ASPECTOS ÉTICOS Y SOCIALES DE LOS S. I. (4)

Comprensión de los aspectos éticos y sociales relacionados con los sistemas

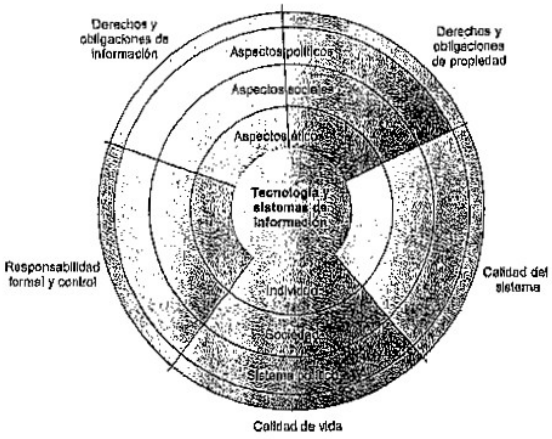
Ética: se refiere a los principios de lo correcto o lo incorrecto que los individuos, en su calidad de agentes morales libres, emplean para tomar decisiones que normen su comportamiento. La tecnología de información se puede emplear para alcanzar el progreso social, aunque también se puede aprovechar para cometer delitos y amenazar los valores sociales más preciados.

Internet y las tecnologías para las empresas digitales facilitan más que nunca la recopilación, integración y distribución de la información, y desencadenan nuevas preocupaciones acerca del uso apropiado de la información del cliente, la protección de la privacidad personal y la protección de la propiedad intelectual.

Otros aspectos éticos que surgen incluyen fincar la responsabilidad formal por las consecuencias de los sistemas de información, establecer estándares para salvaguardar la calidad del sistema que protejan la seguridad de los individuos y de la sociedad, y preservar los valores e instituciones considerados esenciales para la calidad de vida en una sociedad de la información.

Un modelo ético para considerar los aspectos éticos, sociales y políticos

FIGURA 4-1 LA RELACIÓN ENTRE LOS ASPECTOS ÉTICOS, SOCIALES Y POLÍTICOS EN UNA SOCIEDAD DE LA INFORMACIÓN



La introducción de la nueva tecnología de información ha tenido un efecto de ola, ya que ha dado lugar al surgimiento de nuevos aspectos éticos, sociales y políticos que se deben abordar en los niveles individual, social y político. Estos aspectos tienen cinco dimensiones morales: derechos y obligaciones de información, derechos y obligaciones de propiedad, calidad del sistema, calidad de vida y responsabilidad formal y control.

Las instituciones sociales no pueden responder de la noche a la mañana antes estas olas. Las instituciones políticas también requieren tiempo antes de desarrollar nuevas leyes y en ocasiones requieren la manifestación de un daño real antes de actuar. Entre tanto, es posible que uno se vea obligado a actuar, forzado incluso a hacerlo en terrenos legales indefinidos.

Cinco dimensiones morales de la era de la información

Entre los principales aspectos éticos, sociales y políticos propiciados por los sistemas de información se encuentran las siguientes dimensiones morales:

- *Derechos y obligaciones de información*
- *Derechos y obligaciones de propiedad*
- *Responsabilidad formal y control*
- *Calidad del sistema*
- *Calidad de vida*

Tendencias tecnológicas clave que propician el surgimiento de los aspectos éticos

La tecnología de información ha intensificado las preocupaciones éticas, ha sometido a tensión las órdenes sociales y ha vuelto obsoletas o severamente anquilosadas las leyes existentes. Hay cuatro tendencias tecnológicas clave responsables de estas tensiones éticas.

a) La duplicación de cómputo cada 18 meses ha hecho posible que la mayoría de las organizaciones empleen los sistemas de información para sus procesos de producción esenciales. Como resultado, nuestra dependencia de los sistemas ha aumentado, así como nuestra vulnerabilidad a los errores de los sistemas y a la baja calidad de los datos.
Las reglas y las leyes sociales aún no se han ajustado a esta dependencia. No se han aceptado o impuesto de manera universal estándares que aseguren la exactitud y confiabilidad de los sistemas de información.

b) Los avances de las técnicas de almacenamiento de datos y la rápida caída de los costos de almacenamiento han sido los responsables de que las organizaciones privadas o públicas hayan multiplicado las bases de datos de individuos. Estos avances en el almacenamiento de datos han facilitado la infracción rutinaria de la privacidad individual a un bajo costo.

c) Los avances en las técnicas de análisis de grandes concentraciones de datos constituyen otra tendencia tecnológica que acentúa las preocupaciones éticas porque permiten que las compañías y las instituciones gubernamentales averigüen mucha información personal detallada de los individuos. Con las actuales herramientas de administración de datos, las compañías pueden ensamblar y combinar una infinidad de piezas de información relativa a cualquiera de nosotros, la cual es almacenada por las computadoras con mayor facilidad que antes.

Al uso de computadoras para combinar datos desde múltiples fuentes y crear expedientes electrónicos de información detallada sobre individuos se le denomina ***elaboración de perfiles***.

Una nueva tecnología de análisis de datos, denominada ***descubrimiento de relaciones no evidentes (NORA)***, ha dao tanto al sector gubernamental como al privado capacidades más poderosas para crear perfiles. NORA puede captar información sobre personas desde fuentes muy distintas como solicitudes de empleo, registros telefónicos, listados de clientes e incluso de listas deseadas o de preferencias, y asocia las relaciones para encontrar conexiones ocultas que podrían ayudar a identificar criminales o terroristas.
La tecnología NORA puede escanear datos y extraer información conforme se van generando los datos. La tecnología se considera una valiosa herramienta para la seguridad nacional pero al mismo tiempo tiene implicaciones de privacidad, porque puede ofrecer un panorama detallado de las actividades y relaciones de un solo individuo.

d) Los avances en la conectividad de redes, prometen reducir en gran medida los costos de trasladar y acceder a enormes cantidades de datos, así como abrir la posibilidad de extraer grandes

concentraciones de datos de manera remota utilizando pequeñas computadoras de escritorio, permitiendo una invasión de la privacidad a una escala y precisión hasta ahora inimaginables.
El desarrollo de redes de comunicación digital globales ampliamente disponibles a individuos y empresas, plantea muchas preocupaciones éticas y sociales.

La ética en una sociedad de información
La ética es una preocupación de los humanos con libertad de elección. La ética tiene que ver con la elección individual: cuando se enfrentan a vías de acción alternativas ¿cuál es la elección moral correcta? ¿cuáles son las principales características de la elección ética?

Conceptos básicos: responsabilidad, rendición de cuentas y responsabilidad legal

Las elecciones éticas son opciones elegidas por individuos que se hacen responsables de las consecuencias de sus acciones. La ***responsabilidad*** es elemento clave de la acción ética. La responsabilidad significa que usted acepta los posibles costos, deberes y obligaciones de sus decisiones.
La ***rendición de cuentas*** es una característica de los sistemas y las instituciones sociales: implica que existen mecanismos para determinar quien realizo acciones responsables, quien debe rendir cuentas. Los sistemas y las instituciones en los que es imposible averiguar quien realizo que acción no son susceptibles de análisis ético ni pueden realizar acciones éticas. La responsabilidad legal extiende el concepto de responsabilidad al área de las leyes.

La ***responsabilidad legal*** es una característica de los sistemas políticos en los que hay leyes que permiten a los individuos ser compensados por los perjuicios infligidos en ellos por otros actores, sistemas u organizaciones. El *proceso justo* es una característica relacionada con sociedades gobernadas por leyes y es a la vez un proceso en el que las leyes se conocen y entienden además de haber una capacidad de apelar a las autoridades superiores para asegurar que las leyes se hayan aplicado correctamente.

Estos conceptos forman las bases del análisis ético de los sistemas de información. Las tecnologías de información se filtran a través de instituciones sociales, organizaciones e individuos. Cualquier impacto de los sistemas de información que existe es un producto de acciones y conductas de instituciones, organizaciones o individuos. La responsabilidad por las consecuencias del uso de la tecnología recae sobre las instituciones, las organizaciones y los administradores individuales que deciden utilizarla. El uso de tecnología de información de una manera ¨socialmente responsable¨ implica que uno puede y debe rendir cuentas de las consecuencias de sus acciones. En una sociedad política ética, los individuos y otras entidades pueden ser compensados por los daños infligidos por otros, a través de un conjunto de leyes caracterizados por procesos justos.

Análisis éticos
Una situación que tiene aspectos éticos se debe analizar de la siguiente manera:

- Identificar y describir claramente los hechos. Averiguar quien hizo que cosa a quien, cando y como.
- Definir el conflicto o dilema e identificar los valores de orden mas alto en cuestión.
- Identificar los grupos de interés. Protagonistas que están interesados en el desenlace, que han invertido en la situación y que expresan sus opiniones.
- Identificar opciones razonables que se pueden tomar. Tal vez ninguna satisfaga todos los intereses implicados, pero es probable que algunas de ellas lo haga mejor que otras.

- Identificar las posibles consecuencias de las opciones. Algunas opciones pueden ser éticamente correctas, pero desastrosas desde otros puntos de vista. Siempre es necesario preguntarse ¿qué pasaría si siempre se eligiera esta opción?

Principios éticos propuestos

Una vez terminado el análisis, ¿qué principios éticos o reglas deben usarse para tomar una decisión? ¿Qué valores de orden superior deben dar forma el juicio?

1- Tratar a los demás como se quiere que los demás lo traten a uno (la ***regla de oro***)
2- Si una acción no es correcta para todos, no es correcta para nadie. (***imperativo categórico de Kant***)
3- Si una acción no puede efectuarse rápidamente, no debe efectuarse nunca. (***regla del cambio de Descartes***)
4- Efectuar la acción que logra el valor mas alto o mayor (***principio Utilitarista***)
5- Efectuar la acción que produce el menor daño, o que cuesta menos (***principio de Aversión al Riesgo***). Hay que evitar acciones cuyo fallo tendría un costo alto, poniendo mayor atención en aquellas con una probabilidad de fallo de moderada a alta.
6- Suponer que todos los objetos tangibles e intangibles son propiedades de alguien mas, a menos que exista una declaración especifica que diga que no esta así. (***regla ética de ¨nada es gratis¨***)

Aparentar una conducta no ética podría dañar a su compañía y a usted tanto como una verdadera conducta no ética.

Códigos profesionales de conducta

Cuando algunos grupos de personas dicen ser profesionales, adquieren derechos y obligaciones especiales por afirmar que poseen conocimientos o entendimientos especiales, y merecen un respeto especial.

Estos grupos profesionales asumen la responsabilidad de regular sus profesiones, determinando requisitos y aptitudes para ser aceptados. Los códigos de ética son promesas hechas por la profesión de regularse a sí mismos por el interés general de la sociedad.

Los profesionales de la ACM (Association of Computing Machinery) deben considerar la salud, la privacidad y el bienestar general del público durante el desempeño de su trabajo, y que los profesionales deben expresar su opinión profesional a su patrón en lo tocante a cualquier consecuencia para el público.

Algunos dilemas éticos del mundo real

Algunos de los problemas éticos son dilemas éticos obvios, en los que un conjunto de intereses se opone a otro. Otras representan algún tipo de violación de la ética.

Muchas compañías vigilan lo que hacen sus empleados en Internet para evitar que desperdicien los recursos de la compañía en actividades no lucrativas. Por ejemplo, una empresa podría argumentar que le asiste el derecho de utilizar los sistemas de información para incrementar la productividad y reducir el número de sus trabajadores a fin de bajar costos y mantenerse en el negocio. Los empleados desplazados por los sistemas de información podrían argumentar que los empleados tienen cierta responsabilidad por su bienestar. En ocasiones, un análisis detallado de los hechos puede producir soluciones mediante arreglos que concedan algo a cada parte.

Las dimensiones morales de los sistemas de información

Derechos de información: privacidad y libertad en una sociedad de información.

La ***privacidad*** es el derecho de los individuos a que se les deje en paz, sin vigilancia ni interferencia por parte de otros individuos u organizaciones, incluido el gobierno. Los derechos a la privacidad también se trasladan al lugar de trabajo. La tecnología y los sistemas de información amenazan la privacidad de los individuos al hacer barata, rentable y eficaz su invasión.

Casi todas las leyes en materia de privacidad se basan en, ***Prácticas Honestas de Información (FIP)***, que son un conjunto de principios que rigen la recolección y el uso de información acerca de los individuos.

Los principios se basan en una idea de una ¨mutualidad de interés¨ entre el encargado de mantener el expediente y el individuo. El individuo tiene interés en realizar una transacción, y quien mantiene el expediente necesita información acerca del individuo para apoyar la transacción.

Las Practicas de información Equitativas constituye la base de estatutos que plantean las condiciones para manejar información a cerca de individuos en áreas como informes de crédito, educación, expedientes financieros, etc.

Los Principios de Información Equitativa son un conjunto de principios que gobiernan la recolección y uso de información acerca de individuos, y constituye la base de casi todas las leyes estadounidenses y europeas en materia de privacidad.

La Directiva Europea sobre la Protección de Datos

En Europa la Protección de la privacidad es mucho más estricta que en Estados Unidos. Los países europeos no permiten que las empresas utilicen la información de identificación personal sin el consentimiento previo de los clientes.

La Directiva sobre la Protección de Datos exige a las compañías que informen a las personas cuando recopilen información sobre ellas y divulguen cómo se guardará y usará. Los clientes deben proporcionar su consentimiento informando para que las compañías pueden usar legalmente los datos acerca de ellos, y cuentan con el derecho de acceder a esa información, corregirla y pedir que ya no se recopilen más datos. El ***consentimiento informado*** se puede definir como el consentimiento dado con conocimiento de todos los factores necesarios para tomar una decisión racional.

El ***safe harbor*** es una política privada autorregulable y un mecanismo de aplicación que cumple con los objetivos de las regulaciones y legislaciones gubernamentales aunque sin regulación ni aplicación ni aplicación por parte del gobierno.

A las empresas estadounidenses que hacen negocios con empresas europeas se les permite utilizar datos personales de países de la UE. Para utilizar los datos personales, las empresas deben obtener la certificación safe harbor. Con esta política, los estadounidenses y los europeos han podido superar sus diferencias en materia de privacidad y que se realicen las transacciones comerciales.

Retos de Internet a la privacidad

La información enviada a través de una vasta red de redes puede pasar a través de muchos y diferentes sistemas de cómputo antes de arribar a su destino final. Cada uno de estos sistemas tienen la capacidad de vigilar, capturar y almacenar las comunicaciones que pasan a través de ellos.

Gran parte de esta vigilancia y seguimiento de los visitantes al sitio Web ocurre en segundo plano sin el conocimiento del visitante. Estas herramientas para vigilar las visitas ayudan a las organizaciones a determinar quién está visitando sus sitios Web y a enfocar mejor sus ofrecimientos. Algunas vigilan el uso que sus empleados dan a Internet para saber cómo utilizan los recursos de

redes de la compañía. Ahora existen software para "vigilar" el comportamiento en línea de individuos y grupos mientras visitan un sitio Web y realizan compras.

Las ***cookies*** son archivos diminutos que se alojan en el disco duro de una computadora cuando un usuario visita ciertos tipos Web. Las cookies identifican el software del navegador Web del visitante y rastrean las visitas al sitio Web. Cuando el visitante vuelve a un sitio que tiene depositada una cookie, el software del sitio Web buscará en la computadora del visitante, encontrará la cookie e identificará lo que esa persona ha hecho en el pasado. También se puede actualizar la cookie. De este modo, el sitio puede personalizar su contenido para ajustarlo a los intereses de cada visitante.
Sin embargo, si una persona se ha registrado en un sitio, esa información se puede combinar con los datos de la cookie para identificar al visitante. Con los datos personales de otras fuentes se pueden desarrollar perfiles muy detallados de sus visitantes.

Los comerciantes utilizan los ***Web bugs*** como otra herramienta para vigilar el comportamiento en línea. Los Web bugs son pequeños archivos gráficos incrustrados en mensajes de correo electrónico y páginas Web, diseñados para vigilar quién está leyendo el correo electrónico o la página Web y transmitir esa información a otra computadora.
Los ***spyware*** se puede instalar a sí mismo en la computadora de un usuario de Internet al colarse a ésta incrustado en aplicaciones más grandes. Una vez que se instala, el spyware se conecta a sitios Web para enviar al usuario anuncios publicitarios y otro material no solicitado, y también puede reportar a otras computadoras las acciones que realiza el usuario en Internet. El spyware puede registrar lo que el usuario teclea y enviar la información a otros sitios Web sin que el usuario se entere.

Un modelo de opción de exclusión de consentimiento informado permite la recopilación de información personal hasta que el consumidor solicita específicamente que no se recopilen datos. A los defensores de la privacidad les gustaría ver en un uso más amplio de un modelo de opción de aceptación de consentimiento informado en el cual a un negocio se le prohíbe recopilar cualquier información personal a no ser que el consumidor apruebe específicamente la recopilación y uso de la información.

Soluciones Técnicas
Además de la legislación, se puede disponer de nuevas tecnologías para proteger la privacidad del usuario durante su interacción con los sitios Web.
En la actualidad hay herramientas que pueden ayudar a los usuarios a determinar la clase de datos personal que los sitios Web pueden extraer. Las plataformas para las Preferencias de Privacidad (P3P), permite la comunicación automática de políticas de privacidad entre un sitio de comercio electrónico y sus visitantes. Los usuarios puede utilizar P3P para seleccionar el nivel de privacidad que desean mantener al interactuar con el sitio Web.
El estándar P3P permite que los sitios Web publiquen políticas sobre privacidad en un formato que las computadoras pueden entender. Sin embargo, P3P sólo funciona con sitios Web miembros del World Wide Web Consortium.

DERECHOS DE PROPIEDAD: PROPIEDAD INTELECTUAL

Se considera que la propiedad intelectual es una propiedad intangible creada por individuos o corporaciones. La tecnología de información ha dificultado la protección de la propiedad intelectual debido a que la información computarizada se puede copiar o distribuir fácilmente en las redes. La propiedad intelectual está sujeta a varias protecciones bajo tres diferentes prácticas legales: leyes

sobre secretos comerciales, de derechos de autor y de patentes.

Secretos comerciales: todo producto del trabajo intelectual utilizado para un propósito intelectual se puede clasificar como secreto comercial, siempre y cuando no se base en información de dominio público. Las protecciones para los secretos comerciales varían de lugar a lugar.
El software que contiene elementos, procedimientos o compilaciones novedosos o únicos se puede incluir como secreto comercial.
Para tener este derecho, el creador o propietario deben tener cuidado de obligar a empleados y clientes a firmar contratos de no divulgación con el fin de evitar que el secreto se haga de dominio público.
La limitación es que en la práctica es difícil evitar que las ideas caigan en el dominio público cuando el software se distribuye de forma amplia.

Derechos de autor: son una concesión reglamentaria que protege a los creadores de la propiedad intelectual de que otros copien su trabajo con cualquier propósito durante la vida del autor y hasta 70 años después de la muerte de éste. Para los trabajos propiedad de corporaciones, la protección de los derechos de autor se extiende a 95 años a partir de su creación.
La mayoría de los países industrializados tienen sus propias leyes de derechos de autor y hay varias convenciones internacionales y acuerdos bilaterales mediante los cuales los países coordinan y aplican sus leyes.
La protección de derechos de autor impide la copia total o parcial de los programas. La desventaja de la protección de los derechos de autor es que las ideas en que se fundamenta un trabajo no están protegidas, sólo su manifestación en un trabajo. Un competidor puede usar su software, entender cómo funciona y construir un nuevo software que siga los mismos conceptos sin infringir ningún derecho de autor.

Patentes: le da al propietario un monopolio exclusivo durante 20 años de las ideas fundamentales de su invento. Los conceptos fundamentales de una patente son la originalidad, la novedad y la invención. La dificultad está en aprobar los severos criterios de la falta de claridad, originalidad y novedad, así como años de espera para recibir la protección.

Retos a los derechos de propiedad intelectual
Las tecnologías de la información contemporánea, sobre todo el software, plantean un severo reto a los regímenes existentes de la propiedad intelectual y, por consiguiente, generan aspectos éticos , sociales y políticos significativos.
La proliferación de redes electrónicas, incluyendo Internet, ha hecho incluso más difícil proteger la propiedad intelectual. Mediante las redes, la información se puede reproducir y distribuir con mucha mayor amplitud.
Internet se diseño para transmitir libremente información por todo el mundo, incluyendo la información protegida por derechos de autor. La información se puede copiar ilícitamente de un lugar y distribuirla a través de otros sistemas y redes, aunque estas partes no participen voluntariamente en la infracción.
La compartición ilegal de archivos se difundió con tanta amplitud que amenazó la viabilidad de la industria discográfica. A medida que más y más hogares tienen acceso de alta velocidad a Internet, la compartición ilícita de archivos de video planteará amenazas similares a la industria cinematográfica.
La ley de Derechos de Autor para el Milenio Digital (DMCA) establece un Tratado de Organización Mundial de la Propiedad Intelectual que hace ilegal ignorar las protecciones basadas en la tecnología de materiales protegidos por derechos de autor. A los proveedores de servicios de

Internet se les exige que, en cuanto se les notifique del problema, “retiren” de sus servidores los sitios de aquellos que infrinjan los derechos de autor.
Microsoft y otras 1,400 empresas de contenido de software e información están representadas por la Asociación de la Industria de Software e Información (SIIA), que pugnan por nuevas leyes y la aplicación de leyes existentes para proteger la propiedad intelectual en todo el mundo.

Rendición de cuentas, responsabilidad legal y control
Las nuevas tecnologías de información están desafiando a la ley de responsabilidad legal y las prácticas sociales existentes para hacer que los individuos y las instituciones rindan cuentas.

Problemas de responsabilidad legal relacionados con las computadoras
En general, en la medida en que un software de cómputo forma parte de una máquina y que la máquina daña a alguien física o económicamente, los responsables legales de los daños son el productor y el operador del software.
Las cortes se han cuidado de responsabilizar legalmente a los autores de software porque el software cae dentro de un tipo de libro. Históricamente, a los editores de impresos, libros y revistas no se les ha considerado responsables legales por temor a que los reclamos de responsabilidad legal interfieran con los derechos de la Primera Enmienda que garantiza la libertad de expresión.
Dada la participación central del software en la vida diaria, hay muchas probabilidades de que la ley de responsabilidad legal extienda su alcance para incluir el software aunque sólo preste servicios de información.
A pesar de que las Cortes de EEUU han exonerado a cada vez más sitios Web y a proveedores de servicios de Internet por la publicación de materiales de terceros, la amenaza de acciones legales sigue tranquilizando a las pequeñas empresas o a los individuos que no pueden darse el lujo de llevar sus casos a los tribunales.

Calidad de sistemas: calidad de datos y errores del sistema
Aunque las compañías de software tratan de depurar sus productos antes de ponerlos a la venta en el mercado, están conscientes de que envían productos imperfectos al mercado ya que el tiempo y costo de arreglar todos los errores menores impediría que estos productos se pudieran vender alguna vez.
Las tres causas principales de que el rendimiento de un sistema sea bajo son:

1. Los bugs y las fallas de software
2. Las fallas en el hardware o en las instalaciones, ocasionadas por la naturaleza u otras causas
3. Una baja calidad en los datos de entrada

Hay una barrera tecnológica para el software perfecto y los usuarios deben estar atentos a una posible falla catastrófica. La industria del software aún no ha alcanzado los estándares de prueba para producir un software de desempeño aceptable aunque no perfecto.
Sin embargo, la fuente más común de fallas en los sistemas empresariales es la calidad de los datos.

Calidad de vida: equidad, acceso y límites
Los costos sociales negativos de introducir tecnologías y sistemas de información están empezando a crecer al parejo del poder de la tecnología. Aun cuando nos brindan beneficios, las computadoras y las tecnologías de información pueden destruir potencialmente elementos culturales y sociales valiosos.

Equilibrio del poder: el centro comparado con la perisferia
El giro hacia una computación altamente descentralizada, aunada a una ideología de empoderamiento de miles de trabajadores y la descentralización de la toma de decisiones a niveles

organizacionales más bajos ha reducido los temores de la centralización del poder en las instituciones. Sin embargo, mucho del empoderamiento descripto es superficial, pues las decisiones de política clave tal vez estén tan centralizadas como antes.

Celeridad del cambio: tiempo de respuesta reducido para competir

Los sistemas de información han ayudado a crear mercado nacionales e internacionales mucho más eficientes. Es posible que la empresa para la que usted trabaja no tenga tiempo suficiente para responder a los competidores globales y podría ser eliminada en un año junto con su empleo.

Mantenimiento de los límites: familia, trabajo y esparcimiento

El peligro de la ubicuidad de la computación, las telecomunicaciones, la computación nómada y el entorno de cómputo "haga cualquier cosa en cualquier lugar", consiste en que esto podría volverse una realidad. De ser así, se debilitarán los límites tradicionales que separan al trabajo de la familia y el esparcimiento.

Las actividades laborales se extienden ahora más allá de la jornada de ocho horas. El uso extenso de Internet, incluso con fines recreativos y de entretenimiento, aparta a las personas de sus familias y amigos.

Dependencia y vulnerabilidad

Actualmente, nuestros negocios, gobiernos, escuelas y asociaciones privadas, son increíblemente dependientes de los sistemas de información y, por consiguiente, altamente vulnerables si estos sistemas fallaran. La ausencia de estándares y la importancia de algunas aplicaciones de sistemas probablemente requieran estándares nacionales y quizá supervisión normativa.

Delito y abuso informático

El ***delito informático*** es la ejecución de actos ilegales mediante el uso de una computadora o contra un sistema de cómputo. Las computadoras o los sistemas de cómputo pueden ser objeto de un delito, así como el instrumento de un delito.

El simple acceso a un sistema de cómputo sin la autorización o con la intención de causar daño, incluso por accidente, es un delito federal.

El ***abuso informático*** es la ejecución de actos que implican una computadora, que tal vez no sean ilegales pero que no se consideran éticos. El ***spam*** es el correo electrónico basura enviado por una organización o individuo a un público masivo de usuarios de Internet que han manifestado du falta de interés en el producto o servicio que se les intenta vender.

Los costos del spam son muy altos para las empresas por los recursos de cómputo y de red que consumen los miles de millones de mensajes de correo electrónico no solicitado y el tiempo necesario para deshacerse de ellos. Los proveedores de servicios de Internet y los individuos pueden combatir el spam por medio de software de filtrado que bloquea el correo electrónico sospechoso antes de que se deposite en la bandeja de entrada del receptor. Sin embargo, los filtros de spam podrían bloquear mensajes legítimos, y muchos spammer evitan los filtros cambiando continuamente sus cuentas de correo electrónico.

Empleo: pérdida de puestos por la tecnología y la reingeniería

El rediseño de los procesos de negocios podría llegar a ser la causa de que millones de gerentes de nivel intermedio y oficinistas pierdan su trabajo.

Una planeación y sensibilidad cuidadosa de las necesidades del empleado pueden ayudar a las

compañías a rediseñar el trabajo para minimizar las pérdidas de empleos.

Equidad y acceso: incremento de las diferencias raciales y las clases sociales
La información, el conocimiento, las computadoras y el acceso a estos recursos a través de las instituciones educativas y bibliotecas públicas no están distribuidos equitativamente entre los estratos étnicos y clases sociales, como ocurre con muchos otros recursos de información.
Una brecha digital parecida se da en las escuelas de EEUU. Si no se corrige, la brecha digital podría conducir a una sociedad informada, con conocimientos y habilidades de cómputo, contra un gran grupo no informado y carente de conocimiento y habilidades de cómputo.

Riesgos para la salud: RSI, CVS y tecnoestrés
El ***daño por estrés repetitivo*** (RSI) se presenta cuando los grupos musculares se fuerzan mediante acciones repetitivas, con frecuencia por cargas de alto impacto o decenas o miles de repeticiones de cargas de bajo impacto (teclear en la Pc).
El tipo más común de RSI relacionado con la computadora es el ***síndrome del túnel carpiano*** (CTS), en el cual la presión sobre el nervio medio que cruza la estructura del hueso de la muñeca, llamada túnel carpiano, causa dolor. La presión la causa la repetición constante de pulsaciones de teclas. Los síntomas del síndrome de túnel carpiano incluyen insensibilidad, punzadas, incapacidad de asir objetos y hormigueo.
El RSI se puede evitar diseñando estaciones de trabajo con una posición neutral para las muñecas, soportes adecuados para el monitor y descansos para los pies, contribuyen en conjunto a lograr una postura adecuada y a reducir el RSI. Estas medidas se deben apoyar en descansos frecuentes y en la rotación de empleados por diferentes puestos.

El ***síndrome de visión de computadora*** (CVS) se refiere a cualquier condición de tensión en los ojos relacionada con el uso de la pantalla. Sus síntomas, por lo general temporales, incluyen dolores de cabeza, visión borrosa y resequedad e irritación de los ojos.

El ***tecnoestrés*** es una tensión inducida por el uso de la computadora. Sus síntomas incluyen exasperación, hostilidad hacia las personas, impaciencia y fatiga. Las personas que trabajan continuamente con computadoras llegan al punto de esperar que las demás personas e instituciones humanas se comporten como computadoras y den respuestas instantáneas, atentas y carentes de emoción.
Los trabajos relacionados con la computación encabezan ahora la lista de ocupaciones estresantes con base en estadísticas de salud de varios países industrializados.

El crecimiento de Internet y la economía de la información indican que todos los aspectos éticos y sociales descriptos se intensificarán conforme avancemos en el primer siglo de la era digital.