



LIME Access: Solución para entornos de conectividad remota de alta seguridad




- **Introducción:**
 - Riesgos en los entornos de Movilidad basados en PC y Laptop
- **LIME Access: Soluciones de acceso remoto seguro**
 - LIME Access Pen Drive
 - LIME Access Autorun
 - LIME Access USB HD
- **Gestión y personalización**
- **Beneficios para las organizaciones**
- **Escenarios**

- ❖ Robo o pérdida física de los equipos.
- ❖ Virus y malware: acceso a través de la VPN a datos corporativos.
- ❖ Ataques de denegación de servicio.
- ❖ Ataques internos con robo de datos.
- ❖ Equipos de uso general para acceso a Internet: alto riesgo de vulnerabilidades e infección y rastros de accesos corporativos.
- ❖ Acceso ilegítimo vía suplantación de identidad.
- ❖ Filtrado de información por Phising o Pharming en entornos Web.
- ❖ Cambios no autorizados de configuraciones de acceso corporativo.

1. Accesos remotos, por parte de usuarios internos
2. Acceso, por parte de personal externo que se deben conectar, como proveedores de servicios o como trabajadores en outsourcing, bien mediante acceso remoto o bien directamente a la red interna con equipos no proporcionados por la organización.
3. Accesos, por parte de empresas o usuarios externos, para realizar operaciones a través de Internet, que requieran un alto nivel de seguridad en el acceso.
4. Entornos de formación o similares, donde se requiere mantener los equipos dedicados con una maqueta predefinida que no conserve los cambios realizados.
5. Recuperación frente a desastres, disponiendo de un mecanismo alternativo que permita trabajar en cada equipo, aunque éste haya recibido ataques de virus o cualquier otro tipo de malware, que impidan su funcionamiento normal.



- ❖ Solución de acceso seguro a aplicaciones y sistemas desarrollado para las especificaciones de cada cliente.
- ❖ Basado en un sistema operativo ejecutable desde un CD/DVD específico para cada entorno.
- ❖ Acceso seguro a direcciones (puertos) únicas de aplicaciones Web o en modelo cliente/servidor.
- ❖ Arranque del SO en memoria RAM inviolable por amenazas de red (Internet/externas o internas), virus, gusanos, troyanos, spyware, etc.
- ❖ Acceso ubicuo desde cualquier PC ó Laptop. 
- ❖ No accede al sistema de almacenamiento del puesto de trabajo o portátil.



- Arranque automático desde el CD
- Sistema auto contenido, incluyendo toda la funcionalidad necesaria:
 - ✓ Conexión de red vía VPN.
 - ✓ Acceso a las aplicaciones predefinidas.
 - ✓ Personalización para cada organización.
- Configuraciones de seguridad opcionales:
 - ✓ Cifrado de la información del CD: Arranque previa autenticación basada en contraseña o token criptográfico (e-DNI).
 - ✓ Modificaciones de kernel que impiden conexiones con IPs no predefinidas (DNS deshabilitado).
 - ✓ Limitaciones en kernel y configuraciones prefijadas en conexión exterior.
 - ✓ Imposibilidad de ejecutar en memoria algo que no se haya preestablecido.

CD con arranque seguro

- Solo es preciso introducirlo en el ordenador y encenderlo.
- No modifica el Sistema Operativo, se ejecuta en memoria.
- Detecta automáticamente el hardware. Ubicuidad.
- Lanza la aplicación con una dirección o menú pre configurado.
- Una vez terminado se apaga.



- ❖ Solución de acceso remoto a aplicaciones y sistemas, personalizado por usuarios y clientes.
- ❖ Basado en un sistema operativo ejecutable desde un Pen Drive específico para cada entorno, auto contenido y protegido.
- ❖ Información y SO protegidos en caso de pérdida o robo.
- ❖ Acceso seguro a direcciones (puertos) únicas de aplicaciones Web o en modelo cliente/servidor.
- ❖ Arranque del SO en solo lectura en memoria RAM inviolable por amenazas de red (Internet/externas o internas), virus, gusanos, troyanos, spyware, etc.
- ❖ Acceso ubicuo desde cualquier PC ó Laptop.
- ❖ No accede al sistema de almacenamiento del puesto de trabajo o portátil. Permite almacenar datos cifrados en el Pen Drive.





- ❖ Solución de acceso seguro a aplicaciones y sistemas, desarrollado para las especificaciones de cada cliente.
- ❖ Basado en un sistema operativo virtual (burbuja de seguridad) ejecutable desde un USB Disk específico para cada entorno.
- ❖ Ejecución de una imagen virtual de cualquier sistema operativo (Windows, Linux) pre configurado con el entorno de trabajo de cada empleado.
- ❖ Acceso ubicuo desde cualquier PC ó Laptop.
- ❖ Posibilidad de escritura local de datos solo en el USB Disk.
- ❖ Datos cifrados en el USB Disk (autenticación previa).
- ❖ No accede al sistema de almacenamiento estándar del puesto de trabajo o portátil.



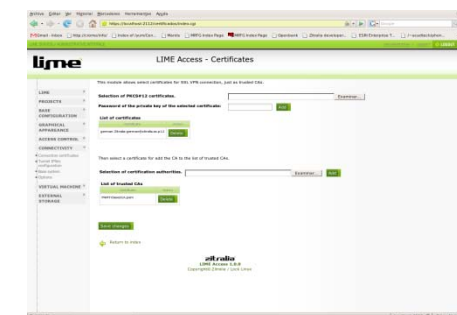
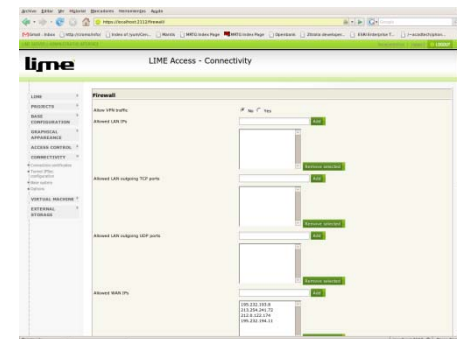
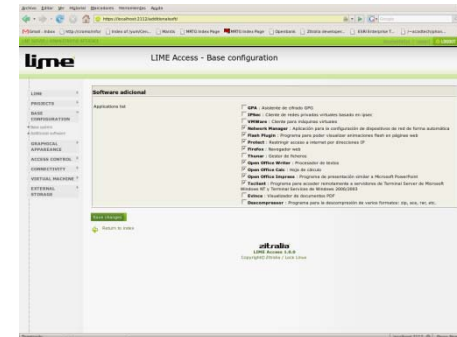
- ❖ Permite disponer de un puesto de trabajo ligero y seguro (Thin Client).
- ❖ La imagen del sistema operativo se REGENERA en cada arranque.
Imagen del SO limpia de infecciones en cada arranque.
- ❖ Distintos sistemas de acceso: VPN-SSL, VPN-IPSEC (Wi-fi, Ethernet, ADSL).
- ❖ Se pueden crear imágenes del SO para distintos perfiles y despliegues geográficos.
- ❖ Mecanismo de generación de imágenes automatizado.

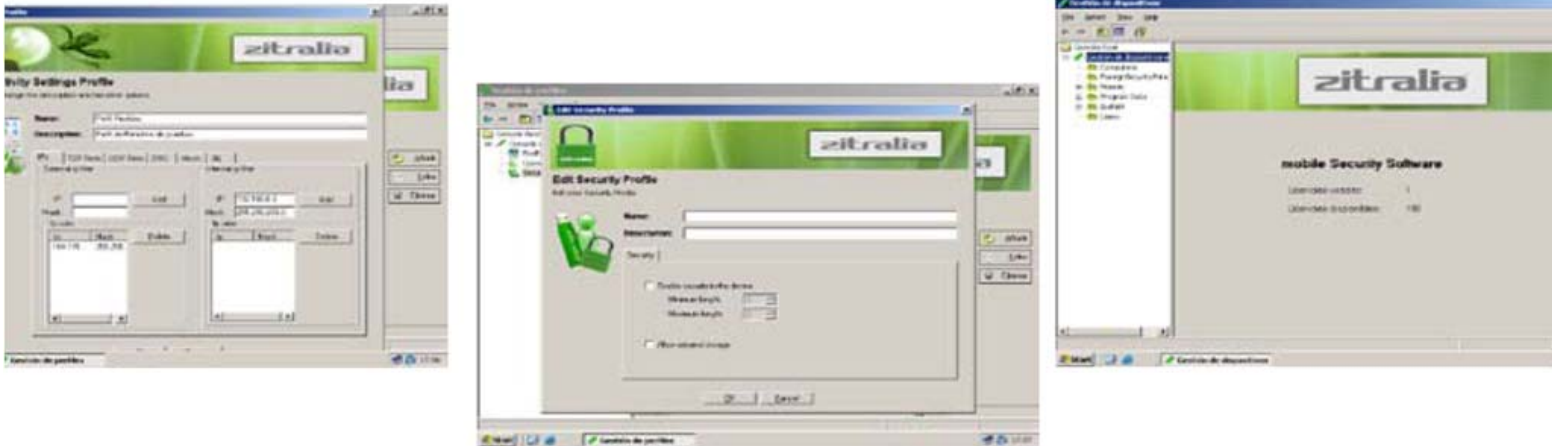
- ❖ Prevención contra el robo o pérdida física del hardware, con pérdida o filtración de información.
- ❖ Prevención contra el acceso no autorizado a información.
- ❖ Previene la ejecución de software no autorizado.
- ❖ Prevención total contra las intrusiones, virus y troyanos.
- ❖ Prevención contra ataques de denegación de servicio.
- ❖ Imposibilidad de realizar acceso ilegítimo vía suplantación de identidad.
- ❖ Imposibilidad de realizar cambios no autorizados de configuraciones de acceso corporativo.
- ❖ Imposibilidad de Filtrado de información por Phising o Pharming en entornos Web.

- ❖ Solución de acceso remoto a aplicaciones y sistemas, desarrollado para las especificaciones de cada cliente con arranque sobre el S.O. del equipo.
- ❖ Creación de una burbuja de seguridad dentro del equipo
- ❖ Acceso seguro a direcciones (puertos) únicas de aplicaciones Web o en modelo cliente/servidor.
- ❖ Información protegida, sin dejar rastros en el equipo
- ❖ Acceso ubicuo desde cualquier PC ó Laptop.
- ❖ No interfiere en los datos almacenados en equipo sobre el que se ejecuta



- ❖ Creación de imágenes personalizadas en función de empresa/perfiles/usuarios.
- ❖ Adaptación Look&Feel de arranque
- ❖ Selección componentes y aplicaciones disponibles (ofimática, TS, Citrix, clientes VPN....)
- ❖ Selección de dominios y direcciones IP, URL, DNS
- ❖ Selección métodos de autenticación y conectividad disponibles
- ❖ Selección posibilidades almacenamiento .
- ❖ Selección de certificados para el establecimiento de conexiones
- ❖ Gestión claves de la información protegida





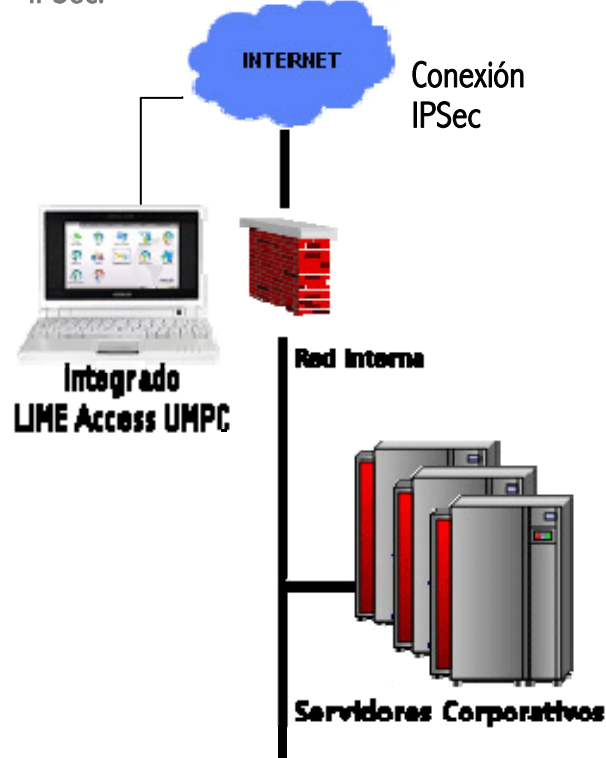
- ❖ Aplicación y modificación de políticas de usuarios/perfiles
- ❖ Alta/Baja de usuarios
- ❖ Direcciones IP y puertos TCP/UDP permitidos/restringidos
- ❖ Comandos remotos y actualizaciones
- ❖ Políticas de almacenamiento



- ❖ Alta Seguridad en entornos de movilidad.
- ❖ Ubicuidad de acceso para empleados, altos cargos, agentes comerciales o funcionarios sin aumentar el riesgo:
Mejora en la productividad y disponibilidad.
- ❖ Alineamiento de la seguridad en entornos de movilidad con los requerimientos críticos de negocio.
- ❖ Reducción del coste de propiedad de los sistemas de acceso remoto de empleados, agentes comerciales, altos cargos, empresas externas, etc.
- ❖ Cumplimiento de normativas de protección de datos en entornos de movilidad.

- Acceso ubicuo seguro por parte de personal en movilidad
- Acceso remoto seguro y controlado por parte del personal externo (outsourcing, call centers, agentes comerciales....)
- Ejecución segura de trámites electrónicos
- Acceso seguro en entornos de teletrabajo
- Ubicuidad de acceso seguro a aplicaciones corporativas desde hoteles, aeropuertos, cibercafés, puestos de trabajo personales y de empresa
- Acceso a aplicaciones críticas en entornos profesionales de alta seguridad (médicos, abogados, funcionarios, brokers financieros, etc.)

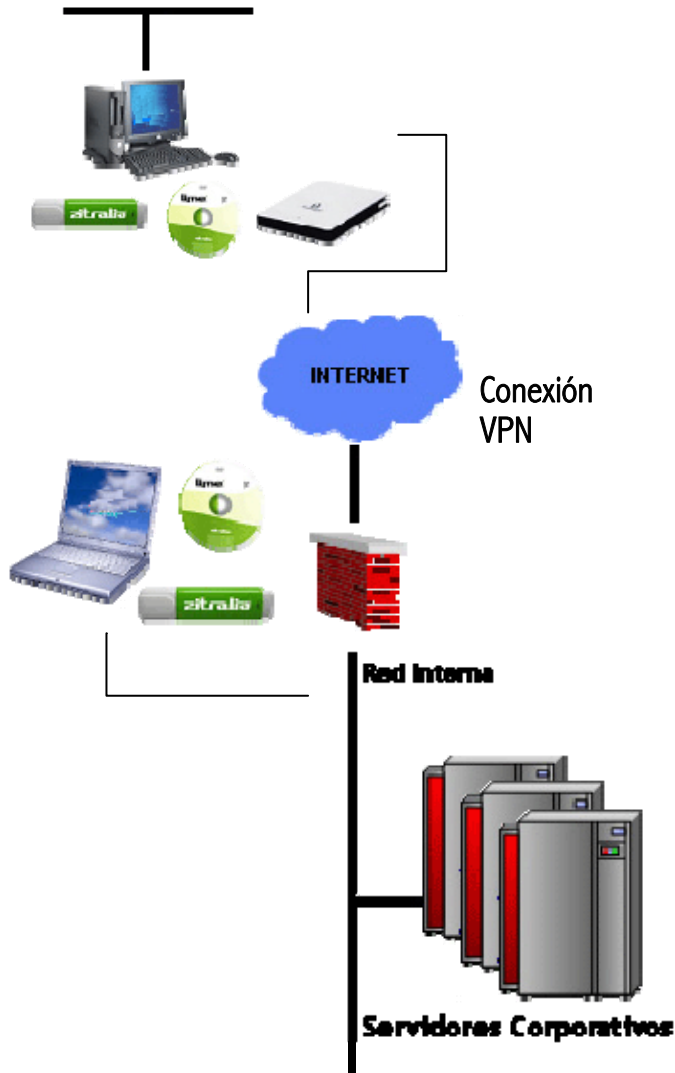
El usuario trabaja de forma remota montando un entorno seguro basado en LIME Access, conectándose a la Red Interna mediante túneles IPSec.



Los usuarios que requieren conectarse de forma remota (por ejemplo, por teletrabajo) deberán poder trabajar como si se encontrarán en un equipo de la red interna.

Para ello, se plantean las opciones:

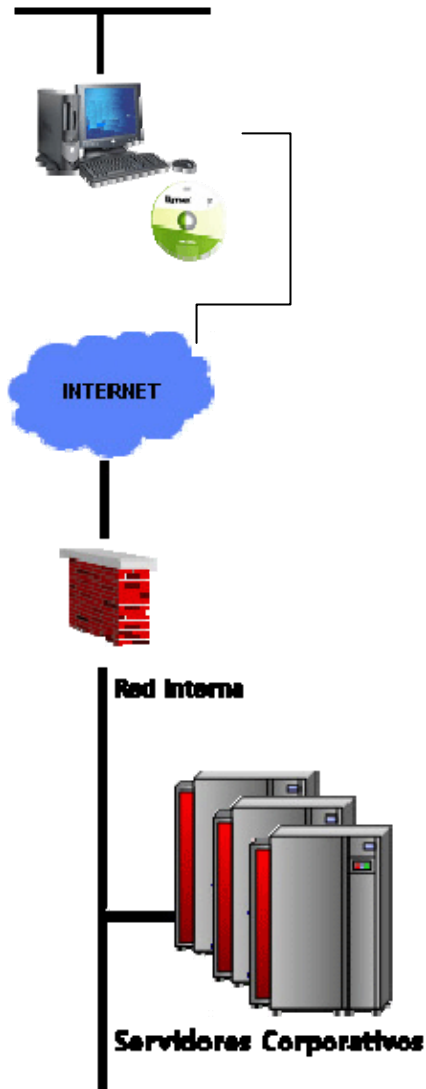
- Utilizar un equipo cualquiera (proporcionado por la empresa, particular del usuario o de terceros) junto con un dispositivo externo (pen-drive o disco USB) que incluya el producto LIME Access.
- Utilizar una burbuja de seguridad integral (LIME Access UMPC), donde se proporciona directamente el equipo de trabajo (UMPC) y se carga la burbuja de seguridad (LIME Access) integrada, sin necesidad de utilizar cualquier otro dispositivo.



Empresas o usuarios externos que suministran servicios a las EE.FF. o personal ajeno trabajando en outsourcing.

En este caso y, en función del servicio a prestar, la funcionalidad y contenido del dispositivo puede ser distinta.

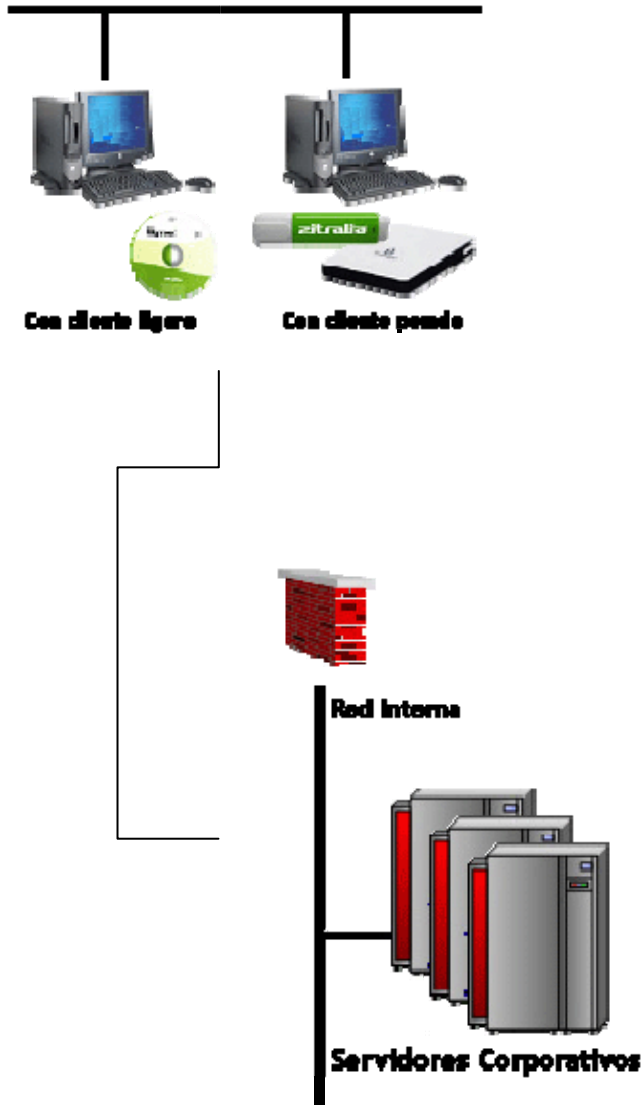
- Autenticación específica para cada usuario, si fuera necesario.
- El soporte deberá incluir las herramientas necesarias para permitir al usuario realizar los servicios necesarios.
- Limitación de IPs, puertos, direcciones, etc. a los que se podrá conectar, y el método de conexión a utilizar: por ejemplo, mediante VPN, en función del servicio a prestar.
- El sistema sólo permitirá que el usuario haga las acciones necesarias para realizar el servicio que tiene asignado.



Usuarios de EE.FF. que deben realizar ciertos trámites, a través de Internet, requiriendo un alto nivel de seguridad.

Para que esta conexión se realice de forma segura se puede distribuir entre estos usuarios un LiveCD que realiza todos los procesos necesarios de forma segura.

- Autenticación específica para cada usuario, si fuera necesario.
- El LiveCD incluirá un navegador que permitirá al usuario conectarse, a través de Internet, para realizar los trámites, pero que no le permitirá la navegación fuera de unas direcciones determinadas.
- Limitación de IPs, puertos, direcciones, etc. a los que se podrá conectar, y el método de conexión a utilizar: por ejemplo, mediante VPN, en función del servicio a prestar.
- El sistema sólo permitirá que el usuario haga las acciones necesarias para realizar el servicio que tiene asignado.



En entornos donde se requiere mantener un entorno totalmente estable, sin modificaciones, se puede utilizar una burbuja de seguridad que incluya la configuración del nuevo curso o acción y que asegure que el resto del entorno sigue siendo el mismo, dando acceso Web y acceso únicamente a aquellos servicios/datos que sean necesarios.

Según el formato del curso o similar, se hará uso de un cliente ligero (CD/DVD) o de un cliente pesado que lanzará una máquina virtual Windows con la ofimática y aplicaciones deseadas para el curso.

- La autenticación de usuario se realiza directamente contra el servidor, pudiendo utilizarse distintos mecanismos de control de acceso (usuario/contraseña, token con certificado, etc.).
- Los datos de trabajo se pueden mantener en el servidor, o en el disco USB según como esté configurado el curso.

Ante eventualidades en las que no se puede trabajar con uno o varios equipos se podrán utilizar dispositivos que permitan a los usuarios seguir con su trabajo normal. En este caso se puede plantear el caso de trabajo sin conexión o trabajo con conexión.



Ante fallos en los equipos se mantienen sistemas autónomos que puedan ser utilizados en cualquier momento, de forma que los usuarios puedan seguir trabajando.

Con conexión:

Se arranca la burbuja de seguridad, realizando las acciones normales para iniciar la sesión de trabajo.

- La autenticación de usuario se realiza directamente contra el servidor, pudiendo utilizarse distintos mecanismos de control de acceso (usuario/contraseña, token con certificado, etc.)
- Los datos de trabajo se pueden mantener en el servidor o en el disco duro USB
- En la opción de HD-USB el sistema arranca una maquina virtual Windows con la Ofimática y herramientas necesarias según el perfil del usuario.

Sin conexión:

Por ejemplo si los servidores también han sufrido algún tipo de desastre.

- Una vez arrancado el sistema auto contenido sobre el equipo de trabajo el usuario trabaja sobre los datos almacenados localmente.

	Laptop sin gestión	Laptop gestionado moderadamente	Desktop sin gestión	Desktop gestionado moderadamente	Lime Access	Lime Access con VMWARE
Usuarios	2.500 usuarios	2.500 usuarios	2.500 usuarios	2.500 usuarios	2.500 usuarios	2.500 usuarios
Unidades	2.500 Laptop 1800€ con monitor incluido y una vida media de 4 años	2.500 Laptop 1800€ con monitor incluido y una vida media de 4 años	2.500 PC´s a 1000€ con monitor incluido y una vida media de 4 años	2.500 PC´s a 1000€ con monitor incluido y una vida media de 4 años	2.500 Disco duro externo USB a un precio de 155€ y una vida media de 4 años	2.500 Disco duro externo USB a un precio de 155€ y una vida media de 4 años
Servidores		5 servidores de gestión a 2.000€ con una vida media de 4 años + 1 admin. sistemas		5 servidores de gestión a 2.000€ con una vida media de 4 años + 1 admin. sistemas	4 Servidores Zitralia + 5 Servidores gestión + 1 admin. sistemas	4 Servidores Zitralia + 5 Servidores gestión + 1 admin. sistemas
Software	Paquete Office + Anti Virus Symantec	Paquete Office + Anti Virus Symantec	Paquete Office + Anti Virus Symantec	Paquete Office + Anti Virus Symantec	Aplicaciones sin coste	Office OEM + SO OEM + Symantec

	Laptop sin gestión	Laptop gestionado moderadamente	Desktop sin gestión	Desktop gestionado moderadamente	Lime Access	Lime Access con VMWARE
Hardware	450,00 €	450,00 €	250,00 €	250,00 €	38,75 €	38,75 €
Mantenimiento Hardware	90,00 €	90,00 €	37,50 €	37,50 €	0,00 €	0,00 €
Software	229,25 €	229,25 €	229,25 €	229,25 €	0,00 €	160,00 €
Licencia Lime Access			0,00 €	0,00 €	21,75 €	21,75 €
Coste servidor		10,60 €		10,60 €	11,80 €	11,80 €
HW, SW e Instalación	769,25 €	779,85 €	516,75 €	527,35 €	72,30 €	232,30 €
Tier 1	135,83 €	122,50 €	97,50 €	87,50 €	51,67 €	51,67 €
Tier 2	247,50 €	173,33 €	190,00 €	132,50 €	64,17 €	64,17 €
Tier 3	104,17 €	95,00 €	81,67 €	76,67 €	147,50 €	147,50 €
IT Operations	487,50 €	390,83 €	369,17 €	296,67 €	263,33 €	263,33 €
Administración	65,00 €	65,00 €	61,67 €	57,50 €	36,67 €	36,67 €
Gestión	65,83 €	65,83 €	56,67 €	56,67 €	39,17 €	39,17 €
Formación usuarios	33,33 €	33,33 €	25,00 €	26,67 €	28,33 €	30,83 €
Administración	164,17 €	164,17 €	143,33 €	140,83 €	104,17 €	106,67 €
Hardware y Software	769,25 €	779,85 €	516,75 €	527,35 €	72,30 €	232,30 €
Ahorros s/Laptop	0,0%	-1,4%	32,8%	31,4%	90,6%	69,8%
Ahorros s/Desktop	-48,9%	-50,9%	0,0%	-2,1%	86,0%	55,0%
Tareas de Administración y Operaciones	651,67 €	555,00 €	512,50 €	437,50 €	367,50 €	370,00 €
Total Costes Directos	1.420,43 €	1.334,33 €	1.029,58 €	965,14 €	441,57 €	603,55 €
Ahorros s/Laptop	0,0%	6,1%	27,5%	32,1%	68,9%	57,5%
Ahorros s/Desktop	-38,0%	-29,6%	0,0%	6,3%	57,1%	41,4%
Inversión 4 años 2.500 usuarios	14.204.280,36 €	13.343.270,77 €	10.295.782,42 €	9.651.439,49 €	4.415.660,99 €	6.035.484,77 €
Ahorros s/Laptop	0,00 €	861.009,59 €	3.908.497,94 €	4.552.840,86 €	9.788.619,36 €	8.168.795,59 €
Ahorros s/Desktop	-3.908.497,94 €	-3.047.488,35 €	0,00 €	644.342,92 €	5.880.121,42 €	4.260.297,65 €

zitralia

