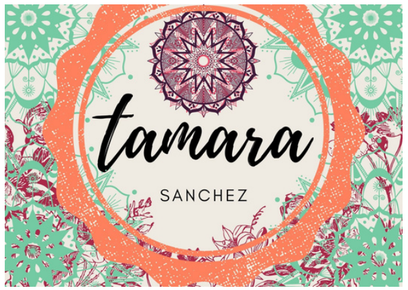
Seguridad y resolución de problemas técnicos



Las acciones de prevención relativas a la seguridad digital son fundamentales ya que a través de elementos electrónicos y digitales realizamos compras, establecemos conversaciones, negocios...etc. Ya que tenemos una actividad tan importante empleando medios digitales el crecimiento de los delitos relacionados con este medio han crecido de manera exponencial.

1) **Realiza un decálogo con acciones y/o elementos (software por ejemplo) que te parecen fundamentales para prevenir y proteger nuestros dispositivos digitales como un ordenador o un móvil. Para protegerlos de virus, software malicioso, troyanos y robo de datos.**

2) **Explica por qué consideras importante cada acción.**

1. Decálogo con acciones y/o elementos para prevenir y proteger nuestros dispositivos

1. Proteger tu privacidad en Internet (comunicaciones seguras, intercambio de datos con un servidor)
2. Mantener el dispositivo actualizado (antivirus, o herramienta para seguridad)
3. Examinar con detenimiento que información hacen pública automáticamente en las distintas redes sociales

4. Crear protección frente a accesos no deseados(contraseñas)

5. Detección de accesos y?o usos no controlados de dispositivo (ofrecer consultas)

6. Impedir Google y otras empresas que rastreen el historial de navegación,("modo incógnito")

7. Usar otro motor de búsqueda o VPN(Red Privada Virtual)

8. Al descargar cualquier software, comprobar qué permisos solicitan

9. Herramientas para proteger la privacidad en los dispositivos móviles

10. Gestión de contraseñas y modificación de ellas usualmente

2.

Decálogo .porque es necesário

Los problemas de privacidad que nos plantea Internet son enormes y avanzan, hace que resulte difícil mantenerse al corriente.

Los datos valen dinero, lo cual es uno de los principales motivos por los que la privacidad en Internet está amenazada.

La aparición del big data implica que tu historial de navegación podría analizarse para llegar a conclusiones sobre ti que no te interesa que se extraigan.

1. Proteger tu privacidad en Internet (comunicaciones seguras, intercambio de datos con un servidor)

.cambiar el nombre de usuario de la red doméstica

.red privada virtual (VPN). Establece una pasarela privada entre tú e Internet y cifra tus comunicaciones para que nadie pueda ver lo que estás haciendo. Aunque utilices una red Wi-Fi pública, una VPN proporciona la misma seguridad que tendrías en tu propia red.
no puede rastrear ni mediante cookies ni mediante otros métodos de seguimiento, porque la VPN también oculta la dirección IP

transacciones sensibles, asegúrar de hacerlo a través de un navegador seguro que utilice el protocolo HTTPS (El protocolo seguro HTTPS utiliza SSL/TSL para cifrar las comunicaciones)

Incluso aunque tu acceso sea seguro, Google u otra empresa de Internet podría rastrear el uso que se hace de la Red, y también es posible que rastreen el proveedor de Internet

Muchos usuarios de Facebook preocupados por la seguridad ahora limitan sus publicaciones a «solo amigos».
No interesa que la dirección de correo electrónico y el número de teléfono estén disponibles para el público a través de los perfiles en las redes sociales

Un software antivirus asegurará la protección de los dispositivos frente a amenazas comunes.
Cuantos más programas y aplicaciones se ejecuta, más posibilidades hay de que uno de ellos se infecte.