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.