Tecnológico de Monterrey

Instituto Tecnológico de Estudios Superiores de Monterrey
Campus Monterrey

Integración de seguridad informática en redes y sistemas de software (Gpo 401)

Propuesta de Marco Ético y Legal

Victoria Valentina Marín Domínguez A00836008

Profesores:
Cristina Verónica González Córdova
Juan José Gaytán Hernández Magro
Aida Judith Gándara Tovar

Monterrey, Nuevo León, a 15 de octubre de 2024

En la actualidad, la tecnología ha sido de lo más revolucionario y crucial en la sociedad, transformando la forma en la que vivimos y trabajamos, constantemente teniendo nuevos cambios e implementaciones, ayudándonos a automatizar, conectarnos, comunicarnos y tener nuevos descubrimientos. Con toda la evolución que conlleva, se han identificado nuevos riesgos y con la expansión de conocimientos también vemos una expansión de ataques por medio de ella. En México es necesario adaptarnos y combatir el uso maligno de las mismas, por lo que es necesario crear legislaciones con un enfoque ético, considerando así los valores sociales y consideraciones como la privacidad, manejo de datos e identidad de los usuarios de las tecnologías, mientras también tomando en cuenta los retos y problemas a nivel global, como lo son el cambio climático y el movimiento a una sociedad más sustentable.

Particularmente en la relación de México con la tecnología y sistemas informáticos es necesario promover valores que no solo nos ayuden a guiar el desarrollo tecnológico, sino también el social y ambiental. La informática tiene la capacidad de transformar economías, gobiernos y sociedades, así como también tiene la capacidad de alterarlas. Por esto es de gran importancia utilizarlas con valores y comportamiento ético en nuestra profesión.

Como valores esenciales considero los siguientes:

- **Transparencia:** En México la transparencia en el uso de datos e información es importante, especialmente por la cantidad de delitos cometidos como robos de identidad, fraudes y extorsiones que suceden al mal manejo de información o uso indebido de programas. La información que puede ser vulnerable incluye información personal, bancaria y de salud. Además muchas personas no conocen cómo se utilizan los datos, lo que genera desconfianza a la hora de estos incidentes. La transparencia es crucial para que los usuarios comprendan qué datos se recopilan, cómo se protegen, y para qué se usan.

- **Responsabilidad social:** El diseño de sistemas tecnológicos debe estar alineado con los intereses de la sociedad mexicana, que enfrenta retos significativos en términos de desigualdad social, corrupción y uso indebido de datos. En un país donde la tecnología está transformando áreas clave como la educación, la salud y la seguridad pública, es imperativo que los desarrolladores asuman la responsabilidad social de crear sistemas que consideren su impacto en la sociedad. Esto incluye diseñar plataformas que prevengan el mal uso de la tecnología, promuevan la inclusión y contribuyan a la mejora del bienestar común.

- **Justicia y equidad:** En México, la brecha digital es una realidad. Muchos mexicanos, especialmente en áreas rurales o de bajos ingresos, no tienen acceso a las mismas oportunidades tecnológicas que aquellos en zonas urbanas o con más recursos. Este contexto de desigualdad digital dificulta el acceso a educación, servicios de salud y empleo. Las soluciones tecnológicas deben diseñarse teniendo en cuenta estas

diferencias, con el objetivo de crear herramientas accesibles que permitan a más personas aprender, usar y beneficiarse de la tecnología.

- **Sostenibilidad:** México enfrenta una serie de desafíos ambientales, como el cambio climático, la escasez de agua y la contaminación, por lo que la tecnología debe diseñarse con un enfoque en la sostenibilidad. El consumo masivo de energía por centros de datos y la producción de dispositivos electrónicos tienen un impacto considerable en el medio ambiente. Es esencial que los profesionales en informática adopten prácticas que minimicen el uso de energía, promuevan el reciclaje de componentes electrónicos y optimicen la eficiencia energética. Además, las soluciones tecnológicas deben buscar la mitigación de los efectos del cambio climático, promoviendo el desarrollo de tecnologías que reduzcan la huella de carbono, gestionen mejor los recursos naturales y ayuden a la preservación del medio ambiente en México.

- **Integridad:** La integridad es vital en una profesión que puede afectar la seguridad y privacidad de las personas. En México, la corrupción y las malas prácticas en muchos sectores han creado un ambiente de desconfianza. Los desarrolladores informáticos deben actuar con los más altos estándares éticos, evitando cualquier tipo de fraude, robo de información o plagio. Mantener la integridad en el manejo de datos sensibles es clave para proteger a los usuarios y evitar situaciones de abuso. Esto incluye asegurar que los sistemas y plataformas sean resistentes a ciberataques y que cualquier fallo o vulnerabilidad sea tratado con transparencia y rapidez, siempre protegiendo el bienestar de los usuarios.

- **Respeto al usuario:** Muchas veces los usuarios no son conscientes de los datos que están proporcionando o cómo se están utilizando. El respeto al usuario implica que solo se recopilen datos con fines legítimos, con el consentimiento informado de los usuarios y garantizando la protección de su privacidad. En el contexto mexicano, donde la confianza en las instituciones digitales aún está en construcción, es fundamental que las empresas tecnológicas y los desarrolladores sean claros y éticos en sus políticas de privacidad y uso de datos.

Una vez considerando la importancia de estos valores, podemos ver que la informática es una profesión clave en la transformación, tiene una gran capacidad de mejorar la eficiencia de los procesos y la comunicación, pero además nos ayuda a solucionar problemas a nivel global, y a medida que se desarrolla la tecnología afecta todos los aspectos cotidianos. La informática juega un rol crucial en un futuro más sostenible.

Actualmente nos enfrentamos a problemas como el cambio climático, deterioro del planeta y la necesidad de resiliencia ante las crisis. En colaboración con políticas y legislaciones, la informática puede contribuir a soluciones efectivas y sostenibles.

La crisis climática es una de las amenazas más grandes que enfrenta la humanidad. La informática puede ayudar a combatir este problema a través del desarrollo de tecnologías para monitorear el medio ambiente, optimizar el uso de recursos naturales y reducir las emisiones de carbono mediante sistemas más eficientes. Los centros de datos, los sistemas de transporte inteligente y la inteligencia artificial pueden ser utilizados para generar un impacto positivo en la reducción del consumo energético. Aunque si bien, también tenemos que considerar algunos efectos negativos como la refrigeración de servidores que guardan datos y las emisiones y uso de energía que estos generan.

Con respecto al deterioro, el crecimiento urbano y el consumo desenfrenado de recursos naturales están dañando nuestro entorno. La informática puede ayudar a atenuar estos impactos a través del desarrollo de ciudades inteligentes, que optimizan el uso de energía y recursos, reduciendo la huella ecológica. Además, las soluciones tecnológicas permiten un monitoreo más eficiente de los ecosistemas y la implementación de estrategias de conservación.

La informática también tiene el poder de contribuir a la mitigación de desastres y la creación de sistemas resilientes que protejan a las comunidades vulnerables. A través de modelos predictivos basados en inteligencia artificial y análisis de data, es posible anticipar fenómenos naturales como terremotos, huracanes o incendios forestales, y actuar con rapidez para minimizar el daño. Además, el diseño de infraestructuras tecnológicas robustas puede garantizar la continuidad de los servicios esenciales durante y después de eventos críticos.

Además tiene el potencial de reducir el impacto ambiental de las actividades humanas, promoviendo tecnologías más limpias y eficientes.

Con estas soluciones podemos observar que es una carrera que está orientada a innovar y buscar soluciones a problemas globales, es importante que a la hora de abordar dichos problemas se tenga una visión ética y comprometida, que permita la mejora a la sociedad.

Dado el contexto, propongo los siguientes artículos de ética a seguir por los profesionistas en el área de informática:

1. Transparencia en el uso de datos

Los profesionales de la informática deben ser transparentes sobre la recopilación, almacenamiento, y uso de datos personales. Esto incluye informar a los usuarios sobre cómo se procesan sus datos y obtener su consentimiento explícito. La confianza de los usuarios es esencial para el éxito de cualquier sistema. En un mundo donde los datos personales pueden ser explotados o mal utilizados, la transparencia protege los derechos de los individuos y fomenta la confianza en los sistemas tecnológicos.

2. Protección de la privacidad y confidencialidad

Es fundamental garantizar la privacidad y confidencialidad de los datos de los usuarios, utilizando medidas de seguridad robustas para proteger la información sensible. La protección de la privacidad es un derecho fundamental. El mal manejo de datos puede generar problemas graves como robo de identidad o violaciones a la privacidad, afectando la vida de los usuarios. Por ello, es necesario implementar políticas de seguridad eficaces.

3. Responsabilidad en la creación de sistemas

Los sistemas informáticos deben ser diseñados con responsabilidad, considerando su impacto en la sociedad y el medio ambiente. Los desarrolladores deben evitar crear tecnologías que puedan ser mal utilizadas o que contribuyan a la desigualdad social o ambiental. Los sistemas mal diseñados o malintencionados pueden generar daños irreparables. La responsabilidad profesional implica prevenir el uso indebido y garantizar que las tecnologías promuevan el bienestar social.

4. Justicia y equidad en el acceso a la tecnología

Las soluciones tecnológicas deben ser accesibles e inclusivas, garantizando que las personas, sin importar su contexto socioeconómico, tengan acceso a las oportunidades tecnológicas. En México, donde existe una brecha digital considerable, es fundamental que los desarrolladores de sistemas consideren las necesidades de las poblaciones vulnerables y busquen reducir la exclusión tecnológica.

5. Promoción de la sostenibilidad

Los profesionales de la informática deben trabajar en la creación de tecnologías que promuevan la sostenibilidad y minimicen el impacto ambiental, optimizando el uso de recursos energéticos y promoviendo la eficiencia. El impacto ambiental de la tecnología es significativo, desde el consumo energético hasta la producción de hardware. Los profesionales tienen la responsabilidad de mitigar estos efectos y contribuir a la lucha contra el cambio climático.

6. Uso ético de la inteligencia artificial

La inteligencia artificial y los algoritmos deben diseñarse y utilizarse de manera justa y transparente, evitando sesgos que puedan perpetuar la discriminación o la exclusión. La IA tiene el poder de influir en decisiones importantes como la contratación de personal o la concesión de créditos. Un uso irresponsable o sesgado puede perpetuar injusticias. La transparencia y equidad en el diseño de estos sistemas es crucial.

7. Innovación con responsabilidad social

Los profesionales deben innovar considerando los beneficios sociales de sus creaciones. Las nuevas tecnologías deben orientarse a resolver problemas como la pobreza, la desigualdad y el cambio climático, promoviendo un mundo más equitativo. La tecnología debe ser un motor para el cambio positivo en la sociedad. Innovar sin tener en cuenta las

implicaciones sociales puede agravar problemas existentes o crear nuevos desafíos para las comunidades más vulnerables.

8. Mantenimiento de la integridad profesional

Los profesionales deben actuar con integridad, evitando plagio, fraude, o la manipulación indebida de datos. La honestidad debe guiar todas las acciones dentro del ejercicio profesional. La integridad es esencial para mantener la confianza entre los colegas, clientes y usuarios. La deshonestidad y el fraude pueden socavar la confianza en la profesión y generar daños económicos o sociales.

9. Prevención y mitigación de riesgos cibernéticos

Es responsabilidad de los profesionales de la informática identificar, prevenir y mitigar los riesgos relacionados con ciberataques y vulnerabilidades en los sistemas, protegiendo así la seguridad de los usuarios. Los delitos cibernéticos están en aumento, afectando tanto a individuos como a instituciones. Los profesionales de la informática tienen la obligación de garantizar que los sistemas que diseñan sean seguros y robustos frente a amenazas externas.

10. Respeto por los derechos del usuario

Los profesionales deben respetar los derechos de los usuarios, como la libertad de elección, el consentimiento informado y la privacidad. Esto implica no utilizar los datos de manera que comprometa la autonomía de los usuarios o que manipule su comportamiento. El respeto por los derechos de los usuarios es la base de una relación ética y justa entre los desarrolladores y quienes utilizan la tecnología. Los usuarios deben tener control sobre su información y cómo se utiliza, sin ser explotados o manipulados.

Como profesional de la informática, me comprometo a actuar con ética, responsabilidad y respeto hacia los derechos humanos, buscando siempre el bienestar social y ambiental. Mi trabajo estará orientado a promover la justicia, equidad y sostenibilidad, y a proteger la privacidad y la seguridad de los usuarios. Asimismo, me comprometo a innovar con integridad y a enfrentar los desafíos globales, como el cambio climático y la desigualdad social, desde el ámbito tecnológico.

Así como es beneficiosa la tecnología, el mal uso de ella puede traer consecuencias, incluyendo consecuencias legales, por lo que es necesario no solo tener medidas éticas, sino además leyes que establezcan formalmente las medidas necesarias para prevenir ataques y el mal uso de las tecnologías.

Actualmente en México, el marco legal tiene muy pocos artículos o leyes relacionadas a sanciones o reconociendo los delitos cibernéticos, algunos de los que encontramos es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley de Seguridad Nacional, está regula el trato de los datos personales por parte de empresas, individuos y organizaciones del sector privado, su objetivo es garantizar la privacidad y

protección de los datos personales de los individuos, promoviendo un uso responsable y ético de la información personal. Sin embargo, estas leyes no consideran los rápidos avances de los delitos cibernéticos y que tan avanzadas son las nuevas tecnologías. No contemplan amenazas como robo de datos, phishing, fraudes, y entre otros.

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea es un referente en cuanto a la protección de la privacidad y datos personales. En comparación, México no cuenta con leyes en términos de sanciones y regulación de la transferencia de datos. Además, el enfoque de la UE hacia la responsabilidad de las empresas tecnológicas es más estricto, mientras que en México las sanciones son menores y, en muchos casos, las acciones tardan en implementarse.

La propuesta de ley de ciberseguridad de 2024 es un paso significativo, aunque todavía necesita incluir un mayor espectro de delitos cibernéticos. En este momento, la propuesta se enfoca principalmente en delitos como el acceso no autorizado, el fraude y el robo de identidad, pero no aborda adecuadamente las amenazas emergentes. Asimismo, no ofrece una protección suficiente para los datos que ya utilizamos.

Como propuestas de mejora al marco legal, tengo los siguientes puntos:

1. **Ampliación de la definición de delitos cibernéticos**

Es fundamental que el marco legal contemple una definición más amplia de los delitos cibernéticos. Con la rápida evolución de la tecnología, surgen nuevas modalidades de ataque que amenazan la seguridad digital, como los dirigidos a dispositivos IoT, drones y vehículos autónomos. Adaptar la legislación a estas realidades permitirá un mejor entendimiento y tratamiento de estos delitos emergentes.

2. **Responsabilidad compartida en ciberseguridad**

Es imperativo establecer obligaciones claras para las empresas y organizaciones que gestionan datos sensibles. No solo deben centrarse en la protección de datos personales, sino también asumir la responsabilidad de garantizar la seguridad de las infraestructuras tecnológicas que utilizan. Este enfoque integral fortalecerá la confianza en los sistemas digitales y fomentará una cultura de responsabilidad.

3. **Regulación y control del ransomware**

La creación de un marco que incluya sanciones más severas para quienes perpetran ataques de ransomware es esencial. Además, es necesario implementar protocolos de respuesta que faciliten la cooperación efectiva entre instituciones públicas y privadas, asegurando una respuesta coordinada y rápida ante tales incidentes.

4. **Fortalecimiento de la ciberseguridad en infraestructuras críticas**

Es vital promulgar una legislación que exija medidas de seguridad rigurosas para las infraestructuras críticas, como la electricidad, las telecomunicaciones y el suministro de agua. Esta normativa debe basarse en estándares internacionales, garantizando así un nivel de protección adecuado ante las amenazas cibernéticas.

5. **Protección de la privacidad en el Internet de las Cosas (IoT)**

Con el creciente uso de dispositivos conectados a internet, es urgente desarrollar regulaciones específicas que aseguren tanto la seguridad como la privacidad de estos dispositivos. Esto no solo protegerá a los usuarios, sino que también fomentará la confianza en el uso de tecnologías emergentes en hogares, empresas y sectores públicos.

6. **Sanciones severas para la filtración de datos**

Las sanciones impuestas a empresas y organizaciones que no protejan adecuadamente los datos personales deben ser significativamente más estrictas. Este alineamiento con las prácticas del GDPR es crucial, ya que las multas podrían representar porcentajes importantes de los ingresos de las empresas infractoras, incentivando así una gestión más responsable de la información.

7. **Educación y sensibilización en ciberseguridad**

La creación de programas nacionales destinados a educar y sensibilizar a la ciudadanía sobre temas de ciberseguridad es esencial. Estos programas deben estar dirigidos a estudiantes, empleados y líderes de organizaciones, fomentando una cultura de conciencia y proactividad frente a los riesgos cibernéticos.

Esta propuesta tiene como objetivo fortalecer el marco legal mexicano, adaptándolo a los desafíos contemporáneos en los ámbitos digitales. Reconoce la complejidad de las amenazas cibernéticas que enfrentamos, así como la necesidad urgente de mejorar la educación y la concientización en torno a estos delitos. Al integrar medidas que aborden tanto la prevención como la sanción de los delitos cibernéticos, se busca crear un entorno más seguro para todos los usuarios de la tecnología. Esto incluye promover programas de educación y sensibilización que empoderen a la ciudadanía, fomentando una cultura de seguridad digital que permita a las personas identificar y mitigar riesgos. Además, es esencial que la legislación evolucione en conjunto con el avance de la tecnología, garantizando así que las normativas se mantengan efectivas y pertinentes en un mundo en constante cambio.

Para verlo de forma más interactiva puede verlo en el siguiente link de genially:

https://view.genially.com/670f3ea6c888e46f946084b8/interactive-content-marco-legal

Referencias

Rivera, S. F. (2024, 8 octubre). *Ley de Ciberseguridad en México: Conoce la Nueva Ley*. https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico

Lab, P. P. (2023, 28 agosto). Ciberseguridad en México. *Public Interest Tech*. https://www.policylab.tech/post/ciberseguridad-en-m%C3%A9xico-1?lang=es

itunews. (s. f.). *AFRONTAR EL CAMBIO CLIMATICO – EL PAPEL DE LAS TIC*. https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=04&ext=html

PricewaterhouseCoopers. (s. f.). *El estado de la tecnología aplicada al cambio climático en 2021*. PwC. https://www.pwc.es/es/publicaciones/sostenibilidad/tecnologia-aplicada-cambio-climatico-2021.html

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. (s. f.).

¿Cuál es el panorama actual de la seguridad informática en México? (s. f.). Ikusi Velatia. https://www.ikusi.com/mx/blog/seguridad-informatica-en-mexico/

Del Consumidor, P. F. (s. f.). Protección de datos personales. gob.mx. https://www.gob.mx/profeco/acciones-y-programas/proteccion-de-datos-personales-271598

Euroinnova International Online Education. (2024, 17 septiembre). Perceptrón: herramienta esencial en los proyectos de learning. *https://www.euroinnova.com/blog/que-es-la-etica-informatica*

OpenAI. (2024)