

PRODUCTOS SEGURIDAD EN LA RED CIBERSEGURIDAD

Los productos descritos a continuación son productos de uso cada vez más necesario en micropymes

Estas micropymes carecen de informáticos internos por lo que la alternativa a la que normalmente acceden es a la adquisición de estas soluciones por cuenta propia generando un nuevo problema ya que hoy por hoy las interacciones entre dispositivos, actualizaciones, interactividad, movilidad de los usuarios, etc hacen que sea necesario disponer de un informático para los servicios esenciales.

Todos estos productos incluyen “informático” por lo que el cliente ahorra costes y evita preocupaciones.

Estas soluciones forman parte de una nueva generación de propuestas llave en mano y totalmente administradas para estas pequeñas empresas que no pueden permitirse tener plantilla propia y que funcionan de manera efectiva evitando gastos de personal adicionales.

SEGURIDAD ACTIVA

Antivirus basados en motores de los más reconocidos fabricantes de antivirus. No solo es una solución de antivirus sino que incluye la administración y supervisión constante del mismo. Es decir, es el típico servicio de antivirus pero con informático incluido.

ANTIVIRUS

- **MURANIUM ANTIVIRUS BASICS**

Antivirus y malware, el típico antivirus potente pero no molesto.

Protege bastante y requiere una administración muy sencilla por lo que resulta muy interesante para la mayoría

- **MURANIUM FULL PROTECTION**

Como el anterior, pero incluye escudos adicionales como el firewall y el análisis de tráfico. Detiene la mayoría no solo de ataques sino también de intrusiones mediante tráfico que no contiene virus

- **MURANIUM EDR SOLUTION**

Incluye además de todo lo anterior, la solución de análisis y diagnóstico con opciones potentes que permiten a los técnicos aislar las amenazas.

Incluye la administración de las actualizaciones del sistema operativo

SEGURIDAD PASIVA

Copias de seguridad incluyendo servicio técnico correctivo (muy importante esto, la mayoría de las copias acaban fallando por qué cambios en los equipos y/o actualizaciones acaban por desconfigurar el entorno. La copia para que sea efectiva requiere revisar periódicamente y contrastar los contenidos copiados con el usuario. Del mismo modo que requiere realizar acciones correctoras. Es un servicio de backup en la nube de alta calidad cuyo más importa

COPIAS DE SEGURIDAD

- **DATAGUARDA BACKUP SERVER**

Copia de seguridad en la nube con servicio de administración y monitorización pensado para servidores

- **DATAGUARDA BACKUP USERS**

Copia de seguridad en la nube con servicio de administración y monitorización pensado para usuarios estratégicos y directivos

- **MURANIUM2x2 HYBRID**

Incluye copia en la nube y copia local. Pero también incluye la copia mediante 2 sistemas de backup

SEGURIDAD PREVENTIVA

Seguridad orientada al entrenamiento de los usuarios para la detección de amenazas según la ley europea de protección de datos. El sistema permite el alta de los usuarios y la gestión automatizada de la formación y los simulacros así como la constante evaluación.

SEGURIDAD PERIMETRAL

Sistemas de seguridad perimetral usando dispositivo físico (Firewall inteligente) mediante análisis de tráfico de red y filtrado avanzado de paquetes permitiendo detectar las amenazas y las fugas de datos antes de que prosperen incluso cuando se realizan con programas indetectables por los antivirus.

FIREWALL

- **MURAMIUM FIREWALL**

Análisis de tráfico a la entrada de red y monitorización y administración del sistema.
monitorización tráfico usando Google Cloud Coste de la instancia incluido

- **MURAMIUM ADVANCED FIREWALL**

Análisis de tráfico a la entrada de red y monitorización y administración del sistema.
monitorización tráfico usando Google Cloud Coste de la instancia incluido análisis detallado de tráfico
usando motores Cloud de Proofpoint ET Open IPS / IDS ampliaciones del
producto

SEGURIDAD INTRINSECA

Seguridad orientada al control de usuarios evitando fugas de datos o el uso indebido de los activos de la organización. Esta seguridad puede aplicarse mediante reglas generales de uso y buenas costumbres que analizan especialmente contenidos y el uso en internet que hacen los usuarios de los equipos o mediante sistemas AD-HOC donde se realiza una vigilancia estrecha del uso de los equipos, acceso a datos, uso de dispositivos USB para extraer información y monitorización de los archivos que salen en el correo o que se suben a la web.

Los sistemas AD-HOC no los valoro en la siguiente estimación pues son más complejos y las opciones son muchas.

Vigilancia y denegación de tráfico organizada por familias de contenidos (adultos, piratería, hacker, juegos, social, etc. etc.) el servicio incluye la creación y mantenimiento de perfiles organizados por grupos según nivel de acceso que se requiera conceder.