CABLE & WIRELESS

Seguridad en Redes Corporativas

José Manuel Fresno
Director de Tecnología
Cable & Wireless
17/06/2004

Agenda

- Punto de Partida: Claves actuales
- Problemáticas de Seguridad e Integridad en las Redes Corporativas
- Servicios de Seguridad proactiva en Redes Corporativas
- Solución VPN: Modelo de Intranet
- Modelo de Protección Perimetral y Seguridad Preventiva
- Recomendaciones Generales de Seguridad en las Redes de Datos
- Marco Legislativo. Soporte a la Seguridad
- Conclusiones

Punto de partida: Claves actuales

- **Evolución de la Tecnología**
  - Disponibilidad de ancho de banda
  - Aumento exponencial de la capacidad de proceso
  - Movilidad de los usuarios
  - Acercamiento de la tecnología al usuario final
  - Alta difusión de la información a través de Internet
  - Dependencia de las redes telemáticas.
- **Convergencia IP**
  - Consolidación de TCPIP como protocolo de transmisión de datos
  - Proliferación de servicios en las redes IP. Voz, video,...
- **Extensión del uso de servicios y aplicaciones electrónicas**
  - Consolidación de aplicaciones en La Red, (e-Comerce, e-banking, e-Learning, e-Medicine, IRC,...)
  - Incorporación de procesos y tramitaciones a través de documentos digitales. (DNI , Pasaporte, Declaraciones ...)

Punto de partida: Redes Publicas y Redes Privadas

- **Terminología:**
- Redes Internas: Soportadas sobre canales de comunicaciones propios
- Redes externas (Extranet): Soportadas sobre canales de comunicación ajenos.
- Red Intranet: Red externa que se comporta hacia los usuarios como interna
- **Aspectos reseñables:**
- Internet se ha consolidado como método de enlace extra e intranet. Las empresas valoran internet como un medio de rendimiento suficiente para conexión de sus oficinas
- La diferenciación entre red privada y publica se desarrolla a nivel virtual.
- La interrelación INTRANET- EXTRANET es confiada a pasarelas integradas en la red de la empresa

Se requieren nuevos recursos y elementos de protección.

Problemáticas de Seguridad e Integridad en las Redes Corporativas

CABLE & WIRELESS

Riesgos y Problemáticas en un mundo abierto

- **Hackers, Crackers, Phreakers,...**
  - Proliferación y Especialización de atacantes a las redes.
- **Ataques a la información**
  - Alta diversificación de ataques y difusión de Virus
    - Gusanos, Troyanos, Java scripts, códigos maliciosos,...
  - Modificación de información
- **Intrusión en la Intranet:**
  - Acceso a información sensible.
  - Evasión de información confidencial y estratégica
- **Denegación de Servicio (DoS) y Bloqueo de recursos**
  - Relay,
  - Bloqueo de aplicaciones y servidores
  - SPAM
  - Aplicaciones P2P
- **Suplantación de Identidad**
  - Suplantación de correos , archivos adjuntos dañinos,falsificaciones

Claves de Seguridad Básica

¿Como actúa un Hacker?

- **Sondeo de puertos**

  - Acceso a través de puertos no bloqueados en los servidores del cliente.

- **Aprovechamiento de Bugs en Aplicaciones**

  - Acceso a través de errores ó situaciones de mal funcionamiento en demonios activos.
  - Fallos de seguridad en los Navegadores de Internet

- **Desbordamiento de buffer**

  - Sobreescritura de espacio de memoria y paso de código malicioso al programa para su ejecución.

- **Cracking de contraseña**

  - Acceso como administrador por usuario default ó acceso a fichero de contraseñas. Suplantación de identidad

Claves de Seguridad Básica

¿Cómo actúa un Hacker?

- **Ataque distribuido:** Denegación de servicio por desbordamiento de memoria. Introdución de troyanos para ataque coordinado

- **Introducción de Virus:** Difusión de Virus Conocidos y Virus Desconocidos y otros códigos activos maliciosos (ActiveX, Java) nuevos- que pueden atacar antes de que la tabla de firmas lo incluyan-.

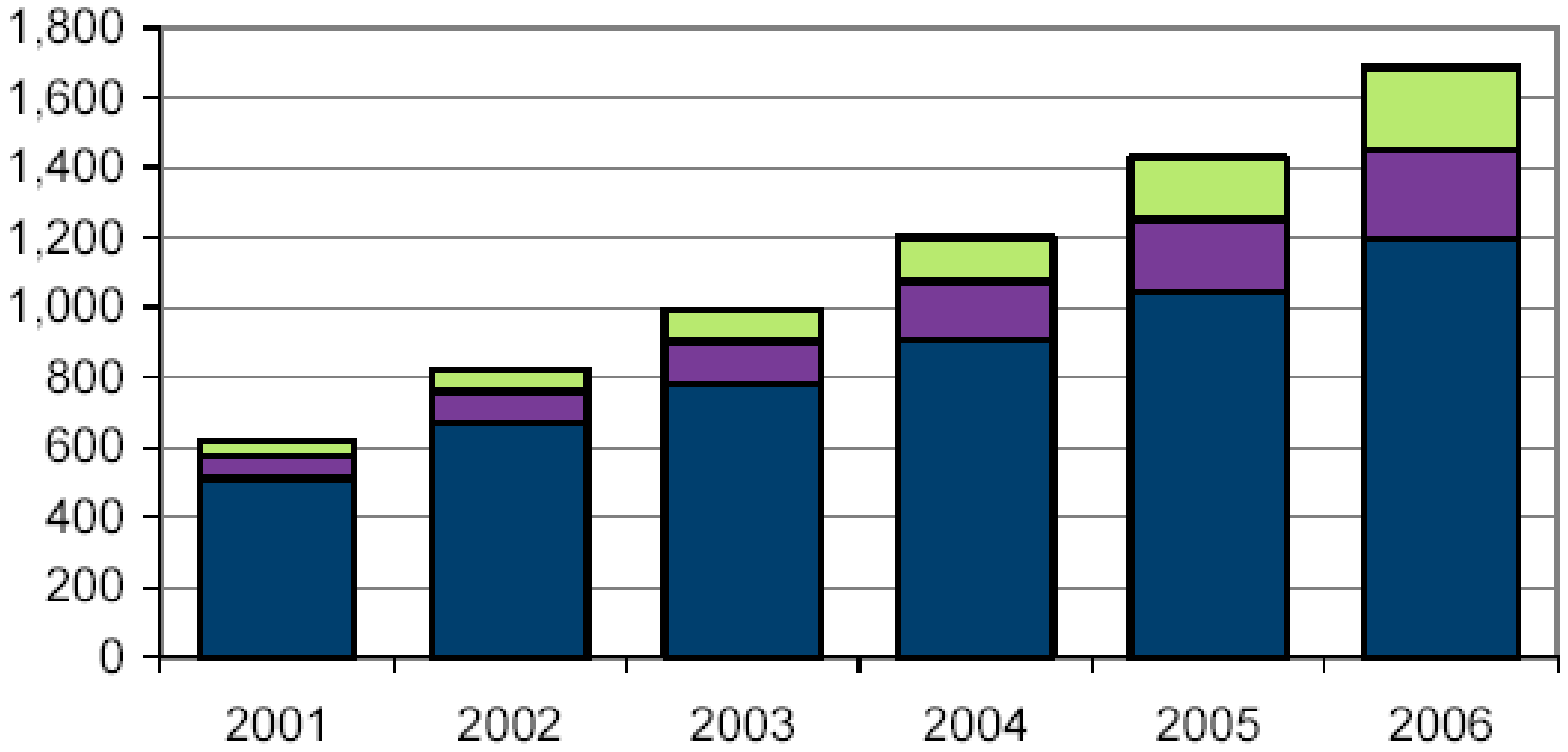
- **Exploits:** Comprometen la seguridad y son utilizados por los hackers para introducir código malicioso de rápida propagación.

- **Scripts Maliciosos:** Inclusión de instrucciónes concatenadas. Son fáciles de construir y se extienden rápidamente.

- **Cookies.** Control de objetivo. Comprometer la privacidad e incremento de spam.

- **Documentos MS Office.** Envío de virus en macros así como código malicioso embebido.

Previsión de Inversiones en Securización de Contenidos

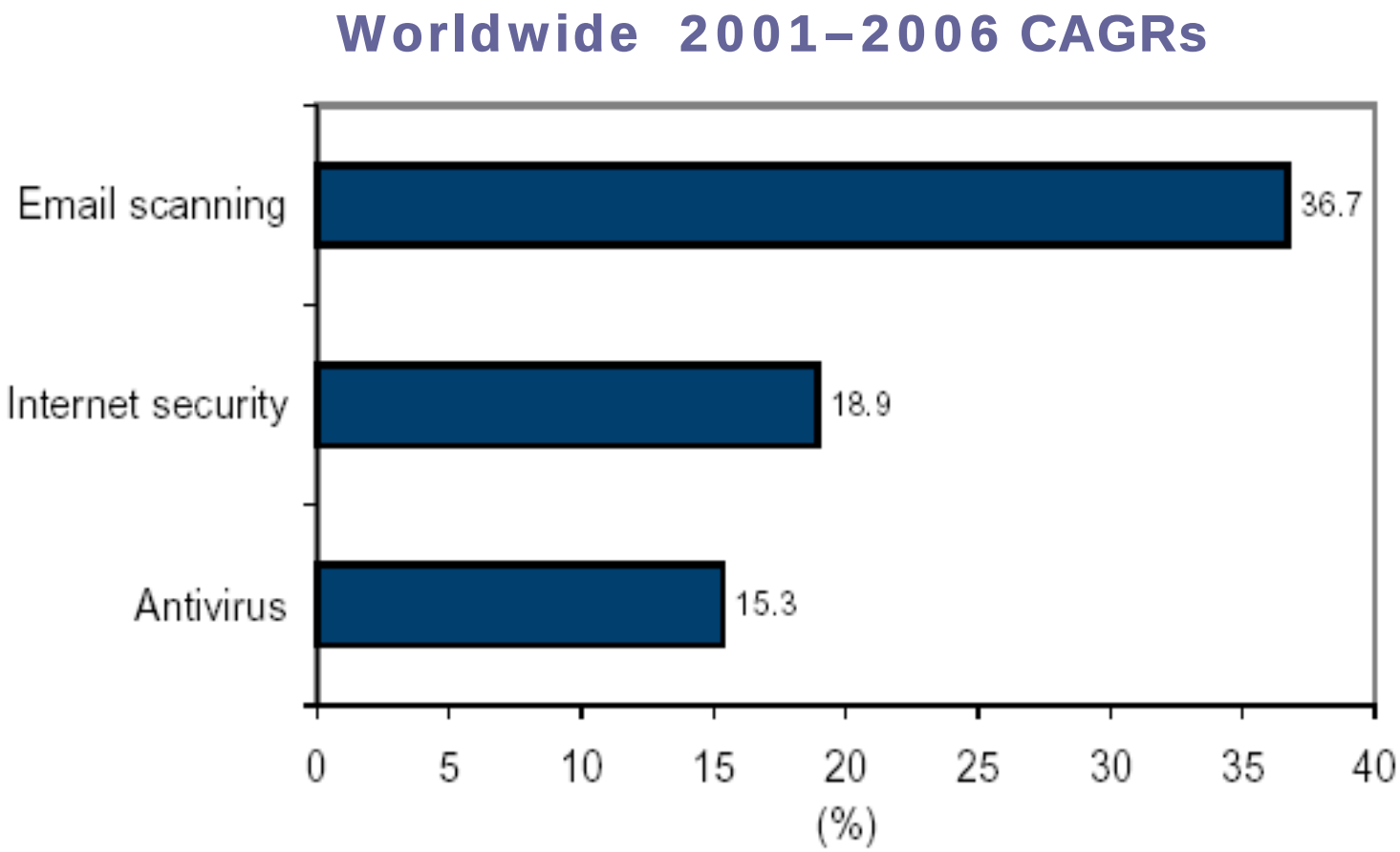


European revenue for SCM software reached $617.6 million in 2001, representing 32.8% growth over 2000.

IDC forecasts that the SCM software market will grow at a 22.2% CAGR and reach $1.6 billion in 2006

*fuente: IDC 2004

Distribución de Inversiones previstas en Protección de seguridad de Contenidos



*fuente: IDC 2004

El problema del e-mail: Difusión de Virus

- La protección antivirus del puesto de usuario no es suficiente.
- El 83% de las infecciones están relacionadas con el servicio de e-mail (Ficheros adjuntos, gusanos, troyanos...)
- Los ataques de virus son de carácter polimorfico y evolutivo
- En la actualidad se reconocen mas de 60.000 virus distintos*
- Se reconocen mas de 500 nuevas variaciones de virus al mes.*
- El crecimiento es exponencial:
  - Actualmente mas de un 150 de cada 1000 PC´s sufren un incidente relacionado con ataques virales al mes.*

*ICSA: International Computer Security Association

Evolución de Virus en redes corporativas

- La escala de crecimiento de Virus ha sido exponencial en los últimos años
- Se alcanzan Cotas de 10 % de virus asociados a e-mail *
- 35 virus interceptados por segundo*

*Estadísticas de MessageLabs May 2004:
909 millones de correos analizados

Gráfica de los Top Ten Virus Mayo 2004

Fuente: MessageLabs

(Scaneo global de mas de 45 millones de e-mails al día de mas de 8500 empresas)

El problema del e-mail: Difusión de SPAM

Envío de información no solicitada vía e-mail de forma masiva a través de listas de distribución

El spam es un mal en expansión. Se estima que **mas del 50% del correo** de hoy en dia es spam.

- Como Afecta:
  - Bloqueo de servidor de e-mail por saturación de mensajes
  - Consumo de ancho de banda en las conexiones Internet corporativas.
  - Consumo de tiempo del usuario para selección
  - Saturación de buzón de usuario
  - Impacto directo en la productividad

- Dificultad de tratamiento:
  - Problemas de corte legal:
    - No existe una ley consensuada Internacional al respecto
    - La identificación y localización de los “spammers” puede ser muy complicada .

SPAM en redes corporativas

Perspectivas de crecimiento:

- **Situación actual en EEUU (Estimación Jupiter Media Metrix)**

  - En 2004 las empresas invertirán 1.300 millones de dólares para enviar 43.000 millones de mensajes a sus potenciales clientes.

  - En 2005 el comprador online recibirá una media de 950 mensajes diarios.

- **Situación actual En España (Estimación Domeus)**

  - El 68% de los usuarios de correo recibe algún tipo de mensaje spam

  - La mayoría de los mensajes spam son sobre rumores, sucesos y mensajes en cadena

  - El 64% de los usuarios consideran el spam como un problema

  - La mayoría de los usuarios (86%) no emplea ningún filtro para evitar el spam ni solicita su baja (70%)

Evolución de SPAM en redes corporativas

- La escala de crecimiento de SPAM ha sido exponencial en los últimos años
- Se alcanzan Cotas de Spam alarmantes:

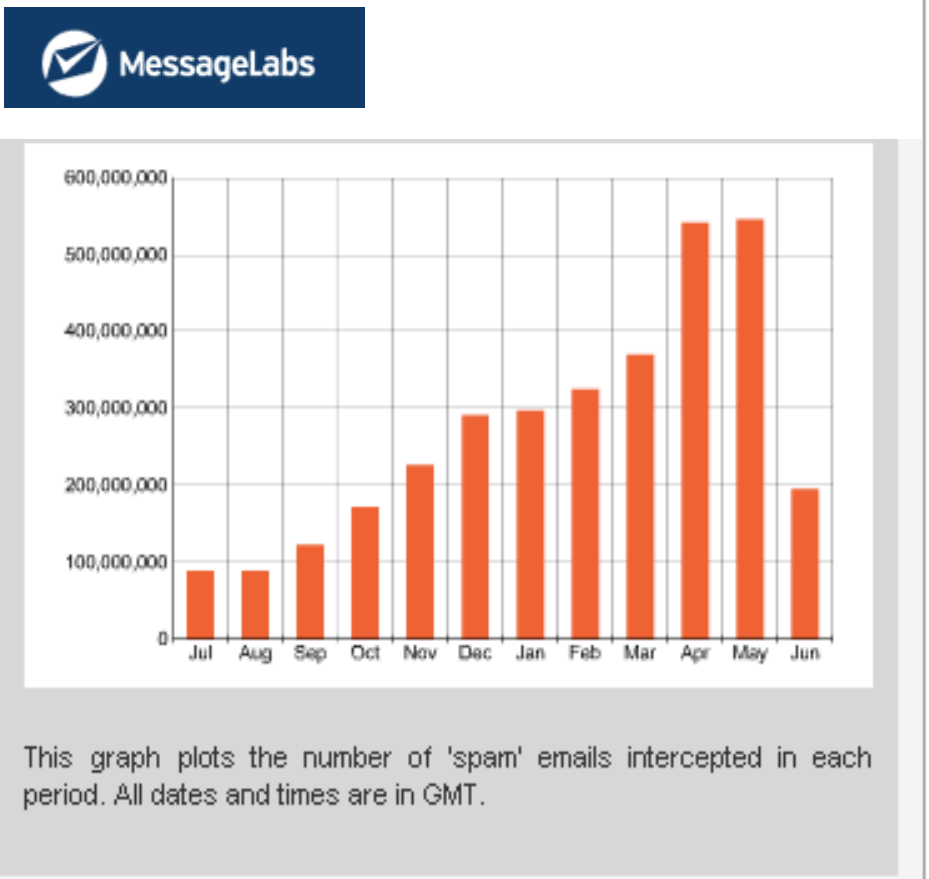
75%*

*Estadísticas de MessageLabs May 2004:
909 millones de correos analizados
691.5 millones no fueron solicitados

Gráfica de SPAM de los últimos 12 meses

Fuente: MessageLabs

(Scaneo global de mas de 45 millones de e-mails al día de mas de 8500 empresas)



Servicios de Seguridad proactiva en Redes Corporativas

CABLE & WIRELESS

Servicios de Seguridad Proactiva

Sistemas de Identificación y Control de Acceso

- **Desde la Red:**

  El mecanismo de autentificación puede incluir elementos de verificación de permisos de usuario:

  – Radius, MS Active Directory, LDAP,…

  – Protocolos de Tunelización y encriptación de datos (L2TP, Ipsec,..)

- **Desde el usuario:**

  La identificación de usuario integra distintos métodos:

  –Elementos Hardware: (Algo que el usuario posee)

  Smartcard, USB Token,Password Token,

  –Sistema de Contraseña: (Algo que el usuario conoce)

  PIN, Contraseña

  –Control Biométrico: (Algo que el usuario es)

  Scan reconocimiento Iris, huella dactilar,…

La identificación en la red debe administrarse de forma centralizada y personalizada

Servicios de Seguridad Proactiva

Sistemas de Firma y Certificación Envío de Información

- **Requerimientos de uso del modelo transmisión electrónica de datos**
  - Auntenticidad del emisor
  - Autenticidad del mensaje
  - Integridad de la información transmitida
  - Garantía de no repudio
- **Sistemas de Certificación**
  - Autoridades Certificadoras: FNMT, ANFE,…
  - Recomendación X.509 CCITT
  - Basados en Clave pública/privada . Encriptación
- **Firma Digital**
  - Verificación de procedencia de un mensaje
  - Generación de firmas de al menos 160 bits

Servicios de Seguridad Proactiva
Plataformas Cortafuegos

Equipamientos de control de tráfico de entrada y salida en nuestra red, basado en políticas de filtrado por tipo de tráfico (puerto TCP ó UDP) y dirección IP.

- **Funciones y características mas valoradas:**
  - Velocidad de paso de paquetes acorde con velocidad de lineas de comunicaciones y segmentos de red
  - Rendimiento acorde con tipo y volumen de tráfico en la red
  - Plataforma escalable. Soporte de clustering y Alta diponibilidad Activa
  - Numero de puertos ampliables (FE y GBE)
  - Filtro de primer nivel contra DoS
  - Aministración remota segura SSH / Radius
  - Gestión de configuración amigable
  - Protocolo ICAP para integración con aplicaciones (AVP´s ó Caches, Trends,...)
  - Inspección profunda de tráfico previo a forwarding
  - Respaldo de actualización por comites y fabricantes solventes
  - Opciones de funciones integradas de IDP, AVP
  - Filtrado de Contenidos

Servicios de Seguridad Proactiva

Servicio de Protección de Intrusión

El servicio IDS se diseña para la identificación y protección de ataques en la red. La acción preventiva de un ataque debe ir orientada a detectar el ataque antes de que éste haya conseguido alcanzar su destino.

- **Bases de funcionamiento**:
  - **Filtrado de tráfico** basado en políticas y firmas de niveles 2 -7
  - **Detección de Anomalías en protocolos**:Permutaciones en uso de protocolo
  - **Detección de puertas traseras:**Detección de tráfico no autorizado disigido a puertos de servidores ó equipos no autorizados
  - **Stateful Inspection.** Detección de patrones de ataque en volúmnes de tráfico relevante
  - **Honeypots**:Desviación de ataques a señuelos virtuales para análisis de origen y tipo de ataque.
  - **Detección de Nivel 2:** Detección de ataques tipo ARP
  - **DoS:** Detección de ataques de denegación de servicio
  - **Spoofing Detection:** Detección de suplantación de direcciones IP
- **Potenciales riesgos de la plataforma:**
  - **Falso negativo:** Ataques no detectados
  - **Falso positivo:** Reconocimiento como ataque de tráfico válido

Servicios de Seguridad Proactiva
Monitor y Gestor de Tráfico

Este tipo de servicios, está orientado a priori a gestión de recursos, dimensionamiento de red, y gestión de fallos, aunque puede colaborar en la identificación de problemas en la red derivado de políticas de uso inadecuado de los canales de transmisión, pudiendo alertar de ataques al administrador de la red .

- **Bases de funcionamiento**:
  - Monitorización on line de equipos de red basada en protocolo SNMP y RMON
  - Generación de alarmas e informes ante superación de umbrales de tráfico preestablecidos
- **Soporte a la seguridad:**
  - Ataques de DoS
  - Aplicaciones P2P no autorizadas
  - Transferencias masivas no autorizadas

Servicios de Seguridad Proactiva
Control Antivirus

Servicios de protección en el perímetro, evitando que los ataques de virus alcancen los servidores de aplicaciones y entorno de usuarios.

- **Funciones básicas del servicio:**
  - Protección multiprotocolo SNMP, FTP, HTTP, POP3,...
  - Protección contra virus basada en actualización continua de firmas reconocidas
  - Protección proactiva contra código malicioso nuevo por análisis previo en entorno de simulación.
  - Protección contra Exploits/Hack como correos bomba, suplantación de correo, agujeros de seguridad, etc.
  - Filtro de correos: tamaño, falsificaciones de archivos, spyware, etc.
- **Potenciales riesgos de la plataforma:**
  - Descarte de correo por falsos positivos
  - Confianza extremada en el servicio, puede descuidar tratamiento antivirus en las estaciones de los usuarios

Servicios de Seguridad Proactiva

Anti-Spam Avanzados

- **Bases de funcionamiento :**

Listas Negras - comprueba si el remitente del correo está en alguna RBL (Realtime Blackhole List), o en un servidor dial-up u open-relay.
Comprobación de DNS - verifica si el remitente utiliza un servidor de correo válido.
Bloqueo por palabras - bloquea correos de acuerdo con ciertas palabras en el Asunto o en el Mensaje.
Anti-spoofing - bloquea correos enmascarados como si vinieran de una empresa conocida.
Cookies - bloquea cookies que ayudan a los spammers a identificar a los destinatarios como cuentas "vivas".
Verificación de Cabecera - inspecciona diferentes firmas de cabeceras y los bloquea si procede.

Análisis Heurístico - detecta y bloquea spam según diferentes características del correo.
Análisis del Texto - categoriza el spam de acuerdo con el contexto como pornografía, hipotecas, viajes, etc.
Firmas de Spam - base de datos actualizable automáticamente que permite detectar y bloquear el spam de acuerdo con las firmas y referencias deSPAM
Filtro de URLs con Spam – bloquea correos con links a lugares o patrocinadores con spam.
Filtro de imágenes Spam – bloquea correos que contienen spam en imágenes asociadas.

Solución VPN : Modelo de Intranet

CABLE & WIRELESS

Bases Generales de VPN

Virtual Private Network

Establecimiento de un canal de comunicación protegido basado en técnicas de Tunelización y Encriptación para transmisión de datos segura a través de una red pública.

- **Tipos de Servicios VPN**

  - **VPN´s de Nivel 2**

    Basadas en circuitos virtuales ATM ó Frame Relay
    Basadas en securización de sesión (SSL)
    Basadas en VPN MPLS de Nivel 2 (Kompella, Martini)

  - **VPN´s de Nivel 3**

    Basadas en Equipo terminal de cliente (CPE)
        Conectividad IPSec establecida entre dispositivos CPE
    Basadas en Network Providers
        Basadas en Redes Centralizadas Ipsec
        Basadas en VPN´s BGP/MPLS

VPN IPSec vs VPN SSL

- **IPSEC IPVPN**

  -Solución favorable para interconexión LAN to LAN o site to site gestionadas.

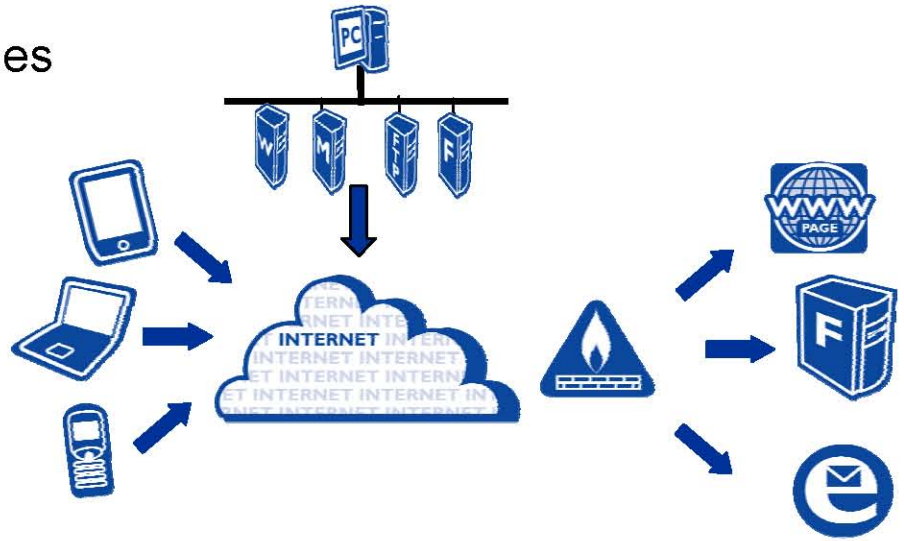
  -Orientación a conexiones frecuentes ó permanentes

- **SSL IPVPN**

  - Solución favorable para enlace Usuario - Red

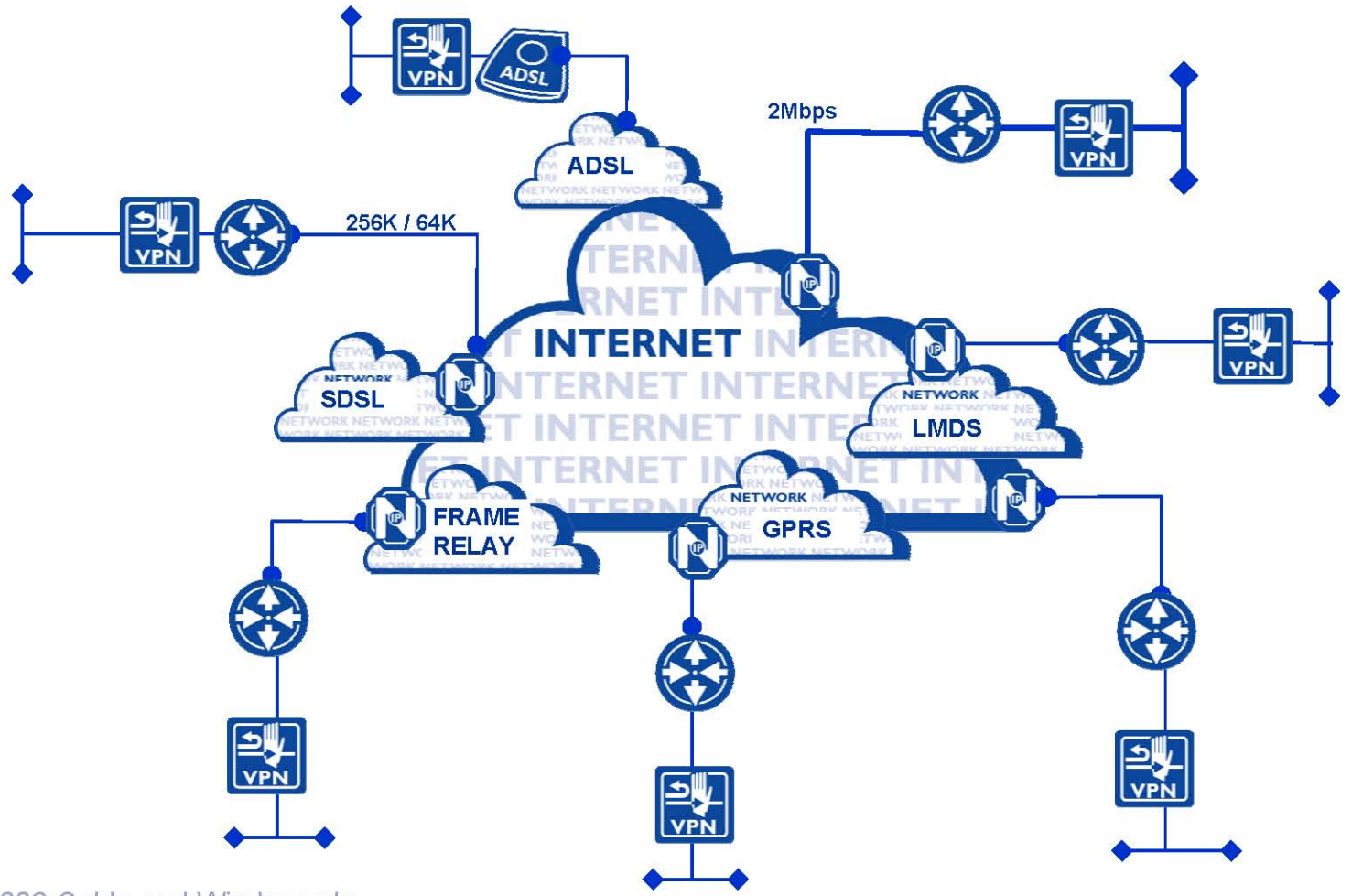
  - Flexibilidad de conexión desde distintas ubicaciones

  - Orientado a conexiones móviles

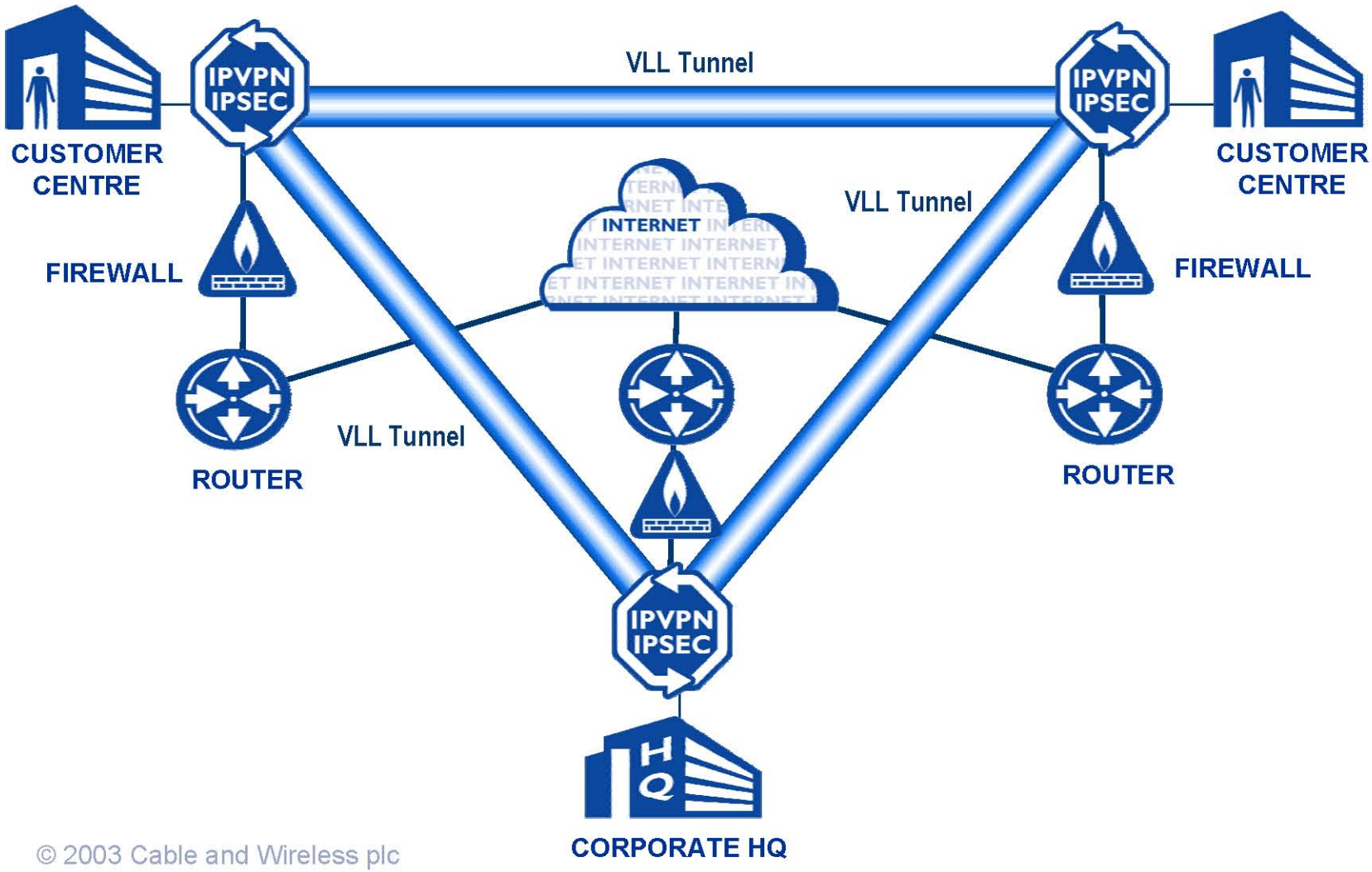


Esquema General VPN

Múltiples Métodos de Acceso
Una sola Red

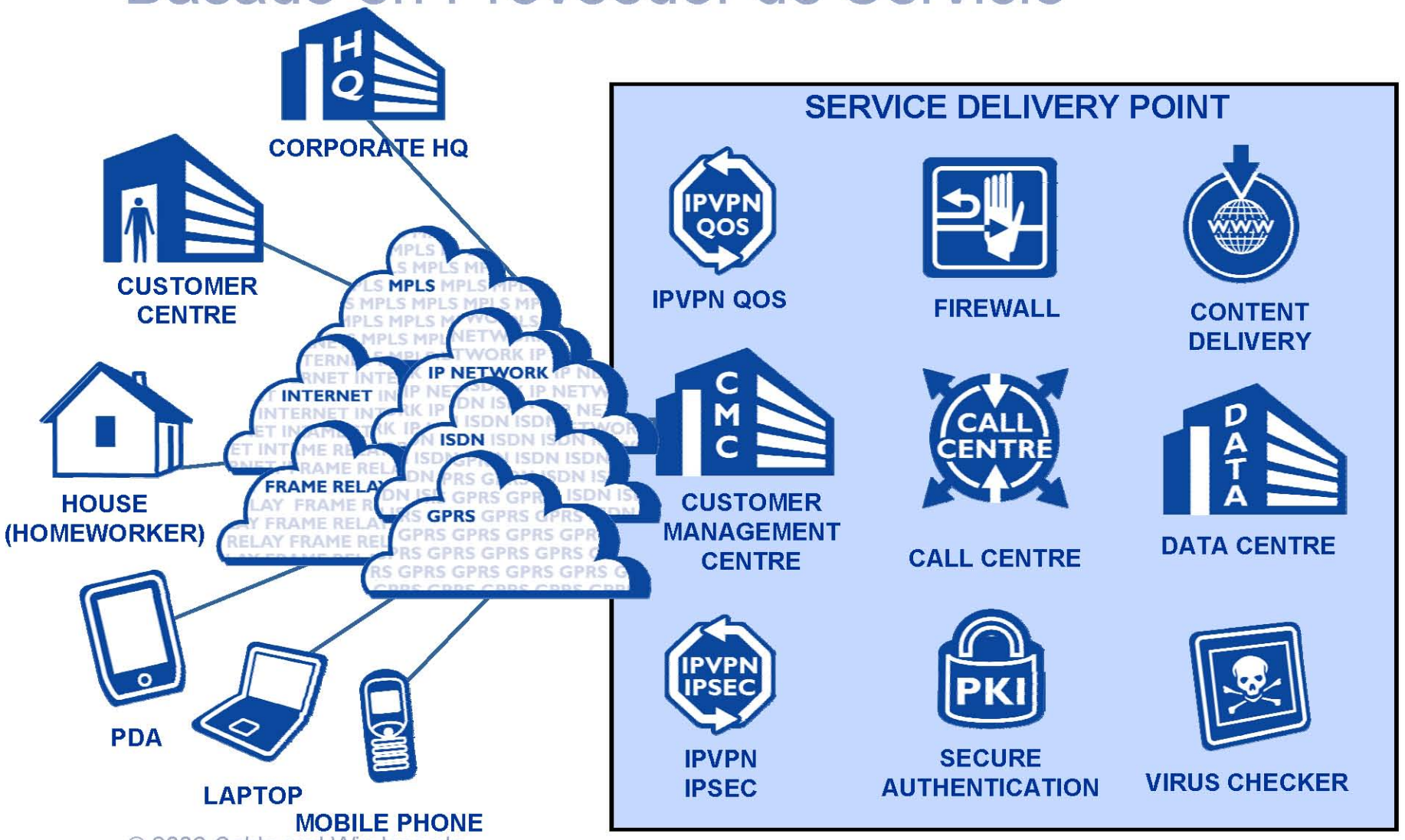


Esquema General VPN
Basado en CPE



Esquema General VPN

Basado en Proveedor de Servicio

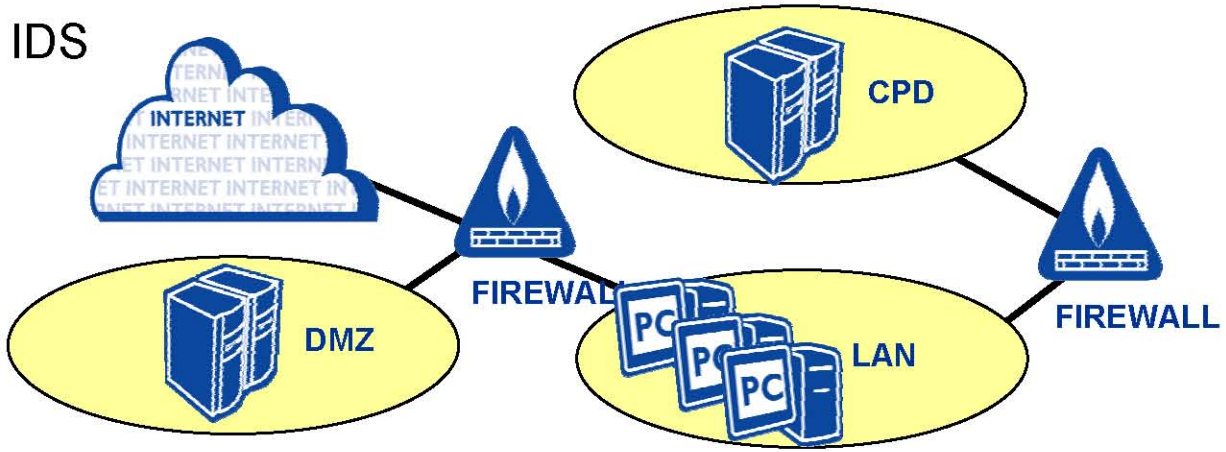


Modelo de Protección Perimetral Seguridad Preventiva

CABLE & WIRELESS

Seguridad Preventiva:
Protección en el entorno LAN

- **Protección Nucleo LAN – CPD – Zonas Públicas/Privadas**
  - Diseño de Red. Segmentación y definición Area DMZ
  - Protección de Redes LAN, Usuarios y Servidores
  - Diseño de Redes con Arquitectura estructurada Vlans 802.1q
  - Redes personalizadas 802.1x
  - Aplicación de Autenticación y políticas multiusuario SSH SSL
  - Técnicas de Redirección de Vlans y puertos SMON
  - Redirección de IDS

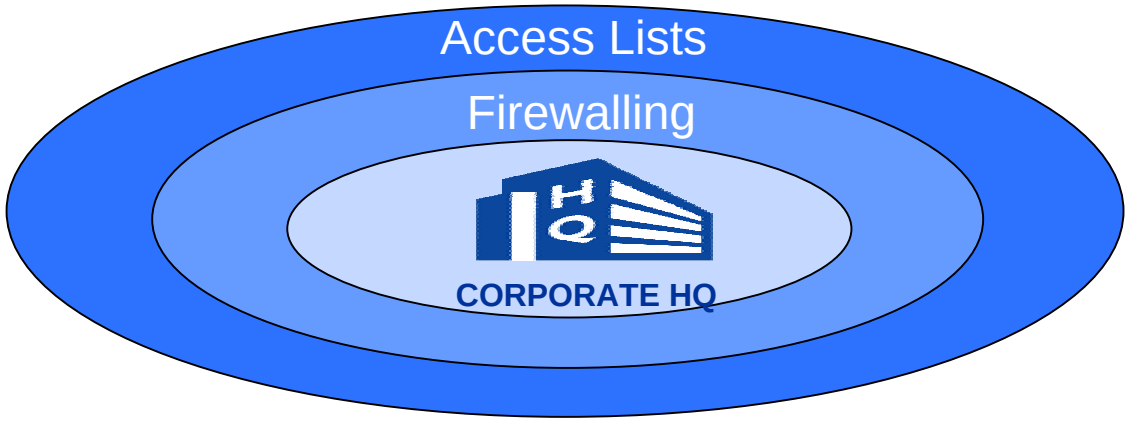


Seguridad Preventiva:
Proteger el Acceso a la Red

- **Protección Perimetral por Niveles. Capas Externas**

  Protección a Nivel 2 y 3 (OSI)

  - Filtrado de Acceso a la red corporativa por ACL´s implementadas en los routers externos
  - Establecimiento de políticas de restricción de tipo de tráfico tráfico y acceso por perfil de usuario
  - Niveles de Protección Tradicionales

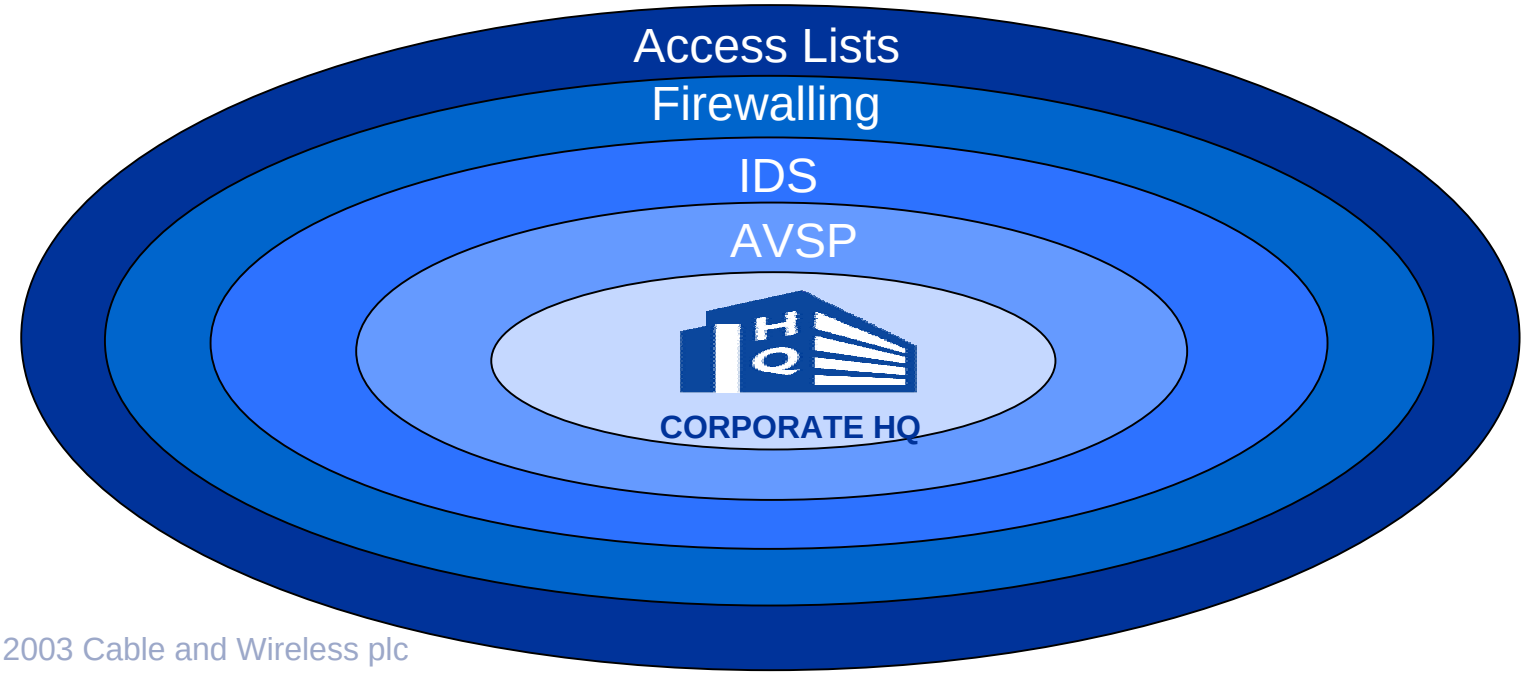


Seguridad Preventiva:
Proteger el Acceso a la Red

- **Protección Perimetral por Niveles. Capa Interna**

  Protección a Nivel 3-7 (OSI)

  - Análisis de Intrusión (IDS). Detección de ataques
  - Protección Antivirus y AntiSpam
  - Capa de protección de Aplicaciones



Recomendaciones Generales de Seguridad en las Redes de Datos

CABLE & WIRELESS

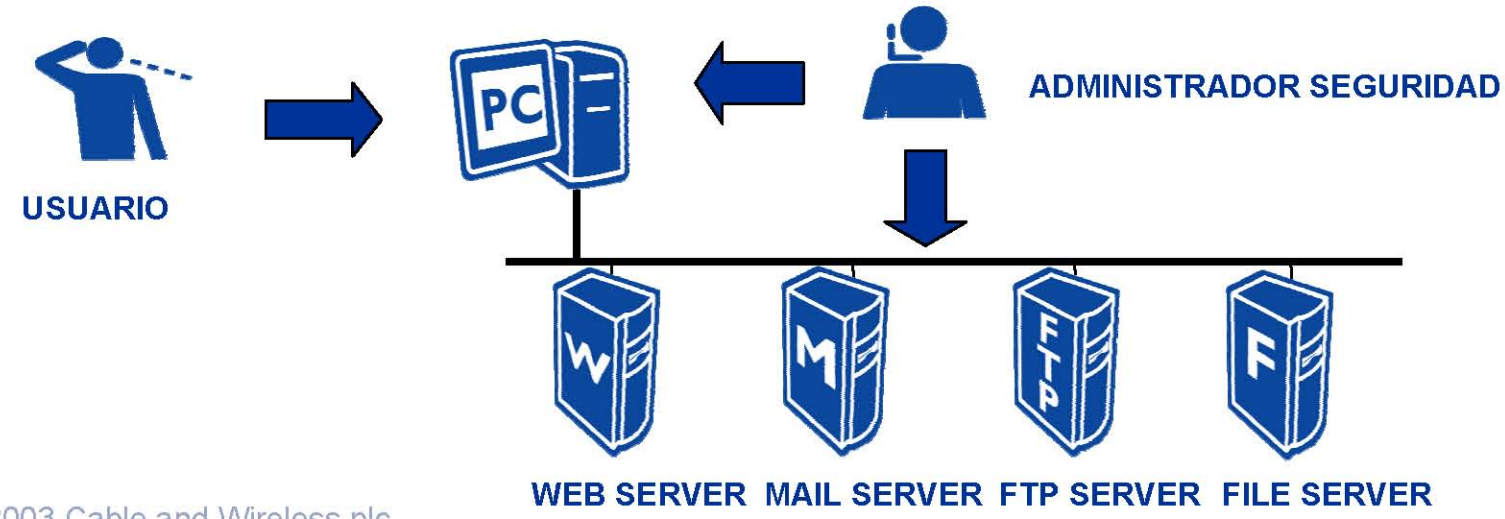
Seguridad Preventiva

- Planificación de arquitectura de Red
- Incorporación de elementos de Monitorización avanzados control de tráfico Interno Externo
- Incorporación de elementos de protección proactivos
- Estudios de vulnerabilidad periódicos
- Modelo de gestión de la Seguridad en la red
- Modificación de claves de acceso periódicamente
- Incorporación de autenticación fuerte en el acceso

La inversión en seguridad no debe ser superior al valor de lo que se protege

Responsabilidad en la Administración de la Red

- **Gestión de seguridad de la red**
  - Creación de una Política de uso de Servicios IT
  - Planificación de actividades en la red
  - Restricción de accesos asociados a perfiles de usuario
  - Mantener al día sobre los fallos de seguridad detectados. Aplicación de parches
  - Actualización de Antivirus en el puesto de usuario
  - Control de log de uso de servicios
  - Gestión de contraseñas y permisos de acceso



Seleccionar la Tecnología de Red adecuada

- **Redes LAN**
  - Arquitectura basada en VLANS (802.1q)
  - Redes Personalizadas (802.1x)
- **Redes MAN - WAN (Metodos de Acceso)**
  - VPN
  - Redes Dedicadas
- **Redes WIFI (802.11i, WEP,…)**
  - Protección de Warxing.
  - Técnicas de securización fuerte

Existe una solución optimizada a cada necesidad

Seguridad en el Puesto de Usuario

Actualización de seguridad acumulativa para Internet Explorer 6 Service Pack 1 (KB832894)

Tamaño de la descarga: **2,8 MB**

Se han detectado unos problemas de seguridad en Internet Explorer que podrían permitir a un usuario malintencionado poner en peligro la seguridad de un sistema que ejecute Windows.

Por ejemplo, **dicho usuario mal intencionado podría ejecutar programas en el equipo mientras se visita una página Web**. Esta actualización afecta a todos los equipos con Internet Explorer instalado, incluso aunque no se ejecute como explorador de Web. Después de instalarla, es posible que deba reiniciar el equipo.

. Más información... Es posible que este sitio esté en inglés.

Es necesario la administración de los entornos de usuario

Marco Legislativo
Soporte a la Seguridad

CABLE & WIRELESS

Marco Legislativo

- **Ley General de telecomunicaciones (LGT)**

Directivas 2002/21/CE Directivas 2002/21/CE, Directivas 2002/21/CE, 2002/20/CE,2002/19/CE, 2002/58/CE, 2002/77/CE y Decisión nº676/2002/CE del Parlamento Europeo y el Consejo

- Objetivos:
  - Establecer una intervención mínima de la Administración, suprimiendo la necesidad de obtener una licencia para poder operar en el sector de las telecomunicaciones
    - Gestión de notificación previa a la CMT
    - Registro de operadores
    - Servicio de acceso a Internet como servicio universal

Marco Legislativo

•Ley 59/2003, sobre Firma Electrónica

• Directiva 1999/93/CE é Real Decreto-Ley 14/1999, sobre firma electrónica

Revisión de terminología y modificaciones debidas al desarrollo tecnológico

• Firma electrónica reconocida

Firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma

Marco Legislativo

•Ley Organica de Protección de Datos de carácter Personal (LOPD)

- •Basada en el Derecho fundamental especificado en el artículo 18.4 de nuestra constitución
  "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"
  Directiva 2002/58/CE (LGT) y Directiva 95/46/CE (LOPD)
  Ley Orgánica 5/1992, LORTAD é Ley Orgánica 15/1999 LOPD

- •Agencia Española de Protección de Datos (AGPD)
  Misión: Velar por el cumplimiento de la legislación sobre protección de datos, controlar su aplicación y defender los derechos previstos para los ciudadanos en la materia.

- •Factor decisivo para la incorporación de medidas de protección y seguridad en la red. La obligación de establecer protección a la privacidad y confidencialidad de datos tratados y transferidos electrónicamente requiere sistemas de autentificación, controles de acceso y cifrado en las comunicaciones.

Marco Legislativo

- **Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)**
  - Incorpora al ordenamiento jurídico español la Directiva 2000/31/CE, del Parlamento Europeo y el Consejo sobre comercio electrónico
  - Aplica a todas las actividades que se realicen por medios electrónicos y tengan carácter comercial
  - Principio de libre prestación de servicios en el territorio de la Unión Europea
  - Objetivo:Favorecer la realización de contratos por vía electrónica
- **Directiva 2002/58/CE, sobre Privacidad de las comunicaciones electrónicas**
  - Regula el envío de correos electrónicos no solicitados (SPAM)

  La ley española responde a la directiva europea que proponía desarrollar dos alternativas : *prohibirlo directamente si no cuenta con autorización expresa*, u obligar a que *fuese claramente identificado como tal -incluyendo el texto publi o pulicidad en el 'asunto' del mensaje*- y que se garantizase el derecho del receptor a apuntarse a listas de exclusión voluntarias.

  El Gobierno español ha optado por la primera medida.

Fuerzas de Seguridad del Estado

Grupo de Delitos Telemáticos de la Guardia Civil
http://www.guardiacivil.org/telematicos/index.htm
Tlf: 34 91 514 64 00/062
C/ Guzmán el Bueno, 119, 28003 Madrid

Brigada de Investigación Tecnológica de la Policía Nacional
http://www.mir.es/policia/bit/index.htm
C/ Julián González Segador, s/n, 28043 Madrid

Atención general.
delitos.tecnologicos@policia.es delitos.tecnologicos@policia.es
Tlf: 915822747 Tlf: 915822747

Conclusiones

CABLE & WIRELESS

Seguridad en Redes Corporativas
Conclusiones I

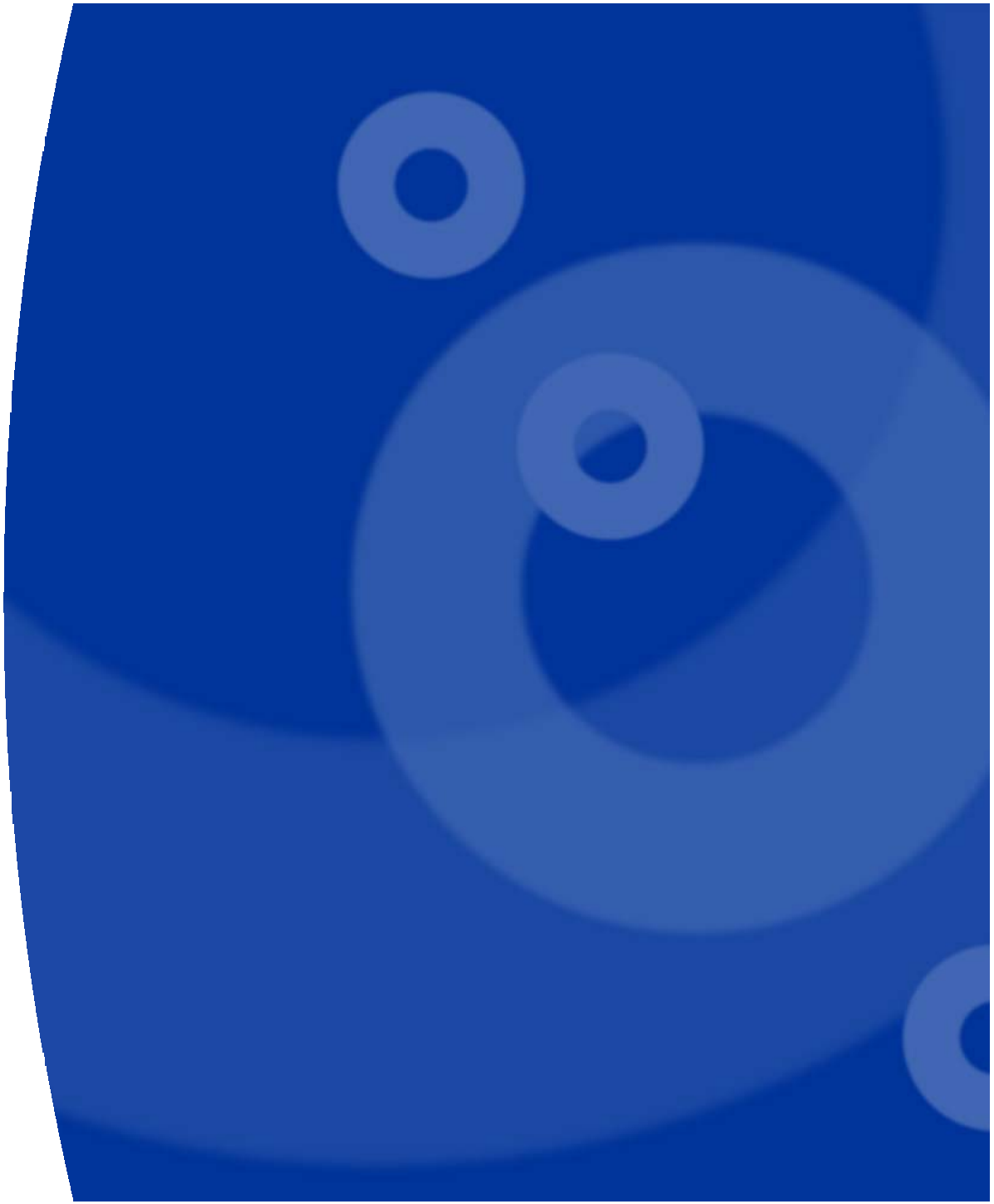
- Es necesario una concienciación de la magnitud del problema potencial.
- El uso crítico de las redes de telecomunicaciones debe obligadamente ir acompañado de inversiones en recursos de protección.
- La legislación actualmente vigente establece nuevas pautas de comportamiento y usos de los sistemas informáticos que debemos conocer.
- La LGT, LOPD y LSSI aunque van evolucionando hoy por hoy son incompletas. Ciertos delitos informáticos son tratados como delitos menores.
- La Universalidad de las comunicaciones no está regulada por normativas Internacionales. No existe un código penal Internacional

Seguridad en Redes Corporativas
Conclusiones II

- La tecnología actual nos permite aplicar técnicas de protección adecuadas a cada tipo de red y empresa.
- El cifrado de las comunicaciones, la autentificación y la firma digital se incorporan como aliados indispensables en nuestras redes.
- La políticas de seguridad deben ser rápidas y proactivas. Las técnicas preventivas de detección temprana evitarán operaciones muy costosas de pérdida de datos.

La transmisión de información es clave en nuestro mundo
La protección de las redes es clave en las comunicaciones

Gracias



CABLE & WIRELESS