

Universidad Internacional de Valencia (VIU)

20GIIN – Ética, Legislación y Profesión

Actividad #2

El uso responsable de la tecnología

Alumno: Gagliardo Miguel Angel

Introducción

Para hablar sobre el uso responsable de la tecnología deberíamos empezar por definir a que llamamos tecnología. Según la RAE¹, tecnología es aquel conjunto de teorías y técnicas que permiten el aprovechamiento práctico del conocimiento científico.

La tecnología es una de las principales herramientas para el desarrollo de las sociedades. Es un habilitador de derechos que permite a las personas trabajar, estudiar, comunicarse, informarse e incluso es utilizada para el ocio y tiempo libre.

Es importante destacar también que en los últimos 20 años hemos visto una adopción sin precedentes en el uso de las Tecnologías de la Información y la Comunicación (TIC) y por esto, en este informe se intentara abordar el uso responsable de la tecnología desde dos grandes puntos de vista: Creadores y profesionales del área de sistemas, y usuarios tanto adultos como jóvenes.

El uso responsable de la tecnología en Profesionales

Merece un apartado especial la responsabilidad de los profesionales que trabajan en Tecnología/TIC, a fin de concientizar sobre las consecuencias de los actos y los resultados de la labor en este sector y el impacto que tiene en el conjunto de la sociedad.

La Association for Computing Machinery (ACM) en su Código de Ética y Conducta Profesional² define una serie de principios sobre los cuales vale la pena reflexionar. En este apartado resaltaremos algunos de los puntos mas importantes del mismo.

1. Principios Éticos Generales

- **Contribuir a la sociedad y el bienestar humano, entendiendo que todos los seres humanos son partes interesadas en la computación:** Este principio, que concierne la vida de todos, reafirma la obligación de los profesionales de TI, tanto individual como colectivamente, para que utilicen sus habilidades para el beneficio de la sociedad, sus miembros y el entorno que los rodea.

Este principio incluye también, promocionar los derechos humanos básicos y proteger la autonomía de cada ser humano.

- **Evitar el daño:** Con “daño” nos referimos a consecuencias negativas, especialmente aquellas que son significativas e injustas. Los ejemplos de daños incluyen lesiones físicas o mentales injustificadas, destrucción o divulgación injustificada de información y daños injustificados a la propiedad, la reputación y el medio ambiente.

Evitar el daño comienza con una cuidadosa consideración de los impactos potenciales sobre todos los afectados por las decisiones. Cuando el daño es una parte intencional del sistema, los responsables están obligados a garantizar que el daño esté éticamente justificado. En cualquier caso, la idea final es asegurarse de minimizar todos los potenciales daños.

- **Ser honesto y digno de confianza:** La honestidad es un componente esencial de la confiabilidad. Un profesional de la computación debe ser transparente y proporcionar una divulgación completa de todas las capacidades, limitaciones y problemas potenciales del sistema pertinente a las partes correspondientes.

Los profesionales de la informática deben ser honestos sobre sus calificaciones y sobre cualquier limitación en su competencia para completar una tarea, deben ser francos sobre cualquier circunstancia que pueda conducir a conflictos de intereses reales o percibidos o que tiendan a socavar la independencia de su juicio.

- **Ser justo y tomar medidas para no discriminar:** Los valores de igualdad, tolerancia, respeto por los demás y justicia rigen este principio.

Los profesionales de la informática deben fomentar la participación justa de todas las personas, incluidas las de los grupos subrepresentados. La discriminación perjudicial por motivos de edad, color, discapacidad, etnia, situación familiar, identidad de género, afiliación sindical, condición militar, nacionalidad, raza, religión o creencias, sexo, orientación sexual o cualquier otro factor inapropiado es una violación explícita de el código.

- **Respetar el trabajo requerido para producir nuevas ideas, invenciones, trabajos creativos y artefactos informáticos:** Los profesionales de la computación deben acreditar a los creadores de ideas, invenciones, trabajos y artefactos, y respetar los derechos de autor, las patentes, los secretos comerciales, los acuerdos de licencia y otros métodos para proteger las obras de los autores.

- **Respetar la privacidad:** La responsabilidad de respetar la privacidad se aplica a los profesionales de la informática de una manera particularmente profunda. La tecnología permite la recopilación, el seguimiento y el intercambio de información personal de forma rápida, económica y, a menudo, sin el conocimiento de las personas afectadas. Por lo tanto, un profesional de la informática debe familiarizarse con las diversas definiciones y formas de privacidad y debe comprender los derechos y responsabilidades asociados con la recopilación y el uso de información personal.

- **Honrar la confidencialidad:** A los profesionales de la informática a menudo se les confía información confidencial, como secretos comerciales, datos de clientes, estrategias comerciales no públicas, información financiera, datos de investigación, artículos académicos previos a la publicación y solicitudes de patentes.

Los profesionales de la informática deben proteger la confidencialidad excepto en los casos en que sea evidencia de la violación de la ley, de las normas organizacionales o del Código de ética. En estos casos, la naturaleza o el contenido de esa información no debe divulgarse excepto a las autoridades competentes.

2. Responsabilidades Profesionales

- **Conocer y respetar las normas vigentes relativas al trabajo profesional:** Por "reglas" nos referimos a leyes y reglamentos locales, regionales, nacionales e internacionales, así como cualquier política y procedimiento de las organizaciones a las que pertenece el profesional.

Los profesionales de la informática deben cumplir con estas reglas a menos que exista una justificación ética convincente para hacer lo contrario. Las reglas que se juzguen poco éticas deben ser desafiadas. Una regla puede ser poco ética cuando tiene una base moral inadecuada o causa un daño reconocible. Un profesional de la computación debería considerar desafiar la regla a través de los canales existentes antes de violarla. Un profesional de la informática que decida violar una regla porque no es ético, o por cualquier otra razón, debe considerar las posibles consecuencias y aceptar la responsabilidad de esa acción.

- **Aceptar y proporcionar la revisión profesional adecuada:** El trabajo profesional de alta calidad en informática depende de la revisión profesional en todas las etapas. Siempre que sea apropiado, los profesionales de la computación deben buscar y utilizar la revisión por pares y partes interesadas. Los profesionales de la informática también deben proporcionar revisiones críticas y constructivas del trabajo de otros.

- **Proporcionar evaluaciones completas y exhaustivas de los sistemas informáticos y sus impactos, incluido el análisis de posibles riesgos:** Los profesionales de la informática se encuentran en una posición de confianza y, por lo tanto, tienen la responsabilidad especial de proporcionar evaluaciones y testimonios objetivos y creíbles a los empleadores, empleados, clientes, usuarios y el público.

Los profesionales de la informática deben esforzarse por ser perspicaces, minuciosos y objetivos al evaluar, recomendar y presentar descripciones y alternativas de sistemas. Se debe tener un cuidado extraordinario para identificar y mitigar los riesgos potenciales en los sistemas de aprendizaje automático. Un sistema para el cual los riesgos futuros no se pueden predecir de manera confiable requiere una reevaluación frecuente del riesgo a medida que el sistema evoluciona en uso, o no se debe implementar. Cualquier problema que pueda resultar en un riesgo importante debe informarse a las partes correspondientes.

- **Realizar trabajos únicamente en áreas de su competencia:** Un profesional de la computación es responsable de evaluar las asignaciones de trabajo potenciales. Esto incluye evaluar la factibilidad y conveniencia del trabajo, y emitir un juicio sobre si la asignación de trabajo está dentro de las áreas de competencia del profesional. Si en cualquier momento antes o durante la asignación de trabajo, el profesional identifica la falta de la experiencia necesaria, debe comunicárselo al empleador o al cliente. El cliente o empleador puede decidir continuar con la tarea con el profesional después de un tiempo adicional para adquirir las competencias necesarias, continuar con la tarea con otra persona que tenga la experiencia requerida o renunciar a la tarea. El juicio ético de un profesional de la computación debe ser la guía final para decidir si trabajar en la asignación.

- **Fomentar la conciencia pública y la comprensión de la informática, las tecnologías relacionadas y sus consecuencias:** Según sea apropiado para el contexto y las habilidades de cada uno, los profesionales de la informática deben compartir conocimientos técnicos con el público, fomentar la conciencia de la informática y fomentar la comprensión de la informática. Estas comunicaciones con el público deben ser claras, respetuosas y acogedoras. Los temas importantes incluyen los impactos de los sistemas informáticos, sus limitaciones, sus vulnerabilidades y las oportunidades que presentan. Además, un profesional de la informática debe abordar con respeto la información inexacta o engañosa relacionada con la informática.

El uso responsable de la tecnología en la juventud

De acuerdo con los datos de la Secretaria de Estado de Digitalización e Inteligencia Artificial de España, en su reporte³ de 2022, el 95% de los niños de 6 a 15 años viven en hogares con los medios o recursos suficientes para asistir a clases o actividades de tele escuela. Esta alta presencia de niñas, niños y adolescentes en espacios digitales aumenta los riesgos a los que podrían ser vulnerables, pues normalmente navegan solos durante varios minutos e incluso horas, abriendo una puerta importante de riesgo a una red de personas y perfiles virtuales falsos que pueden atentar contra su integridad y privacidad.

Por ello, es indispensable fortalecer la cultura de reporte de contenido inapropiado y que vulnere la seguridad e integridad de los menores de edad en entornos digitales. Así mismo, es importante que víctimas y familiares puedan realizar denuncias y reportar de forma anónima y sencilla, páginas de contenido inapropiado detectado en internet.

Para lograr un entorno digital seguro para los menores, así como la protección y promoción de los derechos de las niñas, niños y adolescentes en Internet, es necesario actuar con una responsabilidad compartida y comprometernos como sociedad.

Cada uno de nosotros puede contribuir por el bienestar superior de la niñez a través de acciones de difusión, prevención, información, educación y erradicación de los riesgos en la red, así como en ejercer y promover la denuncia. Es así, como podremos incrementar la confianza digital para aprovechar todas las oportunidades y beneficios que nos brinda la tecnología, para lograr sociedades más fuertes e inclusivas en las que nadie se quede atrás.

El rol de la educación en Nativos Digitales

Podríamos decir que los **nativos digitales** son todas aquellas personas que han nacido y se han formado rodeados de tecnología utilizando la particular “lengua digital” de juegos por ordenador, vídeo e Internet, normalmente nos referimos a las generaciones mas recientes, también conocidas como “Centennials” o “Generacion Z”.

Si bien es cierto que los nativos digitales están muy familiarizados con el uso de la red y la tecnología, no lo están tanto en el abuso que pueden hacer de las mismas otras personas y/u organizaciones malintencionadas, que pretenden comprometer la seguridad de los entornos digitales.

Por eso, entre los principales desafíos que tienen los nativos digitales, destacan:

- **Aprender a hacer un uso seguro de los dispositivos que utilizan:** Hay estudios que ponen de manifiesto “el mito del nativo experto” y revelan que gran parte de los nativos digitales “saben cómo utilizar los dispositivos desde la perspectiva del ocio pero no desde la perspectiva de la seguridad” y que la mayoría, no saben cómo administrar las contraseñas de sus cuentas ni cómo crear contraseñas robustas.

Desde pequeños, deberán ir aprendiendo medidas de seguridad básicas, como gestionar sus cuentas y contraseñas, y de esta manera, ir adquiriendo comportamientos seguros.

- **Cuidar su privacidad en internet y navegar de forma segura:** Muchas veces se habla de la “mala higiene digital” que tienen los nativos digitales, especialmente, los más pequeños: no entienden el concepto de privacidad, comparten las cuentas con sus amigos o dan permisos ilimitados a aplicaciones que descargan, incluyendo las que permiten acceder a todas sus fotos y videos, sin cuestionar lo que puede implicar desde el punto de vista de su privacidad y seguridad.

- **Proteger su identidad digital:** Los menores y, más concretamente los adolescentes, no tienen noción de permanencia en términos de “huella digital”, no reparan en las repercusiones que pueden tener sus publicaciones actuales en un futuro no muy lejano, ni se plantean cómo pueden llegar a afectar incluso a su incorporación en el mercado laboral.

- **Ser conscientes de que hay otras personas que saben mas que ellos en la red y pueden ser, no tengan buenas intenciones:** Los nativos digitales han nacido aprendidos y lo saben. Este exceso de confianza es uno de los mayores inconvenientes de cara a su seguridad y uno de los retos más significativos que deben superar. Normalmente no son conscientes de que hay otras personas en la red que pueden tener más conocimientos que ellos, que les pueden engañar, estafar o suplantar la identidad. Por tanto, deben aprender a controlar su exceso de confianza en el mundo digital.

- **Adquirir pensamiento crítico:** Aprender a discernir las fuentes fiables de las dudosas, cuestionar la información a la que se tiene acceso, identificar una página web falsa o simplemente, saber, que todo el contenido que aparece en la red no es la verdad absoluta. En definitiva, adquirir un pensamiento crítico desde pequeños será un elemento clave en su educación digital.

- **Aprender a cuidar su salud física y mental:** Los menores deben aprender a hacer un uso racional y equilibrado de la tecnología ya que un uso excesivo y no controlado de esta, puede crear adicción, pudiendo afectar a sus relaciones sociales, rendimiento escolar, actividades deportivas, sueño, etc. Desde el inicio en el uso de la tecnología, es conveniente establecer un horario de uso de los dispositivos y que aprendan a gestionar correctamente sus tiempos.

El uso responsable de la tecnología en inmigrantes digitales

Aquellos que han nacido con anterioridad a la eclosión tecnológica pero que conviven en la sociedad digital actual y han tenido que adaptarse a estos nuevos escenarios digitales son los denominados “inmigrantes digitales”, nomenclatura en la que podríamos incluir a gran parte de los padres de hoy en día.

Uno de los rasgos diferenciales entre los inmigrantes digitales y los nativos está en la **dependencia considerablemente menor de la tecnología**, especialmente en lo referente a las relaciones interpersonales y la necesidad de compartir cada instante en las redes.

Para que los nativos digitales puedan obtener la guía y acompañamiento que necesitan en su vida digital, los padres tienen ante sí grandes retos en la transmisión de una cultura tecnológica responsable en el entorno familiar. A destacar:

- **Aprender a transmitir hábitos de navegación seguros y hacer un uso responsable de la tecnología:** Para que desde muy pequeños conozcan las conductas de riesgo, las sepan identificar y aprendan a evitarlas.

- **Enseñarles a gestionar las experiencias negativas de forma eficaz:** Haciendo que acudan a ellos siempre que se sientan inseguros o hayan cometido errores, así como detectar cuáles son las respuestas más adecuadas y efectivas para cada situación.

Conclusiones

Como podemos observar, el uso responsable de la tecnología es compartido por todos los actores de la sociedad. Tanto por los profesionales del área de las TIC como por aquellos que no lo son pero aun así, tienen una enorme responsabilidad educando a aquellos que en el presente y potencialmente en el futuro lo harán, dado que los trabajos en las próximas décadas serán no solo transformados si no moldeados por la tecnología.

Referencias

[1] RAE – Tecnología: <https://bit.ly/3Hq44VZ>

[2] ACM Code of Ethics and Professional Conduct - <https://www.acm.org/code-of-ethics>

[3] Secretaria de Estado de Digitalización e Inteligencia Artificial – Uso de tecnología en los hogares españoles (2022): <https://bit.ly/3neR4vk>

[4] clubsostenibilidad.org – Informe de Tecnología Responsable: <https://bit.ly/2uRIe7y>