I. RESPONSABILIDADES PROFESIONALES.

Un profesional de la informática debería...

1.1 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.

1.2 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.

1.3 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.

1.4 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.

1.5 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.

1.6 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.

1.7 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.

1.8 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.

1.9 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.