

INDICE DE LA PRESENTACIÓN



PRESENTACIÓN

- OBJETIVO
- ORIGEN DE LA INFORMACIÓN



SITUACIÓN TECNOLÓGICA, USO DE LAS TIC



RIESGOS. ¿POR DONDE LLEGAN?



PROTEGERNOS DE LOS RIESGOS. HERRAMIENTAS DE SEGURIDAD



NUESTROS HIJOS Y LAS TIC



CONSEJOS A LOS JOVENES



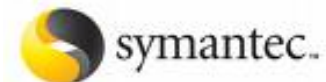
DECALOGO BUEN USO INTERNET



ANTIVIRUS

BUENAS PRÁCTICAS

- Actualice la herramienta antivirus con frecuencia para conseguir una protección eficaz.
- Active la actualización automática en la configuración del producto.
- Verifique cada mensaje nuevo de correo antes de abrirlo, sobre todo los que contengan ficheros adjuntos y los de origen sospechoso.
- Evite la descarga e instalación de programas desde sitios Web que no ofrezcan garantías.



Avast Home · Avira AntiVir Personal · AVG Free Antivirus.

SOFTWARE ANTIESPÍA

BUENAS PRÁCTICAS

- Actualice la herramienta con frecuencia para garantizar una protección efectiva.
- Verifique la procedencia y fiabilidad de los ficheros adjuntos en su correo electrónico.
- No descargue ficheros (ejecutables, salvapantallas, software...) que procedan de fuentes desconocidas.



A-squared Free · Spybot S&D · Ad-Aware 2008 Free

CORTAFUEGOS

BUENAS PRÁCTICAS

- Identifique las aplicaciones confiables y los usuarios autorizados.
- Revise los mensajes y el registro de actividad del cortafuegos con frecuencia.
- Controle no sólo las conexiones salientes sino también las entrantes.



Windows Firewall · Zone Alarm · Ashampoo · Comodo

CONTROL PARENTAL

BUENAS PRÁCTICAS

- Es necesario establecer permisos en el ordenador donde será instalada la herramienta para evitar que la protección parental pueda ser desactivada.
- Actualizar la herramienta con nuevos sitios de contenido inadecuado.
- Revisar el registro de actividad para comprobar los sitios visitados.



TechMission · File Sharing Sentinel · K9 Web Protection

BUENAS PRÁCTICAS

- Nunca acceda a la banca electrónica haciendo clic en enlaces o utilizando los favoritos del navegador. Escriba siempre la «URL» (por ejemplo: <http://www.mibanco.es>) de la entidad directamente sobre el navegador.
- Verifique que la página web es segura —empieza por «https://»— y que está certificada —tiene un candado en la parte inferior derecha—. Haciendo doble clic sobre este candado puede confirmar que la web es legítima.
- No acceda a la banca «on-line» desde ordenadores o sitios no confiables (cibercafés, aeropuertos...).
- Utilice siempre contraseñas difíciles de averiguar, especialmente para la banca electrónica. Utilice contraseñas específicas para cada servicio / aplicación.
- Mantenga limpio su equipo de virus y otros códigos maliciosos, software malicioso, mediante el uso de herramientas contra el software malicioso actualizadas.
- Si tiene alguna sospecha de estafa, consulte con la entidad bancaria.