



Tirada: 5.000		Superficie: <b>456,00 cm<sup>2</sup></b> Ocupación: <b>74.03%</b> Valor: <b>1.109,89</b>	 1 / 2	
Difusión: 5.000				
Audiencia: 17.500				Nacional Bimestral Seguridad y Prevención
Ref: 1128628				1ª Edición 01/09/2006 Página: 24

# SEGURIDAD PERIMETRAL:

¿Está nuestra organización preparada para quedarse sin servicio informático durante semanas?

## LA SEGURIDAD PERIMETRAL ES FUNDAMENTAL PARA LA SOLIDEZ DE LA RED Y LA PROTECCIÓN ANTE DESASTRES



**Manuel Monterrubio**

CONSEJERO  
DELEGADO/EXPERTO  
EN DISASTER  
RECOVERY  
ALHAMBRA EIDOS

La utilización de las redes de comunicaciones como canal de comunicación con el ciudadano en el caso de instituciones o de negocio para empresas es ya muy importante en las organizaciones españolas. Cada vez son más los usuarios que se atreven a intercambiar información comercial y datos críticos. El incremento en la velocidad de acceso ha hecho proliferar las posibilidades de los intrusos en su intento por adquirir valiosa información y también por destruirla. Hemos de poner en práctica, si aún no lo tenemos, Planes de Seguridad Corporativa y Planes de Recuperación ante Desastres. Si no lo hacemos, tarde o temprano se caerá el servicio informático que prestamos y sin querer ser agorero alguno a lo mejor deja de ser el responsable del mismo.

El mercado de la seguridad está muy diversificado, con múltiples áreas y productos. Es un sector que demanda de los proveedores de servicios y de los fabricantes unas capacidades cada vez más avanzadas y acordes a las exigen-

cias de los clientes, sin incrementar los recursos dedicados. En el caso de la seguridad perimetral nos encontramos al menos con dos tipos de proveedores: por un lado, los que se encargan de asegurar la red y de mantener los intrusos a distancia, y, por otro, los que ponen todos los medios necesarios para evitar los ataques contra los contenidos (provenientes la mayoría de las veces de virus y códigos maliciosos).

**En resumen generalmente, se adoptan sistemas básicos de protección, pero pocas veces nos tomamos suficientemente en serio la seguridad**

Por su parte, las empresas e instituciones son conscientes de que la Web es uno de los medios más utilizados por los usuarios para la demanda de productos y servicios de todo tipo, convirtiéndose en una parte estratégica de la sociedad. Por tal motivo, para cualquier entidad es de vital importancia contar con aplicaciones que protejan la seguridad de su entorno informático.

En los últimos años, las acciones básicas que los responsables de infor-

mática han puesto en marcha, han venido dadas por la protección antivirus dado el miedo a la destrucción de la información pero, a menudo se infravalora la habilidad de posibles atacantes.

Igual que nadie dejaría en un polígono industrial una nave abierta durante toda la noche y el fin de semana, tampoco debemos confiar en dejar puertas abiertas a nuestra red y a menudo existen... y muchas.



En este sentido, lo mínimo que una empresa o institución de cualquier tipo (ayuntamiento, diputación, organismo autonómico o estatal) debería plantearse es la protección de su información crítica. Esta información debe estar a salvo tanto de la pérdida por causa de fallos de sistemas como de todo tipo de desastres como de intrusos.

### La seguridad perimetral «lógica»

Un buen sistema y plan de seguridad perimetral lógico al menos debe contemplar: la protección ante intrusiones externas e internas, la máxima protección de la información privada y la protección contra virus.

Hoy día cualquier responsable de informática conoce sistemas de encriptación VPN que permiten garantizar la privacidad de las comunicaciones, firewalls y productos antivirus potentes. En el mercado existen dispositivos que incorporan además buena parte de estas tecnologías, asegurando la integridad de la red a precios competitivos.

Asimismo, existen en España varias compañías que ayudan a elaborar un completo plan de seguridad perimetral

Tirada: 5.000		Superficie: <b>472,00 cm<sup>2</sup></b> Ocupación: <b>76.62%</b> Valor: <b>1.149,16</b>	 2 / 2	
Difusión: 5.000				
Audiencia: 17.500				Nacional Bimestral Seguridad y Prevención
Ref: 1128628				1ª Edición 01/09/2006 Página: 25



«lógico» igual que existen empresas de seguridad «tradicional» que vallarían unas instalaciones físicas, pondrían cámaras infrarrojas, alarmas, perros guardianes e incluso haciendo uso de la hipérbole, electrificarían el perímetro.

### La ley de protección de datos, ataque a ayuntamientos, pinchar teléfonos.

Realmente, las grandes empresas y los grandes organismos del Estado son conscientes de la importancia de mantener la integridad y privacidad de los sistemas pero las instituciones de tamaño medio y las pymes tienen más dificultad para «identificar» la importancia de estos sistemas.

A lo largo de 2006 hemos conocido por televisión los ataques a ayuntamientos en los que desaparecían ordenadores con toda la información del municipio. Esto, aparte de suponer un problema grave para el ayuntamiento, contraviene lógicamente las normas

básicas de seguridad que exige la LOPD.

Aunque este ejemplo es de ataque físico, deja patente la importancia de las medidas de seguridad (en este caso seguridad perimetral «tradicional», evidentemente tan importante como la «lógica»).

En resumen generalmente, se adoptan sistemas básicos de protección (casi siempre antivirus y firewalls personales), aunque cada vez son más las organizaciones que apuestan por incluir también dispositivos más avanzados, pero pocas veces nos tomamos suficientemente en serio la seguridad.

Además, con la introducción de los servicios convergentes de la VoIP, en los que las comunicaciones de voz se han transformado en datos, las empresas necesitan disponer de soluciones que garanticen la integridad de la red, de los datos, de las conversaciones que circulan por ella, etc. Pinchar una conversación hoy día puede ser «muy fácil» para determinados técnicos. ♦

## A mayor protección, menos amenazas y menores desastres

**E**n los últimos años la conciencia de la necesidad de medidas de seguridad ha aumentado mucho pero aún queda mucho por hacer.

De esta forma, para cualquier organización, de cualquier tamaño, es importante contar con un Plan de Seguridad Corporativo —e integral— que ayude a la toma de decisiones y que contemple al menos una serie de puntos básicos como la seguridad física; los sistemas y redes; el acceso a usuarios y passwords; las aplicaciones; los datos; la detección de intrusiones y la respuesta a incidentes. Así nos aseguraremos de que todos los aspectos de la organización están bajo control, tanto por amenazas externas, como internas.

Si se produce un ataque, y dependiendo del tamaño del organismo ante el que nos encontremos el servicio de informática puede que esté parado semanas. ¿Esta preparada la organización? Por ello también es importantísimo disponer de un Plan de Recuperación ante Desastres. ¿Qué ocurre si han destruido (física o lógicamente) nuestros servidores? ¿Cuánto tiempo tardaremos en recuperarnos? Diseñar un sencillo plan de recuperación ante desastres puede no llevar demasiada carga de trabajo y como dice un buen consultor de nuestra compañía «es mejor tener un plan de recuperación de desastres que tener un desastre de recuperación».