

**¿SU EMPRESA ESTA**

**SEGURA FRENTE A**

**INTERNET?**



## Seguridad para pequeñas y medianas empresas

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. **Cada vez es mayor el número de atacantes y los fallos de seguridad provenientes del interior mismo de la organización.**

**DRAGOMAR INFORMATICA OFRECE UNA SOLUCION INTEGRAL Y FACIL DE MANTENER** con la cuál podrá olvidarse de la seguridad de su empresa. **UN SEGURO A TODO RIESGO.**

La pérdida de información está provocando en las empresas **importantísimas pérdidas económicas**. Según un estudio de Symantec, *"casi una cuarta parte de las pymes europeas sufrieron ataques el año pasado, en España el porcentaje fue de una quinta parte como consecuencia a dichos ataques sus organizaciones sufrieron caídas del sistema (85 por ciento) y Pérdidas de información (50 por ciento)"*

**ACTIVA**



**TU SEGURIDAD**

# Fallos de seguridad a los que está expuesta su empresa

"ESPERAR A QUE SE PRODUZCA UN CRIMEN, ES POR DEFINICION, DEMASIADO TARDE"

## SEGURIDAD FRENTE A INTERNET:



**Virus, Troyanos, Gusanos y Demás:** Los virus, gusanos y troyanos son programas malintencionados que pueden provocar daños en el equipo y en la información del mismo. También pueden hacer más lento Internet e, incluso, pueden utilizar su equipo para difundirse a amigos, familiares, colaboradores y el resto de la Web

Podremos **escanear todo el tráfico que llega desde el exterior y en el interior de nuestra empresa** eliminando cualquier paquete sospechoso, sin requerir instalación en el cliente y totalmente configurable.



**Spywares:** Los Spyware son pequeños programas que se instalan en nuestro sistema con la finalidad de robar nuestros datos y espiar nuestros movimientos por la red. Luego envían esa información a empresas de publicidad de Internet para comercializar en nuestros datos

Podremos **escanear todo el tráfico que llega desde el exterior y en el interior de nuestra empresa** eliminando cualquier paquete sospechoso, sin requerir instalación en el cliente y totalmente configurable



**Spam:** Se llama spam a la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados. Generalmente, se trata de publicidad de productos, servicios o de páginas web

Tendremos **a nuestra disposición servidores ANTISPAM dedicados** a capturar dicho material además de poder ir ampliando las listas de spam por nuestra cuenta.



**Accesos no deseados (Hackers, Cracker):** Generalmente siempre tenemos algún puerto abierto hacia el exterior en nuestra red por necesidades de la empresa y de esto se aprovechan para intentar acceder a ella produciendo un fallo de seguridad grave.

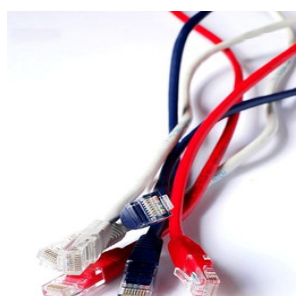
Podremos **bloquear cualquier tipo de acceso a nuestra empresa desde el exterior como también cualquier tipo de salida desde el interior**

# Fallos de seguridad a los que está expuesta su empresa



**Pérdida de información:** Ataques y amenazas de red proceden de muchas fuentes y una mera protección antivirus ya no basta para proteger las redes esenciales de la empresa. El Servicio de Detección y Prevención de Intrusiones (IDP) proporciona a los clientes lo último en defensa contra la actividad invisible de red dañina y sospechosa. Trabajamos con empresas de todo el mundo, 24 horas al día, para aislar las últimas vulnerabilidades de aplicaciones y SO, creando las últimas tecnologías de detección y prevención para mantener a los clientes un paso por delante de los hackers.

Mediante un mecanismo de **detección y prevención de intrusiones (IDP)** escucharemos el tráfico en la red para **detectar actividades anormales o sospechosas**, y de este modo, **reducir el riesgo de intrusión**.



**Ataques y anomalías en nuestra red:** Es posible detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos. Es usado por administradores de sistemas para analizar posibles problemas de seguridad, pero también es utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red.

Mediante un mecanismo de **protección de tráfico de la red (ADP)** escucharemos el tráfico en la red para **detectar posible flujo de tráfico de red ANORMAL, protocolos anormales y escaneos de puertos**



**Conexiones poco seguras entre sedes:** Si queremos trabajar desde casa o tenemos varias sedes separadas geográficamente y necesitamos trabajar como si estuvieran dentro de una misma red, necesitamos algún tipo de protección ya que la información que sale por Internet está desprotegida y a merced de cualquier intruso.

Podremos comunicarnos remotamente desde nuestra casa u otra sede a nuestra red local de la empresa de una manera fiable y segura a través de Internet asegurando la **confidencialidad** (en el caso de ser interceptados los datos, no pueden ser descodificados) e **integridad** (además de no ser interpretados los datos no pueden ser modificados) de los datos.



**Cortes de conexión a Internet:** Si tenemos una única línea de ADSL, se pueden producir cortes de conexión con nuestra compañía de Internet y dejar a nuestra empresa sin conexión con el exterior.

Nuestra solución de seguridad ofrece la **posibilidad de tener una tarjeta 3G en modo de backup** para poder seguir navegando en la red si se produce un problema en nuestra línea ADSL habitual **asegurando INTERNET 24h 365 días**.

## Fallos de seguridad a los que está expuesta su empresa



**Línea ADSL demasiado lenta:** Si tenemos una única línea de ADSL, es posible que la velocidad de la red no responda a las necesidades de la empresa, ya sea por la velocidad máxima permitida en la zona como por el exceso de demanda de los usuarios.

Nuestra solución de seguridad ofrece la **posibilidad de tener 2 líneas de ADSL a la vez** y asegurar un balanceo de carga por lo que **siempre estaremos utilizando la línea menos saturada.**

### SU RED FRENTE AL MAL USO INTERNO:

*"Las amenazas más grandes para la seguridad de la información no vienen a menudo de hackers. Vienen de los propios empleados de una compañía."*



**Filtrado de contenidos WEB:** Navegar por Internet se ha convertido en una parte esencial del trabajo y muchas veces en una exigencia. Sin embargo, su uso inapropiado redonda en menor productividad, empleo impropio de los recursos, acoso, responsabilidad legal y problemas de recursos humanos

Mediante el filtrado de contenidos podemos limitar el acceso a contenidos explícitos **evitando la navegación no productiva para el entorno laboral.**



**Aplicaciones con restricción:** Messenger, Emule, video/sonido streaming, Juegos online, etc... son aplicaciones que ralentizan la red de la empresa y hacen que la productividad global baje notablemente.

Podremos no solo **bloquear en su totalidad cualquier aplicación** que pueda consumir ancho de banda de su red, sino que además **permite restricciones parciales** para éste tipo de aplicaciones.

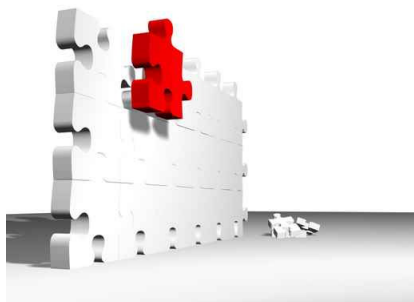
## Fallos de seguridad a los que está expuesta su empresa



**Excesivo consumo de ancho de banda por un usuario:** Es posible que ciertos usuarios en nuestra empresa posean cierta libertad para trabajar con programas específicos que puedan consumir de una manera notable el ancho de banda de nuestra red

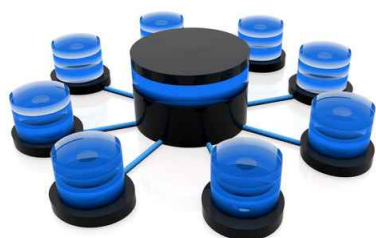
Podremos establecer límites de consumo de ancho de banda para determinados usuarios y en los horarios que se estimen oportunos.

### OTROS DATOS A SU FAVOR:



#### **Escalabilidad:**

Nuestro dispositivo se puede configurar como una sola solución de seguridad de red personalizada, utilizando una **gran variedad extensiva de servicios integrados perfectamente.**



#### **Mantenimiento centralizado:**

Todas las opciones de seguridad de nuestro dispositivo **se configuran desde un mismo panel de control**, facilitando el mantenimiento completo de la seguridad de nuestra empresa.

## MANTENIMIENTO DE SU SEGURIDAD

En Dragomar Informática **queremos que se olvide por completo de la seguridad de su empresa**, por lo que si ha contratado nuestra solución de seguridad y por una pequeña cuota mensual, nosotros nos encargamos de los diversos temas de seguridad de su empresa



### **Crear / mantener nuevas reglas :**

En el apartado de antivirus, podemos configurar patrones de ficheros que o no van a ser escaneados nunca o que directamente siempre se van a eliminar cuando se detecten. Por ejemplo, hay virus que siempre crean un archivo ejecutable con el mismo nombre, por lo que añadiendo el nombre del fichero en la lista negra de la sección de antivirus, estamos mejorando la defensa contra virus.



### **Actualizar remitentes bloqueados :**

El spam se controla mediante unos servidores dedicados que tienen en sus bases de datos las direcciones de correo de SPAM más conocidas, pero diariamente se va generando nuevo spam, por lo que podemos añadir manualmente los remitentes que pensemos que son spam y de una forma centralizada afectará a toda la empresa



### **Configurar conexiones seguras :**

Configurar que usuarios son seguros para permitir conexiones directas con ellos, desde clientes de terminal Server, de vnc, de ftp, etc. Para tener siempre asegurada la conexión con el exterior.



### **Gestión de conexiones VPN:**

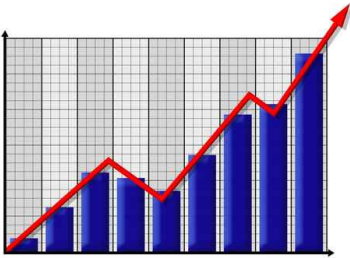
Creación y mantenimiento de usuarios y reglas de VPN para asegurar la Conexión segura entre sedes.

# MANTENIMIENTO DE SU SEGURIDAD



## **Configuración aplicaciones con restricción:**

Configuración y mantenimiento del acceso a dichas aplicaciones.



## **Gestión de estadísticas mensuales:**

Podrá recibir mensualmente estadísticas varias sobre intentos de acceso a su red, gestión de accesos a web de su empresa, etc para llevar un control más exhaustivo de su seguridad



## **Actualización firmware:**

Muchas veces la actualización del firmware añade mejoras a un dispositivo, como una característica adicional, una habilidad nueva o solucionar un problema de seguridad.

