**Ambiente ideal**

Equipamiento (Hardware):

1. Firewalls
2. Filtros de contenido (Correo)
3. Filtros AntiSpam (Correo)
4. Filtros web (Navegación)
5. Proxis
6. Sistema IPS:

Intrusion prevention System

1. Sistema de correlación de eventos
2. Sistema UEBA
3. Equipamiento Forense:

Dump de Memoria, Volcado de disco.

1. Plataforma MISP
2. Escaneador de Vulnerabilidades (Nessus)

Adicionalmente al Hardware se requiere cubrir siguientes aspectos:

* **Establecer una política de seguridad**, que se puede reflejar en documentos y que constituye la base del entorno de seguridad de una empresa y definir las responsabilidades, requisitos de seguridad y funciones a seguir por los empleados.
* **Proteger los equipos de escritorio y portátiles**: los virus, troyanos y, en general, cualquier software malicioso puede infectar nuestros ordenadores y hacerlos vulnerables a cualquier agente externo. La respuesta parece evidente, pero no siempre se aplica: instalar un antivirus y, debido a la rapidez con la que avanzan los sistemas de información (incluyendo el *malware*), mantenerlo actualizado de manera conveniente.
* El correo electrónico y, en general, el acceso a Internet **suelen ser los mayores problemas a los que se enfrenta una empresa en materia de seguridad informática**. Toda seguridad es poca para evitar que un empleado de nuestra empresa acabe instalándose (lo más seguro es que sin querer), un agente malicioso que acabe infectando al resto de equipos o, quien sabe, a los propios servidores de la empresa. Aplicar un firewall o evitar el correo electrónico no deseado (spam) pasan por ser algunas de las soluciones muy a tener en cuenta.
* En este sentido, si nuestra empresa trabaja con ordenadores conectados en red, **es imprescindible protegerla**. Dejar al mando a una sola persona o un grupo de personas muy reducido que gestionen esta seguridad, aunque sea en principio caro, puede resultar mucho más caro a la larga. Utilizar contraseñas seguras para el acceso a la red(no el típico "1234"), proteger la red Wifi, ocultando por ejemplo el SSID o utilizando cifrado WPA2, o configurar un firewall a nivel de red pueden ser buenas soluciones.
* En el momento que los servidores están infectados, el resto de red es susceptible de estar infectada. Es recomendable identificar a los sitios web y **establecer conexiones seguras con nuestros clientes**, si puede ser mediante el uso de certificados web. También es altamente recomendable mantener los servidores físicos en lugares seguros o con acceso restringido, para evitar posibles robos y evitar que sean vulnerables a catástrofes físicas.
* **Mantener los datos a salvo**. Aunque esta premisa es bastante evidente, por desgracia no son pocas las ocasiones en las que se incumple. Es importante realizar copias de seguridad de nuestros sistemas cada periódicamente, cifrar los datos confidenciales o utilizar sistemas de alimentación ininterrumpida (SAI) en caso de que usemos ordenadores de sobremesa.
* **Implementando un directorio activo** facilitamos las tareas tanto de seguridad como de funcionalidad, centralizando la propagación de permisos a los usuarios y facilitando la estructuración de la información. Es conveniente tener actualizado nuestros servicios de bases de datos.
* En las empresas no solo existen ordenadores personales. **También debemos proteger los dispositivos móviles**, y para ello debemos concienciar a nuestros empleados, que al fin y al cabo son los que los van a manejar.
* Por último, debemos ser **cuidadosos a la hora de gestionar los datos de carácter personal**. En muchas ocasiones se subcontratan servicios que suponen acceso a datos personales. Cualquiera de las partes podrá proponer la firma de un contrato de acceso a datos, que deberá formalizarse preferiblemente por escrito, de manera que acredite fehacientemente su celebración y contenido

En algunas ocasiones, además, **la mayor amenaza muchas veces no proviene del exterior, sino del interior de nuestro propio entorno**.

Trabajadores descontentos, clientes insatisfechos e incluso algunos competidores puede resultar ser nuestro mayor problema. Ni que decir tiene lo complicado de vigilar esto pero es conveniente tratar de monitorizar quién ha hecho qué en cada momento y ver a qué páginas web ha accedido. Todo esto puede resultar caro, pero puede salir muy caro a la larga si no se gestiona una política de seguridad adecuada.

Los siguientes aspectos comunicativos han demostrado su utilidad práctica, por lo que merece la pena tomarlos en consideración:

* Sitio web público
* Zona reservada a los miembros en el sitio web
* Formularios web para comunicar incidentes
* Listas de correo
* Correo electrónico personalizado
* Teléfono / fax
* SMS
* Las «anticuadas» cartas tradicionales, en soporte de papel
* Informes mensuales o anuales

**Planes de mitigación:**

1. Disaster recovery
2. Check list
3. Trabajo en terreno