CENGAGE Learning

# ÉTICA EN LA TECNOLOGÍA DE LA INFORMACIÓN

## Quinta Edición

George W. Reynolds
Strayer University

# ÉTICA EN LA TECNOLOGÍA DE LA INFORMACIÓN

Quinta Edición

George W. Reynolds
*Strayer University*

Traducción
Anaid Zendejas Escandón
Traductora profesional

Revisión Técnica
Mtro. Armando Cerda Miranda
Instituto Tecnológico y de Estudios
Superiores de Monterrey,
Campus Estado de México

CENGAGE Learning

Australia • Brasil • Corea • España • Estados Unidos • Japón • México • Reino Unido • Singapur

CENGAGE Learning®

***Ética en la tecnología de la información. Quinta edición***
George W. Reynolds

**Presidente de Cengage Learning Latinoamérica:**
Fernando Valenzuela Migoya

**Director Editorial, de Producción y de Plataformas Digitales para Latinoamérica:**
Ricardo H. Rodríguez

**Editora de Adquisiciones para Latinoamérica:**
Claudia C. Garay Castro

**Gerente de Manufactura para Latinoamérica:**
Raúl D. Zendejas Espejel

**Gerente Editorial en Español para Latinoamérica:**
Pilar Hernández Santamarina

**Gerente de Proyectos Especiales:**
Luciana Rabuffetti

**Coordinador de Manufactura:**
Rafael Pérez González

**Editor:**
Omegar Martínez

**Diseño de portada:**
Studio Bold
studiobold.mx

**Composición tipográfica:**
Studio Bold
studiobold.mx



Datos para catalogación bibliográfica:
Traducido del libro *Ethics in Information Technology*, Fifth Edition.
George W. Reynolds
Publicado en inglés por Cengage Learning ©2015.
ISBN: 978-1-285-19715-9

Datos para catalogación bibliográfica:
Reynolds, George W.
*Ética en la tecnología de la información*, 5a. ed.
ISBN: 978-607-522-844-0

Visite nuestro sitio en:
http://latinoamerica.cengage.com

Impreso en México
1 2 3 4 5 6 7 18 17 16 15

# TABLA DE CONTENIDO

# PREFACIO

Nos encontramos emocionados de haber publicado la quinta edición de Ética en la Tecnología de la Información. Esta nueva edición se edifica bajo el éxito de las ediciones anteriores, cumpliendo con la necesidad de obtener un recurso que ayuda a que los lectores comprendan muchos de los aspectos legales, éticos y sociales que se asocian a la Tecnología de la Información (TI). Para esta edición, hemos respondido a las propuestas que nos han hecho estudiantes, editores y revisores, de manera que ahora podemos entregarles un texto renovado, y más completo. Creemos que estarás satisfecho con los resultados.

La quinta edición de Ética en la Tecnología de la Información, llena un vacío de información que existe en la práctica y gestión de negocios asociada con los profesionales de la TI. Un libro de texto introductorio típico dedicaría solamente un capítulo a la ética y la tecnología de la información, espacio que insuficiente para cubrir el amplio espectro de temas y problemáticas relacionadas con la TI. Una cobertura tan limitada no cumple los requisitos de los gerentes de negocios o los profesionales de la TI: las personas responsables de manejar los problemas éticos que surgen en el sitio de trabajo. Hace falta realizar un análisis de las distintas situaciones éticas que surgen en la TI así como consejos prácticos para manejar este tipo de problemas.

La quinta edición de Ética en la Tecnología de la Información, tiene contenido suficiente como para que un profesor pueda utilizarlo durante un curso semestral de cómputo ético. Los profesores también pueden utilizar este libro como material suplementario para cursos como "Introducción a la Gestión en Sistemas de Información", "Principios de la Tecnología de la Información", "Perspectivas Gerenciales en la Tecnología de la Información", "Seguridad Informática", "Comercio Electrónico", etc.

## LO NUEVO

Ética para la *Tecnología de la Información*, Quinta Edición, ha sido revisado y actualizado para incorporar los bastos y nuevos desarrollos de las problemáticas éticas que han surgido desde que se publicó la edición anterior. Hemos ampliado los siguientes temas: el aumento en los riesgos de seguridad implicados en las políticas empresariales tipo Trae Tu Propio Dispositivo (BYOD, por sus siglas en inglés); el papel

que juega la Agencia de Seguridad Nacional en descifrar códigos utilizados para encriptar comunicados privados, o la involucración de la Agencia en la intercepción de señales a nombre del gobierno federal; el proceso ético implicado en el uso de compañías de gestión de reputación en línea; el uso de pleitos estratégicos contra la participación pública (SLAPP por sus siglas en inglés) así como las demandas anti-SLAPP; el robo de secretos comerciales pertenecientes a Estados Unidos y Europa Occidental, que cometió China; así como el papel de la telesalud y la telemedicina en la transmisión de cuidado médico.

Todas las viñetas de apertura, así como dos tercios de los casos comentados al final de cada capítulo, son contenidos renovados y ampliamente actualizados. Se presentan docenas de ejemplos reales y nuevos en cada capítulo. Al menos 50 por ciento de las secciones: "Preguntas de Auto Evaluación", "Preguntas para Discutir" y "¿Qué harías tú? ", contienen ejercicios nuevos. Basándonos en la retroalimentación obtenida por revisores, hemos incrementado el número de ejercicios incluidos en las secciones: "Preguntas para Discutir" y "¿Qué harías tú?". Los profesores de cursos virtuales utilizan estas secciones como fundamentos para crear foros de discusión en línea que permitan a los estudiantes compartir una variedad de perspectivas y experiencias, así como crear una comunidad de aprendizaje. Dichas discusiones proveen a los estudiantes con la oportunidad de comprender con mayor profundidad el material, pues los ayuda a confrontar sus habilidades de pensamiento crítico.

## ORGANIZACIÓN

Cada uno de los 10 capítulos de este libro se enfoca en un aspecto diferente de la ética de la tecnología de la información:

- El Capítulo 1, "Panorama de la Ética", provee una introducción a la ética, ética de negocios y la relevancia de discutir la ética en la TI. El capítulo define la distinción entre moral, ética y ley. Identifica las formas de negligenca más comunes cometidas por empleados. Discute y define el concepto de responsabilidad social corporativa. Da cinco razones sobre la importancia de la práctica de una buena ética de negocios y provee un modelo para mejorar la ética corporativa. Analiza el papel de los directivos éticos y la junta de directores, para establecer un programa ético organizacional que sea fuerte y sustancioso. El capítulo también destaca la necesidad de un código de ética organizacional y describe los pasos clave para establecer un programa ético sólido. Sugiere un modelo para la toma de decisiones éticas y también discute cuatro enfoques filosóficos de uso común para la toma de decisiones éticas. El capítulo termina con una discusión acerca del papel de la ética en la TI.
- El Capítulo 2, "Ética para los trabajadores y usuarios de la Tecnología de la Información", comienza con una viñeta que expone los fraudes de TI en los que se vio involucrada la Nómina de la Ciudad de Nueva York. Este capítulo explica la importancia de la ética en las relaciones de negocios de los profesionales de la TI, incluyendo las relaciones que existen entre los empleados de la TI y sus empleadores, clientes, proveedores, otros profesionales, usuarios de la TI y la sociedad en general. En él se enfatiza la importancia de las organizaciones profesionales de la TI y sus códigos éticos. Discute los papeles que juegan la certificación y el licenciamiento en la legitimación de los estándares profesionales. También se señalan las dificultades que existen en el licenciamiento de los empleados de la TI. De la misma manera, toca algunos de los problemas éticos que enfrentan los usuarios de la TI, como son: piratería de software, uso inapropiado de recursos informáticos o el intercambio inapropiado de información. Se describen las acciones que pueden tomarse para apoyar e implementar prácticas éticas por parte de los usuarios de la TI. El capítulo también introduce el concepto de observancia y el papel del comité de auditoría y los

miembros de los equipos internacionales de auditoria, para asegurar que, tanto la organización de TI, como los usuarios de la TI, cumplan con los lineamientos y políticas organizacionales, así como las distintas prácticas legales y regulatorias que existen.

- El Capítulo 3, "Delito Informático", describe los tipos de decisiones éticas que deben tomar los profesionales de la TI, así como las necesidades empresariales que deben considerar cuando lidian con problemas de seguridad. El capítulo identifica los incidentes de seguridad informáticos más comunes y provee numerosas razones para justificar la causa del aumento en estos incidentes, incluyendo el uso del cómputo en la nube, software de virtualización y las políticas empresariales tipo "Trae Tu Propio Dispositivo". Describe algunos de los ataques hacker más comunes: virus, gusanos, caballos de troya, denegación de servicios distributiva, rootkits, spam, phishing, spear-phising, smishing, vishing y ransom ware. Además de proveer una clasificación útil de los delitos informáticos y sus perpetradores, el capítulo resume las principales leyes federales que manejan este tipo de delitos. Se destaca cómo implementar un cómputo confiable para gestionar las vulnerabilidades de seguridad y cómo responder a incidentes de seguridad específicos para resolver rápidamente problemas, y mejorar las medidas de seguridad actuales. Presentamos un proceso para realizar una evaluación de las amenazas internas y externas que sufren las redes informáticas de una organización. El capítulo discute la necesidad de tener una política de seguridad corporativa, y ofrece tanto un procedimiento para establecerla, como un número de ejemplos de políticas relacionadas con los aspectos de seguridad. Esta información puede ser útil para desarrollar rápida, y efectivamente, nuevas políticas de seguridad. Se discute el papel del Equipo de Preparación de Emergencia de Computadora de los Estados Unidos (US-CERT) y del Departamento de Seguridad Nacional en la defensa contra el terrorismo cibernético.

- El Capítulo 4, "Privacidad", comienza con una viñeta acerca de la Agencia de Seguridad Nacional y su papel en la interceptación de señales de comunicación hechas a nombre del gobierno federal. Este capítulo explica cómo se deben implementar los derechos de privacidad que afectan a la TI, y discute varios conceptos clave de la legislación acerca del derecho a la privacidad, y cómo ha cambiado ésta a lo largo de los años. Se explican y se discuten la Cuarta Enmienda, así como las leyes diseñadas para proteger los registros financieros y médicos personales, incluyendo el derecho a la privacidad de los niños. Se cubre el tema de la vigilancia electrónica, junto con las leyes asociadas a esta actividad, incluyendo la Ley de Vigilancia de la Inteligencia Extranjera y la Ley de Unión y Fortalecimiento de los Estados Unidos mediante los Instrumentos Adecuados para Interceptar y Obstruir el Terrorismo (USA Patriot). Durante el capítulo se abarcan varias regulaciones que afectan la exportación de datos personales de un país a otro. En él, explicamos cómo se pueden utilizar los negocios de información personal- que emplean la TI- para obtener o mantener clientes (o monitorear empleados). También se discuten las preocupaciones de quienes abogan por el derecho a la privacidad, principalmente respecto a cuánta información debe ser almacenada, con quién puede ser compartida, cómo se almacena en primer lugar, y cómo se debe utilizar. Estas preocupaciones también se extienden a las prácticas de recolección de datos de los que aplican la ley, así como para el gobierno. Se identifican las violaciones y robo de información mediante distintas tácticas empleadas por ladrones de identidades. El capítulo también presenta algunas medias de seguridad que pueden impedir este tipo de robos. En él también discutimos el uso expandido del descubrimiento electrónico, el monitoreo del sitio de trabajo, la vigilancia por cámaras, así cómo la creación de perfiles del consumidor. Por último, se ofrecen lineamientos y principios para tratar de manera responsable los datos de los consumidores.

- El Capítulo 5, "Libertad de Expresión", trata los problemas que emergen gracias al uso creciente del Internet como un medio más para la Libertad de Expresión. En él, analizamos los tipos de dis-

curso protegidos por la Primera Enmienda de la Constitución de los Estados Unidos. El capítulo inicia con una discusión acerca de *Reputation Changer*, una compañía en línea que gestiona la reputación y ayuda a muchos negocios a manejar la información dañina potencial de las redes. Se discuten los distintos tipos de anonimato que facilitan la comunicación de los usuarios del Internet, y cómo es que estos tipos de anonimato representan un problema para las personas que podrían resultar afectadas adversamente por este intercambio comunicativo. Describe los intentos del uso de legislación (como la aplicación de la Ley de Decencia en Telecomunicaciones, la Ley de la Protección Infantil en las Redes, y la Ley de la Protección Infantil en Internet) y tecnología (como los filtros de internet), para controlar el acceso a contenido inapropiado del público infantil, o contenido innecesario en un ambiente de negocios. Se analiza la utilización del Pleito Estratégico contra la Participación Pública, así como las demandas John Doe para revelar las identidades de los comentadores anónimos. También cubrimos la difamación, el discurso de odio, pornografía en Internet y spam.

- El Capítulo 6, "Propiedad Intelectual", define la propiedad intelectual y explica los distintos niveles de protección de la propiedad que ofrecen los derechos de autor, las patentes y las leyes de secretos comerciales. La viñeta inicial discute el robo de valiosos secretos comerciales cometido por una compañía China agravando una firma estadunidense. Se discute la posibilidad de que el robo de secretos comerciales cometido por compañías chinas a compañías norteamericanas y europeas representa la "transferencia de riqueza más grande de la historia". A través de varios ejemplos analizamos las violaciones de derechos de autor, patente y marcas registras. Desarrollamos varias normas internacionales clave cuyo objetivo es la protección de la propiedad intelectual, algunos ejemplos incluyen: la Ley de Priorización de Recursos y Organización de la Propiedad Intelectual, el Acuerdo General sobre Aranceles Aduaneros y Comercio, el acuerdo de la Organización Mundial de Comercio sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio, el Tratado de la Organización Mundial de la Propiedad Intelectual, así como el Acta de Derechos de Autor Digitales del Milenio. El capítulo explica las patentes de software y el uso de los acuerdos de licencia cruzada. También trata los problemas clave de la propiedad intelectual, como: plagio, ingeniería reversa, códigos de fuente abierta, inteligencia competitiva, violación de marcas registradas y ciberocupación. También se analiza el uso de acuerdos de confidencialidad y cláusulas de no competencia en los contratos. Finalmente, el capítulo, cubre varios problemas clave relevantes para la ética de la TI, incluyendo el plagio, software de ingeniería reversa, los códigos de fuente abierta, la recolección de inteligencia competitiva y la ciberocupación.

- El Capítulo 7, "Desarrollo de Software", provee una discusión exhaustiva sobre el proceso de desarrollo de software y la importancia de mantenerlo como un producto de calidad. La viñeta de inicio ilustra la susceptibilidad de la bolsa de valores ante los problemas o errores de software. El capítulo destaca los problemas que los fabricantes de software deben considerar cuando decidan qué tan bien deben de desarrollar sus productos; particularmente cuando el software implica procesos de seguridad crítica y sus fallas podrían ocasionar la pérdida de vidas humanas. Los temas que incluye el resto de esta sección son: responsabilidad de productos de software, análisis de riesgos y enfoques sobre las pruebas de evaluación de calidad. El capítulo también analiza la Integración de Modelos de Madurez de Capacidades (CMMI por sus siglas en inglés), la familia de estándares ISO 9000, y el análisis modal de fallos y efectos (FMEA por sus siglas en inglés).

- El Capítulo 8, "El Impacto de la Tecnología de la Información sobre la Productividad y Calidad de Vida", analiza el efecto que las inversiones en TI han tenido sobre el estándar de vida y la productividad laboral alrededor del mundo. Se discute el incremento del uso del teletrabajo (también conocido como teleconmutación), junto con los pros y contras de este tipo de arreglo laboral. El

capítulo también analiza el concepto de brecha digital, y perfila algunos programas diseñados para eliminar este distanciamiento social. En esta sección se analiza el impacto de la TI en la transmisión del cuidado médico y costos de salud. Se discuten los beneficios y costos potenciales asociados a los registros médicos. Se definen los conceptos de tele salud y tele medicina, así como su papel en la transmisión del cuidado médico.

- El Capítulo 9, "Redes Sociales", analiza el uso de las redes sociales; Identifica el uso que hacen los negocios sobre éstas, y desarrolla los distintos problemas éticos asociados su uso. La viñeta inicial describe el papel de las redes sociales en la emergencia de muchos problemas de privacidad. Se cubren las aplicaciones de negocios de las redes sociales, incluyendo su uso en publicidad, marketing, proceso de contratación y mejora en la comunicación con el empleado y el servicio al cliente. Los problemas éticos asociados con las redes sociales incluyen bullying cibernético, ciber acoso, encuentros con depredadores sexuales y la carga de material inapropiado. Todos estos temas se discuten en el capítulo, así como las comunidades de vida virtual y los problemas éticos asociados con los mundos virtuales.
- El Capítulo 10, "Ética en las Organizaciones de Tecnología de la Información", cubre algunos de los problemas éticos que enfrentan las organizaciones de la TI, éstos incluyen aquellas dificultades asociadas con el uso no tradicional de empleados, como son empleados temporales, contratistas, empresas consultoras, empleados H-1B, y el uso de la subcontratación y la subcontratación externa. El Capítulo también discute los riesgos, protecciones y decisiones éticas relacionadas con las denuncias al interior de una firma, presenta un proceso para manejar de forma segura y efectiva una situación de este tipo. Además de introducir el concepto de cómputo verde, el capítulo analiza los problemas éticos que enfrentan, tanto los fabricantes de TI, como sus usuarios, cuando una compañía considera transformarse al cómputo verde y bajo qué costo lo hará. Explica la utilización de la Herramienta de Evaluación Ambiental de los Productos Electrónicos para comparar, evaluar y seleccionar los productos eléctricos basándose en un conjunto de 51 criterios ambientales. Finalmente, se examina el código de conducta de las industrias electrónicas y de información y comunicación de la tecnología, diseñadas para abordar problemas éticos en las áreas de seguridad y justicia laboral, responsabilidad ambiental y eficiencia de negocios.
- El Apéndice A incluye una discusión profunda sobre el desarrollo de la ética y la moral.
- El Apéndice B provee las respuestas de la sección de Auto Evaluación que se encuentra al final de cada capítulo.

## PEDAGOGÍA

Ética de la Tecnología de la Información, Quinta Edición, emplea una variedad de características pedagógicas que enriquecen la experiencia del aprendizaje, y promueven el interés de profesores y estudiantes.

- **Epígrafe** Cada capítulo comienza con una cita busca estimular el interés por el contenido del capítulo.
- **Viñeta** Al comienzo de cada capítulo, creamos un breve apartado que contiene un ejemplo del mundo real cuya función es ilustrar los problemas que serán discutidos en el resto del capítulo. Esto con el propósito de aumentar el interés del lector.
- **Preguntas a Considerar** Preguntas de enfoque cuidadosamente elaboradas. Le siguen a la viñeta con el objetivo de subrayar los temas que se analizarán a lo largo del capítulo.

- **Objetivos de Aprendizaje** Éstos aparecen al comienzo de cada capítulo. Se presentan a manera de preguntas que los estudiantes deben considerar al momento de realizar la lectura del capítulo.
- **Conceptos Clave** Aparecen en negritas a lo largo del texto, y se enlistan al final del capítulo. También se encuentran definidos en el glosario que se encuentra al final del libro.
- **Lista de control del gerente** Cada lista de control ofrece un listado de preguntas prácticas y útiles, que deberían ser consideradas cuando se toma una decisión de negocios.

### Material de Final del Capítulo

Material que ayuda a los estudiantes a retener conceptos clave y ampliar su comprensión sobre conceptos y relaciones importantes al interior de la TI. Las siguientes secciones se incluyen al final de cada capítulo:

- **Resumen.** Cada capítulo incluye una síntesis de los problemas clave que se trataron a lo largo de éste. Estos conceptos se relacionan con los Objetivos de Aprendizaje de cada capítulo.
- **Preguntas de Auto Evaluación.** Preguntas que ayudan a los estudiantes a revisar y probar su comprensión sobre conceptos clave. Las respuestas a estas preguntas se encuentran incluidas en el Apéndice B.
- **Preguntas para Discutir.** Preguntas abiertas que ayudan a los profesores a generar discusiones en clase. Buscan acercar al estudiante con los conceptos revisados, y los ayuda a explorar los numerosos aspectos de la ética en la TI.
- **¿Qué harías tu?.** Estos ejercicios presentan dilemas realistas que promueven el pensamiento crítico de los estudiantes sobre los principios éticos presentados en el texto.
- **Casos.** En cada capítulo, se emplean tres casos de la vida real para reforzar la importancia de los principios y conceptos de la ética de la TI, con estos casos se demuestra cómo es que las compañías manejan los problemas éticos. Las preguntas que **siguen** a cada caso enfocan a los estudiantes en los problemas clave y les demandan aplicar los conceptos que se presentaron en el capítulo. Un conjunto de casos de estudios adicionales, provenientes de las ediciones anteriores, se encontrarán disponibles en el sitio Web de Cengage con el objetivo de proveer al profesor de un material de casos más amplios a partir del cual pueda seleccionar los que más le convengan.

## SOBRE EL AUTOR

Con más de 30 años de experiencia gubernamental, institucional y en organizaciones comerciales de la TI, George W. Reynolds ha llevado una gran riqueza de experiencias sobre el cómputo y su industria a este proyecto. Ha sido autor de más de dos docenas de textos y ha enseñado en la University of Cincinnati, Xavier University (Ohio), Miami University (Ohio), y el College of Mount St. Joseph. Actualmente enseña en Strayer University.

### Herramientas de Enseñanza

Este libro cuenta con una serie de recursos para el profesor, los cuales están disponibles únicamente en inglés y sólo se proporcionan a los docentes que lo adopten como texto en sus cursos. Para mayor información, póngase en contacto con el área de servicio al cliente en las siguientes direcciones de correo electrónico:

- Cengage Learning México y Centroamérica clientes.mexicoca@cengage.com

- Cengage Learning Caribe clientes.caribe@cengage.com
- Cengage Learning Cono Sur clientes.conosur@cengage.com
- Cengage Learning Pacto Andino clientes.pactoandino@cengage.com

Al igual que los recursos impresos adicionales, las direcciones de los sitios web señaladas a lo largo del texto, y que se incluyen a modo de referencia, no son administradas por Cengage Learning Latinoamérica, por lo que ésta no es responsable de los cambios y actualizaciones de las mismas.

## AGRADECIMIENTOS

Me gustaría expresar mi aprecio a un cierto número de personas que ayudaron en la creación de este libro: Charles McCormick, Jr., Editor de Adquisiciones, por creer en mí y promover la terminación de este proyecto; Jennifer Feltri-George y Divya Divakaran, Gestoras de Contenido, por guiar este libro durante su producción; Kate Mason, Desarrollador de Contenido, por supervisar y dirigir este esfuerzo; Mary Pat Shaffer, Editor de Desarrollo, por todo su apoyo y útiles sugerencias y ediciones; Naomi Friedman, por escribir muchas de las viñetas y los casos; y a mis estudiantes, que me dieron excelentes ideas y consejos para construir el texto. También me gustaría agradecer a Clancy Martin por escribir el Apéndice A. Me gustaría agradecer al excelente conjunto de revisores que ofrecieron muchas sugerencias de gran utilidad:

Pat Artz, Bellevue University
Astrid Todd, Guilford Technical Community College
Charles Watkins, Baker College

Y por último, agradezco a mi familia por todo el apoyo que me brindaron para darme el tiempo de escribir este texto.

—George W. Reynolds

# 1 PANORAMA DE LA ÉTICA

**Epígrafe**

La integridad es hacer lo correcto, incluso cuando nadie te esté observando.

*–Anónimo*

## VIÑETA

**Presidente y directivo general de Cisco aboga por la conducta ética**

Cisco es una corporación multinacional de origen estadunidense que diseña, vende y manufactura equipo de redes. Las operaciones de la compañía generaron $46 billones en ventas y $8 billones en ingresos netos para el año fiscal del 2012[1]. Cisco ha sido galardonada con el premio "World's Most Ethical Company" (la "Compañía Más Ética del Mundo") otorgado por el Intitute Ethisphere. Cisco ha obtenido este

premio por cinco años consecutivos (2008-2012)[2]. Su Presidente y Director General, John Chambers declara: "Un compromiso fuerte con la ética es crítico para el éxito a largo plazo de nuestra compañía. El mensaje para cada empleado está claro: cualquier tipo de éxito que no sea alcanzado de manera ética, no será considerado como exitoso. En Cisco, conservamos los más altos estándares éticos, y no toleraremos nada que se encuentre debajo de éstos"[3].

Cisco realiza varios programas enfocados en cumplir sus metas de responsabilidad corporativa social. Por ejemplo, la compañía provee entrenamiento ético a sus 70,000 empleados, y se enorgullece de donarles suficientes beneficios a los empleados como para lograr adoptar un buen equilibrio entre vida y trabajo. A los empleados de Cisco se les recomienda donar dinero y hacer horas de voluntariado en organizaciones sin fines de lucro alrededor del mundo. Así mismo, Cisco administra la energía y la emisión de los gases con efecto invernadero generada por sus operaciones.

La compañía exige a sus más de 600 proveedores, los mismos estándares de calidad respecto a la ética, prácticas laborales, salud y seguridad, así como respecto al medio ambiente. Comunica su Código de Conducta a proveedores, monitorea su cumplimiento, y ayuda a mejorar su rendimiento. Cisco colabora con grupos industriales para elevar los estándares y construir capacidades sustentables a lo largo de su cadena de proveedores. La compañía utiliza sus mayores áreas de experiencia en la tecnología de redes para mejorar tanto la entrega, como la calidad de la educación y el cuidado médico. También interviene para ayudar a cumplir necesidades humanas críticas en tiempos de desastre al proveer acceso a alimentos, agua potable, refugios y otras formas de ayuda. Por ejemplo, en el 2012, los empleados de Cisco donaron $1.25 millones de dólares y 12,500 horas de voluntarios al Programa Global de Alivio del Hambre. Tanto el Presidente de Cisco, como su Directivo Emérito, John Morgridge, igualaron las donaciones de sus empleados, triplicando la donación potencial[4].

### Preguntas a Considerar

1. ¿Qué significa que un individuo actúa de manera ética? ¿Qué significa que una organización actúe de manera ética?
2. 2 ¿Cómo debería equilibrar sus recursos una organización al perseguir su supervivencia y a la vez perseguir el cumplimiento de sus metas de responsabilidad social?

## OBJETIVOS DE APRENDIZAJE

**Conforme leas este capítulo, considera las siguientes preguntas:**

1. ¿Qué es la ética, y por qué es importante actuar de acuerdo a un código ético?

2. ¿Por qué cada vez es más importante la ética de negocios?
3. ¿Qué están haciendo las organizaciones para mejorar su ética de negocios?
4. ¿Qué es la responsabilidad social corporativa?
5. ¿Por qué las organizaciones se interesan en adoptar una buena ética de negocios y una responsabilidad social corporativa?
6. ¿Qué enfoque puedes tomar para asegurar una toma de decisiones éticas?
7. ¿Qué tendencias han incrementado el riesgo del uso de la tecnología de la información de manera no ética?

## ¿QUÉ ES LA ÉTICA?

Cada sociedad crea un conjunto de reglas para establecer los límites de una conducta generalmente aceptada. Estas reglas normalmente son expresadas en declaraciones sobre cómo debe comportarse la gente, y las reglas individuales, en su conjunto, forman el código moral bajo el cual se rige una sociedad. Desafortunadamente, las reglas suelen tener contradicciones, y muchas veces las personas no están seguras de cuál regla deben seguir. Por ejemplo, si tú observas que un amigo copia la respuesta de un examen, es probable que te encuentres en un dilema entre mostrar lealtad a tu amigo o tener el valor de decir la verdad. En algunas ocasiones las reglas no parecen abarcar situaciones nuevas, así que los individuos deben determinar cómo aplicar las reglas existentes o desarrollar nuevas. Puede ser que tú apoyes fuertemente la privacidad personal, pero, ¿crees que a una organización debe prohibírsele monitorear el uso del correo electrónico e Internet de sus empleados?

El término moralidad se refiere a las convenciones sociales sobre lo correcto y lo incorrecto. Nociones tan ampliamente compartidas que se convierten en la base de un consenso establecido. Sin embargo, los puntos de vista individuales sobre qué es una conducta moral, pueden variar por edad, grupo cultural, etnia, religión, experiencia de vida, educación y género. Existe un acuerdo ampliamente aceptado sobre la inmoralidad del asesinato, robo o la provocación de incendios; pero algunas conductas aceptadas por una sociedad pueden ser inaceptables para otra. Incluso en la misma sociedad los individuos pueden tener fuertes desacuerdos sobre problemas morales importantes. En los Estados Unidos, por ejemplo, los problemas sobre el aborto, investigación de células madre, pena de muerte y el control de armas se debaten constantemente, y las personas de ambos lados del debate sienten que sus razones tienen una base moral sólida.

### Definición de ética

La ética es el conjunto de creencias que tiene una sociedad sobre el conducirse de una buena o mala manera. La conducta ética se confirma de las normas generalmente aceptadas, muchas de las cuales son casi universales. Sin embargo, aunque casi cualquier

persona podría estar de acuerdo en que cierto tipo de conductas —como mentir o engañar— son conductas no éticas, las opiniones sobre lo que constituye una conducta ética pueden variar dramáticamente. Por ejemplo, las actitudes hacia la piratería de software —una forma de violación de los derechos de autor que implica la creación de copias de software o el permitir que otros tengan acceso al software sobre el que no tienen derechos o licencia— varían desde una oposición fuerte, hasta a la aceptación de la práctica como un enfoque estándar para conducir negocios. En el 2011, un estimado de 43 por ciento de todos los softwares de computadoras personales que se encontraban en circulación fue declarado como pirata, con un valor comercial de $63 billones (dólares americanos)5. Zimbabwe (92%), Georgia (91%), Bangladesh (90%), Libia (90%), y Moldavia (90%) son, consistentemente, los países con las tasas de piratería más altas. Los Estados Unidos (19%), Luxemburgo (20%), Japón (21%), y Nueva Zelandia (22%), se encuentran entre los países con tasas de piratería más bajas[6].

Conforme los niños crecen, aprenden tareas complicadas —como caminar, hablar, nadar, andar en bicicleta o escribir el alfabeto— que llevarán a cabo como un hábito por el resto de sus vidas. Las personas también desarrollan hábitos que les hacen más fácil escoger lo que una sociedad considera bueno o malo. Una virtud es un hábito que inclina a las personas a hacer lo que es aceptable, un vicio, en cambio, es un hábito considerado como una conducta inaceptable. Justicia, generosidad y lealtad son ejemplos de virtudes, mientras que la vanidad, ambición, envidia y la ira se consideran vicios. Las virtudes y vicios de las personas ayudan a definir su sistema de valores personales, el complejo escenario de valores morales que rigen sus vidas.

## La importancia de la integridad

Tus principios morales son proposiciones sobre lo que crees que rige la conducta adecuada. Cuando eras niño, tal vez te enseñaron a no mentir, engañar o robar. Como adulto que enfrenta decisiones más complejas, generalmente reflexionas sobre tus principios cuando consideras qué hacer en distintas situaciones: ¿Es correcto mentir para proteger los sentimientos de otra persona? ¿Deberías intervenir a un compañero de trabajo que parece tener una dependencia a sustancias químicas? ¿Es aceptable exagerar tu experiencia laboral en un currículo? ¿Podrías omitir procedimientos en un proyecto sólo para cumplir con el plazo de entrega?

Una persona que actúa con integridad, actúa de acuerdo a un código de principios personales. Un criterio para actuar con integridad —una de las piedras angulares de la conducta ética— es extender a todas las personas el mismo respeto y consideración que tú mismo esperas recibir de los otros. Desafortunadamente, la consistencia es una meta difícil de lograr, particularmente cuando te encuentras en una situación que conflictúa tus estándares de moralidad. Por ejemplo, podrías creer que es importante hacer lo que tu empleador exige de ti, y al mismo tiempo creer que deberías ser remunerado justamente por tu trabajo. Por lo tanto, si tu empleador insiste en que, debido a restricciones presupuestarias, no debes reportar las horas extras que has trabajado, surgiría un conflicto moral. Puedes hacer lo que tu jefe te exige o puedes insistir en ser recompensado justamente, pero no puedes elegir ambas. En esta situación, es probable que te veas forzado a comprometer alguno de tus principios y actuar con una aparente falta de integridad.

Otra forma de inconsistencia emerge si aplicas tus estándares morales de manera diferente de acuerdo a la situación o a las personas involucradas. Si eres consistente y actúas con integridad, aplicarías los mismos estándares morales a todas las situaciones. Por ejemplo, tú podrías considerar que es moralmente aceptable decir una pequeña mentira blanca para ahorrarle un poco de dolor o vergüenza a un amigo, pero, ¿le mentirías a un

compañero de trabajo o a un cliente sobre un problema de negocios solo para evitar fricciones? Claramente, muchos dilemas éticos no son tan simples como pensar en el bien contra el mal, sino que involucran elecciones entre un tipo de bien contra otro tipo de bienestar. A manera de ejemplo, para algunas personas es "correcto" proteger la vida silvestre de Alaska, y también es "correcto" encontrar nuevas fuentes de petróleo para mantener las reservas de Estados Unidos, pero, ¿cómo equilibraríamos ambas preocupaciones?

### Diferencia entre moral, ética y ley

La **moral** son las creencias personales sobre el bien y el mal, mientras que el término ética, describe los estándares o códigos de conducta que un cierto grupo (nación, organización, profesión) espera de un individuo que pertenece a dicho grupo. Por ejemplo, la ética de la profesión legislativa exige que los abogados defensores defiendan a un cliente acusado con la mejor de sus capacidades, incluso si saben que el cliente es culpable del crimen más censurable y moralmente objetable que uno pueda imaginar.

La **ley** es un sistema de reglas que nos dicen lo que podemos y no podemos hacer. Las leyes son aplicadas por un conjunto de instituciones (policía, cortes y cuerpos legislativos). Los actos legales son actos que se conforman con lo estipulado por la ley. Los actos morales se conforman con lo que un individuo considera como lo que debe de hacerse. Las leyes pueden proclamar un acto como legal, aunque muchas personas puedan considerar el acto como inmoral, por ejemplo, el aborto.

El resto de este capítulo provee una introducción a la ética en el mundo de los negocios. Discute la importancia de la ética en los negocios, describe lo que los negocios pueden hacer para mejorar su ética, provee consejos para crear un ambiente laboral ético, y sugiere un modelo ético para la toma de decisiones. El capítulo concluye con una discusión sobre la ética y su relación con las Tecnologías de la Información (TI).

## ÉTICA EN EL MUNDO DE LOS NEGOCIOS

La ética ha logrado encabezar la agenda de los negocios debido a que los riesgos asociados con una conducta inapropiada han incrementado, tanto en probabilidad como en un impacto que podría resultar potencialmente negativo. En la década anterior hemos observado el colapso y el rescate de instituciones financieras como el Banco de América, CitiGroup, Countrywide Financial, Fannie Mae, Freddie Mac, Lehman Brothers, y American International Group (AIG) , todos ocasionados por decisiones imprudentes o poco éticas respecto a la aprobación de hipotecas, préstamos y líneas de crédito a individuos u organizaciones descalificadas. También hemos atestiguado el encarcelamiento de varios ejecutivos o directivos generales sentenciados a prisión por cargos relacionados con comportamientos poco éticos, incluyendo al ex-inversionista Bernard Madoff, quien estafó a sus clientes con un estimado de $65 billones de dólares[7]. Claramente, el comportamiento poco ético ha provocado consecuencias negativas de seriedad que han llegado a tener impacto mundial.

Varias tendencias han incrementado la probabilidad de un comportamiento poco ético. En primer lugar, para muchas organizaciones, el aumento de la globalización ha creado un ambiente laboral mucho más complejo, ambiente que abarca diversas culturas y sociedades, haciendo cada vez más difícil aplicar los principios y códigos éticos de manera consistente. Por ejemplo, varias compañías estadunidenses han movido sus operaciones a países en desarrollo, en donde los empleados trabajan en condiciones que serían inaceptables en partes más desarrolladas del mundo.

En segundo lugar, en la difícil y poco predecible economía de hoy en día, las organizaciones se ven desafiadas diariamente para mantener sus ingresos y ganancias. Algunas organizaciones están tentadas a recurrir a conductas poco éticas para seguir generando ganancias. Por ejemplo, el Presidente de la compañía de subcontratación Satyam Computer Services, con base en la India, admitió haber sobrevaluado el capital de la compañía por más de $1 billón de dólares. La revelación de este secreto representó el escándalo corporativo más grande de la India, ocasionando que el gobierno tomara acción para proteger los trabajos de los 53,000 empleados de la compañía[8].

Empleados, accionistas, y agencias de regulación son, cada día, más susceptibles a violaciones de estándares de contabilidad, fallas en la comunicación de cambios sustanciales en las condiciones empresariales, inconformidad con las prácticas sanitarias y de seguridad, y la producción de productos inseguros o que se encuentren por debajo del estándar. Una vigilancia tan enaltecida eleva el riesgo de pérdidas financieras para los negocios que no adoptan prácticas éticas o que inician prácticas por debajo de los estándares requeridos. También existe el riesgo de las demandas criminales o civiles que resultan en multas o la encarcelación de individuos.

Une ejemplo clásico de los múltiples riesgos de la toma poco ética de decisiones es el caso del escándalo financiero de Enron. En el 2000, Enron empleó a cerca de 22,000 personas y obtuvo una ganancia anual de $101 billones de dólares. Durante el 2001, se reveló que gran parte de los ingresos de Enron fueron el resultado de tratos con asociaciones limitadas, que la misma empresa controlaba. Además, como resultado de una contabilidad defectuosa, gran parte de las deudas y pérdidas de Enron no fueron reportadas en sus estados financieros. Conforme se reveló el escándalo financiero, las acciones de Enron cayeron de $90 dólares por acción a menos de $1 dólar por acción, y la compañía se vio forzada a declararse en bancarrota[9]. El caso de Enron fue notorio, pero han ocurrido muchos otros escándalos corporativos a pesar de las medidas de seguridad que surgieron como resultado del debacle de Enron. A continuación mostramos algunos ejemplos de fallas en la ética empresarial cometidas por empleados de organizaciones de la TI:

- En el 2011, IBM acordó pagar $10 millones de dólares para conciliar los cargos civiles que surgieron de una demanda hecha por la Comisión de la Bolsa de Valores (SEC) alegando que la firma había violado la Ley de Prácticas Extranjeras Corruptas al sobornar a funcionarios del gobierno en China y Corea del Sur para asegurar la venta de productos de IBM. (La Ley hace ilegal que las corporaciones enlistadas en la bolsa de valores de los Estados Unidos sobornen a funcionarios extranjeros). Supuestamente, los sobornos ocurrieron durante una década e incluyeron cientos de miles de dólares en efectivo, electrónicos y gastos de entretenimiento y viajes a cambio de millones de dólares en contratos de gobierno[10].
- Los fundadores de las tres compañías de póquer por Internet más grandes del mundo, fueron acusadas de utilizar métodos fraudulentos para esquivar las leyes estadunidense contra las apuestas, obteniendo billones de dólares de residentes de este país que apostaban en su sitio[11].
- La Office of the Comptroller of the Currency (OCC), que supervisa a los grandes bancos de Estados Unidos, acusó a Citibank en el 2012, de fallar con el cumplimiento de las reglas que aplicaban a la Ley de Secreto Bancario. Esta ley fue diseñada para detectar e impedir el lavado de dinero, el financiamiento terrorista y otros actos criminales. Citibank no admitió ni denegó las acusaciones, pero la

compañía accedió a proveer a la OCC con un plan que delineara cómo llevaría a cabo un programa para el cumplimiento de estas observaciones[12].

No es raro que los individuos altamente exitosos y poderosos actúen de maneras poco morales, como bien hemos visto en estos ejemplos. Este tipo de personas actúan de manera agresiva para obtener lo que quieren y están acostumbrados a tener acceso a información privilegiada, contactos y otros recursos. Incluso su éxito hace que con frecuencia incremente su creencia de que tienen la habilidad y el derecho a manipular los resultados de cualquier situación. La corrupción moral de las personas en el poder, que con frecuencia es facilitada por una tendencia de las personas a hacerse de la vista gorda cuando sus líderes actúan de manera inapropiada, ha sido denominada **síndrome de Bathsheba**, referente a la historia bíblica del Rey David, que se corrompió por todo el poder y éxito que tuvo[13]. De acuerdo a la historia, David se obsesionó con Bathsheba, la esposa de uno de sus generales y eventualmente, ordenó que su esposo fuera en una misión que implicaba una muerte certera, de forma que él pudiera casarse con Bathsheba.

Incluso los empleados con un nivel más bajo pueden verse involucrados en dilemas éticos. A continuación, ilustramos las situaciones con algunos ejemplos:

- A un empleado de bajo nivel del Departamento de Servicios Técnicos de Distrito de Monroe, Florida, se le confió la responsabilidad de la adquisición y distribución de los teléfonos celulares del distrito. Pocos meses después de su jubilación, la empleada fue acusada de robar 52 iPhones y iPads con el dinero del gobierno para después venderlos a amigos y colegas de trabajo[14].
- El Soldado de Primera Clase, Bradley Manning, es el presunto responsable de la liberación de miles de informes confidenciales de la embajada de Estados Unidos, incidente que llegó a ser conocido como Cablegate. Este incidente provocó que muchas personas se cuestionaran seriamente sobre la seguridad del Departamento de Defensa, y condujo a la creación de muchos cambios en el manejo de la inteligencia y otra información clasificada en varias [falta palabra] y departamentos de inteligencia de los Estados Unidos[15].
- De acuerdo a CyberSource Corporation (subsidiaria de Visa Inc., que ofrece manejo de servicios de pagos en negocios electrónicos), las ganancias en línea que se pierden por fraude incrementaron en un 26 por ciento del 2010 al 2011, alcanzando la cantidad de $3.4 billones de dólares en pérdidas. Esto representa 1 por ciento de los $340 billones obtenidos por ventas en negocios electrónicos en los Estados Unidos y Canadá[16].

Esta es sólo una pequeña muestra de los incidentes que han conducido a un incremento en la atención sobre la ética corporativa al interior de muchas organizaciones de la TI. La ***Tabla 1-1*** identifica los tipos de falta de conducta más comunes observados en los sitios laborales.

### Responsabilidad Social Corporativa

La **Responsabilidad Social Corporativa** (CSR por sus siglas en inglés) es el concepto que establece que una organización debe actuar de manera ética al asumir la responsabilidad del impacto de sus acciones sobre el medio ambiente, la comunidad y el bienestar de sus empleados. Fijar metas de CSR promueve que una organización alcance estándares éticos y morales más altos. Como destacamos en la viñeta de apertura, Cisco es un

**Tabla 1-1**
Formas comunes de falta de conducta en los empleados

**Fuente:** Ethics Resource Center, "2011 National Business Ethics Survey: Workplace Ethics in Transition," © 2011, www.ethics.org/nbes/files/FinalNBES-web.pdf.

| Tipo de falta de conducta | Porcentaje de empleados encuestados que observan este comportamiento |
|---|---|
| Uso indebido del tiempo de la compañía | 33% |
| Conducta abusiva | 21% |
| Mentir a los empleados | 20% |
| Abuso de los recursos de la compañía | 20% |
| Violación de las políticas de Internet de la compañía | 16% |
| Discriminación | 15% |
| Conflictos de interés | 15% |
| Uso inapropiado de las redes sociales | 14% |
| Violaciones de seguridad o sanitarias | 13% |
| Mentir a los accionistas externos | 12% |
| Robo | 12% |
| Falsificación de reportes de horas de trabajo | 12% |

ejemplo de una organización que se ha fijado, y alcanzado, un número de metas de CSR para sí mismo, y como resultado, ha sido reconocido como una compañía altamente ética.

La **cadena de abastecimiento sustentable** es un componente de la CSR que se enfoca en el desarrollo y mantenimiento de una cadena de abastecimiento que cumple con las necesidades del presente sin comprometer la capacidad de que las generaciones futuras realicen sus necesidades. La cadena de abastecimiento sustentable toma en cuenta problemáticas como las prácticas laborales justas, la conservación de energía y recursos, derechos humanos y la responsabilidad comunitaria. Muchos fabricantes de equipo de la TI han hecho de la cadena de abastecimiento sustentable una prioridad, en parte, debido a que se deben de adherir a las distintas directivas y regulaciones que propone la Unión Europea (incluyendo la Restricción de Sustancias Peligrosas en Aparatos Eléctricos y Electrónicos, y la Regulación de Registro, Evaluación, Autorización y Restricción de Químicos (REACH) para que se les permita vender sus productos en países que pertenecen a la Unión Europea. En muchos casos, cumplir con la cadena de abastecimiento sustentable puede conducir a aminorar los costos de producción. Por ejemplo, desde el 2001, Intel ha invertido cerca de $45 millones de dólares en esfuerzos para reducir sus costos energéticos. Como resultado de dicha iniciativa, la compañía ha ahorrado, en promedio, $23 millones de dólares por año[17].

Cada organización debe decidir si la CSR es una prioridad, y de determinarlo así, debe especificar sus metas de CSR. La persecución de algunas metas de la CSR puede conducir al incremento en ganancias, facilitando que los directivos y accionistas de las organizaciones apoyen las metas en esta área. Por ejemplo, muchas cadenas de comida rápida (incluyendo a McDonald's, Wendy's y Burger King) han ampliado sus menús para incluir ofertas bajas en grasa, en un intento por cumplir una meta de CSR de proveer elecciones saludables a sus clientes, mientras se intenta capturar a un mercado más amplio[18].

Sin embargo, si la búsqueda por conseguir una meta específica de la CSR conduce a una disminución en las ganancias, los directivos se pueden ver desafiados para modificar o hacer a un lado la meta que originalmente buscaban. Por ejemplo, algunos fabricantes de automóviles en los Estados Unidos han introducido autos que se mueven gracias a

energía eléctrica renovable, esto como parte de una meta de responsabilidad social corporativa que ayuda a aminorar la dependencia de los Estados Unidos a recursos como el petróleo. No obstante, los ciudadanos estadunidenses se han tardado en adoptar los autos eléctricos, y los fabricantes han tenido que ofrecer financiamientos con tasas de intereses bajas, descuentos por pagos en efectivo, bonos de venta o el subsidio de arrendamientos para lograr que los autos salgan del piso de ventas. Fabricantes y vendedores luchan para generar un incremento en las ganancias de la venta de autos eléctricos, y los directivos de las compañías automotrices deben considerar qué tanto tiempo deben invertir en continuar con esta estrategia.

## ¿Por qué es importante adoptar una buena ética y responsabilidad social corporativa?

Las organizaciones tienen al menos cinco buenas razones para perseguir sus metas de CSR y promover un ambiente laboral en donde los empleados sean motivados para actuar éticamente cuando tomen decisiones de negocios:

- Ganar buena voluntad de la comunidad
- Crear una organización que opera de forma consistente
- Adoptar buenas prácticas de negocios
- Evitar publicidad desfavorable

A continuación, mostramos algunos ejemplos de fallas en la ética empresarial cometidas por empleados de organizaciones de TI:

#### Ganar el visto bueno de la comunidad

Aunque las organizaciones existen principalmente para ganar ingresos o proveer servicios a sus clientes, también tienen algunas responsabilidades fundamentales con la sociedad. Como discutimos en la sección anterior, las compañías suelen declarar estas responsabilidades en metas específicas de su CSR. Las compañías también pueden emitir una declaración formal de sus valores, principios o creencias. Observa la ***Figura 1-1*** para analizar un ejemplo de una declaración de valores.

**Nuestros valores**
Como compañía y como individuos, nosotros valoramos la integridad, honestidad, excelencia personal, la auto-crítica constructiva, el desarrollo continuo y el respeto mutuo. Estamos comprometidos con nuestros clientes y socios, y tenemos una gran pasión por la tecnología. Nos gustan los grandes desafíos y nos enorgullecemos cuando vemos que podemos sobrepasarlos con éxito. Nos asumimos responsables ante nuestros clientes, accionistas, socios y empleados al honrar nuestros compromisos, proveer resultados y seguir luchando por obtener la calidad más alta.

**Figura 1-1**
Declaración de valores de Microsoft

**Crédito:** Microsoft Statement of Values, "Our Values," tomado de www.microsoft.com. Reimpreso bajo permiso.

Todas las organizaciones exitosas, incluyendo las compañías de tecnología, reconocen que deben atraer y mantener clientes leales. La filantropía es una manera bajo la que una organización puede demostrar sus valores y ponerlos en acción al crear conexiones positivas con sus accionistas. (Un **accionista** es una persona que gana o pierde dinero en acciones dependiendo de la resolución de una situación dada). Como resultado, mu-

chas organizaciones inician o apoyan actividades de responsabilidad social, que pueden incluir hacer contribuciones a organizaciones caritativas, instituciones sin fines de lucro, proveer beneficios para los empleados superiores a lo estipulado por la legislación, y abocar recursos organizacionales a iniciativas que son socialmente más deseables que redituables. La ***Tabla 1-2*** provee algunos ejemplos de actividades CSR apoyadas por organizaciones de TI.

La buena voluntad que las actividades CSR generan, pueden facilitar que las corporaciones conduzcan a salvo sus negocios. Por ejemplo, una compañía conocida por tratar bien a sus empleados tendrá más éxito en competir por los mejores candidatos a un puesto de trabajo. Por otro lado, las compañías que tiene una mala reputación en la comunidad pueden sufrir desventajas. Por ejemplo, una corporación que contamina el ambiente puede encontrar que la mala publicidad reduce las ventas, impide las relaciones con algunos socios de negocio y atrae atención negativa por parte del gobierno.

#### Crear una organización que opera de forma consistente

Las organizaciones desarrollan y mantienen sus valores para crear una cultura corporativa y definir un enfoque consistente para aproximarse a las necesidades de sus accionistas-inversionistas, empleados, clientes, proveedores y la comunidad. Dicha consistencia asegura que los empleados sepan lo que se espera de ellos y puedan emplear los valores de la organización. para ayudarlos en la toma de decisiones. La consistencia también significa que los accionistas, clientes, proveedores y la comunidad sepan lo que pueden esperar de la organización, que en el futuro se comportará como lo ha hecho en el pasado. Es especialmente importante para las organizaciones multinacionales o globales presentar una cara consistente a sus accionistas, clientes y proveedores sin importar en donde vivan éstos o en donde se lleven a cabo las operaciones de negocios. Aunque los sistemas de valores de cada compañía son diferentes, muchas comparten los siguientes:

- Operar con honestidad e integridad, manteniéndose fieles a los principios organizacionales.
- Operar de acuerdo a los estándares de conducta ética, tanto en palabra como en acción.

| Organización | Ejemplo de actividad socialmente responsable |
|---|---|
| Dell Inc. | Su iniciativa "Powering the Positive" incluye programas como Children's Cancer Care, Youth Learning, Disaster Relief y Social Entrepreneurship[19]. |
| Google | Recientemente, Google invirtió $250 millones de dólares en proyectos de energía eléctrica y solar[20]. |
| IBM | Los empleados de IBM donaron 3.2 millones de horas de servicio comunitario en 120 países en el 2011[21]. |
| Oracle | Oracle apoya las instituciones K–12 con becas de educación tecnología y programas que alcanzan 1.5 millones de estudiantes cada año[22]. |
| SAP, North America | SAP apoya muchas iniciativas de responsabilidad corporativa cuyo objetivo es mejorar la educación, también dona regalías de empleados a agencias y escuelas sin fines de lucro y promueve y apoya el voluntariado de sus empleados[23]. |
| Microsoft | Microsoft lleva a cabo una campaña anual de donación, y sus empleados han contribuido con cerca de $1 billón de dólares donado a 31,000 organizaciones sin fines de lucro alrededor del mundo desde 1983[24] |

**Tabla 1-2**
Ejemplos de actividades socialmente responsables de organizaciones de la TI

**Fuente:** Derecho Reservado © Cengage Learning. Adaptado de múltiples fuentes. Ver Notas Finales 19, 20, 21, 22, 23, 24.

# DELITOS INFORMÁTICOS

**Epígrafe**

El criminal más peligroso es el hombre dotado de razones, pero sin sentido de la moralidad.

*–Martin Luther King, Jr.*

## VIÑETA

**Los ataques de Ramsomware de Reveton**

En agosto de 2012, el Centro de Quejas de Delitos Informáticos (IC3), asociación entre el FBI y el Centro Nacional de Delitos de Cuello Blanco, fue inundado de reportes de un nuevo tipo de crímenes cibernéticos. Todas las víctimas a lo largo de los Estados Unidos reportaron que mientras se encontraban navegando en Internet, sus computadoras se bloquearon, y recibieron el siguiente mensaje que supuestamente pro–

venía del FBI: "Este sistema operativo se encuentra bloqueado debido a violaciones de las leyes federales de los Estados Unidos (Artículo 1, Sección 8, Cláusula 8; Artículo 202, Articulo 210 del Código Penal de Estados Unidos que prevé una pena de privación de la libertad de cuatro a doce años)". El mensaje continuaba acusando a la víctima de visitar sitios pornográficos o distribuir contenido protegido por derechos de autor. Se les dijo a las víctimas que podían desbloquear sus computadoras después de pagar una multa de $200 dólares en las próximas 72 horas después de la recepción del mensaje. El mensaje estaba repleto del logo oficial del FBI[1].

El incidente señaló el comienzo de un aumento en los ataques de ransomware. El **Ransomware** es un tipo de malware que deshabilita una computadora o Smartphone hasta que la víctima paga una multa, así que es un tipo de secuestro. A diferencia de otros virus, la Versión Reveton de ransomware no se activa al abrir un archivo o un archivo adjunto. Más bien se trata de un malware "de conducción por descarga", es decir, virus que se descargan de manera automática en el momento en el que el usuario visita un sitio web infectado[2].

De manera inmediata, el FBI emitió una alerta, pero en menos de un mes, los expertos en ciberseguridad ya habían identificado 16 variantes de ransomware. Los virus habían infectado 68 000 direcciones de IP únicas. Se estima que en un día promedio, cerca de 170 víctimas habían pagado la multa de $200 dólares y habían recibido códigos de desbloqueo falsos[3]. Las computadoras comprometidas no se podían arreglar a través de la instalación o actualización de un software antiviral, pues se encontraban bloqueadas. Debido a que muchos propietarios de PCs para el hogar no están acostumbrados a respaldar sus sistemas de manera regular, muchas víctimas tuvieron que enfrentar la pérdida de sus datos. La cuota de $200 dólares era lo suficientemente baja como para motivar su pago. Una visita a un servicio profesional de TI para reparar el daño podría costar el mismo tiempo y más dinero para resolver el problema. Un pago rápido a través de un sistema de tarjetas prepagadas, como MoneyPak, podría ahorrarle a las víctimas muchas molestias.

Estados Unidos no fue el primer país en ser golpeado por estos ataques. A principios de 2012, varias bandas de delincuentes atacaron Francia, Alemania y el Reino Unido. Los ataques de ransomware surgieron por primera vez en Rusia en el 2009. Desde entonces, se han esparcido a casi cualquier país del mundo, golpeando con frecuencia los sistemas de Estados Unidos y Japón. Symantec, una compañía de seguridad de TI, estima que estas bandas extorsionan cerca de $5 millones de dólares a sus víctimas en línea[4]. El aumento en los ataques de ransomware se debe, sin duda, a su gran éxito. En Francia, por ejemplo, casi 4 por ciento de las víctimas pagaron las extorsiones durante los fraudes monetarios realizados por virus de un tipo distinto a Reveton[5].

El ransomware Reveton se descarga mediante el popular kit de herramientas de malware en lengua rusa, denominado Citadel. La última versión de Citadel también puede obtener contraseñas a partir de

los buscadores de Internet y cambiar los sitios web para engañar a los usuarios y que éstos les provean su información de acceso[6].

En diciembre de 2012, el Reino Unido arrestó a tres personas que parecían estar involucradas en los ataques del ransomware Reveton[7]. Sin embargo, encontrar a los perpetradores, es inusual y no siempre es la mejor manera para combatir este crimen. Las agencias de aplicación de la ley, así como las compañías de seguridad, le han recomendado al público tomar medidas preventivas para evitar ser víctimas de este tipo de ataques. El tipo de medidas preventivas que pueden tomar los usuarios es mantener actualizado softwares como Java, Acrobat Reader, Adobe Flash, Windows, así como el explorador de Internet de preferencia. Uno de los primeros ataques de ransomware Reveton utilizó una vulnerabilidad de una versión de Java que había sido actualizada el mes anterior[8]. Los usuarios de computadoras también pueden evitar infecciones al emplear software de seguridad que identifique sitios web sospechosos, y evitando hacer clic en los anuncios en línea de compañías que se vean sospechosas[9]. No obstante, tal vez la mejor manera de evitar el esparcimiento de estos ataques, es promover que las víctimas reporten el crimen y se rehúsen a cumplir con las demandas de los delincuentes.

### Preguntas a Considerar

1. ¿Por qué están incrementando los ataques de ransomware?
2. ¿Qué puedes hacer para prevenir este tipo de ataques en tu computadora?
3. ¿Cómo crees que las víctimas deberían responder a los ataques de ransomware? ¿Tienen una obligación ética hacia las futuras víctimas?

### Objetivos de aprendizaje

**Conforme leas este capítulo, considera las siguientes preguntas:**

1. ¿Qué compensaciones y problemas éticos se encuentran asociados con la protección de los datos y sistemas de información?
2. ¿Por qué ha surgido un incremento dramático en el número de incidentes relacionados con la seguridad informática en los últimos años?
3. ¿Cuáles son los tipos más comunes de ataques de seguridad informáticos?
4. ¿Quiénes son los principales perpetradores de crímenes informáticos, y cuáles son sus objetivos?
5. ¿Cuáles son los elementos clave de un proceso multilateral para manejar las vulnerabilidades de seguridad basándose en el concepto de garantías razonables?

6. ¿Qué acciones se deben llevar a cabo en respuesta a un incidente de seguridad?
7. ¿Qué es el cómputo forense, y qué papel juega en la respuesta a los incidentes cibernéticos?

## INCIDENTES DE SEGURIDAD EN LAS TI: UN GRAN PROBLEMA

La seguridad de las tecnologías de la información empleada en los negocios es de mayor importancia. Se debe proteger la información confidencial de las empresas, así como la información privada de los clientes y empleados. Los sistemas deben ser protegidos contra actos malintencionados de robo o alteración. Aunque la necesidad de un sistema de seguridad es obvia, con frecuencia debe ser balanceada contra otras necesidades del negocio. Los gerentes empresariales, profesionales de TI y usuarios de las TI enfrentan varias decisiones éticas respecto a la seguridad de las TI, algunos ejemplos son los siguientes:

- ¿Si una firma es víctima de un delito informático, debería seguir el procesamiento de los criminales a todo costo, mantener un perfil bajo y evitar publicidad negativa, informar a los clientes afectados, o tomar algún tipo de acción?
- ¿Cuánto dinero y esfuerzo se debe gastar para protegerse contra los delitos informáticos? (En otras palabras, ¿qué tan seguro es estar lo suficientemente seguro?)
- Si una compañía se da cuenta de que ha producido un software con defectos que posibilitan el ataque de hackers a los datos de sus clientes o sus empleados, ¿qué acciones debería tomar?
- ¿Qué debería hacerse si las protecciones de seguridad recomendadas dificultan la conducción de negocios entre clientes y empleados, resultando en pérdidas de ventas y un incremento en los costos?

La ***Tabla 3-1*** muestra la ocurrencia de incidentes de seguridad cibernética en 149 organizaciones estadounidenses que respondieron a la Encuesta de Seguridad y Delitos Informáticos 2010/2011.

### ¿Por qué prevalecen los incidentes informáticos?

En el ambiente informático actual, mismo que incrementa en complejidad, en expectativas por parte de los usuarios, que posee sistemas que cambian y se expanden constantemente, y en el cual aumenta la dependencia al software con vulnerabilidades conocidas, no debe sorprendernos que se incrementen de manera dramática el número, variedad y el impacto de los distintos incidentes de seguridad. Los incidentes de seguridad cibernéticos ocurren alrededor de todo el mundo. Los equipos de cómputo personales de los

| Tipo de incidente | Porcentaje de organizaciones que experimentan este tipo de incidente | | |
|---|---|---|---|
| | 2008 | 2009 | 2010 |
| Infección de malware | 50% | 64% | 67% |
| Ser representados de manera fraudulenta como los emisores de mensajes de correo electrónico que solicitan información personal | 31% | 34% | 39% |
| Pérdida de laptops o hardware móvil | 42% | 42% | 34% |
| Abuso de acceso a Internet o correo electrónico cometido por empleados (ej. entrar a sitios pornográficos o utilizar software pirata) | 44% | 30% | 25% |

**Tabla 3-1**
Incidentes de seguridad informática más comunes

**Fuente:** "2010/11 Computer Security Institute Computer Crime & Security Survey", cortesía del Instituto de Seguridad Computacional.

países en desarrollo están expuestos a un mayor riesgo de que sus computadoras sean infectadas por malware. La ***Tabla 3-2*** muestra la posición de los peores y mejores países en término de computadoras infectadas por malware determinado por Kaspersky Lab, un proveedor de software de seguridad y servicios informáticos.

De forma independiente, la Alianza de Software Corporativo, analizó recientemente a los 24 países que representan a la mayor parte de los usuarios de la tecnología de la comunicación e información a nivel mundial. Se calificó a los países basándose en datos de privacidad, seguridad cibernética, control de los delitos informáticos, protección de la propiedad intelectual, infraestructura de la TI, libre comercio, interoperabilidad tecnológica y la compatibilidad de las leyes penales con los estándares internacionales que tratan los delitos informáticos. Japón resultó ser el país mejor calificado, seguido de Australia, Alemania, Estados Unidos y Francia. Brasil tuvo la peor calificación, principalmente porque no tiene una ley que garantice la privacidad de la transferencia de datos, y porque sus leyes contra los delitos informáticos son extremadamente débiles. Se estima que en el 2011, hackers informáticos robaron cerca de $1 billón de dólares a negocios de Brasil, país en donde 32 por ciento de sus empresas fueron víctimas de ataques cibernéticos[10].

#### Incrementar la complejidad incrementa la vulnerabilidad

El ambiente informático se ha vuelto enormemente complejo. Las redes, computadoras, sistemas operativos, aplicaciones, sitios web, switches, routers, y puertas de enlace se conectan unas con otras manejadas por cientos de millones de líneas de código. Este ambiente continúa creciendo en complejidad día con día. El número de posibles puntos de

| Países con tasas altas de computadoras infectadas | | Países con tasas bajas de computadoras infectadas | |
|---|---|---|---|
| País | Tasa | País | Tasa |
| Sudán | 70% | Japón | 6% |
| Bangladesh | 64% | Alemania | 9% |
| Irak | 62% | Suiza | 10% |
| Ruanda | 57% | Luxemburgo | 10% |
| Nepal | 56% | Dinamarca | 11% |

**Tabla 3-2**
Posición de los países basándose en el porcentaje de computadoras infectadas

**Fuente:** Stefan Tanase, "Q1/2011 Malware Report", Kaspersky Lab, 17 de mayo de 2011.

entrada a una red se expande de manera continua conforme se añaden más dispositivos, lo cual incrementa la posibilidad de tener violaciones de seguridad.

Para complicar aún más este asunto, los trabajadores de muchas organizaciones operan en el ambiente de cómputo en la nube, en donde el software y el almacenamiento de datos son servicios provistos vía Internet ("la nube"); los servicios corren en la computadora de una organización y se accede a ellos mediante un explorador de Internet. Esto representa un cambio significativo en cómo se almacenan, se accede y se transfieren los datos, esto conlleva muchos problemas de seguridad. El empleo sin gestión de los servicios de la nube (por ejemplo, el uso de un sitio web de transferencia de archivos, para pasar documentos grandes a clientes o proveedores) representa un riesgo significativo. Los gerentes empresariales y de TI deberían insistir en que sus empleados escogieran un servicio a partir de una lista validada de servicios de cómputo en la nube, esto con el fin de evitar problemas en potencia. La ***Tabla 3-3*** provee algunas preguntas clave para evaluar los servicios de la nube. La respuesta preferida a cada pregunta es *sí*.

La virtualización también introduce otras complicaciones en el ambiente informático actual. El **software de virtualización** opera en una capa de software que corre encima del sistema operativo. Permite que múltiples máquinas virtuales —cada una con su propio sistema operativo— corran en una sola computadora. Cada una de estas **máquinas virtuales** se desempeña como si fuera una computadora aparte, completando las tareas requeridas por los usuarios y las aplicaciones asignadas a la máquina virtual. La virtualización se aprovecha del hecho de que la gran mayoría de servidores físicos utiliza menos de 10 por ciento de su capacidad de hardware. Con la virtualización, la carga de trabajo de varios servidores físicos puede ser manejada por varias máquinas virtuales separadas, pero albergadas en un solo servidor físico. Entonces, la virtualización incrementa el intercambio de recursos y el uso del sistema, reduciendo el número de servidores que se requieren para manejar las necesidades de procesamiento de una organización. Tener pocos servidores significa menos espacio para el equipo de cómputo, y menos energía para operar y enfriar los servidores. Por lo tanto, la virtualización reduce costos y espacios físicos[11]. Sin embargo, operar en un ambiente virtual complica el ambiente operativo y aumenta el potencial de daño si uno de los servidores virtuales es atacado por un hacker.

#### Expectativas del usuario de cómputo avanzado

Hoy, el tiempo significa dinero, y entre más rápido puedan resolver problemas los usuarios de computadoras, más pronto serán productivos. Como resultado, los centros de asistencia de cómputo se encuentran bajo una presión intensa para responder rápidamente

**Tabla 3-3**
Preguntas para evaluar el servicio de cómputo en la nube

**Fuente:** Course Technology/Cengage Learning

| Pregunta | Sí | No |
|---|---|---|
| ¿Las interfaces entre el servicio de la nube y la de los usuarios son seguras? ¿Mantienen un nivel apropiado de control de acceso? | | |
| ¿Se codifican los datos cuando viajan a través de Internet? | | |
| ¿El servicio posee almacenamiento seguro y control de acceso a los datos almacenados en la nube? | | |
| ¿El servicio provee un respaldo en el caso de un desastre natural o causado por el humano que provoque la falla de éste? | | |
| ¿El proveedor de servicio en la nube tiene buena reputación y es financieramente viable? | | |

todas las preguntas de los usuarios. Bajo coacción, el personal de los centros de asistencia a veces olvida verificar las identificaciones de los usuarios o revisar si están autorizados a realizar la tarea o acción que demandan conocer. Además, aunque la mayoría ha sido advertidos de no hacerlo, algunos usuarios de cómputo comparten su nombre de inicio y contraseña con otros trabajadores que han olvidado sus propias contraseñas. Esto puede permitir que los empleados obtengan acceso a sistemas de información y datos para los que no estaban autorizados.

#### Expandir y cambiar los sistemas introduce nuevos riesgos

Los negocios se han movido de una era de computadoras individuales, en donde los datos críticos se almacenaban en una computadora principal aislada en un cuarto cerrado, a una era en donde las computadoras personales se conectan a redes con millones de computadoras, todas capaces de compartir información. Los negocios se han movido rápidamente al comercio electrónico, cómputo portátil, grupos colaborativos de trabajo, negocios globales y sistemas de información interorganizacional. Las tecnologías de la información se han vuelto ubicuas y son unas herramientas necesarias para que las organizaciones alcancen sus metas. No obstante, cada vez es más difícil mantenerse al tanto de los cambios tecnológicos, evaluar continuamente y de manera exitosa los riesgos de seguridad e implementar enfoques para lidiar con éstos.

#### Lleva tu propio dispositivo

La política empresarial denominada **lleva tu propio dispositivo** (**BYOD** por sus siglas en inglés), es una política que permite, y en algunos casos, promueve, que los empleados utilicen sus propios dispositivos portátiles (smartphones, tablets o computadoras personales) para acceder a los recursos y aplicaciones de cómputo, como correo electrónico, bases de datos corporativas, intranet de la corporación, e Internet. Los defensores de la BYOD dicen que esta política mejora la productividad de los empleados al permitir que éstos utilicen un dispositivo con el que ya se encuentran familiarizados, mientras que también ayuda a crear una imagen de compañía en donde ésta se percibe como flexible y progresiva. La mayor parte de las compañías han notado que, simplemente no pueden prevenir que sus empleados utilicen sus propios dispositivos para realizar sus labores. Sin embargo, esta práctica eleva varios problemas de seguridad, pues es posible que este tipo de dispositivos también se utilicen para actividades no laborales (navegar en la red, bloguear, hacer compras, visitar sitios de redes sociales, etc.) que los exponen a malware con mayor frecuencia de lo que sucedería si se utilizara un dispositivo con un uso estrictamente laboral. Este malware podría ser diseminado a lo largo de todos los equipos de la compañía. Además, la BYOD dificulta seriamente resguardar de manera adecuada los dispositivos portátiles adicionales con sus distintos sistemas operativos y la miríada de aplicaciones que existe.

#### Mayor dependencia a software comercial con vulnerabilidades conocidas

En computación, un **exploit**, es un ataque a un sistema de información que se aprovecha de una vulnerabilidad particular de un sistema. Con frecuencia este ataque se debe a un diseño pobre del sistema o a una mala implementación. Una vez que se descubre la vulnerabilidad, los desarrolladores de software crean y emiten una "solución" o un parche para eliminar el problema. Los usuarios del sistema o aplicaciones son responsables de obtener e instalar el parche, que pueden descargar normalmente de la red. (Estos parches son adicionales a otro tipo de mantenimiento y proyectos de trabajo que realizan los desarrolladores de software). Por ejemplo, se descubrió una vulnerabilidad crítica en el software

de la compañía Oracle, Java 7. Esta anomalía posibilitaba a los hackers para irrumpir en computadoras. Oracle liberó un parche de emergencia para corregir este problema[12].

Cualquier tipo de retraso para instalar el parche expone al usuario a una potencial violación de seguridad. La necesidad de instalar un parche para prevenir que un hacker se aproveche de esta vulnerabilidad del sistema puede crear un dilema ético para el personal de apoyo de sistemas que tratan de equilibrar una agenda muy ocupada. ¿Deberían instalar un parche que, de no ser instalado, podría ocasionar una violación de seguridad, o deberían completar alguna labor del proyecto que tienen asignado para que éste pueda ser entregado a tiempo? Desde el 2006, el número de nuevas vulnerabilidades de software identificadas ha excedido las 4 600 por año (un promedio de 13 diarias), como se muestra en la ***Tabla 3-4***.

Claramente, puede ser difícil estar al tanto de todos los parches que se requieren. Una preocupación central es el **ataque del día cero**, que se lleva a cabo antes de que la comunidad de seguridad o el desarrollador de software sepa sobre la existencia de la vulnerabilidad o antes de que la haya reparado. Uno esperaría que aquél que descubre una vulnerabilidad en el día cero, le proveería este conocimiento a los creadores del software para que puedan arreglar el problema. Sin embargo, en algunos casos, este conocimiento se vende en el mercado negro a terroristas cibernéticos, gobiernos u otras organizaciones que lo pueden utilizar en ataques a computadoras de sus rivales. Los exploits del día cero pueden llegar a tener precios de hasta $250 000 dólares[13].

Las compañías estadunidenses dependen cada día más de software comercial con vulnerabilidades conocidas. Aun cuando las vulnerabilidades son expuestas, muchas organizaciones de TI prefieren utilizar el software instalado "ya como está" en lugar de implementar los parches que harán más difícil de usar o eliminarán algunas de las características sugeridas por clientes o clientes potenciales que les ayudarán a vender el software.

## Tipos de exploits

Existen muchos tipos de ataques informáticos, y todo el tiempo se están inventando nuevas variedades de éstos. En esta sección se discuten algunos de los ataques más comunes: virus, gusanos, caballos de Troya, spam, ataque de denegación de servicio, rootkit, phishing, spear-phishing, smishing y vishing.

Aunque solemos pensar que este tipo de exploits están dirigidos a las computadoras, smartphones como el iPhone de Apple, Research in Motion de BlackBerry y varios smartphones con sistema operativo Android de Google, continúan haciéndose cada vez más parecidos a una computadora. Cada vez más, los usuarios de smartphones almacenan toda una variedad de datos personales en sus celulares, incluyendo números de tarjeta

**Tabla 3-4**
Número total de nuevas vulnerabilidades de software identificadas anualmente

| Año | Número de vulnerabilidades de software identificadas |
|---|---|
| 2006 | 4842 |
| 2007 | 4644 |
| 2008 | 5562 |
| 2009 | 4814 |
| 2010 | 6253 |
| 2011 | 4989 |

**Fuente:** "Internet Security Threat Report: 2011 Trends", Symantec, abril 2012, wwww.symantec.com/content/en/us/Enterprise/other_resources/b-1str_main_report_2011_21239364.en-ys.pdf

de crédito o números de cuenta bancarias. Los smartphones se usan para navegar la Web y realizar transacciones bancarias electrónicas. Entre más personas utilicen sus smartphones para estos propósitos, más atractivos se volverán para ser el objetivo de ladrones cibernéticos. Como se discutió en la viñeta de apertura, el ransomware es una forma de malware, que cuando se descarga al teléfono móvil, toma control del dispositivo y sus datos hasta que el propietario acepta pagar el rescate que pide el atacante[14]. Otra forma de malware en smartphones se encarga de hacer cargos a las cuentas del usuario mandando mensajes automáticos a los números que cargan cuotas al recibir un mensaje[15].

#### Virus

El término *virus informático* se ha convertido en un concepto ambiguo, pues se utiliza para describir muchos tipos distintos de códigos malignos. Técnicamente, un **virus** es una pieza de código de programación, usualmente disfrazado de algo más, que causa que las computadoras se comporten de manera inesperada, normalmente de forma indeseable. Con frecuencia, los virus se encuentran vinculados a un archivo, de manera que cuando se abre el archivo en la computadora, éste se ejecuta. Otros virus se almacenan en la memoria de la computadora e infectan archivos cuando se enciende la computadora, o los modifica o los crea. La mayor parte de los virus crean un "payload", o software dañino que causa que la computadora se desempeñe de forma inesperada. Por ejemplo, el virus puede estar programado para mostrar ciertos mensajes en la pantalla, borrar o modificar ciertos documentos, o reformatear el disco duro.

Un verdadero virus no se puede esparcir de computadora a computadora por sí mismo. Un virus se esparce a otras computadoras cuando el usuario de una computadora abre un archivo adjunto infectado, descarga un programa infectado o visita un sitio web infectado. En otras palabras, los virus se diseminan por la acción del usuario "infectado".

Los macrovirus se han convertido en un tipo de virus bastante común y fácil de crear. Los atacantes utilizan una aplicación de macrolenguaje (como Visual Basic o VBScript) para crear programas que infecten documentos y plantillas. Una vez que se abre un documento infectado, el virus se ejecuta e infecta las aplicaciones y plantillas del usuario. Los macros pueden insertar palabras, números o frases no deseadas en los documentos o alterar las funciones del comando. Después de que un macrovirus infecta las aplicaciones del usuario, se puede agregar a todos los documentos creados con la aplicación. El virus "WM97/Resume.A" es un macro virus de Word que se disemina vía correo electrónico bajo el título "Resume- Janet Simons". Si el receptor del correo hace clic en el archivo adjunto, el virus borra todos los datos almacenados en los discos del usuario.

#### Gusanos

A diferencia de los virus informáticos, que requieren del usuario para diseminar archivos infectados a otros usuarios, un **gusano** es un programa dañino que reside en la memoria activa de la computadora y se duplica a sí mismo. Los gusanos difieren de los virus en que éstos se pueden propagar sin intervención humana, mandando copias de sí mismos a otras computadoras a través del correo electrónico.

El impacto negativo de un ataque por gusanos a las computadoras de una compañía puede ser considerable: pérdida de datos y programas, pérdida de productividad dado que los empleados no pueden utilizar sus computadoras, pérdida de productividad adicional cuando los empleados intentan recuperar sus datos y programas y un gran esfuerzo por parte de los empleados de TI para limpiar el desastre y restaurar los equipos para llevarlos a la normalidad. El costo para reparar los daños hechos por cada uno de los gusanos Code Red, SirCam, y Melissa se estimó en más de $1 billón de dólares, así que

junto con los daños hechos por Conficker, Storm y ILOVEYOU, los daños ascendieron a más de $5 billones de dólares[16,17].

#### Caballos de Troya

Un **caballo de Troya** es un programa en el cual se esconde un código maligno dentro de un programa aparentemente inocuo. El payload maligno del programa puede estar diseñado para permitir que el hacker destruya los discos duros, corrompa archivos, controle las computadoras de manera remota, lance ataques contra otras computadoras, robe contraseñas o números del seguro social, espíe a los usuarios grabando las teclas que pulsan y se transmitan a un servidor operado por terceros.

Un caballo de Troya puede ser entregado a través de un archivo adjunto de correo, descargarse de un sitio web o contraerse mediante un dispositivo de medios removibles, como un CD/DVD o una memoria USB.

Una vez que un usuario ejecuta el programa que hospeda al caballo de Troya, el payload se inicia también, sin dar ningún tipo de señal. Los programas más comunes para hospedar este tipo de programas son los salvapantallas, sistemas de tarjetas de felicitación y juegos.

Win-7-Anti-Virus 2012 es un antivirus falso que se infiltra en las computadoras de los usuarios a través de un caballo de Troya. Una vez dentro de la computadora del usuario, esta herramienta simula un sistema de escaneo cuyo propósito es encontrar numerosas infecciones de malware. Después dice poder remover estas infecciones si compras la herramienta y provees información de tu tarjeta de crédito[18].

Otro tipo de caballo troyano es la **bomba lógica**, que se ejecuta cuando es iniciada por un evento específico. Por ejemplo, las bombas lógicas pueden inicializarse por el cambio de un archivo particular, al pulsar una serie específica de teclas, o cuando llega una fecha u hora específica.

#### Spam

El spam de correo electrónico es el abuso de los sistemas de correo electrónico para enviar correos no solicitados a grandes cantidades de personas. La mayor parte del spam es publicidad de bajo costo, muchas veces de productos cuestionables, como pornografía, embauques para hacerse rico de manera fácil o simplemente correos basura. El spam también es un método de publicidad extremadamente barato, que muchas compañías utilizan. Por ejemplo, una compañía podría mandar un correo a una gran sección de clientes potenciales para anunciar el lanzamiento de un nuevo producto como un intento para incrementar las ventas iniciales. El spam también se utiliza para entregar gusanos y otro tipo de malware.

El costo de crear una campaña de correos electrónicos para un producto o servicio es de varios cientos o pocos miles de dólares, en comparación con las campañas de miles de dólares. Además, las campañas por correo electrónico sólo tardan unas pocas semanas en desarrollarse, comparado con los tres meses o más que tardan en desarrollarse las campañas por correo oficial. La retroalimentación en promedio, es de 48 horas para el correo electrónico, mientras que el correo normal tarda semanas. Sin embargo, el beneficio del spam a las compañías puede verse comprometido por un público con una reacción negativa al recibir anuncios publicitarios que no solicitaron.

El spam forza material cuestionable y no deseado a las bandejas de entradas de los usuarios, impidiendo la capacidad de que éstos se comuniquen de manera efectiva y esconde los correos relevantes entre una multitud de mensajes no requeridos. Esto le cuesta millones de dólares anualmente a los proveedores de Internet y sus usuarios. A

los últimos les cuesta el tiempo de buscar correo por correo para marcar el spam y borrarlo, actividad que puede ser costosa si éstos pagan su conexión a Internet por hora. También le cuesta dinero a los proveedores de servicio de Internet (ISPs por sus siglas en inglés) y a los servicios en línea para transmitir spam, que se reflejan en cargos a todos sus suscriptores.

La **Ley para el Control del ataque de Pornografía y Marketing no Solicitados** (**CAN-SPAM**) entró en efecto en enero de 2004. La ley establece que es legal enviar spam siempre y cuando el mensaje cumpla con ciertos requisitos: los spammers no pueden disfrazar su identidad utilizando una dirección remitente falsa, el correo debe incluir una etiqueta especificando que es un anuncio o una solicitud, y el correo debe incluir una manera para que los receptores indiquen su deseo de no recibir más mensajes masivos. A pesar de las medidas propuestas por la CAN-SPAM, el porcentaje de spam en los mensajes de correo electrónico fue en promedio de 68 por ciento en octubre de 2012, de acuerdo a Securelist, un blog manejado por la firma de seguridad Kaspersky Labs[19].

Muchas compañías —incluyendo Google, Microsoft y Yahoo!— ofrecen servicios de correo electrónico gratuitos. Los spammers buscan utilizar cuentas de correo de este tipo de empresas que tienen una reputación respetable o en proveedores de correo electrónico basados en la Web, pues de esta forma su spam puede enviarse sin costo alguno y es menos probable que sea bloqueado. Los spammers pueden burlar el proceso de registro de los servicios de correo electrónico gratuito al lanzar un ataque bot coordinado que inicie sesiones en miles de cuentas de correo a la vez. Estas cuentas son empleadas por los spammers para enviar miles de mensajes de correo de manera gratuita e imposible de rastrear.

Una solución parcial a este problema es el uso de CAPTCHA para asegurar que sólo los humanos obtengan cuentas gratuitas. El software **CAPTCHA** (**Prueba de Turing Completamente Automática y Pública para diferenciar Computadoras de Humanos**) genera y evalúa pruebas que los humanos pueden aprobar, pero que los programas más sofisticados de computadora no pueden aprobar. Por ejemplo, los humanos pueden leer el texto distorsionado de la ***Figura 3-1***, pero un simple programa de computadora no puede hacerlo.


**Figura 3-1**
Ejemplo de CAPTCHA

**Fuente:** Ejemplo de CAPTCHA de www.recaptcha.net. Cortesía de Carnegie Mellon University.

Este no es un libro de texto común de Tecnologías de la Información. Un libro de texto típico dedicaría solamente un capítulo a la ética, espacio insuficiente para cubrir el amplio espectro de temas y problemáticas relacionadas con la TI.

Una cobertura tan limitada no cumple los requisitos de los gerentes de negocios o los profesionales de la TI: manejar los problemas éticos que surgen en el sitio de trabajo. Hace falta realizar un análisis de las distintas situaciones éticas que surgen en la TI así como consejos prácticos para manejar este tipo de problemas.

Por eso, esta quinta edición de **Ética en la tecnología de la información** tiene contenido, ejemplos, situaciones, casos y cuestionarios suficientes como para que pueda utilizarse durante un curso semestral sobre cómputo ético. También se puede utilizar este libro como material suplementario para cursos como "Introducción a la Gestión en Sistemas de Información", "Principios de la Tecnología de la Información", "Perspectivas Gerenciales en la Tecnología de la Información", "Seguridad Informática", "Comercio Electrónico" y muchos otros más.

ISBN-13: 978-607-522-844-0
ISBN-10: 607-522-844-6

CENGAGE Learning®

Visita nuestro sitio en http://latinoamerica.cengage.com