


Ética y seguridad informática





Respeto de la privacidad



- Consentimiento informado. Tener el ok de la otra parte para usar sus datos.
 - Seguridad de la información. Mantener los datos a salvo.
 - Transparencia. Tener políticas de seguridad claras sobre el uso de la información
 - Acceso y control. Permitir al usuario ver sus datos y poderlos actualizar.
 - Responsabilidad ética. Corregir el problema en caso de fuga de datos.
- 


Ciberbullying




- Que es? Importancia de mantener un comportamiento ético en linea
 - Políticas y normativas.
 - Anonimato responsable. Fomentar la identidad digital.
 - Reporte y respuesta rápida.
 - Control parental.
 - Cultura de empatía y respeto.
- 


Responsabilidad en línea




- Educación y concienciación. Riesgos y consecuencias de comportamientos irresponsables.
 - Reconocimiento de las consecuencias éticas de las acciones en línea.
 - Integridad de la información. Verificar antes de compartir.
 - Comportamiento ético en redes sociales.
 - Uso ético de la tecnología. Respetar derechos de autor.
- 


Plagio digital



- Copiar y pegar sin citar la fuente
 - Reutilizació de gràfics o fuentes sin permiso
 - Compra de trabajos académicos en linea
 - Auto-plagio
 - Uso indebido de código fuente
- 


Propiedad intelectual



- Respetar los derechos de autor de los programas.
 - Conocer el software libre que es otra opción.
 - Evitar la participación en piratería informática.
 - Evitar el acceso a sistemas sin autorización.
- 

Contraseñas seguras



- Longitud
 - Complejidad. Mayúsculas+minúsculas+carácteres
 - Evita información personal.
 - No uses palabras comunes.
 - Contraseñas únicas.
 - Evita patrones obvios. (1234)
 - Nombres de usuario y contraseñas distintos.
 - Actualiza regularmente.
- 

Prevención de malware y virus

- Software de seguridad. Antivirus, firewall.
- Actualizaciones del sistema.
- Navegación segura.
- Correos electrónicos y phishing.
- Respaldo de datos.
- Restricciones de permisos. No admin.
- Instalar actualizaciones y parches. También de terceros.
- Redes seguras.
- Monitoreo de actividades inusuales.(Rendimiento lento)

Redes seguras:

- Cambie habitualmente las claves de su enrutador Wifi.
- Evite redes wifi no seguras.



This work is licensed under
a Creative Commons Attribution-ShareAlike 3.0 Unported License.
It makes use of the works of
Kelly Loves Whales and Nick Merritt.