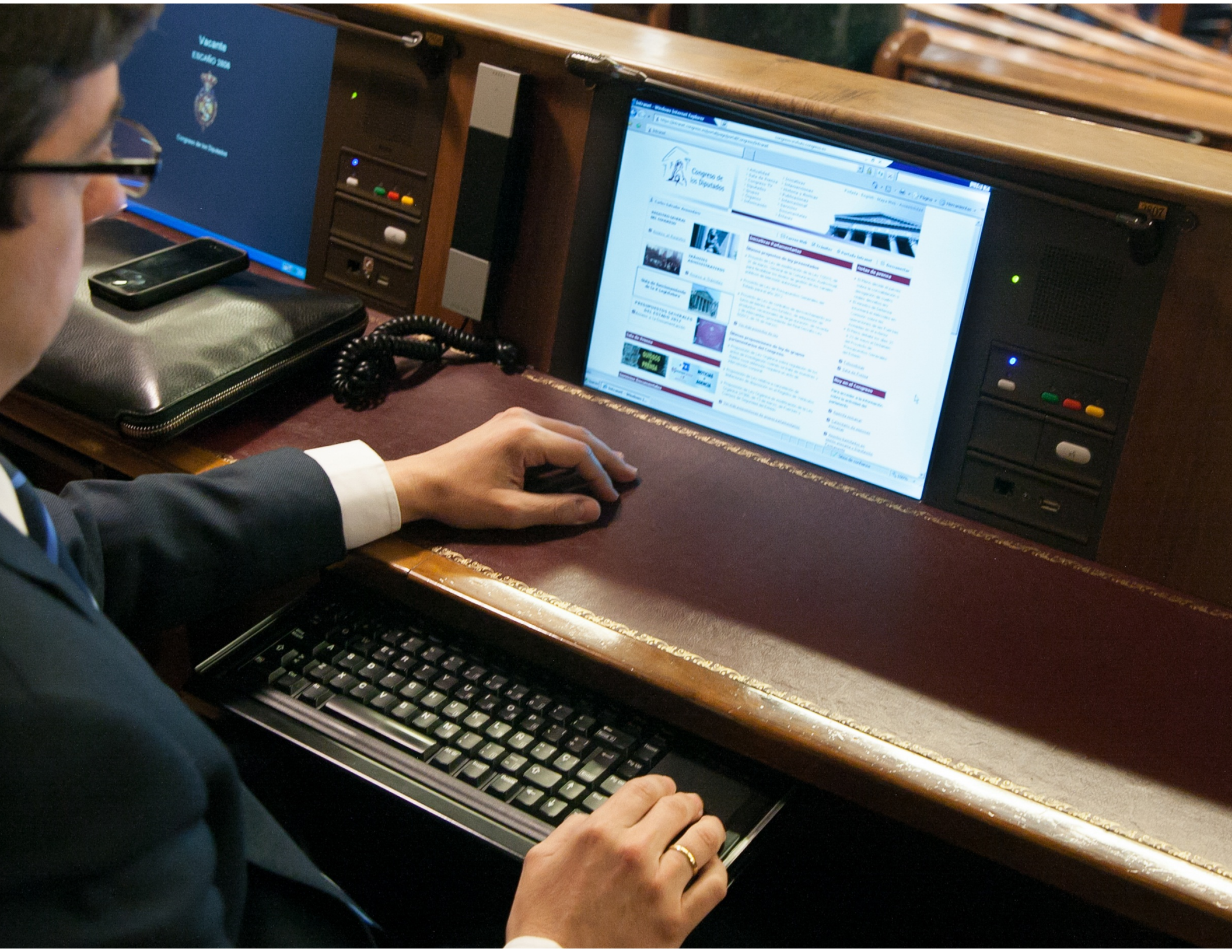
Redes de comunicaciones

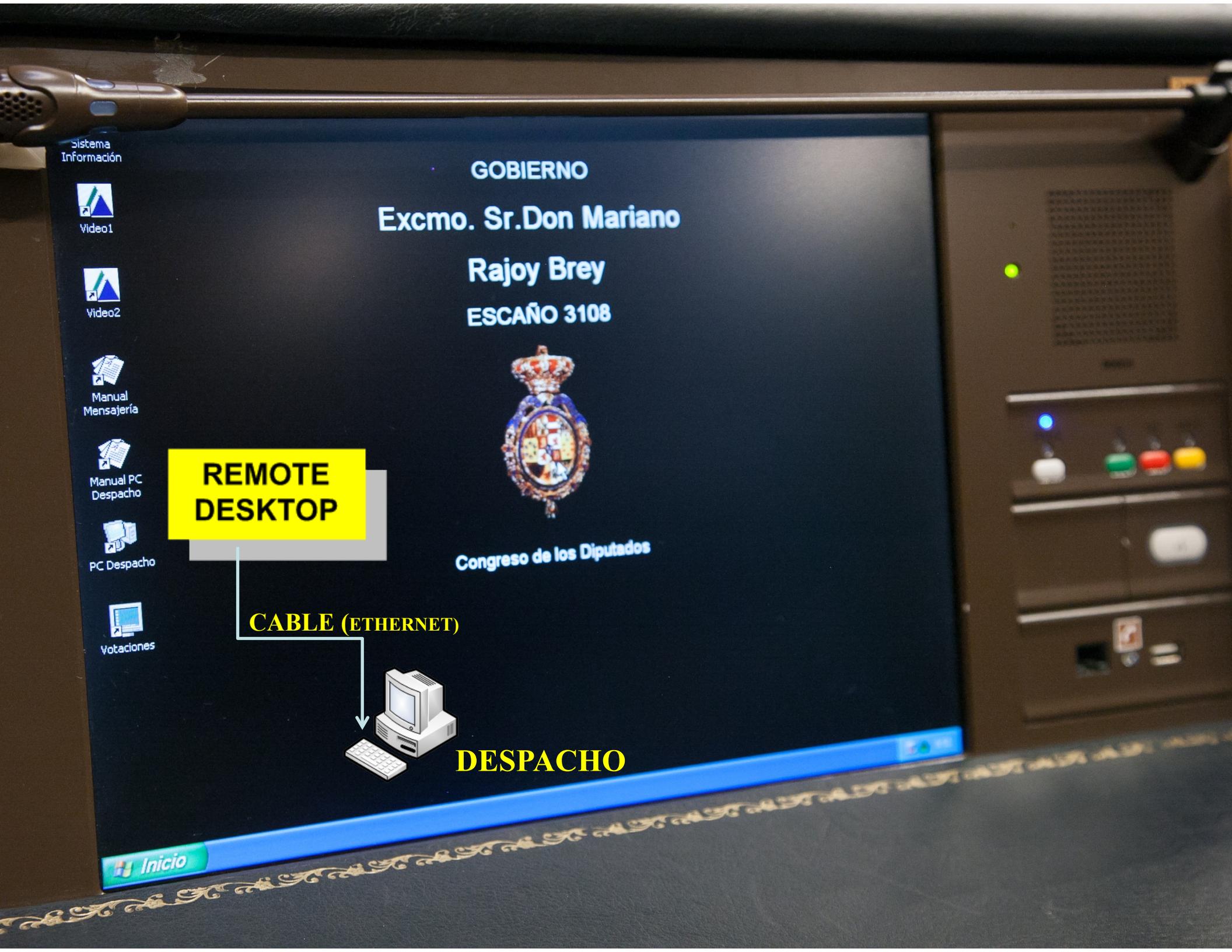


- CABLE (ETHERNET IEEE 802.3)
  - 1.500 PCs (Securizada; Certificado: 802.1x)
  - 350 Thin-Clients (Hemiciclo)

- WIFI (IEEE 802.11g, n)
  - SECURIZADA (Certificado: 802.1x) → Diputados, Funcionarios, …
  - ABIERTA ..... → Periodistas; Visitantes, …


THIN CLIENT

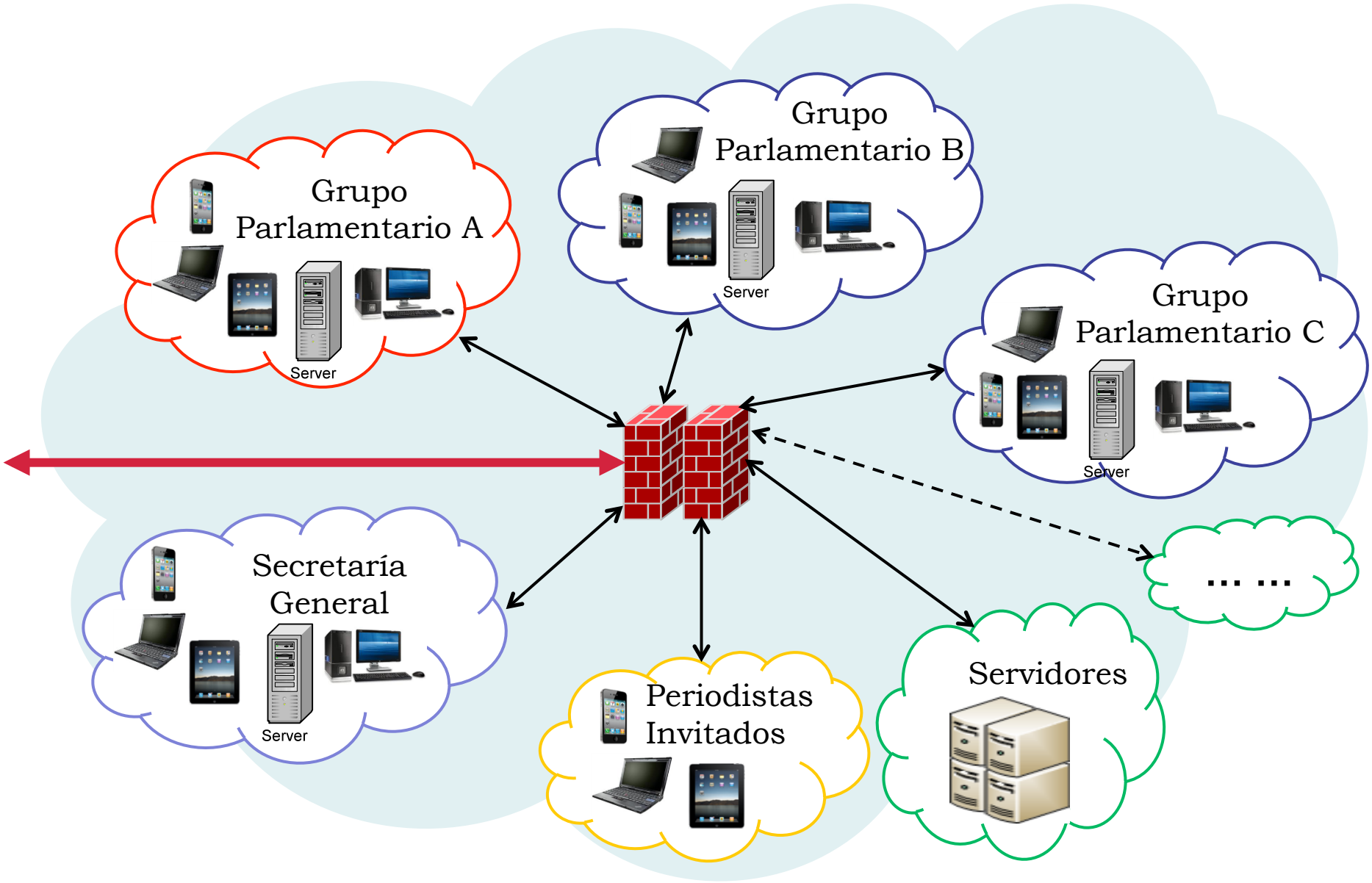

Vacante
Congreso de los Diputados


Sistema Información
Video1
Video2
Manual Mensajería
Manual PC Despacho
PC Despacho
Votaciones
GOBIERNO
Excmo. Sr.Don Mariano
Rajoy Brey
ESCAÑO 3108
Congreso de los Diputados
REMOTE DESKTOP
CABLE (ETHERNET)
DESPACHO
Inicio

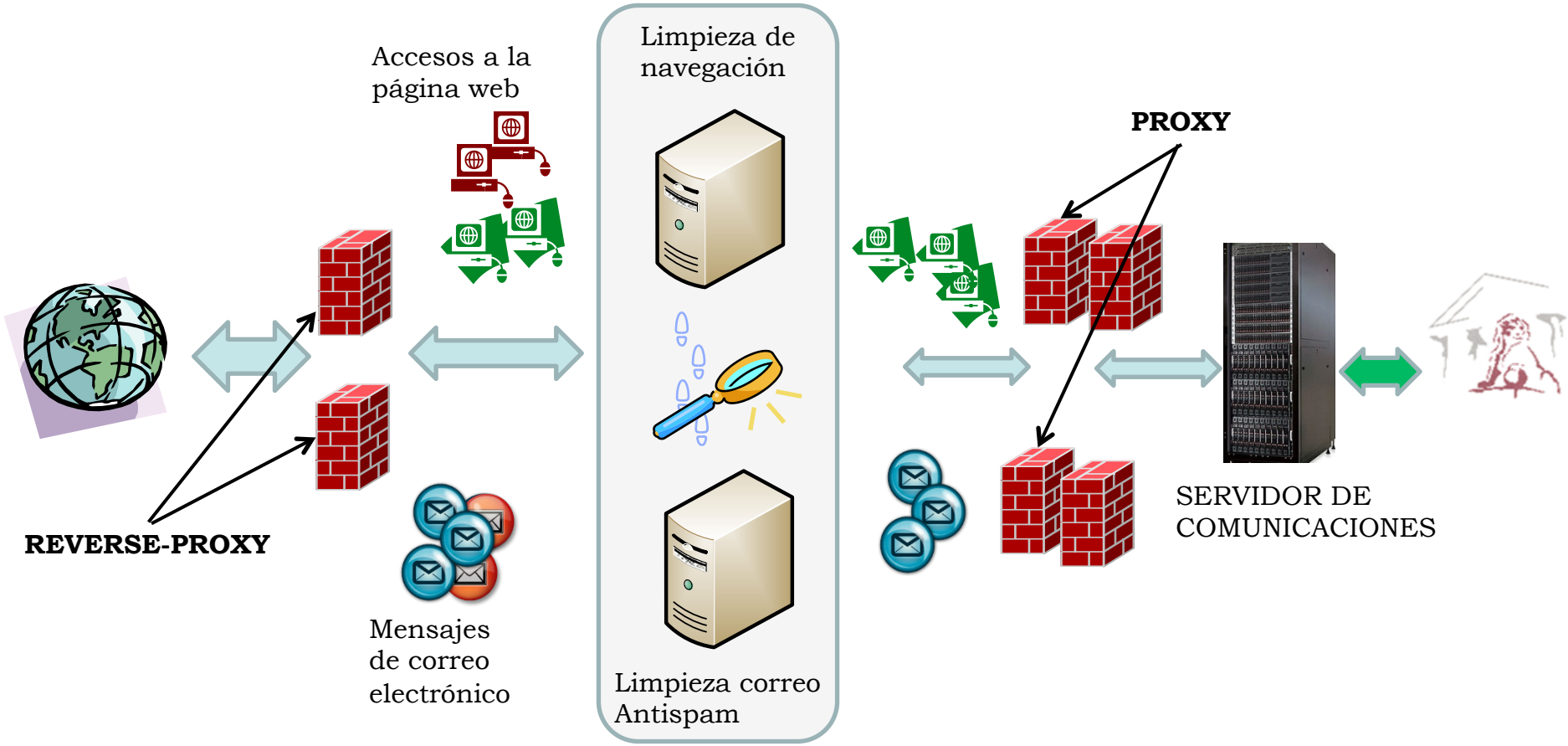
CONFIGURACIÓN DE LA RED INTERNA

- La red interna se configura en **distintas redes virtuales de área local** (VLANs), cada una de ellas destinada a un colectivo específico
  - Cada Grupo Parlamentario tiene la suya
  - Existen otras reservadas a:
    - Secretaría General
    - Periodistas, visitantes, etc.
    - Servicios informáticos
    - … … …
- Funcionan con acceso totalmente independiente
- Esta configuración afecta a las dos redes, tanto a la de cable como a la WiFi
- Cada dispositivo (PC, Laptop, iPad, iPhone) se conecta de forma automática a la VLAN a la que pertenece, siempre que tenga instalado el certificado electrónico correspondiente
- Otros dispositivos externos que no tienen certificado se conectan a la VLAN definida para periodistas, invitados, etc.

RED INTERNA – REDES VIRTUALES DE AREA LOCAL (VLANs)



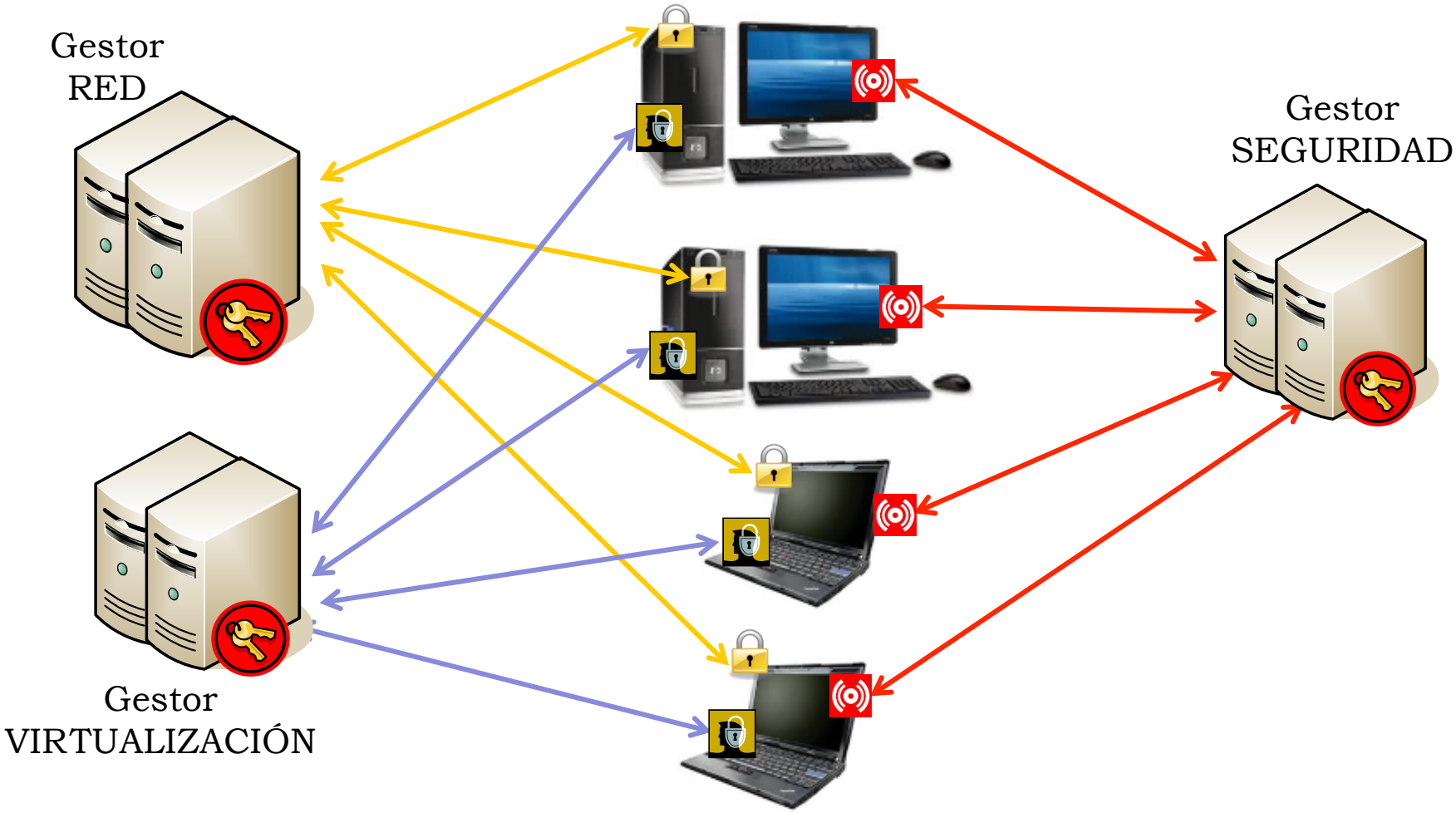
PROTECCIÓN PERIMETRAL



PUESTOS DE TRABAJO (PCs y LAPTOPs)

- Protección con antivirus y firewall local
- Gestión de seguridad mediante un servidor centralizado
- Actualización continua de firmas de seguridad
- **Certificado de equipo** para conexión a la red. Cada equipo conectado por CABLE o por la WIFI securizada se conecta a la red virtual de área local (VLAN) a la que pertenece su usuario
- **Certificado de usuario** para acceso a aplicaciones virtualizadas y, en el caso de portátiles, para el acceso remoto

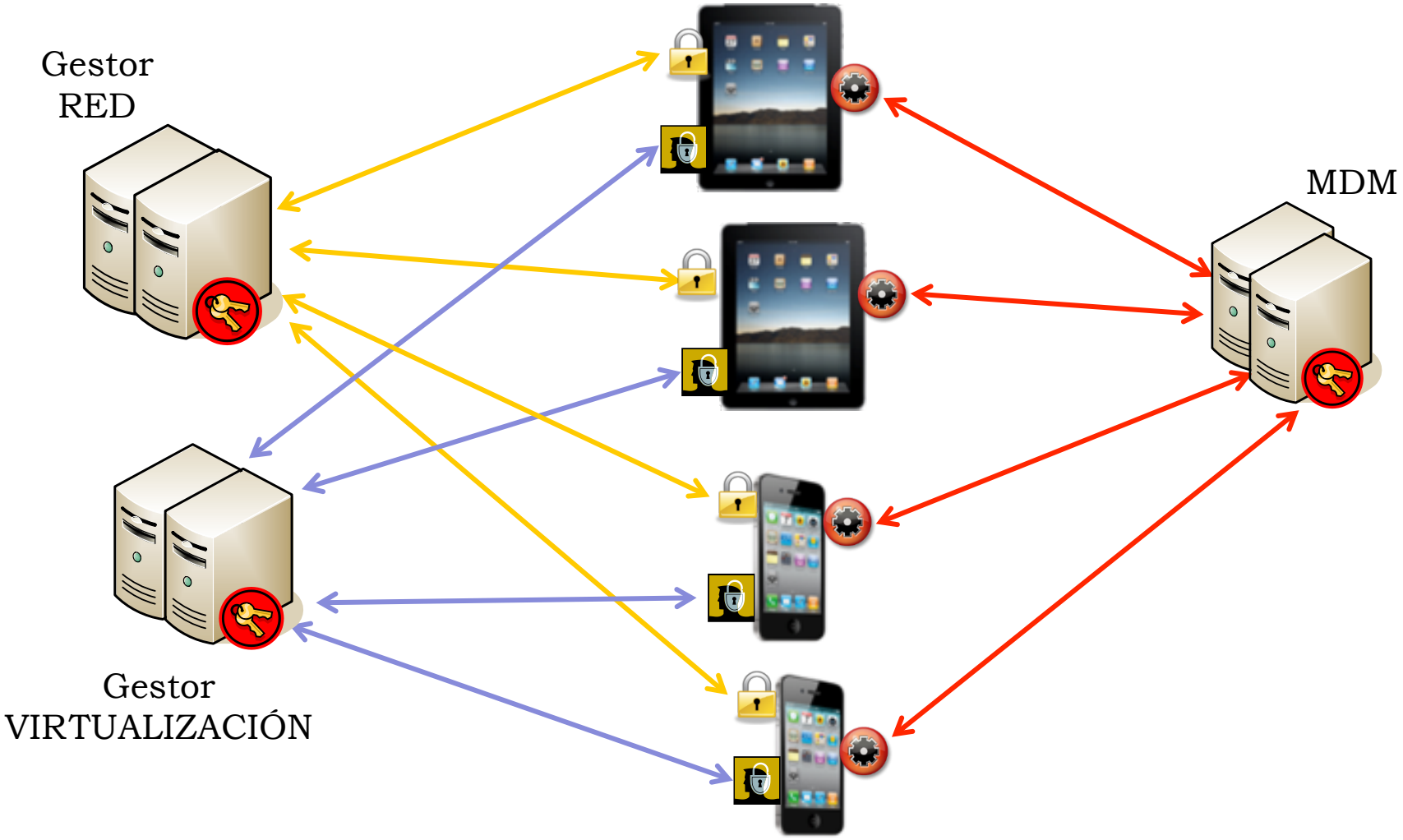
PUESTOS DE TRABAJO (PCs y LAPTOPs)



DISPOSITIVOS MÓVILES (iPad y iPhone)

- 800 dispositivos
- Gestionados mediante MDM (Mobile Device Management) que contempla: seguridad, protección y distribución de aplicaciones
- **Certificado de equipo** para conexión a red. Cada dispositivo se conecta mediante la WIFI securizada a la red virtual de área local (VLAN) a la que pertenece su propietario
- **Certificado de usuario** para acceso remoto a la red interna del Congreso. Virtualización de aplicaciones

DISPOSITIVOS MÓVILES (iPad y iPhone)



ATAQUES MÁS HABITUALES

- Intentos de escaneo de puertos y de servidores. Muy frecuentes
- Denegación de servicio - DDoS (Distributed Denial of Service) - Envío masivo de peticiones a los puertos del servidor web y del correo electrónico
- Envío masivo de correos con el fin de saturar los buzones de los diputados (no siempre spam)
- Envío masivo de fragmentos UDP (User Datagram Protocol). Los ataques más enérgicos intentan colapsar el ancho de banda de los Proveedores de Servicios de Internet (ISPs)
- Recientemente, desde varios países, intentos de aprovechar la vulnerabilidad “Heartbleed” de OpenSSL

OBJETIVOS DEL ATAQUE

La práctica totalidad de la información gestionada en el sistema informático es pública

La mayoría de los ataques están dirigidos a impedir el normal funcionamiento del trabajo parlamentario y su difusión a través de Internet

En menor medida tienen como objetivo descubrir hipotéticas debilidades del sistema (respuesta: hackers éticos)

Los ataques más frecuentes se encaminan a:

- Bloquear o suplantar la página web
- El envío masivo de mensajes con objeto de saturar los buzones de correo electrónico
- Acceder a la zona técnica restringida con diferentes intenciones

"RAZONES" DE LOS ATAQUES

- Forma de respuesta contra:
  - decisiones políticas y económicas
  - legislación
  - intervenciones parlamentarias o de personas relevantes en el campo político y económico
- Reto tecnológico
- Para obtener notoriedad

ATACANTES

- Colectivos organizados que reivindican cambios y los exigen fuera de lo establecido por la normativa
- *Freelances* tecnológicos
- Campañas ciudadanas en las redes sociales ante hechos o decisiones que consideran relevantes
- Personal interno

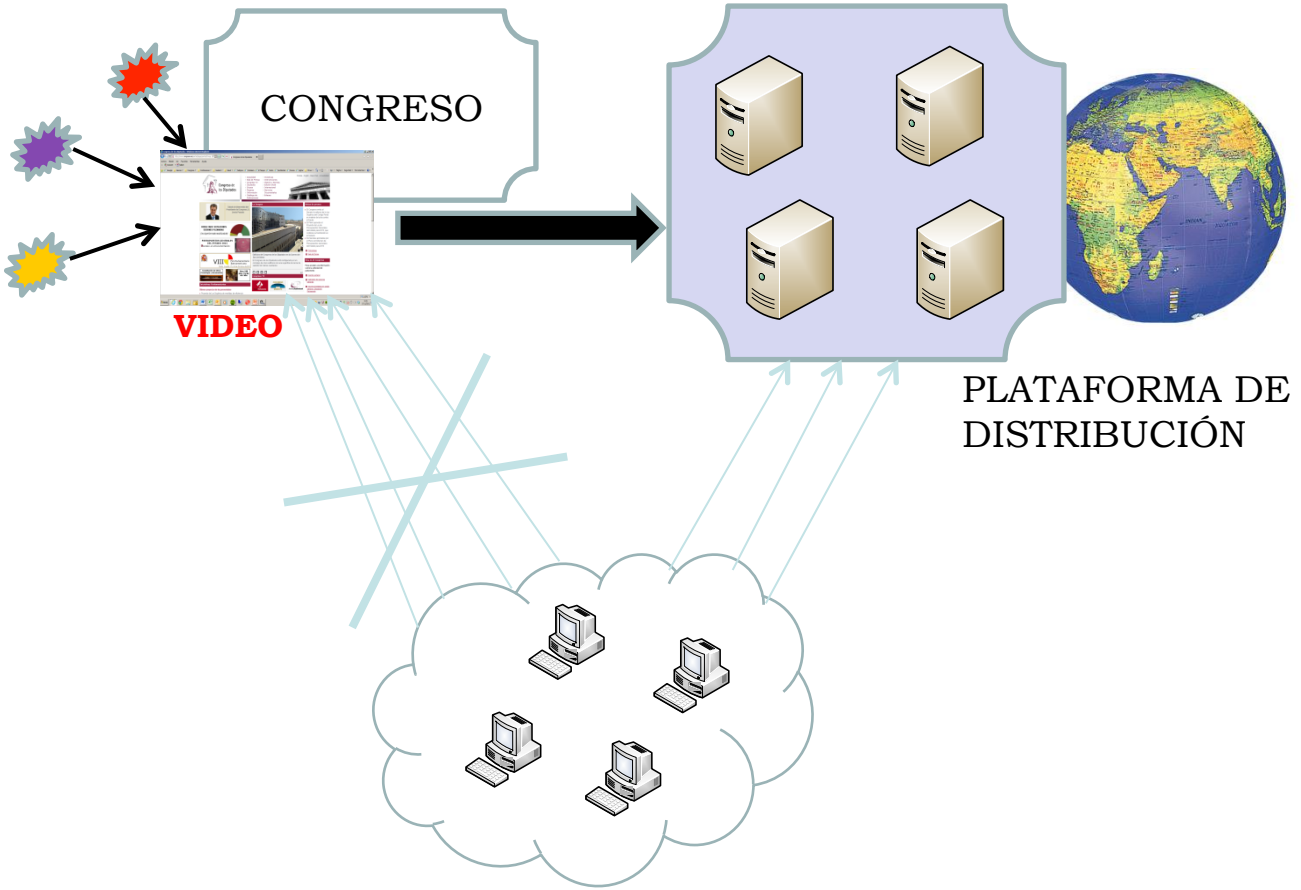
Ejemplo de evolución prevista

REUBICACIÓN DE LA PÁGINA WEB

Ataques continuos
(fines de semana)

En ocasiones:

- con muchos medios
- muy organizados
- apoyo internacional



Resistencia

- Aprendizaje
- Gran dedicación
- Discreción

RECURSOS HUMANOS

- Centro de TIC del Congreso de los Diputados

  Ejecuta la política de seguridad y activa el protocolo de actuación

- Asistencia técnica externa

  Ejerce labores de vigilancia y asesoramiento técnico en horario 24x7

- Suscripción a las alarmas y contacto con el CERT (*Computer Emergency Response Team) del* CCN (Centro Criptológico Nacional) español, que tiene la capacidad de respuesta a incidentes de seguridad de la información

MUCHAS GRACIAS POR SU ATENCIÓN

JAVIER DE ANDRÉS BLASCO
DIRECTOR DE TIC
CONGRESO DE LOS DIPUTADOS
ESPAÑA