ACM Code of Ethics and Professional Conduct

Código de Ética y Conducta Profesional de ACM

Preámbulo

Las acciones de los profesionales de la Informática cambian el mundo. Para actuar de forma responsable, deben reflexionar sobre los impactos amplios de su trabajo, siempre en pos del bien público. El Código de Ética y Conducta Profesional de ACM ("el Código") da cuenta de la conciencia de la profesión.

El Código está diseñado para inspirar y guiar la conducta ética de todos los profesionales de la Informática, incluyendo a los profesionales actuales y futuros, a los instructores, los estudiantes, las personas influyentes y a cualquiera que utilice la tecnología informática para generar un impacto. Además, el Código sirve como una base para corregir posibles infracciones. El Código incluye principios formulados como declaraciones de responsabilidad, basados en la idea de que el bien público siempre es la primera prioridad. Cada principio esta complementado con guías que proporcionan explicaciones para ayudar a los profesionales de la Informática a comprenderlo y aplicarlo.

La Sección 1 describe los principios éticos fundamentales que forman la base del Código. La Sección 2 aborda consideraciones adicionales más específicas sobre la responsabilidad profesional. La Sección 3 guía a las personas que tienen un rol de liderazgo, ya sea en el lugar de trabajo o como voluntarios. Cada miembro de ACM debe comprometerse a respetar la conducta ética; y los principios implicados en el cumplimiento de este Código se presentan en la Sección 4.

El Código, en general, aborda el modo en el que los principios éticos fundamentales se aplican a las conductas de un profesional de la Informática. El Código no es un algoritmo para resolver problemas éticos; sino que sirve como un punto de partida para la toma de decisiones éticas. Al abordar un problema particular, un profesional de la informática puede enfrentarse a múltiples principios que deben ser tenidos en cuenta, y aquellos principios pueden mostrar diferentes grados de relevancia para el problema abordado. Las preguntas relacionadas con este tipo de cuestiones pueden ser mejor respondidas de la mano de una consideración cuidadosa de los principios éticos fundamentales, considerando al bien público como la mayor prioridad. La profesión informática

en su totalidad sale beneficiada cuando el proceso ético de toma de decisiones es responsable y transparente para todas las partes interesadas. Discusiones abiertas sobre cuestiones éticas promueve la responsabilidad y la transparencia.

1. PRINCIPIOS ÉTICOS GENERALES.

Un profesional de la Informática debería...

1.1 Contribuir a la sociedad y al bienestar humano, reconociendo que todas las personas son partes interesadas en la Informática.

Este principio, que se refiere a la calidad de vida de todas las personas, subraya la obligación de los profesionales de la Informática, tanto individual como colectivamente, de utilizar sus habilidades en beneficio de la sociedad, de sus miembros y del entorno que les rodea. Esta obligación implica la promoción de los derechos humanos fundamentales y la protección del derecho a la autonomía de cada individuo. Un objetivo esencial de los profesionales de la informática es minimizar las consecuencias negativas de la Informática, como las amenazas a la salud, la seguridad, la seguridad personal y la privacidad. Cuando los intereses de múltiples grupos entran en conflicto, las necesidades de los menos favorecidos deben recibir ser priorizadas y recibir una mayor atención.

Los profesionales de la computación deben evaluar si los resultados de sus esfuerzos respetarán la diversidad, si serán utilizados de manera socialmente responsable, satisfaciendo las necesidades sociales y si serán ampliamente accesibles. Se les anima a contribuir activamente a la sociedad mediante el trabajo voluntario y altruista que beneficie el bien público.

Además de un entorno social seguro, el bienestar humano requiere de un entorno natural seguro. Por lo tanto, los profesionales de la Informática deberían promover la sostenibilidad del medio ambiente tanto a nivel local como global.

1.2 Evitar el daño.

En este documento "daño" equivale a consecuencias negativas, especialmente cuando son significativas e injustas. Los ejemplos de daño incluyen lesiones físicas o mentales injustificadas, destrucción injustificada o divulgación de información y daños injustificados a la propiedad, la reputación y el medio ambiente. Esta lista no es exhaustiva.

Las acciones bienintencionadas, incluidas las que cumplen funciones asignadas, pueden causar daños. Cuando el daño es involuntario, los responsables están obligados a deshacer o mitigar el daño tanto como sea posible. Para evitar daños es necesario comenzar por una evaluación cuidadosa de los posibles impactos para todos los afectados por la toma de decisiones. Por otra parte, cuando el daño es parte intencional del sistema, los responsables están obligados a garantizar que el daño está éticamente justificado. En cualquier caso, es necesario asegurarse de que todos los daños son minimizados.

Para minimizar la posibilidad de dañar a los demás de manera indirecta o no intencional, los profesionales de la computación deben seguir las buenas prácticas generalmente aceptadas, a menos que exista una razón ética convincente para hacerlo de otra manera. Además, es necesario analizar cuidadosamente las consecuencias de la agregación de datos y las propiedades emergentes de los sistemas. Quienes participan en sistemas generalizados o de infraestructura también deberían considerar el Principio 3.7.

Un profesional de la Informática tiene la obligación adicional de informar sobre cualquier signo de riesgo del sistema que pueda ocasionar daños. Si los responsables no actúan para reducir o mitigar dichos riesgos, puede ser necesario dar la voz de alarma para reducir el daño potencial. Sin embargo, una información capciosa o equivocada sobre riesgos potenciales puede ser dañina. Antes de informar sobre los riesgos, un profesional de la Informática debe evaluar cuidadosamente los aspectos relevantes de la situación.

1.3 Ser honesto y confiable.

La honestidad es un componente esencial de la confiabilidad. Un profesional de la Informática debe ser transparente y proporcionar una información completa de todas las capacidades del sistema, de las limitaciones y los posibles problemas a los actores interesados. Sostener afirmaciones deliberadamente falsas o engañosas, fabricar o falsificar datos, ofrecer o aceptar sobornos y otras conductas deshonestas son infracciones al Código.

Los profesionales de la Informática deben ser honestos acerca de sus certificaciones y sobre cualquier limitación en sus competencias para completar una tarea. Los profesionales de la informática deben ser francos sobre cualquier circunstancia que pueda conducir a conflictos de interés, ya sean reales o percibidos. De lo contrario pueden poner en tela de juicio la independencia de su criterio. A su vez, es necesario cumplir con sus compromisos.

Los profesionales de la Informática no deben tergiversar las políticas o procedimientos de una organización, y no deben hablar en nombre de una organización a menos que estén autorizados para hacerlo.

1.4 Ser justo y tomar medidas para no discriminar.

Este principio está gobernado por los valores de igualdad, tolerancia, respeto por los demás y justicia. La justicia implica que, incluso en los procesos de decisión más cuidadosos, se proporcione alguna vía razonable para la reparación de posibles agravios.

Los profesionales de la Informática deberían fomentar la participación justa de todas las personas, incluyendo a los miembros de grupos insuficientemente representados. La discriminación prejuiciosa basada en la edad, el color, la discapacidad, la etnia, el estado civil, la identidad de género, la afiliación sindical, el estado militar, la nacionalidad, la raza, la religión o creencias, el sexo, la orientación sexual o cualquier otro factor es una violación explícita a este Código. El acoso, incluido el acoso sexual, la intimidación y otros abusos de

poder y autoridad, son formas de discriminación que, entre otros daños, limitan el acceso equitativo a los espacios virtuales y físicos donde se produce dicho hostigamiento.

El uso de la información y la tecnología puede causar inequidades nuevas o ampliar las existentes. Las tecnologías y las prácticas deben ser lo más inclusivas y accesibles que sea posible, y los profesionales de la Informática deben tomar medidas para evitar el desarrollo de sistemas o tecnologías que privan del derecho a decidir u oprimen a las personas. diseño que falle en la inclusión y el acceso equitativo puede ocasionar una discriminación injusta.

1.5 Respetar el trabajo necesario para producir nuevas ideas, inventos, trabajos creativos y artefactos informáticos.

El desarrollo de nuevas ideas, inventos, obras creativas y artefactos informáticos crea valor para la sociedad, y aquellos que realizan el esfuerzo para desarrollarlos esperan obtener beneficios de su trabajo. Por lo tanto, los profesionales de la Informática deberían respetar la autoría de los creadores de ideas, inventos, trabajos y artefactos, los derechos de autor, las patentes, el secreto comercial, los acuerdos de licencias y otros métodos para proteger el trabajo de los autores.

Tanto la costumbre como la ley reconocen la necesidad de algunas excepciones de cara al bien público. Los profesionales de la Informática no deberían oponerse a los usos razonables de sus obras intelectuales. Por ejemplo, la contribución de tiempo y energía a proyectos que ayudan a la sociedad, como el desarrollo de software libre, de código abierto, puesto a disposición del dominio público, ilustra un aspecto positivo de este principio. Los profesionales de la Informática no deberían reclamar la propiedad del trabajo que ellos, u otras personas, hayan compartido en forma de recursos públicos.

1.6 Respetar la privacidad.

La responsabilidad de respetar la privacidad forma parte del código ético de los profesionales de la informática. La tecnología permite la recopilación, el control 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 de privacidad y debe comprender los derechos y responsabilidades asociados con la recopilación y el uso de datos personales.

Los profesionales de la Informática deberían usar datos personales únicamente con fines legítimos, sin violar los derechos de individuos y grupos. Para ello es necesario tomar precauciones para evitar la re-identificación de datos anónimos y la recopilación de datos no autorizados, garantizar la exactitud de los datos, conocer la procedencia de los datos y protegerlos contra el acceso no autorizado y la divulgación accidental. Los profesionales de la Informática deberían desarrollar políticas y procedimientos transparentes que permitan a las personas

comprender qué datos se están recopilando y cómo se usan, dar su consentimiento informado en relación a la recopilación automática de datos, así como revisar, obtener, corregir imprecisiones y eliminar sus datos personales.

Un sistema informático debe recopilar únicamente el mínimo de información personal necesaria. Los períodos de retención y eliminación de esta información deben ser claramente definidos, cumplidos y comunicados a los interesados. La información personal recopilada para un propósito específico no debe ser utilizada para otros fines sin el consentimiento de la persona. Las colecciones de datos integrados pueden comprometer las características de privacidad de las colecciones originales. Por lo tanto, los profesionales de la Informática deben tomar precauciones en materia de privacidad al integrar colecciones de datos.

1.7 Respetar la confidencialidad.

A los profesionales de la Informática se les suele confiar información confidencial como secretos comerciales, datos de clientes, estrategias comerciales que no son públicas, información financiera, datos de investigación, artículos académicos aún no publicados y solicitudes de patentes. Los profesionales de la Informática deben proteger la confidencialidad, excepto en los casos en que encuentren evidencias de la violación de una ley, de los reglamentos de la organización o del Código. En estos casos, la naturaleza o el contenido de esa información sólo debe ser comunicada a las autoridades correspondientes. Un profesional de la informática debe evaluar cuidadosamente si tales divulgaciones son consistentes con el Código.

2. RESPONSABILIDADES PROFESIONALES.

Un profesional de la informática debería...

2.1 Esforzarse por lograr una alta calidad tanto en los procesos como en los productos del trabajo profesional.

Los profesionales de la Informática deberían promover el trabajo de calidad, tanto el propio como el de sus colegas. Es necesario respetar la dignidad de los empleadores, los empleados, los colegas, los clientes, los usuarios y cualquier otra persona afectada directa o indirectamente por el trabajo durante todo el proceso. Los profesionales de la Informática deben respetar el derecho de los involucrados a una comunicación transparente sobre el proyecto. Los profesionales deben ser conscientes de cualquier consecuencia negativa que pudiera afectar a alguna parte interesada y resultar en trabajo de mala calidad, y deben resistir cualquier posible incentivo para descuidar esta responsabilidad.

2.2 Mantener altos estándares de competencia profesional, conducta y práctica ética.

La informática de calidad depende de individuos y equipos que asumen la responsabilidad, personal y grupal, de adquirir y mantener la aptitud profesional. La aptitud profesional parte del conocimiento técnico y la conciencia del contexto social en donde este trabajo podría ser usado. La aptitud profesional también

implica habilidad en la comunicación, el análisis reflexivo y el reconocimiento y gestión de desafíos éticos. La actualización de competencias debe ser un proceso continuo y puede incluir el estudio independiente, la asistencia a conferencias o seminarios, y otras instancias de educación, tanto formal como informal. Las organizaciones profesionales y los empleadores deberían alentar y facilitar estas actividades.

2.3 Conocer y respetar las reglas vigentes relacionadas con el trabajo profesional.

Las "Reglas" incluyen leyes y regulaciones locales, regionales, nacionales e internacionales, así como también 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 no hacerlo. Las reglas que se juzgan como no éticas deben ser impugnadas. Una regla puede no ser ética cuando tiene una base moral inadecuada o cuando causa daños reconocibles. Un profesional de la informática debe ser capaz de cuestionar la regla a través de los canales existentes antes de violar la regla. Un profesional de la Informática que decide violar una regla porque no es ética, o por cualquier otro motivo, debe considerar las posibles consecuencias y aceptar la responsabilidad de esta acción.

2.4 Aceptar y proporcionar una revisión profesional adecuada.

El trabajo de calidad en Informática depende de la revisión profesional en todas sus etapas. Cuando corresponda, los profesionales de la Informática deben procurar una revisión entre pares e involucrar a las partes interesadas. Los profesionales de la Informática deben ser capaces de proporcionar, además, revisiones constructivas y críticas del trabajo ajeno.

2.5 Realizar evaluaciones integrales y exhaustivas de los sistemas informáticos y de sus impactos, incluyendo un análisis de los posibles riesgos.

A los profesionales de la Informática se les asigna 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, también, a la sociedad. Los profesionales de la Informática deben procurar ser perspicaces, exhaustivos y objetivos cuando evalúan, recomiendan y presentan descripciones de un sistema o alternativas a éste. Los profesionales de la informática deben tener un especial cuidado para poder identificar, y mitigar, los riesgos potenciales en los sistemas de aprendizaje automático. Un sistema cuyos riesgos futuros no pueden ser predichos requiere una reevaluación frecuente del riesgo a medida que el sistema evoluciona. De lo contrario, no debería desplegarse. Cualquier problema que pueda ocasionar un riesgo mayor debe ser reportado a las partes involucradas.

2.6 Trabajar solo en sus ámbitos de competencia.

Un profesional de la Informática es responsable de evaluar el trabajo que le es asignado. Esto implica juzgar si es factible y conveniente, y evaluar si el trabajo asignado se encuentra dentro de su ámbito de aptitud profesional. Si en algún momento, antes o durante la asignación de trabajo, el profesional considera que carece de la experiencia necesaria, debe comunicarlo al empleador o cliente. Éstos pueden decidir realizar la tarea con el profesional contemplando un tiempo adicional para que éste adquiera las habilidades necesarias, asignar la tarea a otra persona que tenga los conocimientos necesarios, o cancelar el trabajo. El juicio ético de un profesional de la Informática debe ser determinante a la hora de decidir si se debe aceptar la tarea asignada o no.

2.7 Fomentar la conciencia ciudadana sobre la Informática, las tecnologías relacionadas y sus consecuencias.

En correspondencia con el contexto y las capacidades de cada uno, los profesionales de la Informática deberían compartir sus conocimientos técnicos con la ciudadanía, fomentar el conocimiento sobre la Informática y alentar la su comprensión. La comunicación con la ciudadanía debe ser clara, respetuosa y cordial. Cuestiones como el impacto de los sistemas informáticos, sus limitaciones, sus vulnerabilidades y oportunidades, deben ser tenidas en cuenta. Además, un profesional de Informática debe ser capaz de abordar la información inexacta o engañosa relacionada con la Informática.

2.8 Acceder a los recursos informáticos y de comunicación sólo cuando esté autorizado, o cuando sea necesario para proteger el bien público.

Las personas y las organizaciones tienen derecho a restringir el acceso a sus sistemas y sus datos siempre que las restricciones sean consistentes con los demás principios de este Código. En consecuencia, los profesionales de la computación no deben acceder a un sistema, software o datos ajenos sin contar con motivos válidos para asegurar que tal acción sería autorizada o consistente con la defensa del bien público. El acceso público a un sistema no es condición suficiente. En circunstancias excepcionales, un profesional de Informática puede utilizar el acceso no autorizado para interrumpir o inhibir el funcionamiento de sistemas maliciosos. En estos casos es especialmente importante que se tomen precauciones para evitar daños a terceros.

2.9 Diseñar e implementar sistemas robustos, accesibles y seguros.

Las violaciones de seguridad informática causan daños. Una seguridad robusta debe ser una consideración primordial al diseñar e implementar sistemas. Los profesionales de la Informática deben implementar los mecanismos necesarios para garantizar que el sistema funcione de la manera prevista, y deben tomar las medidas adecuadas para proteger los recursos contra un posible uso indebido, modificación o ataque por denegación de servicio, tanto accidental e intencional. Debido a que las amenazas pueden surgir o cambiar después de desplegar un

sistema, los profesionales de la computación deben integrar técnicas y políticas de mitigación de daños, tales como el monitoreo, la aplicación de parches de seguridad y la producción de informes de vulnerabilidad. Los profesionales de la Informática deben tomar, a su vez, medidas para garantizar que las partes afectadas por filtraciones de datos sean notificadas de manera oportuna y clara, ofreciendo la orientación y corrección adecuadas.

Para garantizar que el sistema informático cumpla su propósito, las funciones de seguridad deben estar diseñadas de forma tan intuitiva y fácil de usar como sea posible. Los profesionales de la Informática deberían evitar las precauciones de seguridad que sean confusas e inapropiadas, así como las que impiden un uso legítimo.

En los casos en los que un posible mal uso o un potencial daño es predecible o inevitable, la mejor opción puede ser la no implementación del sistema.

3. PRINCIPIOS DE LIDERAZGO PROFESIONAL.

El liderazgo puede ser producto de una designación formal o puede surgir de manera informal a partir de influencia ejercida sobre los pares. En esta sección, "líder" equivale a cualquier miembro de una organización o grupo que ejerza influencia o cumpla con responsabilidades educativas o gerenciales. Si bien estos principios competen a todos los profesionales de la Informática, los líderes tienen una responsabilidad mayor para defenderlos y promoverlos, tanto dentro de sus organizaciones como a través de ellas.

Un profesional de la Informática, especialmente quien cumpla funciones de liderazgo, debería...

3.1 Asegurar que el bien público sea la preocupación central en el trabajo profesional.

Las personas, incluyendo a los usuarios, clientes, colegas y cualquier otra persona afectada directamente o indirectamente, deben ser siempre la preocupación principal en Informática. El bien público siempre debe ser considerado explícitamente al evaluar las tareas asociadas con la investigación, el análisis de requisitos, el diseño, la implementación, las pruebas, la validación, el despliegue, el mantenimiento, el retiro y la eliminación. Los profesionales de la Informática deben centrar su atención en ello, más allá de las metodologías o técnicas utilicen en su práctica.

3.2 Articular, fomentar la aceptación y evaluar el cumplimiento de las responsabilidades sociales por parte de los miembros de la organización o grupo.

Las organizaciones y grupos técnicos afectan a la sociedad en general, y sus líderes deben aceptar las responsabilidades asociadas a ello. Las organizaciones -a través de procedimientos orientados a la calidad, la transparencia y el bienestar de la sociedad- reducen el daño a la sociedad y estimulan su concienciación sobre la influencia de la tecnología en nuestras vidas. Por lo tanto,

los líderes deben impulsar la plena participación de los profesionales de la Informática en el cumplimiento de las responsabilidades sociales y desalentar las tendencias a hacer lo contrario.

3.3 Administrar el personal y los recursos para mejorar la calidad de la vida profesional.

Los líderes deben garantizar que mejoren, y no se degrade, calidad de la vida profesional. Los líderes deben tener en cuenta el desarrollo personal y profesional, los requisitos de accesibilidad, la seguridad física, el bienestar psicológico y la dignidad humana de todos los trabajadores. Se deben usar estándares ergonómicos para la interacción persona-computadora apropiados en el lugar de trabajo.

3.4 Articular, aplicar y apoyar políticas y procesos que reflejen los principios del Código.

Los líderes deben procurar el desarrollo de políticas organizacionales claramente definidas que sean consistentes con el Código y comunicarlas efectivamente a las partes interesadas. Además, los líderes deben alentar y reconocer el cumplimiento de esas políticas, así como tomar las medidas adecuadas cuando se cometan infracciones. El diseño o implementación procesos que, deliberadamente o por negligencia, infrinjan o permitan la infracción de los principios del Código son éticamente inaceptables.

3.5 Crear oportunidades para que los miembros de la organización o el grupo crezcan como profesionales.

Las oportunidades educativas son esenciales para todas las organizaciones y los miembros del grupo. Los líderes deben garantizar que existan oportunidades disponibles para que los profesionales de la Informática mejoren sus conocimientos y habilidades profesionales, sus prácticas éticas y sus especialidades técnicas. Estas oportunidades deben incluir experiencias para que los profesionales de la Informática se familiaricen con las consecuencias y limitaciones de determinados tipos de sistemas. Los profesionales de la Informática deben ser plenamente conscientes de los peligros implícitos en los enfoques simplificados, la improbabilidad de anticipar todas las condiciones operativas posibles, la inevitabilidad de los errores de software, las interacciones entre los sistemas y sus contextos, y otros asuntos relacionados con la complejidad de su profesión. Por lo tanto, se les debe confiar la tarea de asumir responsabilidades por el trabajo que hacen.

3.6 Tener cuidado al modificar o retirar sistemas.

Los cambios de interfaz, la eliminación de funciones e incluso las actualizaciones de software tienen un impacto en la productividad de los usuarios y en la calidad de su trabajo. Los líderes deben tener cuidado al cambiar o discontinuar el soporte a los sistemas de los que las personas aún dependen. Los líderes deben investigar exhaustivamente las alternativas viables para eliminar el soporte de un sistema heredado. Si estas alternativas son arriesgadas o impracticables, el

desarrollador debe ayudar a las partes interesadas a migrar hacia una alternativa. Los usuarios deben ser notificados de los riesgos del uso continuado de un sistema que no es mantenido mucho antes de que se elimine el soporte. Los profesionales de la Informática deberían ayudar a los usuarios del sistema a controlar la viabilidad operativa de sus sistemas informáticos ya comprender que es posible que sea necesario reemplazar oportunamente funciones inadecuadas u obsoletas, o incluso, sistemas completos.

3.7 Reconocer y cuidar los sistemas que se integran en la infraestructura de la sociedad.

Incluso los sistemas informáticos más simples tienen el potencial de afectar todos los aspectos de la sociedad, especialmente cuando se integran con actividades cotidianas como el comercio, los viajes, el gobierno, la atención médica y la educación. Cuando las organizaciones y grupos desarrollan sistemas que se convierten en una parte importante de la infraestructura de la sociedad, sus líderes tienen la responsabilidad adicional de ser buenos administradores de estos sistemas. Establecer políticas para el acceso justo al sistema, incluso para aquellos que puedan haber sido excluidos, es una parte importante de la administración. Ésta requiere, además, que los profesionales de la Informática monitoreen el nivel de integración de sus sistemas en la infraestructura de la sociedad. A medida que el nivel de adopción cambia, es probable que las responsabilidades éticas de la organización o grupo también cambien. El monitoreo continuo de la forma en la cual la sociedad está usando un sistema permitirá que la organización o grupo se mantenga consistente con las obligaciones éticas descritas en el Código. Cuando no existen normas de cuidado apropiadas, los profesionales de la Informática tienen el deber de garantizar que se desarrollen.

4. CUMPLIMIENTO DEL CÓDIGO.

Un profesional de la informática debería...

4.1 Defender, promover y respetar los principios del Código.

El futuro de la Informática depende de la excelencia técnica y ética. Los profesionales de la informática deben adherir a los principios del Código y contribuir a mejorarlos. Los profesionales de la Informática que reconocen incumplimientos del Código deben tomar medidas para resolver los problemas éticos identificados, incluso, cuando sea razonable, expresando su preocupación a la persona o personas que se cree que violan el Código.

4.2 Tratar las violaciones del Código como inconsistentes con la afiliación a ACM.

Cada miembro de ACM debe alentar y apoyar la adhesión de todos los profesionales de la Informática independientemente de su afiliación a ACM. Los miembros de ACM que reconocen una violación del Código deben evaluar

reportarla a ACM, con la posibilidad de resultar en acciones correctivas, tal como se especifica en el Código de Ética de ACM y en la Política de Aplicación de la Conducta Profesional.

El Código y las directrices fueron desarrolladas por el Grupo de Trabajo 2018 del Código ACM: Comité Ejecutivo Don Gotterbarn (Presidente), Bo Brinkman, Catherine Flick, Michael S Kirkpatrick, Keith Miller, Kate Varansky y Marty J Wolf. Miembros: Eve Anderson, Ron Anderson, Amy Bruckman, Karla Carter, Michael Davis, Penny Duquenoy, Jeremy Epstein, Kai Kimppa, Lorraine Kisselburgh, Shrawan Kumar, Andrew McGettrick, Natasa Milic-Frayling, Denise Oram, Simon Rogerson, David Shama, Janice Sipior, Eugene Spafford y Les Waguespack. La Task Force fue organizada por el Comité de Ética Profesional de ACM. Las contribuciones significativas al Código también fueron hechas por los miembros internacionales de ACM. Este Código y sus directrices fueron adoptadas por el Consejo de ACM el 22 de junio de 2018.

On this page

Preámbulo

1. PRINCIPIOS ÉTICOS GENERALES.

1.1 Contribuir a la sociedad y al bienestar humano, reconociendo que todas las personas son partes interesadas en la Informática.

1.2 Evitar el daño.

1.3 Ser honesto y confiable.

1.4 Ser justo y tomar medidas para no discriminar.

1.5 Respetar el trabajo necesario para producir nuevas ideas, inventos, trabajos creativos y artefactos informáticos.

1.6 Respetar la privacidad.

1.7 Respetar la confidencialidad.

2. RESPONSABILIDADES PROFESIONALES.

2.1 Esforzarse por lograr una alta calidad tanto en los procesos como en los productos del trabajo profesional.

2.2 Mantener altos estándares de competencia profesional, conducta y práctica ética.

2.3 Conocer y respetar las reglas vigentes relacionadas con el trabajo profesional.

2.4 Aceptar y proporcionar una revisión profesional adecuada.

2.5 Realizar evaluaciones integrales y exhaustivas de los sistemas informáticos y de sus impactos, incluyendo un análisis de los posibles riesgos.

2.6 Trabajar solo en sus ámbitos de competencia.

2.7 Fomentar la conciencia ciudadana sobre la Informática, las tecnologías relacionadas y sus consecuencias.

2.8 Acceder a los recursos informáticos y de comunicación sólo cuando esté autorizado, o cuando sea necesario para proteger el bien público.

2.9 Diseñar e implementar sistemas robustos, accesibles y seguros.

3. PRINCIPIOS DE LIDERAZGO PROFESIONAL.

3.1 Asegurar que el bien público sea la preocupación central en el trabajo profesional.

3.2 Articular, fomentar la aceptación y evaluar el cumplimiento de las responsabilidades sociales por parte de los miembros de la organización o grupo.

3.3 Administrar el personal y los recursos para mejorar la calidad de la vida profesional.

3.4 Articular, aplicar y apoyar políticas y procesos que reflejen los principios del Código.

3.5 Crear oportunidades para que los miembros de la organización o el grupo crezcan como profesionales.

3.6 Tener cuidado al modificar o retirar sistemas.

3.7 Reconocer y cuidar los sistemas que se integran en la infraestructura de la sociedad.

4. CUMPLIMIENTO DEL CÓDIGO.

4.1 Defender, promover y respetar los principios del Código.

4.2 Tratar las violaciones del Código como inconsistentes con la afiliación a ACM.

Código de Ética y Conducta Profesional de ACM

计算机协会道德□职业行为准则

Supporting the Professionalism of ACM Members

The ACM Committee on Professional Ethics (COPE) is responsible for promoting ethical conduct among computing professionals by publicizing the Code of Ethics and by offering interpretations of the Code; planning and reviewing activities to educate membership in ethical decision making on issues of professional conduct; and reviewing and recommending updates to the Code of Ethics and its guidelines.

Guidance in Addressing Real-World Ethical Challenges

The Integrity Project, created by ACM's Committee on Professional Ethics, is a series of resources designed to aid ethical decision making. It includes case studies demonstrating how the principles can be applied to specific ethical challenges, and an Ask an Ethicist advice column to help computing professionals navigate the sometimes challenging choices that can arise in the course of their work.

Ask an Ethicist

Ask an Ethicist invites ethics questions related to computing or technology. Have an interesting question, puzzle or conundrum? Submit yours via a form, and the ACM Committee on Professional Ethics (COPE) will answer a selection of them on the site.

Using the Code

With the release of the updated Code of Ethics, ACM has created companion case studies that demonstrate how the principles of the Code can be applied to specific ethical challenges. Illustrative examples of hypothetical violations of or adherence to specific principles found in the Code—highlighting key nuances and directives—form the basis of the case studies.

Code of Ethics Enforcement Procedures

ACM expects all ACM and ACM Special Interest Group (SIG) members to make a commitment to engage in ethical professional conduct and abide by ACM’s Code of Ethics. This policy describes ACM’s procedure for enforcing the Code and may be used for complaints brought to ACM via ACM's other policies.

PDF of the ACM Code of Ethics