

Curso de aprendizaje electrónico oficial de Microsoft

Versión de
impresión



2698AE

**Seguridad y privacidad de la
computadora**

CONTRATO DE LICENCIA PARA EL USUARIO FINAL DEL CONTENIDO CON LICENCIA DE MICROSOFT: DIGITAL LITERACY CURRICULUM

LEA ATENTAMENTE: Estos términos de licencia ("**Términos de Licencia**") son un acuerdo vinculante entre usted (una persona o entidad) y Microsoft Corporation ("**Microsoft**") y rigen el uso de todos los materiales de enseñanza de Microsoft que acompañan a estos Términos de Licencia. **AL UTILIZAR LOS MATERIALES Y/O AL INSTALAR O UTILIZAR EL SOFTWARE QUE ACOMPAÑA A ESTOS TÉRMINOS DE LICENCIA (COLECTIVAMENTE, "CONTENIDO CON LICENCIA"), USTED ACEPTA LOS TÉRMINOS DE ESTA LICENCIA. SI USTED NO ESTÁ DE ACUERDO CON DICHS TÉRMINOS, NO UTILICE ESTE CONTENIDO CON LICENCIA.**

1. DEFINICIONES.

- 1.1. "**Centros de Enseñanza Autorizados**" se refiere a centros de enseñanza de tecnología colectivos ("**CTLC**") sin ánimo de lucro (o similares), a centros colectivos o a cualquier otra entidad que Microsoft pueda designar como entidad autorizada para el Uso de "Digital Literacy Curriculum" de Microsoft.
- 1.2. "**Sesiones de Enseñanza Autorizadas**" se refiere a las sesiones de enseñanza no comerciales en las que se utilizan materiales del Curso y que se imparten en Centros de Enseñanza Autorizados para enseñar a personas (a) materias como informática y tecnología de la información de nivel básico y/o (b) el uso de tecnología, productos o servicios de Microsoft. En cada Sesión de Enseñanza Autorizada deberá impartirse el contenido de un (1) Curso.
- 1.3. "**Currículo**" se refiere a cualquier material incluido en "Digital Literacy Curriculum". El Currículo consiste en cinco Cursos, cada uno de los cuales ofrece entrenamiento sobre el contenido de una tecnología concreta.
- 1.4. "**Curso**" se refiere a los cursos ofrecidos por "Digital Literacy Curriculum" de Microsoft; cada uno de los cuales ofrece entrenamiento sobre el contenido de una tecnología concreta y consiste en un componente de enseñanza y una valoración.
- 1.5. "**Dispositivos**" se refiere a un única computadora, dispositivo, estación de trabajo, terminal o cualquier otro dispositivo digital, electrónico o analógico de un Centro de Enseñanza Autorizado.
- 1.6. "**Documentos**" se refiere a la documentación impresa o electrónica, como evaluaciones, manuales, cuadernos de ejercicios, hojas de datos y P+F que puedan estar incluidos en el Contenido con Licencia.
- 1.7. "**Contenido del Profesor**" se refiere al Contenido con Licencia, que acompaña a estos Términos de Licencia o que se encuentra en el sitio Web, destinado al Uso exclusivo de los Profesores para que impartan enseñanza a los Alumnos durante una Sesión de Enseñanza Autorizada.
- 1.8. "**Contenido con Licencia**" se refiere a los materiales de enseñanza para un Curso concreto que acompañan a estos Términos de Licencia. El Contenido con Licencia puede incluir, entre otros, los elementos siguientes: (i) materiales del Curso, (ii) Elementos Multimedia, (iii) software y (iv) Documentos.
- 1.9. "**Elementos Multimedia**" se refiere a las fotografías, imágenes prediseñadas, animaciones, sonidos y clips de video y música que puedan acompañar a estos Términos de Licencia.
- 1.10. "**Enseñanza Autodidacta**" se refiere a un programa autodidacta, que el Alumno realiza a su propio ritmo y sin un Profesor presente, (a) relativo al contenido del Curso o de los Cursos de la Sesión de Enseñanza Autorizada en la que está matriculado, para lo que utiliza Dispositivos en Centros de Enseñanza Autorizados, o (b) para las sesiones de enseñanza en línea en un Curso a través del sitio Web y/o un curso que el Alumno ha descargado del sitio Web y/o ha instalado desde un CD, para lo que utiliza dispositivos personales propios.
- 1.11. "**Alumnos**" se refiere a personas que se han matriculado debidamente en una Sesión de Enseñanza Autorizada en un Centro de Enseñanza Autorizado y/o a alumnos que participan en Enseñanza Autodidacta.
- 1.12. "**Profesores**" se refiere al personal debidamente contratado por el Centro de Enseñanza Autorizado para impartir u ofrecer una Sesión de Enseñanza Autorizada a los Alumnos.
- 1.13. "**Uso**" se refiere al uso no comercial del Contenido con Licencia por parte de a) Alumnos, exclusivamente para realizar Enseñanza Autodidacta, y b) Profesores, exclusivamente para impartir clases, laboratorios educativos o programas relacionados concebidos para enseñar a otros Profesores y/o Alumnos el uso de la tecnología, productos o servicios relacionados con la materia del Contenido con Licencia, así como también para enseñar los conceptos relacionados con esa tecnología, productos o servicios. En estos Términos de Licencia, "Uso" no incluirá el uso del Contenido con Licencia con fines comerciales ni empresariales generales.

1.14. “Usted” se refiere a Centros de Enseñanza Autorizados, Profesores y/o Alumnos, según corresponda.

2. **GENERAL.** Estos Términos de Licencia se aplicarán a actualizaciones, suplementos, componentes complementarios o componentes de servicios basados en Internet del Contenido con Licencia que Microsoft pueda proporcionarle a Usted o poner a su disposición (cada uno, un “**Componente**”); sin embargo, si aparecen términos de licencia independientes tras la instalación de un Componente (“**Términos de Licencia de Componente**”), prevalecerán las condiciones de los Términos de Licencia de Componente con respecto al Componente correspondiente. Microsoft se reserva el derecho de dejar de suministrarle a Usted o de poner a su disposición, mediante el Uso del Contenido con Licencia, los servicios basados en Internet. Estos Términos de Licencia también rigen todos los servicios de soporte técnico de productos, si existe alguno, relacionados con el Contenido con Licencia, excepto los que puedan estar incluidos en otro contrato entre Usted y Microsoft. Una modificación o anexo a estos Términos de Licencia puede acompañar al Contenido con Licencia.

3. **INSTALACIÓN Y DERECHOS DE USO.** Siempre que cumpla con estos Términos de Licencia, Usted podrá ejercer los siguientes derechos:

3.1 Alumnos

Usted puede (a) tener acceso y hacer Uso de una copia del Contenido con Licencia a través del sitio Web y/o (b) descargar el Contenido con Licencia del sitio Web o instalarlo desde un CD y hacer Uso de una copia de dicho Contenido con Licencia en un único dispositivo y exclusivamente con el objeto de usarlo para su enseñanza personal. No puede compartir este derecho, o el Contenido con Licencia, con otras personas.

3.2 Centros de Enseñanza Autorizados

Usted puede conceder en sublicencia a cada Alumno el derecho a hacer Uso de una (1) copia del Contenido con Licencia en un único Dispositivo y exclusivamente para el Uso en la enseñanza personal del Alumno del contenido del Curso en que esté matriculado (i) durante una Sesión de Enseñanza Autorizada y (ii) para Enseñanza Autodidacta de dicho Curso.

3.3 Centros de Enseñanza Autorizados o Profesores

(a) Para cada Sesión de Enseñanza Autorizada, los Profesores o un Centro de Enseñanza Autorizado pueden

(i) instalar copias individuales del Contenido con Licencia de cada Curso en los Dispositivos del aula que los Alumnos utilizarán en dicha sesión, siempre que el número de copias en Uso no exceda el número de Alumnos para esa Sesión de Enseñanza Autorizada; O BIEN

(ii) instalar una copia del Contenido con Licencia de cada Curso en un servidor de red, siempre que el número de Dispositivos con acceso a ese Contenido con Licencia en cada servidor no exceda el número de Alumnos para la Sesión de Enseñanza Autorizada.

(b) Para la Enseñanza Autodidacta de los Alumnos, los Profesores o un Centro de Enseñanza Autorizado pueden

(i) instalar copias individuales del Contenido con Licencia de cada Curso en los Dispositivos del aula que los Alumnos utilizarán para dicho tipo de enseñanza, siempre que el número de copias en Uso no exceda el número de Alumnos debidamente matriculados para el contenido del Curso; O BIEN

(ii) instalar una copia del Contenido con Licencia de cada Curso en un servidor de red, siempre que el número de Dispositivos con acceso a ese Contenido con Licencia en cada servidor no exceda el número de Alumnos matriculados para el contenido del Curso, y siempre que dicho Centro de Enseñanza Autorizado coloque un monitor en las aulas en las que el Contenido con Licencia esté instalado durante los períodos en que dicho Centro de Enseñanza Autorizado permita que los Alumnos participen en la Enseñanza Autodidacta.

(c) Un Profesor para una Sesión de Enseñanza Autorizada, o el Centro de Enseñanza Autorizado correspondiente, puede instalar y hacer Uso de una (1) copia del Contenido con Licencia del Curso, que es el contenido de dicha sesión, en un único Dispositivo y exclusivamente para el Uso en la enseñanza personal del Profesor y para la preparación de la Sesión de Enseñanza Autorizada. Cada Profesor puede asimismo realizar una segunda copia de dicho Contenido con Licencia e instalarla en el dispositivo personal del Profesor para el Uso exclusivo de dicho Profesor.

SIN LIMITAR LA GENERALIDAD DE LO ANTERIOR, SE PROHÍBE EXPRESAMENTE LA COPIA O REPRODUCCIÓN DEL CONTENIDO CON LICENCIA EN CUALQUIER SERVIDOR O UBICACIÓN PARA SU POSTERIOR REPRODUCCIÓN O REDISTRIBUCIÓN.

4. DESCRIPCIÓN DE OTROS DERECHOS Y LIMITACIONES DE LA LICENCIA

4.1 Errores; Cambios; Nombres Ficticios.

(a) Usted reconoce y acepta que (i) el Contenido con Licencia (que contiene, entre otros elementos, Documentos, elementos gráficos relacionados y otros Componentes incluidos junto con el presente documento) puede contener imprecisiones técnicas o errores tipográficos; y que (ii) Microsoft puede hacer mejoras y/o cambios en el Contenido con Licencia o en cualquiera de sus partes en cualquier momento y sin previo aviso.

(b) Usted entiende y acepta que, a menos que se indique lo contrario, los nombres de las compañías, productos, personas, personajes y datos mencionados en el Contenido con Licencia pueden ser ficticios y no designan de ningún modo a ninguna persona, compañía, producto o acontecimiento real.

4.2 Uso y Reproducción de Documentos.

(a) Centros de Enseñanza Autorizados y Profesores.

Siempre que cumpla con estos Términos de Licencia, usted podrá imprimir y/o reproducir una versión impresa de (i) todos los Documentos, o partes de los mismos, y/o (ii) los materiales del Curso, o partes de éstos, incluida la reproducción de una versión impresa de los materiales del Curso en su totalidad. Si Usted elige reproducir el Documento y/o los materiales del Curso, Usted acepta que:

(1) Dichos Documentos o materiales del Curso serán para Uso exclusivo en las Sesiones de Enseñanza Autorizadas.

(2) Los Documentos y/o materiales del Curso no se publicarán ni expondrán en ninguna computadora de red (salvo lo antes dispuesto explícitamente en la Sección 3.3(a)(ii) y/o 3.3(b)(ii)) ni se emitirán en soporte alguno.

(3) Las copias de los Documentos, o partes de los mismos, sólo se distribuirán a Alumnos y Profesores para el contenido del Curso en el cual el Alumno está matriculado o para el cual el Profesor imparte enseñanza, respectivamente.

(4) Las versiones impresas de todos los materiales del Curso, o partes de los mismos, se distribuirán exclusivamente a Profesores para el contenido del Curso para el cual imparte enseñanza y/o a Alumnos para el contenido del curso para el cual están matriculados.

(5) Cualquier reproducción incluirá el aviso de derechos de autor original de los materiales del Curso y/o del Documento o, si no aparece ningún aviso de derechos de autor en el Documento, un aviso de derechos de autor a favor de Microsoft que tenga un formato sustancialmente idéntico al indicado a continuación.

(b) Alumnos.

Siempre que cumpla con estos Términos de Licencia, usted podrá imprimir y copiar todos los Documentos o los materiales del Curso, o partes de los mismos. Si Usted elige reproducir el Documento y/o los materiales del Curso, Usted acepta que:

(1) Usted utilizará dichos Documentos impresos y/o partes de los materiales impresos del Curso exclusivamente para el uso en su enseñanza personal.

(2) Usted no publicará, expondrá, emitirá ni transmitirá los Documentos o materiales del Curso a otras personas o en una red.

(3) Usted incluirá en cada copia ya sea los avisos de derechos de autor y marcas registradas originales de los materiales del Curso y/o del Documento o un aviso que indique lo siguiente:

Modelo de aviso:

“© 2006. Reimpreso con permiso de Microsoft Corporation. Reservados todos los derechos.

Se concede el permiso para reproducir los materiales aquí contenidos siempre y cuando dichos materiales se reproduzcan exclusivamente para su uso junto con Digital Literacy Curriculum de Microsoft, y que éstos se proporcionen a Alumnos y Profesores de la

manera establecida en el documento Términos de Licencia de Microsoft Corporation que acompaña a este Curso.

Microsoft y Windows son marcas comerciales o marcas registradas de Microsoft Corporation en EE.UU. y/o en otros países. Otros nombres de productos y compañías mencionados aquí pueden constituir marcas comerciales de sus respectivos propietarios”.

4.3 *Uso de Elementos Multimedia.* Usted no puede modificar los Elementos Multimedia.

4.4 *Uso de los Componentes en el Contenido del Profesor.* Exclusivamente para impartir una Sesión de Enseñanza Autorizada, y respetando los términos y condiciones de este CLUF, los Profesores pueden reproducir o personalizar, para sus propios fines, aquellas partes del Contenido con Licencia que estén lógicamente asociadas con la instrucción de una Sesión de Enseñanza Autorizada, incluidos, entre otros, notas para el profesor, módulos y elementos de evaluación correspondientes a cada Sesión de Enseñanza Autorizada.

4.5 *Modificaciones.* De acuerdo con estos Términos de Licencia, los Profesores o Estudiantes pueden copiar o modificar la versión de Microsoft Word de los materiales del Curso; sin embargo, si decide ejercer los anteriores derechos, Usted acepta cumplir todos los demás términos y condiciones de estos Términos de Licencia, incluidas, entre otras, las Secciones 4.5, 4.6 y 7.

4.6 *Modificaciones permitidas.* Si Usted realiza cualquier modificación conforme a estos Términos de Licencia, acepta: (a) que utilizará dichas modificaciones exclusivamente para su propia enseñanza personal; (b) que identificará claramente dichas modificaciones como propias, y no declarará ni insinuará que Microsoft autorizó o aprobó dichas modificaciones; (c) que no realizará modificación alguna que constituya la creación de trabajos obscenos o escandalosos; (d) que defenderá, indemnizará y salvaguardará a Microsoft ante reclamaciones, acciones judiciales, daños, pérdidas, sanciones, multas, costos y gastos, incluidos los honorarios razonables de abogados, que surjan o resulten de dichas modificaciones; y (e) que no transferirá ni cederá los derechos de dichas modificaciones y/o de una versión modificada del Contenido con Licencia a terceros (salvo lo dispuesto expresamente para los Profesores en el punto (b) anterior) sin la autorización expresa y por escrito de Microsoft.

Si Usted es Profesor, además de todo lo indicado anteriormente, Usted también acepta: (a) que dichas modificaciones no se utilizarán para impartir enseñanza, excepto en una Sesión de Enseñanza Autorizada o para su propia enseñanza personal; (b) que Usted solamente podrá distribuir las versiones modificadas del Contenido con Licencia a Alumnos matriculados en una Sesión de Enseñanza Autorizada a otros Profesores del programa Digital Literacy Program que (i) impartan enseñanza sobre el contenido del Curso que sea la materia de objeto de las modificaciones y (ii) estén debidamente contratados como Profesores en los Centros de Enseñanza Autorizados para los cuales impartan enseñanza; y (c) que Microsoft se reserva el derecho a revisar y/o aprobar cualquier modificación que Usted efectúe al Contenido con Licencia.

4.7 *Reproducción y redistribución del Contenido con Licencia.* A excepción de lo indicado explícitamente en estos Términos de Licencia, Usted no puede reproducir o distribuir el Contenido con Licencia ni ninguna de sus partes (incluidas las modificaciones permitidas) a terceros sin la autorización expresa y por escrito de Microsoft.

5. **PROPIEDAD.** Estos Términos de Licencia sólo le proporcionan algunos derechos con respecto al Contenido con Licencia. Salvo que las leyes aplicables permitan lo contrario, Usted sólo puede hacer uso del Contenido con Licencia tal como se permite expresamente en estos Términos de Licencia. Microsoft se reserva los demás derechos. El Contenido con Licencia está protegido por leyes y tratados sobre derechos de autor y propiedad intelectual. Pertenecen a Microsoft o sus proveedores la titularidad, los derechos de autor y los demás derechos de propiedad intelectual sobre el Contenido con Licencia. Usted no puede eliminar ni ocultar ningún aviso de derechos de autor, de marca comercial u otras notificaciones que aparezcan en el Contenido con Licencia, o en alguno de sus componentes, tal y como se le entregaron a Usted. **El Contenido con Licencia se otorga bajo licencia y no es objeto de venta.**

6. **LIMITACIONES EN MATERIA DE INGENIERÍA INVERSA, DESCOMPILACIÓN Y DESENSAMBLAJE.** Usted no podrá utilizar técnicas de ingeniería inversa, descompilar ni desensamblar el Contenido con Licencia, excepto y únicamente en la medida en que dicha actividad esté expresamente permitida por la legislación aplicable, no obstante la presente limitación.

7. **LIMITACIONES A LA VENTA, ALQUILER, ETC. Y A DETERMINADAS CESIONES.** Usted no puede proporcionar servicios de alojamiento comercial ni dar en venta, alquiler, arrendamiento, sublicencia o cesión copias del Contenido con Licencia, o de alguna de sus partes (incluida cualquier modificación permitida) ya sea de manera independiente o como parte de una colección, producto o servicio.

8. **CONSENTIMIENTO AL USO DE DATOS.** Usted acepta que, de conformidad siempre con la legislación aplicable, Microsoft y las sociedades de su grupo puedan recopilar y utilizar la información técnica recopilada como parte de los servicios de soporte técnico de productos que se le proporcionen, si los hubiera, relacionados con el Contenido con Licencia. Microsoft sólo puede utilizar esta información para mejorar nuestros productos o para proporcionarle servicios o tecnologías personalizados, y no revelará esta información de manera que le identifique a Usted personalmente.

9. **VÍNCULOS A SITIOS DE TERCEROS.** Usted puede conectarse a sitios de terceros mediante el Uso del Contenido con Licencia. Los sitios de terceros no están bajo control de Microsoft, y Microsoft no es responsable del contenido de ningún sitio de terceros, de ningún vínculo contenido en un sitio de terceros, ni de ningún cambio o actualización que se realice en un sitio de terceros. Microsoft no es responsable de las difusiones por Web ni de ningún otro tipo de transmisión recibida desde un sitio de terceros. Microsoft le proporciona a Usted estos vínculos a sitios de terceros sólo por comodidad, y la inclusión de cualquiera de ellos no implica aprobación del sitio de terceros por parte de Microsoft.

10. **CONTENIDO CON LICENCIA Y SERVICIOS ADICIONALES.** Estos Términos de Licencia se aplicarán a los Componentes que Microsoft le pueda proporcionar a Usted o poner a su disposición después de la fecha en que Usted obtenga la copia inicial del Contenido con Licencia, a no ser que proporcionemos Términos de Licencia de Componente u otros términos de Uso con esos Componentes. Microsoft se reserva el derecho de dejar de suministrarle a Usted o de poner a su disposición, mediante el Uso del Contenido con Licencia, los servicios basados en Internet.

11. **TERMINACIÓN.** Sin perjuicio de cualquier otro derecho, Microsoft podrá poner término a estos Términos de Licencia, en caso de que usted no cumpla con los términos y condiciones de los mismos. En caso de que su contrato como Profesor a) caduque, b) Usted le ponga término voluntariamente y/o c) un Centro de Enseñanza Autorizado le ponga término, estos Términos de Licencia caducarán automáticamente. En dicho caso, Usted deberá destruir todas las copias del Contenido con Licencia y todas sus partes componentes.

12. **EXCLUSIÓN. MICROSOFT PROPORCIONA EL CONTENIDO CON LICENCIA Y LOS SERVICIOS DE SOPORTE TÉCNICO TAL CUAL Y EN EL ESTADO EN QUE SE ENCUENTRAN, QUE USTED MANIFIESTA CONOCER Y ACEPTAR, Y MICROSOFT EXCLUYE EN ESTE ACTO TODAS LAS GARANTÍAS Y CONDICIONES, YA SEAN EXPRESAS, IMPLÍCITAS O PREVISTAS POR LA LEY, INCLUIDAS, ENTRE OTRAS, TODAS LAS GARANTÍAS, DEBERES O CONDICIONES DE COMERCIABILIDAD, IDONEIDAD PARA UN FIN PARTICULAR, CONFIABILIDAD O DISPONIBILIDAD, EXACTITUD O INTEGRIDAD DE LAS RESPUESTAS, RESULTADOS, TITULARIDAD, AUSENCIA DE INFRACCIÓN, ESFUERZO RAZONABLE, AUSENCIA DE VIRUS INFORMÁTICOS Y AUSENCIA DE NEGLIGENCIA, TODO ELLO CON RESPECTO AL CONTENIDO CON LICENCIA Y LA PRESTACIÓN O FALTA DE PRESTACIÓN DE SOPORTE TÉCNICO U OTROS SERVICIOS. USTED ASUME TODO EL RIESGO QUE SURJA DEL USO O DEL RENDIMIENTO DEL CONTENIDO CON LICENCIA Y DE LOS SERVICIOS DE SOPORTE TÉCNICO.**

13. **EXCLUSIÓN DE RESPONSABILIDAD POR OTROS DAÑOS. EN NINGÚN CASO MICROSOFT SERÁ RESPONSABLE POR DAÑOS ESPECIALES, FORTUITOS, PUNITIVOS, INDIRECTOS O DERIVADOS O DE CUALQUIER OTRO TIPO (INCLUIDOS LOS DAÑOS POR LUCRO CESANTE, PÉRDIDA DE INFORMACIÓN CONFIDENCIAL O DE OTRO TIPO, INTERRUPCIÓN DE NEGOCIOS, PÉRDIDA DE PRIVACIDAD, INCUMPLIMIENTO DE OBLIGACIONES, YA SEA DE BUENA FE O CON DILIGENCIA RAZONABLE, NEGLIGENCIA Y CUALQUIER PÉRDIDA PECUNIARIA O DE OTRO TIPO), QUE SE DERIVEN O DE OTRO MODO ESTÉN RELACIONADOS CON EL USO O INCAPACIDAD DE USAR EL CONTENIDO CON LICENCIA, LA PRESTACIÓN O FALTA DE PRESTACIÓN DE LOS SERVICIOS DE SOPORTE TÉCNICO O DE OTRO TIPO, INFORMACIÓN, SOFTWARE Y CONTENIDO RELACIONADO A TRAVÉS DEL CONTENIDO CON LICENCIA O QUE DE OTRO MODO ESTÉN RELACIONADOS CON EL CONTENIDO CON LICENCIA O ESTOS TÉRMINOS DE LICENCIA, INCLUSO EN CASO DE ERROR, DE AGRAVIO (INCLUYENDO NEGLIGENCIA), RESPONSABILIDAD ESTRUCTA, RUPTURA DE CONTRATO O DE LA GARANTÍA DE MICROSOFT, Y AUN EN EL CASO DE QUE SE HUBIERA INFORMADO A MICROSOFT DE LA POSIBILIDAD DE DICHOS DAÑOS. DEBIDO A QUE ALGUNOS ESTADOS O JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LIMITACIÓN DE RESPONSABILIDAD POR DAÑOS CONSECUCIONALES O INCIDENTALES, ES POSIBLE QUE LA LIMITACIÓN ANTERIOR NO SE APLIQUE EN SU CASO.**

14. **LIMITACIÓN DE RESPONSABILIDAD. NO OBSTANTE LOS DAÑOS EN LOS QUE USTED PUEDA INCURRIR POR CUALQUIER RAZÓN (INCLUIDOS, ENTRE OTROS, LOS DAÑOS A LOS QUE SE HACE REFERENCIA AQUÍ Y TODOS LOS DAÑOS DIRECTOS O GENERALES, DE NATURALEZA CONTRACTUAL O CUALQUIER OTRA), LA RESPONSABILIDAD TOTAL DE MICROSOFT EN VIRTUD DE ESTOS TÉRMINOS DE LICENCIA Y EL ÚNICO RECURSO DE QUE USTED DISPONDRÁ FRENTE A TODO LO AQUÍ DICHO SE LIMITARÁ A LOS DAÑOS REALES SUFRIDOS POR USTED, AL CONFIAR RAZONABLEMENTE EN EL CONTENIDO CON LICENCIA, HASTA LA CANTIDAD QUE PAGÓ REALMENTE POR EL CONTENIDO CON LICENCIA O HASTA CINCO DÓLARES ESTADOUNIDENSES, LO QUE RESULTE MAYOR. LAS ANTERIORES LIMITACIONES Y EXCLUSIONES DE ESTA SECCIÓN Y DE LAS ANTERIORES SECCIONES 12 Y 13 SE APLICARÁN EN LA MÁXIMA MEDIDA PERMITIDA POR LA LEY APLICABLE, INCLUSO EN EL SUPUESTO DE QUE ALGÚN RECURSO FRACASE EN SU FINALIDAD ESENCIAL.**

15. **LEGISLACIÓN APLICABLE.** Si Usted adquirió este Contenido con Licencia en los Estados Unidos de América, estos Términos de Licencia se regirán por las leyes del Estado de Washington y, respecto a cualquier disputa que pueda surgir acerca del mismo, Usted se somete a la jurisdicción de los tribunales federales y estatales ubicados en King County,

Washington (EE.UU.). Si adquirió este Contenido con Licencia en Canadá, a menos que esté expresamente prohibido por la legislación local, estos Términos de Licencia se regirán por las leyes vigentes en la Provincia de Ontario, Canadá; y, respecto a cualquier disputa que pueda surgir acerca del mismo, acepta la jurisdicción de los tribunales federales y provinciales establecidos en Toronto, Ontario. Si Usted adquirió este Contenido con Licencia en la Unión Europea, Islandia, Noruega o Suiza, entonces estos Términos de Licencia se regirán por las leyes del Estado de Washington (EE.UU.) en la máxima medida permitida por la legislación local. Si Usted adquirió este Contenido con Licencia en cualquier otro país, entonces estos Términos de Licencia se regirán por las leyes del Estado de Washington (EE.UU.) en la máxima medida permitida por la legislación local.

16. **CONTRATO COMPLETO; DIVISIBILIDAD.** Estos Términos de Licencia (incluidos todos los anexos o modificaciones del mismo que se incluyan con el Contenido con Licencia) constituyen el contrato completo entre Usted y Microsoft en relación con el Contenido con Licencia y los servicios de soporte técnico (si los hay), y sustituyen o anulan todas las comunicaciones, propuestas y manifestaciones anteriores o simultáneas, orales o escritas, relativas al Contenido con Licencia o a cualquier contenido de estos Términos de Licencia. Si alguna disposición de estos Términos de Licencia fuera declarada no válida, sin aplicación o ilegal, las restantes disposiciones seguirán plenamente vigentes.

Si tuviera Usted alguna duda con respecto a estos Términos de Licencia o si por cualquier motivo Usted deseara comunicarse con Microsoft, consulte la dirección que se proporciona en este Contenido con Licencia para ponerse en contacto con la filial de Microsoft que atiende a su país, o bien visite el sitio Web de Microsoft en <http://www.microsoft.com>.

La información que contiene este documento, incluidas las direcciones URL y otras referencias a sitios Web de Internet, está sujeta a modificaciones sin previo aviso. A menos que se indique lo contrario, los nombres de ejemplo de compañías, organizaciones, productos, nombres de dominio, direcciones de correo electrónico, logotipos, personas, personajes, lugares y datos mencionados son ficticios, y no representan de ningún modo a ninguna persona, compañía, producto o acontecimiento reales. Es responsabilidad del usuario el cumplimiento de todas las leyes de derechos de autor aplicables. A menos que se indique lo contrario y sin limitar los derechos que confieren las leyes de derechos de autor, ninguna parte de este documento se podrá reproducir, almacenar o introducir en un sistema de recuperación, ni transmitir, de cualquier forma o por cualquier medio (ya sea electrónico, mecánico, fotocopia, grabación o de cualquier otro tipo), o con ningún propósito, sin el consentimiento expreso y por escrito de Microsoft Corporation.

Los nombres de los fabricantes, productos o direcciones URL se proporcionan únicamente con fines informativos y Microsoft Corporation no ofrece garantía expresa ni implícita relacionada con estos fabricantes o con el uso de los productos con tecnologías Microsoft. La inclusión de un fabricante o producto no implica que éstos estén avalados por Microsoft. Se incluyen vínculos a sitios de terceros. Esos sitios no están bajo el control de Microsoft y Microsoft no se hace responsable del contenido ni de los vínculos de ninguno de los sitios incluidos ni de las modificaciones o actualizaciones que se realicen en ellos. Microsoft no se responsabiliza de las transmisiones por Web o de cualquier otro tipo recibidas desde cualquiera de los sitios incluidos. Microsoft facilita estos vínculos únicamente para su comodidad y la inclusión de un vínculo no implica la aprobación por parte de Microsoft del sitio ni de ningún producto que contenga.

Microsoft puede ser titular de patentes, solicitudes de patentes, marcas comerciales, derechos de autor u otros derechos de propiedad intelectual sobre el contenido de este documento. A menos que se estipule expresamente por escrito en un contrato de licencia por escrito de Microsoft, el suministro de este documento no le otorga ninguna licencia sobre estas patentes, marcas, derechos de autor u otros derechos de propiedad intelectual.

© 2006 Microsoft Corporation. Reservados todos los derechos.

Microsoft, Encarta, FrontPage, Hotmail, MSN, Outlook, Windows Media y Windows son marcas registradas o marcas comerciales de Microsoft Corporation en EE.UU. y/o en otros países.

Todas las demás marcas comerciales pertenecen a sus respectivos propietarios.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Except as otherwise noted above, without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links are provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, *<The publications specialist places the list of trademarks provided by the copy editor here. Microsoft is listed first, followed by all other Microsoft trademarks in alphabetical order.>* are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

<The publications specialist inserts mention of specific, contractually obligated to, third-party trademarks, provided by the copy editor>

All other trademarks are property of their respective owners.

Tabla de contenido

Descripción general del curso

Información del curso

Módulo 1: Seguridad y privacidad de la computadora

Descripción general de la seguridad y la privacidad de la computadora

Protección de la computadora y los datos

Protección de toda la familia ante las amenazas de seguridad

Mantenimiento de la computadora segura y actualizada

Ética informática

Resumen del módulo

Glosario

Descripción general del curso

Una computadora es un dispositivo muy valioso e importante del que podría depender para muchas tareas que realiza a lo largo del día. Además, podría usarla para almacenar información personal u oficial que no puede permitirse perder. Sin embargo, la computadora y los datos que contiene pueden sufrir daños o ser destruidos. Por lo tanto, es fundamental que tome algunas medidas de protección para mantener su computadora segura y actualizada.

En este curso se describen algunas de las amenazas comunes a las que se enfrenta su computadora y cómo puede proteger su computadora y los datos que contiene contra estas amenazas.

Información del curso

En este curso se ofrece una descripción general de la seguridad y la privacidad de la computadora. Conocerá los tipos de amenazas a los que se enfrenta su computadora y aprenderá a protegerla de ellas. Asimismo, conocerá los problemas éticos que presentan la computadora e Internet, además de los aspectos legales del intercambio de información.

Detalles del curso	Descripción
Descripción del destinatario	El destinatario de este curso es cualquier persona que quiera poseer habilidades en tecnología digital.
Requisitos previos	Los alumnos deben poseer un nivel básico de comprensión lectora, suficiente como para leer un periódico local. Los alumnos deben haber finalizado el primer curso de Conceptos básicos sobre computadoras o tener conocimientos informáticos equivalentes.
Objetivos del curso	Cuando haya completado este curso, será capaz de: <ul style="list-style-type: none">• Explicar los principales riesgos a los que se expone el hardware y los datos a causa de un accidente, la avería de un dispositivo, el entorno, un error humano o actos malintencionados.• Tomar medidas para minimizar estos riesgos.
Más información	Para obtener más información, consulte el sitio Web de Microsoft Learning (http://go.microsoft.com/fwlink/?LinkId=34834) .

Lección 1

Descripción general de la seguridad y la privacidad de la computadora

Contenido de la lección

	Introducción a la seguridad y la privacidad de la computadora
	Introducción a las amenazas para las computadoras y sus soluciones
	Juego Ordenar elementos: Amenazas para las computadoras y sus soluciones
	Autoevaluación

Introducción a la lección

Los documentos importantes, como los fiscales, suele almacenarlos de forma segura con el fin de que no se pierdan o estropeen. También se asegura de que nadie tenga acceso a ellos sin permiso.

Si usa computadoras con asiduidad, es posible que tenga mucha cantidad de información almacenada en ellas. Esta información puede ser datos fiscales, cartas personales o correspondencia comercial. Es necesario asegurarse de que otras personas no consultan esta información sin su permiso. Y también debemos protegerla de posibles daños.

En esta lección, aprenderá por qué es necesario proteger el hardware, el software y los datos electrónicos de su computadora ante posibles daños, pérdidas y robos. También conocerá las distintas soluciones y dispositivos que puede usar para proteger los datos de su computadora.

Objetivos de la lección

Cuando haya completado esta lección, será capaz de:

- Explicar el significado de los términos seguridad y privacidad con respecto a la informática.
- Identificar las distintas amenazas existentes en el mundo de las computadoras y las correspondientes soluciones.

Cualquier factor que pueda dañar la computadora o los datos que contiene supone una amenaza para ella. Existen distintos tipos de amenazas para las computadoras. Los desastres naturales, tales como terremotos o huracanes, pueden causar un daño físico generalizado. También puede ocurrir que el usuario u otra persona elimine por error archivos importantes, lo que puede causar el mal funcionamiento de la computadora. Si la computadora está conectada a una red, se volverá incluso más vulnerable a las amenazas. Por ejemplo, otro usuario podría usar la red para obtener acceso no autorizado a su computadora.

Existen varias medidas que puede tomar para reducir estas amenazas y la posibilidad de sufrir pérdidas causadas por un daño. Por ejemplo, puede restringir el acceso a su computadora y crear copias de seguridad de los datos importantes, que podría usar si éstos se eliminan o alteran. Siguiendo algunas instrucciones básicas, puede minimizar los riesgos de que se produzcan daños en su computadora, y garantizar su seguridad y privacidad.

Seguridad de la computadora

El hardware de la computadora puede sufrir daños a causa de un error humano o desastres naturales, como terremotos, inundaciones y huracanes. Asimismo, es necesario proteger los datos y el software de la computadora ante posibles pérdidas y alteraciones, ya sean accidentales o intencionadas. La seguridad de la computadora está relacionada con las medidas que se pueden tomar para evitar estos daños, tanto en la computadora como en sus datos.

Privacidad de la computadora

En su computadora almacena documentos o archivos personales que no desearía que nadie leyera. La privacidad de la computadora implica que ninguna persona sin su permiso puede obtener acceso a sus datos, tales como mensajes de correo electrónico y archivos personales. La privacidad de la computadora está relacionada con las medidas que puede tomar para restringir el acceso a sus datos. También implica tener especial cuidado a la hora de proporcionar cualquier información personal a través de Internet. Podría hacerse un mal uso de ella para obtener acceso a sus cuentas personales, como cuentas bancarias o de correo electrónico.

Existen distintas amenazas a las que se enfrentan las computadoras y los datos almacenados en ellas. Por ejemplo, puede que alguien intente robar el hardware de su computadora o puede que algunos de sus componentes resulten dañados debido a calor o frío excesivos. Estas amenazas se pueden clasificar en tres categorías principales: amenazas naturales o ambientales, amenazas humanas malintencionadas y amenazas humanas no malintencionadas. En la siguiente tabla se enumeran las distintas amenazas que afectan a la seguridad y la privacidad de la computadora. También se describen las medidas que se pueden tomar para proteger los datos y la computadora de estas amenazas.

Amenazas naturales o ambientales

Elemento	Descripción
Categoría	<p>Algunas de las principales amenazas naturales y ambientales para las computadoras son las siguientes:</p> <ul style="list-style-type: none"> • Desastres naturales, como inundaciones, terremotos y huracanes: estos desastres pueden llegar a causar una destrucción masiva. Las computadoras de la zona afectada pueden sufrir importantes daños físicos, incluyendo generalmente la pérdida total de los datos. • Incendios: los incendios pueden dañar las computadoras de manera permanente. Incluso si el fuego no alcanza directamente a la computadora, el calor provocado es suficiente para fundir los delicados componentes de su interior. Además, el humo contiene unas partículas diminutas que pueden dañar la computadora, especialmente el disco duro. • Calor o frío extremos: la mayoría de los componentes internos de una computadora están diseñados para funcionar dentro de un intervalo específico de temperatura. En el caso de producirse calor o frío excesivos, es posible que algunos de ellos empiecen a funcionar incorrectamente y sea necesario sustituirlos. Si la computadora estuvo en el exterior y se expuso a temperaturas extremas, deje que vuelva a adquirir la temperatura ambiente antes de encenderla. • Problemas de voltaje (sobrevoltaje/picos): el sobrevoltaje o los picos son un aumento repentino del voltaje de alimentación que puede dañar permanentemente algunos de los componentes de la computadora. Por ejemplo, un aumento repentino del voltaje puede destruir la placa base de la computadora. El sobrevoltaje puede producirse por un rayo que cae con una gran cantidad de carga eléctrica. Esta carga se transmite por las líneas telefónicas o eléctricas hasta la computadora y daña sus componentes internos.
Solución	<p>Las computadoras requieren condiciones ambientales óptimas para funcionar correctamente. Éstas son algunas de las medidas que puede tomar para proteger su computadora de las amenazas naturales y ambientales, y minimizar los daños causados por éstas:</p> <ul style="list-style-type: none"> • Realizar copias de seguridad de los datos: implica crear varias copias de los

	<p>datos. Los desastres, como inundaciones y terremotos, pueden producirse sin aviso. Los datos siempre son únicos e insustituibles. Si crea una copia de seguridad, podrá recuperar los datos en caso de que se pierdan. Para disponer de una mayor capacidad de recuperación, intente mantener una copia de los datos importantes en una ubicación física distinta, como otro edificio o ciudad.</p> <ul style="list-style-type: none"> • Instalar las computadoras en ubicaciones seguras: instale la computadora en un lugar donde no sea probable que sufra daños por factores ambientales. Por ejemplo, evite instalarla en salas que estén expuestas a un exceso de polvo o humedad. • Controlar el entorno operativo: debe mantener un nivel de temperatura y humedad óptimo para garantizar el correcto funcionamiento de la computadora. Puede hacerlo si instala determinados dispositivos, como aparatos de aire acondicionado o controladores de humedad. • Protección contra sobrevoltaje y acondicionamiento de la línea: use determinados dispositivos, como protectores contra sobrevoltaje y acondicionadores de línea, que conectan la computadora con la fuente de alimentación. Esta conexión ofrece protección ante el sobrevoltaje o los picos de la línea eléctrica. No obstante, si se produce un fuerte sobrevoltaje, sigue existiendo el riesgo de que se produzcan daños y, por lo tanto, es fundamental mantener copias de seguridad de los datos importantes. Si hay una fuerte tormenta, debe apagar la computadora y desconectarla de la red eléctrica para evitar posibles daños causados por un rayo. • Sistema de alimentación ininterrumpida (SAI): instale dispositivos, como un SAI, que puedan proporcionar una alimentación ininterrumpida a la computadora. Un SAI ofrece una batería de reserva en caso de que se produzca una interrupción del suministro eléctrico. De este modo, se evitan posibles daños en el software a causa de un apagado repentino de la computadora. Un SAI también ofrece características integradas de protección contra sobrevoltaje y acondicionamiento de la línea.
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Amenazas humanas (malintencionadas)

Elemento	Descripción
Categoría	<p>A continuación, se enumeran algunos ejemplos de amenazas humanas malintencionadas:</p> <ul style="list-style-type: none"> • Empleados descontentos: un empleado de su oficina que esté descontento puede intentar deliberadamente alterar o destruir los datos de su computadora. • Piratas informáticos: un <i>pirata informático</i> es una persona que intenta obtener acceso de forma ilegal a su computadora cuando se conecta a Internet. Una vez que logra obtener acceso, puede robar o dañar los datos almacenados en ella. • Robo físico: cualquier persona puede robar su computadora o sus componentes si tiene acceso a ella. Con la popularidad adquirida por las computadoras portátiles, el robo físico de computadoras se convirtió en un hecho muy habitual. • Robo virtual: puede llegar a convertirse en una víctima del robo virtual, algo también más común en el caso de computadoras conectadas a Internet. Un

	<p>ejemplo de robo virtual es el <i>robo de identidad</i>, donde un pirata informático puede robar su información personal para usurpar su identidad. Con esta identidad falsa, el pirata informático puede obtener acceso a sus recursos financieros o realizar alguna actividad ilegal. Otro ejemplo de robo virtual es la <i>piratería de software</i>, que hace referencia al robo de un programa o diseño informático. También puede hacer referencia a la distribución y el uso no autorizados de un programa informático.</p>
Programa	<p>Ciertas personas malintencionadas pueden dañar los datos almacenados en su computadora mediante programas creados especialmente para este fin. Algunos ejemplos de estos programas son los siguientes:</p> <ul style="list-style-type: none"> • Virus, gusanos y caballos de Troya: los <i>virus</i> son programas informáticos que pueden dañar los datos o el software de una computadora, o robar la información almacenada en ella. Estos virus pueden llegar a la computadora, sin su conocimiento, a través de Internet o de dispositivos de almacenamiento, como disquetes y CD-ROM. Algunos virus están diseñados para crear ataques contra otras computadoras. Los <i>gusanos</i> son virus que se replican una vez que atacan una computadora, lo que dificulta su eliminación. Un <i>caballo de Troya</i> es otro tipo de virus que se oculta como un programa de software útil, por ejemplo un juego o una herramienta. Una vez que un caballo de Troya llega a la computadora, comienza a actuar como un virus y causa daños en los datos almacenados en ella. • Spyware: son programas que se instalan en su computadora sin su conocimiento. Pueden enviar en secreto información sobre sus hábitos de exploración del Web u otros detalles personales a otras computadoras a través de la red. • Fraudes en Internet: cuando se usa Internet se pueden recibir algunas ofertas atractivas a través de mensajes de correo electrónico o conversaciones de salones de chat. Debe tener mucho cuidado a la hora de aceptar alguna de estas ofertas, ya que pueden formar parte de fraudes planeados que pueden causarle pérdidas económicas. • Depredadores en línea: son individuos que atraen a cualquier persona que esté en línea para mantener relaciones inapropiadas y poco éticas. El usuario o su familia pueden convertirse en víctimas de los depredadores en línea. Estos depredadores establecen contacto con sus víctimas mediante el correo electrónico o los salones de chat.
Solución	<p>A continuación, se enumeran algunas medidas que puede tomar para minimizar los riesgos asociados con amenazas humanas malintencionadas:</p> <ul style="list-style-type: none"> • Almacenamiento de datos en ubicaciones seguras: guarde sus datos en ubicaciones seguras que tengan acceso limitado para otras personas. De este modo, minimizará la posibilidad de robo o alteración de los datos. Windows XP Service Pack 2 ofrece el cifrado a nivel de carpeta. El cifrado de las carpetas da como resultado la codificación de sus datos. De este modo, se puede evitar el acceso no autorizado a los mismos. • Protección contra virus y spyware: existen algunas medidas básicas que se pueden tomar para reducir la amenaza de virus y de spyware. Debe tener

	<p>precaución al abrir un archivo adjunto de un mensaje de correo electrónico o instalar un programa de software desde un sitio Web. Las características integradas en el software de correo electrónico, como Microsoft® Office Outlook® 2003, permiten bloquear mensajes de correo electrónico no deseado y comprobar la existencia de virus y gusanos. La forma más eficaz de instalar software antivirus y anti spyware es hacerlo mediante un proveedor de confianza. Estos programas de software permiten comprobar la existencia de virus y de spyware en la memoria de la computadora, además de evitar la entrada de otros nuevos. También es necesario actualizar el software antivirus y anti spyware con regularidad para que pueda reconocer nuevos virus y spyware. La mayoría de este tipo de software ofrecen actualizaciones automáticas que instalan automáticamente la versión actualizada del software en la computadora.</p> <ul style="list-style-type: none"> • Firewall: la instalación de un firewall es otra medida eficaz que puede tomar para proteger su computadora de amenazas malintencionadas. Un <i>firewall</i> permite filtrar el tráfico de Internet antes de que llegue a una computadora o una red privada. Ofrece asimismo protección adicional contra amenazas, como piratas informáticos y virus. Un firewall ayuda además a garantizar la privacidad de la computadora, ya que restringe el acceso externo a la computadora por parte de algún usuario no autorizado.
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Amenazas humanas (no malintencionadas)

Elemento	Descripción
Categoría	<p>A continuación, se enumeran algunos ejemplos de amenazas humanas no malintencionadas:</p> <ul style="list-style-type: none"> • Errores humanos: muchas veces, los daños producidos en una computadora se deben a un error humano no intencionado. Por ejemplo, puede que elimine por error un archivo importante que provoque el mal funcionamiento de la computadora. • Daños en el hardware: debido a que los componentes de la computadora son muy delicados, corren el riesgo de sufrir daños por algún descuido. Por ejemplo, si la computadora portátil se cae accidentalmente, podría causar daños a los componentes de hardware, como la placa base o el CD ROM. En consecuencia, perdería los datos almacenados en la computadora.
Solución	<p>A continuación, se describen las medidas que puede tomar para proteger su computadora de las amenazas humanas no malintencionadas y minimizar los daños causados por éstas:</p> <ul style="list-style-type: none"> • Proteger el hardware de daños accidentales y ambientales: puede tomar varias medidas para evitar cualquier daño no intencionado en la computadora. Coloque la computadora en una zona sin polvo ni vibraciones y que esté fuera del alcance de posibles golpes. El lugar donde coloque la computadora debe estar bien ventilado para evitar cualquier daño debido al calor. Mantenga la computadora alejada de cualquier sustancia magnética, agua o descarga estática. Por ejemplo, no coloque la computadora en el suelo ni sobre una

alfombra. Use un regulador de voltaje para evitar daños eléctricos. Evite comer y beber cerca del teclado, y use una funda protectora para protegerlo de posibles derrames. La mesa o estante de la computadora debe ser firme y estable para evitar que la computadora se caiga, incluso si recibe un golpe.

- **Realizar copias de seguridad de los datos:** realice copias de seguridad de los datos importantes de la computadora con regularidad. Si crea varias copias de los datos, podrá protegerlos de posibles pérdidas causadas por borrado o destrucción accidentales.

Tema:**Juego Ordenar elementos: Amenazas para las computadoras y sus soluciones de la lección: Descripción general de la seguridad y la privacidad de la computadora**

Ordene los tipos de soluciones en sus categorías correspondientes escribiendo el número de frase en el cuadro de opción pertinente.

Frase	
1	Inundaciones y huracanes
2	Temperaturas muy elevadas
3	Daños fortuitos en el hardware
4	Sobrevoltaje
5	Robo virtual
6	Piratas informáticos
7	Virus y spyware
8	Robo de hardware
9	Rayos
10	Errores humanos
11	Fraudes

Opción 1	Opción 2	Opción 3
Amenazas ambientales	Amenazas malintencionadas	Amenazas no malintencionadas

Nota: las respuestas correctas se muestran en la siguiente página.

Opción 1		Opción 2		Opción 3
Amenazas ambientales		Amenazas malintencionadas		Amenazas no malintencionadas
9, 4, 2, 1		11, 8, 7, 6, 5		10, 3

Pregunta 1

¿Cuál de las siguientes afirmaciones describe de mejor manera la privacidad de la computadora?

Seleccione la respuesta correcta.

<input type="checkbox"/>	Proteger una computadora de incendios y terremotos
<input type="checkbox"/>	Proteger una computadora del sobrevoltaje
<input type="checkbox"/>	Evitar que un amigo vea los datos de su computadora sin su permiso
<input type="checkbox"/>	Evitar que se eliminen por error archivos importantes de la computadora

Pregunta 2

¿Cuál de las siguientes medidas de seguridad puede adoptar para proteger mejor su computadora y sus datos de las amenazas naturales o ambientales?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Protección contra sobrevoltaje
<input type="checkbox"/>	Software antivirus
<input type="checkbox"/>	Firewall
<input type="checkbox"/>	Control de humedad

Nota: las respuestas correctas se muestran en la siguiente página.

Respuesta 1

¿Cuál de las siguientes afirmaciones describe de mejor manera la privacidad de la computadora?

Seleccione la respuesta correcta.

<input type="checkbox"/>	Proteger una computadora de incendios y terremotos
<input type="checkbox"/>	Proteger una computadora del sobrevoltaje
<input type="checkbox"/>	Evitar que un amigo vea los datos de su computadora sin su permiso
<input type="checkbox"/>	Evitar que se eliminen por error archivos importantes de la computadora

Respuesta 2

¿Cuál de las siguientes medidas de seguridad puede adoptar para proteger mejor su computadora y sus datos de las amenazas naturales o ambientales?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Protección contra sobrevoltaje
<input type="checkbox"/>	Software antivirus
<input type="checkbox"/>	Firewall
<input type="checkbox"/>	Control de humedad

Lección 2

Protección de la computadora y los datos

Contenido de la lección

	Protección del entorno operativo y los datos de la computadora
	Protección de las transacciones en línea y en red
	Seguridad del correo electrónico y la mensajería instantánea
	Juego Ordenar elementos: Medidas para proteger la computadora y los datos
	Autoevaluación

Introducción a la lección

Para tener acceso a su caja de seguridad del banco, necesita proporcionar su identificación. Esta identificación sirve para garantizar que nadie más pueda tener acceso a sus pertenencias.

De igual modo, es posible implementar distintas medidas de seguridad para minimizar la amenaza a la que se enfrenta su computadora y los datos que contiene. Esta lección es una introducción a algunas recomendaciones comunes que le ayudarán a proteger el sistema operativo, el software y los datos de su computadora.

Objetivos de la lección

Cuando haya completado esta lección, será capaz de:

- Identificar distintos métodos comunes para proteger el sistema operativo, el software y los datos de su computadora.
- Identificar las distintas formas de proteger las transacciones en línea y en red.
- Identificar las medidas comunes para proteger las transacciones de mensajería instantánea y correo electrónico.

Imagine que guardó un informe de un proyecto confidencial en su computadora. Estuvo trabajando durante semanas para preparar este informe y ahora desea compartirlo con su supervisor. Sólo tiene una copia en su computadora y es importante proteger el informe de cualquier alteración o eliminación. Sin embargo, otro empleado usa su computadora mientras está ausente y elimina el informe del proyecto de su computadora. Para evitar este tipo de situaciones, puede tomar medidas para proteger los datos de su computadora.

En la siguiente tabla se describen las medidas que puede tomar para proteger el entorno operativo y los datos de su computadora.

La siguiente tabla contiene la transcripción de una animación en línea.

Implementar la identificación de usuario

Una forma eficaz de minimizar el riesgo de los datos y el entorno operativo es impedir que aquellas personas no autorizadas tengan acceso a la computadora.

Para conseguirlo, se pueden configurar cuentas para los usuarios autorizados de la computadora, según las cuales cada usuario obtendrá un nivel de acceso apropiado.

Por ejemplo, en Microsoft® Windows® XP Service Pack 2 puede configurar cuentas de usuario para cada uno de los miembros de la familia u otros usuarios.

También podrá decidir si se asignará más privilegios a usted mismo o, si se trata de una cuenta para un menor, limitará las funciones de dicha cuenta.

La siguiente tabla contiene la transcripción de una animación en línea.

Establecer un nombre de usuario y contraseña

Del mismo modo, puede aumentar la seguridad y limitar el acceso no autorizado a la computadora si configura un nombre de usuario y una contraseña. En casi todas las oficinas, cada empleado tiene un nombre de usuario y una contraseña exclusivos que deben proporcionar para tener acceso a las computadoras. En Microsoft Windows se pueden configurar nombres de usuario y contraseñas.

La siguiente tabla contiene la transcripción de una animación en línea.

Mantener las contraseñas seguras



Una contraseña actúa como una clave para poder usar una computadora. Por lo tanto, cualquier persona que conozca la contraseña podrá tener acceso a la computadora y alterar los datos.

La contraseña debe permanecer segura. Tenga cuidado al escribir la contraseña para evitar que otros puedan verla, y no la comparta con otras personas.

No anote la contraseña ni la deje sobre la computadora o el escritorio. Si cree que la contraseña ya no es segura, cámbiela de inmediato antes de que cualquiera haga un mal uso de ella.

La siguiente tabla contiene la transcripción de una animación en línea.

Bloquear la computadora



Cuando deja la computadora encendida y sin supervisión, alguien puede alterar el software y los datos de la computadora. Esto puede evitarse si bloquea temporalmente la computadora mientras no la usa.

Cuando una computadora se bloquea, inmediatamente se oculta el contenido de la pantalla y no se permite que se realice ninguna operación hasta que se desbloquee mediante la combinación correcta de nombre de usuario y contraseña.

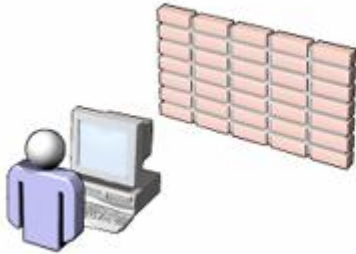
Los pasos exactos necesarios para bloquear una computadora varían según el sistema operativo que use. Por ejemplo, en Windows XP Service Pack 2 la computadora se bloquea presionando CTRL+ALT+SUPR y, a continuación, haciendo clic en el botón Bloquear equipo del cuadro Seguridad de Windows.

Tenga en cuenta que la característica de bloqueo de computadoras no está disponible en todos los sistemas operativos.

La siguiente tabla contiene la transcripción de una animación en línea.

Curso: Seguridad y privacidad de la computadora

Instalar software protector



Una computadora debe protegerse continuamente de amenazas como los virus y el spyware. En ocasiones, el daño que un virus puede causar es considerable y puede hacer que pierda datos importantes o que tenga que volver a instalar el sistema operativo y otro tipo de software. Para proteger la computadora de virus y de spyware deberá instalar un software antivirus y anti spyware. Estos programas de software protectores sirven para detectar y eliminar los virus y spyware que hay en la computadora, así como para evitar que ésta vuelva a infectarse. Es conveniente instalar un firewall, que filtra el contenido que llega a la computadora. Con un firewall la computadora también estará protegida frente a los piratas informáticos, ya que restringe el acceso de otros usuarios en línea.

La siguiente tabla contiene la transcripción de una animación en línea.

Cifrar los datos

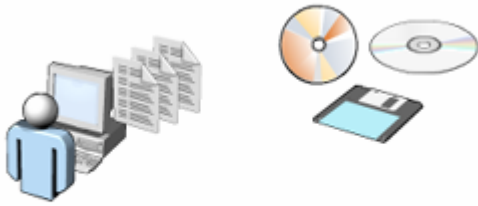


Se llama cifrado a la conversión de los datos a un formato ilegible para protegerlos del acceso no autorizado. Un usuario autorizado puede volver a convertir los datos cifrados a un formato legible y que se pueda usar. Esto se conoce como descifrado.

Actualmente, varios productos de software incorporan una forma de cifrar datos. En el caso de Windows XP Service Pack 2, el cifrado es transparente para el usuario que cifra el archivo; esto quiere decir que no tendrá que descifrar el archivo manualmente para poder usarlo, sino que simplemente podrá abrirlo y modificarlo de la forma habitual.

La siguiente tabla contiene la transcripción de una animación en línea.

Realizar una copia de seguridad de los datos



También podrá impedir que los archivos se pierdan o sufran daños, si hace copias de los archivos importantes y los almacena en un medio de almacenamiento distinto, como un CD, un DVD o un disquete.

Este proceso se denomina copia de seguridad de datos. Las copias de seguridad deben conservarse en ubicaciones seguras, con el fin de poder usar estos datos en caso de que los originales se pierdan o dañen.

La siguiente tabla contiene la transcripción de una animación en línea.

Mantener la computadora actualizada



A medida que surgen nuevas amenazas, las compañías de software crean periódicamente actualizaciones que se pueden instalar en la computadora.

Estas actualizaciones complementan el software o el sistema operativo ya instalado en la computadora para disminuir la vulnerabilidad frente a las amenazas de seguridad.

Asegúrese de actualizar el software antivirus con regularidad para que pueda detectar la presencia de nuevos virus.

La conexión de una computadora a Internet supone su entrada en un mundo de información y entretenimiento. No obstante, también hace que su computadora sea vulnerable a las distintas amenazas en línea. Por ejemplo, los virus podrían pasar más fácilmente de una computadora infectada a la suya. Es posible reducir los riesgos de estas amenazas en línea combinando varias recomendaciones, como la creación de contraseñas seguras, el cifrado de datos y el uso de un software antivirus.

En la siguiente tabla se describen las distintas medidas que puede tomar para proteger las transacciones en línea y en red.

Medida	Descripción	
Usar contraseñas seguras	<p>Una contraseña segura es una contraseña compleja que no se puede averiguar fácilmente. La contraseña debe contener una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, como el símbolo de <i>Y comercial</i> y el <i>signo de número</i>, y no puede contener palabras ni nombres completos.</p> <p>Una contraseña segura es su principal defensa ante las amenazas de seguridad y privacidad. Las contraseñas seguras deben crearse para:</p> <ul style="list-style-type: none"> • El acceso local a computadoras independientes • El acceso a redes • El acceso a sitios Web que tienen información confidencial, como detalles personales o financieros • El acceso a cualquier dato importante • Los datos personales almacenados en su computadora 	
Proteger la computadora de piratas informáticos y spyware	<p>Mientras navega por Internet, es posible que un programa de software instalado en su computadora esté transmitiendo su información personal a un pirata informático en otro país. Estos programas son ejemplos de spyware. Por lo general, se instalan en su computadora sin que lo sepa y transfieren datos confidenciales en secreto desde su computadora a los piratas informáticos. En algunas ocasiones, las empresas instalan spyware en las computadoras usadas por los empleados para realizar un seguimiento de sus actividades informáticas.</p> <p>Puede instalar en su computadora programas de software como Microsoft Defender para evitar que el spyware se instale en ella de forma inadvertida.</p>	

	<p>También debe instalar un software antivirus y un firewall en la computadora para protegerla de virus y piratas informáticos.</p>	
<p>Borrar el historial y la memoria caché regularmente</p>	<p>Los sitios y las páginas Web que visita mientras navega por Internet se guardan en el <i>historial</i> del explorador. También se almacenan algunos archivos en la memoria temporal de su computadora. Esta memoria temporal se conoce como <i>memoria caché</i>. Los archivos almacenados en esta memoria registran información de las páginas Web que se visitan.</p> <p>No obstante, algunos de estos archivos temporales de Internet pueden contener información personal, como su nombre de usuario y contraseña, a la que podrían tener acceso los piratas informáticos. Para evitar que estos piratas tengan acceso a su información personal, elimine el contenido del historial del explorador y la memoria caché con cierta regularidad.</p>	
<p>Eliminar cookies regularmente</p>	<p>Al visitar un sitio Web, puede que su nombre aparezca en él. Esto es posible gracias al uso de <i>cookies</i>, que son pequeños archivos creados en su computadora por los sitios Web visitados previamente para identificar y realizar un seguimiento de sus preferencias. Su finalidad es ofrecer una experiencia más personal al visitar un sitio Web. No obstante, las cookies también pueden suponer una amenaza para la privacidad de la computadora, ya que contienen información personal. Por ejemplo, las cookies podrían contener los detalles de la tarjeta de crédito que usó al realizar compras en línea. Por estos motivos, se recomienda eliminar las cookies regularmente para evitar un mal uso de su información personal.</p>	
<p>Evitar compartir información personal</p>	<p>Algunos sitios Web requieren que se rellenen formularios donde se solicita información personal, como el nombre, el sexo y la edad. En los sitios de comercio electrónico, incluso podría tener que compartir los detalles de su cuenta bancaria o el número de su tarjeta de crédito. No obstante, no olvide que los piratas informáticos pueden tener acceso a esta información y hacer un mal uso de ella. Algunas compañías podrían usar también esta información para enviarle mensajes de correo electrónico comerciales no deseados. Por ello, antes de compartir cualquier información personal en un sitio Web, asegúrese de que se trata de un sitio seguro y de que es</p>	

	estrictamente necesario proporcionar la información.	
Asegurarse de que las transacciones en línea se realizan en sitios seguros	<p>Al realizar compras en línea, normalmente debe proporcionar información confidencial, como el número de su cuenta bancaria o los detalles de su tarjeta de crédito. Por lo tanto, es muy importante asegurarse de que sólo se realizan transacciones en línea en sitios Web seguros. Un sitio Web es seguro si su nombre tiene el prefijo <i>https</i>. Este prefijo indica que el sitio Web implementa el protocolo <i>Capa de sockets seguros (SSL)</i>. SSL es un protocolo de seguridad de Internet que garantiza una comunicación de datos segura mediante el cifrado de la información transmitida. El protocolo SSL certifica que el sitio Web es genuino y garantiza que no se hará un mal uso de los datos proporcionados en él.</p> <p>Cuando se obtiene acceso a un sitio Web seguro, la mayoría de los exploradores Web muestran un mensaje para confirmar que se obtuvo acceso a un sitio Web seguro. El icono de candado cerrado de la parte inferior derecha de la pantalla del explorador también ayuda a identificar un sitio Web seguro. Además, se puede comprobar el certificado de seguridad de un sitio Web antes de realizar una transacción en línea en dicho sitio.</p>	
Configurar los componentes de seguridad mediante el Centro de seguridad de Windows	<p>El Centro de seguridad de Windows es una característica de Windows XP Service Pack 2 que ofrece una cómoda herramienta para comprobar el estado de la configuración de seguridad esencial y realizar un seguimiento del software antivirus instalado en la computadora. Puede abrir el Centro de seguridad desde el Panel de control. Este centro tiene tres componentes principales:</p> <ul style="list-style-type: none"> • Firewall de Windows: debe habilitar el firewall antes de conectarse a Internet. El firewall ayuda a evitar que cualquier contenido malintencionado, como virus y gusanos, tenga acceso a su computadora. También evita que los piratas informáticos obtengan acceso a ella. • Actualizaciones automáticas: esta característica busca las actualizaciones de seguridad relevantes disponibles en el sitio Web de Microsoft Windows Update. A continuación, descarga e instala automáticamente las actualizaciones en la computadora. Al habilitar esta característica 	

	<p>garantiza que su computadora permanecerá actualizada y protegida frente a las nuevas amenazas de seguridad de Internet.</p> <ul style="list-style-type: none"> • Opciones de Internet: en el Centro de seguridad puede configurar las opciones de Internet para su computadora. Con estas opciones puede establecer el nivel de seguridad en bajo, medio o alto. Si cambia el nivel de seguridad, afectará al modo en que su explorador maneja algunos archivos de Internet, como las cookies y el contenido activo. También puede restringir el tipo de contenido que llega a su computadora a través de Internet. 	
Deshabilitar el contenido activo	<p>El <i>contenido activo</i> hace referencia a pequeños programas que se instalan en su computadora mientras navega por Internet. Su función principal es ofrecer una experiencia de Internet interactiva a través de vídeos y barras de herramientas. Sin embargo, en algunos casos, estos programas pueden usarse para ocasionar daños en los datos almacenados en la computadora o instalar software malintencionado sin su consentimiento. Con las opciones del explorador, puede deshabilitar el contenido activo para evitar que su computadora sufra daños.</p>	
Usar la ayuda de seguridad que le ofrece su ISP	<p>Use el soporte del proveedor de servicios Internet (ISP) para la seguridad en línea. Este soporte puede ofrecerse como software antivirus y anti spyware. Algunos ISP ofrecen incluso protección de firewall, filtrado de virus en correo electrónico y protección contra correo electrónico no deseado.</p>	

El correo electrónico y la mensajería instantánea (MI) se usan de forma generalizada en la comunicación personal y empresarial. Sin embargo, los piratas informáticos, depredadores en línea e individuos que crean gusanos y virus, usan el correo electrónico y la mensajería instantánea con fines malintencionados. Por ejemplo, estas personas pueden enviar archivos adjuntos de correo electrónico con software malintencionado. También pueden usar el correo electrónico para solicitar información confidencial o para atraerle hacia ofertas falsas. Por lo tanto, es importante que tome ciertas medidas para garantizar la seguridad del correo electrónico y la mensajería instantánea.

Para garantizar la seguridad del correo electrónico, evite abrir los mensajes con archivos adjuntos, no responda al correo no deseado, no responda al correo comercial no solicitado y protéjase de la suplantación de identidad. Para garantizar la seguridad de la mensajería instantánea, charle sólo con personas que conozca y no abra archivos adjuntos que reciba a través de mensajería instantánea. En la siguiente tabla se describen las medidas que garantizan la seguridad del correo electrónico y la mensajería instantánea.

La siguiente tabla contiene la transcripción de una animación en línea.

Evitar abrir los mensajes de correo electrónico con archivos adjuntos

Puede enviar archivos adjuntos en los correos electrónicos para compartirlos con sus amigos. Del mismo modo, puede recibir una fotografía o un archivo de música como archivo adjunto en un mensaje de correo electrónico.

Sin embargo, debe tener cuidado al abrir un correo con un archivo adjunto, dado que es una de las vías más comunes para que un virus se propague.

La siguiente tabla contiene la transcripción de una animación en línea.

No responder al correo no deseado

Es posible que reciba mensajes de correo electrónico irrelevantes o que no desee procedentes de remitentes desconocidos. Estos mensajes reciben el nombre de correo no deseado.

Se recomienda no responder a los remitentes de tales mensajes, ya que el correo electrónico no deseado a menudo es de carácter malintencionado y puede incluir contenido dañino para la computadora. Los programas de correo electrónico, como Microsoft Outlook, incluyen una carpeta de correo electrónico no deseado en la que es posible almacenar todo el correo sospechoso.

La siguiente tabla contiene la transcripción de una animación en línea.

No responder al correo comercial no solicitado

Es posible que reciba mensajes de correo electrónico no solicitado de compañías que hacen publicidad de sus productos y servicios. Estos mensajes también pueden presentarse en forma de encuestas en línea en las que se solicita que incluya información personal.

No obstante, existe la posibilidad de que el fin de estos mensajes comerciales sea el robo de identidad y, respondiendo a ellos, puede estar compartiendo información confidencial sin saberlo. Por lo tanto, se aconseja no responder a estos mensajes no solicitados. También puede eliminarlos cuando los reciba.

La siguiente tabla contiene la transcripción de una animación en línea.

Protegerse de la suplantación de identidad

La suplantación de identidad es una actividad habitual que sirve para obtener información personal de los usuarios de computadoras con el fin de usarla posteriormente con fines malintencionados.

Por ejemplo, alguien le envía mensajes de correo electrónico fingiendo que proceden de un banco o de una organización de confianza y le pide información confidencial como el número de la tarjeta de crédito o la contraseña.

Esta información se venderá o se usará para causarle pérdidas económicas. Por lo tanto, debe comprobar la autenticidad de estos mensajes de correo electrónico antes de responder con cualquier tipo de información personal.

La siguiente tabla contiene la transcripción de una animación en línea.

Charlar sólo con personas conocidas

Debe restringir las conversaciones por chat únicamente a aquellas personas que conozca. Si se comunica con personas nuevas o desconocidas, resultará más vulnerable ante amenazas como los depredadores o los fraudes en línea.

La siguiente tabla contiene la transcripción de una animación en línea.

No abrir archivos adjuntos recibidos a través de mensajería instantánea

La mensajería instantánea es una forma muy habitual de recibir datos adjuntos malintencionados. Por lo tanto, debe evitar abrir cualquier archivo adjunto que reciba en un mensaje instantáneo, a menos que esté absolutamente seguro de su origen. Un archivo adjunto de mensajería instantánea podría contener un virus o spyware que pueden dañar la computadora.

Tema: Juego Ordenar elementos: Medidas para proteger la computadora y los datos

Ordene los tipos de soluciones en sus categorías correspondientes escribiendo el número de frase en el cuadro de opción pertinente.

Frase	
1	Establecer un nombre de usuario y contraseña
2	Usar una combinación de bloqueo
3	Visitar sitios Web seguros
4	Eliminar cookies regularmente
5	Realizar una copia de seguridad de los datos
6	Borrar la memoria caché

Opción 1		Opción 2
Protección de los datos de la computadora		Eliminación de las amenazas en línea

Nota: las respuestas correctas se muestran en la siguiente página.

Opción 1		Opción 2
Protección de los datos de la computadora		Eliminación de las amenazas en línea
5, 2, 1		6, 4, 3

Pregunta 1

Una de las formas más eficaces de proteger el software y los datos de una computadora es restringir su uso a un grupo definido de personas. ¿Cuál de los siguientes métodos puede usar para ello?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Actualizar el sistema operativo
<input type="checkbox"/>	Configurar cuentas de usuario.
<input type="checkbox"/>	Instalar software antivirus.
<input type="checkbox"/>	Mantener las contraseñas seguras.

Pregunta 2

Mientras usa Internet se crean varios tipos de archivo en su computadora. Algunos pueden suponer una amenaza para la seguridad, pero realmente su existencia es para beneficio del usuario. ¿Cuáles de los siguientes elementos son ejemplos de estos archivos?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Cookie
<input type="checkbox"/>	Virus
<input type="checkbox"/>	Archivos de contenido activo
<input type="checkbox"/>	Gusano

Pregunta 3

¿Cuáles de los siguientes métodos usará para proteger las transacciones de correo electrónico y mensajería instantánea?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Eliminar los mensajes de correo electrónico procedentes de remitentes desconocidos sin abrirlos.
<input type="checkbox"/>	Reenviar los mensajes de correo electrónico no solicitados a un amigo para pedirle opinión.
<input type="checkbox"/>	Contestar con información personal a un mensaje de correo electrónico si el remitente es un

	empleado del banco.
	Evitar abrir archivos adjuntos recibidos en mensajes instantáneos.

Nota: las respuestas correctas se muestran en la siguiente página.

Respuesta 1

Una de las formas más eficaces de proteger el software y los datos de una computadora es restringir su uso a un grupo definido de personas. ¿Cuál de los siguientes métodos puede usar para ello?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Actualizar el sistema operativo
<input type="checkbox"/>	Configurar cuentas de usuario.
<input type="checkbox"/>	Instalar software antivirus.
<input type="checkbox"/>	Mantener las contraseñas seguras.

Respuesta 2

Mientras usa Internet se crean varios tipos de archivo en su computadora. Algunos pueden suponer una amenaza para la seguridad, pero realmente su existencia es para beneficio del usuario. ¿Cuáles de los siguientes elementos son ejemplos de estos archivos?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Cookie
<input type="checkbox"/>	Virus
<input type="checkbox"/>	Archivos de contenido activo
<input type="checkbox"/>	Gusano

Respuesta 3

¿Cuáles de los siguientes métodos usará para proteger las transacciones de correo electrónico y mensajería instantánea?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Eliminar los mensajes de correo electrónico procedentes de remitentes desconocidos sin abrirlos.
<input type="checkbox"/>	Reenviar los mensajes de correo electrónico no solicitados a un amigo para pedirle opinión.
<input type="checkbox"/>	Contestar con información personal a un mensaje de correo electrónico si el remitente es un empleado del banco.
<input type="checkbox"/>	Evitar abrir archivos adjuntos recibidos en mensajes instantáneos.

Lección 3

Protección de toda la familia ante las amenazas de seguridad

Contenido de la lección

	Protección de la privacidad
	Depredadores en línea
	Instrucciones para proteger a toda la familia de los depredadores en línea
	Juego de los paneles: Protección de toda la familia ante los depredadores en línea
	Autoevaluación

Introducción a la lección

Las computadoras no se usan únicamente en los colegios, las escuelas y las oficinas, sino que también se usan habitualmente en los hogares. Se usan con distintas finalidades, como mantener las cuentas del hogar, intercambiar mensajes de correo electrónico con familiares y amigos, navegar por Internet y jugar o escuchar música. Todos los miembros de la familia pueden encontrarle alguna utilidad a la computadora.

Debido al uso cada vez mayor de las computadoras en el hogar y en el trabajo, es importante que todos comprendan las distintas amenazas asociadas con el uso de las computadoras e Internet. En esta lección, conocerá las distintas medidas que pueden ayudarle a proteger su computadora de estas amenazas.

Objetivos de la lección

Cuando haya completado esta lección, será capaz de:

- Identificar las medidas más habituales que se usan para proteger la privacidad.
- Explicar cómo actúan los depredadores en línea.
- Identificar los procedimientos para proteger a sus hijos de los depredadores en línea.

Con la creciente popularidad de las computadoras e Internet, su privacidad puede verse comprometida de varias formas. Todos los miembros de su familia deben evitar las amenazas que afectan a la privacidad. Puede tomar estas sencillas medidas para proteger a toda la familia de la invasión de la privacidad.

Proteja su identidad

Evite compartir información personal con cualquier persona, a menos que la conozca. Ésta es la regla de oro de la protección de la privacidad. Cuando intercambie mensajes de correo electrónico o charle a través de la mensajería instantánea, asegúrese de no revelar detalles personales acerca de su persona u otras personas que conozca. Use también contraseñas seguras para tener acceso a su computadora y conexiones de correo electrónico.

Realice copias de seguridad de su computadora y datos importantes con regularidad

Es aconsejable realizar copias de seguridad de todo tipo de datos importantes y confidenciales almacenados en la computadora. Estos datos podrían ser documentos, bases de datos o información de contacto. Puede usar varios medios de almacenamiento, como un disco compacto u otra unidad de disco duro, para realizar las copias de seguridad. Si realiza copias de seguridad de los datos contenidos en la computadora con regularidad, podrá recuperarlos en el caso de que los originales se pierdan o se dañen. También es aconsejable almacenar los datos de las copias de seguridad en un lugar seguro y restringir el acceso a ellos mediante contraseñas y cifrado.

Compruebe la seguridad de su sistema con regularidad

Compruebe el nivel de seguridad de su sistema con regularidad. Los sistemas operativos modernos tienen características integradas que permiten realizar un seguimiento de la capacidad de la computadora para protegerse de las distintas amenazas de seguridad y privacidad. Por ejemplo, el Centro de seguridad de Windows es un componente de Windows XP Service Pack 2 que le ayuda a mantener la configuración del firewall, programar las actualizaciones de software y comprobar la validez del software antivirus instalado en la computadora.

Ejecute detecciones de virus a diario

Cada día, cuando tiene acceso a Internet, existe la posibilidad de que su computadora se infecte con un virus. Por lo tanto, es importante que

ejecute una detección de virus en la computadora todos los días. También debe mantener el software antivirus de la computadora actualizado para protegerla de nuevos virus.

Use un programa anti spyware

Los programas spyware pueden obtener acceso a su computadora en secreto y transmitir información personal sobre el usuario o su familia. Use un software anti spyware que controle estos programas malintencionados y mantenga el software actualizado.

Realice las transacciones en línea en sitios seguros con proveedores acreditados

Al realizar una transacción en línea, debe proporcionar en el sitio Web cierta información personal, como los detalles de su tarjeta de crédito o su cuenta bancaria. Si esta información se revelara a otras personas, podría usarse para realizar un fraude económico. Por lo tanto, es muy importante realizar las transacciones en línea sólo en sitios Web seguros.

Comunique cualquier abuso al ISP

La mayoría de los ISP acreditados cuentan con términos y condiciones que no permiten a sus usuarios realizar ninguna práctica ilegal o poco ética. Debe comunicar al ISP si alguien intentó invadir su privacidad en línea, enviándole correo no deseado, o piratear su computadora. De este modo, el ISP podrá tomar medidas contra estas personas.

Filtre los mensajes de correo electrónico procedentes de remitentes desconocidos o anónimos

Es posible que reciba mensajes de correo electrónico de personas que no conoce. Estos mensajes, conocidos como correo no deseado, pueden ser muchas veces portadores de virus o spyware. Los piratas informáticos que intentan recuperar su información personal pueden también enviarle correo no deseado. Por lo tanto, es importante que tenga cuidado con este tipo de mensajes. Los programas de software de correo electrónico permiten crear filtros que le permitan bloquear el correo no deseado. También debe asegurarse de que nunca responde a correo no deseado, ya que puede hacer que aumenten los mensajes no deseados y comparta por error información personal.

Cifre los mensajes de correo electrónico confidenciales, si es posible

El cifrado es un modo fácil y eficaz de garantizar que sus comunicaciones por correo electrónico permanecen confidenciales. El cifrado es el proceso de codificar un mensaje de correo electrónico de tal manera que no sea legible para ninguna otra persona, excepto para el lector al que va dirigido.

<p>La mayoría del software de correo electrónico, como Outlook, ofrece esta característica de cifrado de correo.</p>	
----------------------------------------------------------------------------------------------------------------------	--

Internet es un medio de comunicación muy popular entre las personas de todo el mundo. Puede ponerse en contacto con una persona sin conocer realmente su identidad y sus intenciones. Algunas personas pueden hacer un mal uso de este aspecto de la comunicación por Internet para atraer a gente joven con el fin de mantener relaciones inapropiadas o peligrosas. Los individuos que se dedican a tales actividades se conocen como *depredadores en línea*.

Los depredadores en línea se dirigen normalmente a los menores, especialmente los adolescentes. Es en esa etapa cuando los jóvenes se van alejando poco a poco de los padres y buscan nuevas relaciones. Los depredadores en línea intentan establecer una relación de confianza e intimidad con ellos. Intentan atraer la atención de sus víctimas, como los menores, con el fin de establecer relaciones inapropiadas. No obstante, los menores no son las únicas víctimas de estos depredadores. También lo son los adultos, en este caso, con un fin de explotación económica.

Los depredadores atrapan a sus víctimas estableciendo contacto mediante los salones de chat, la mensajería instantánea, el correo electrónico o los paneles de discusión. De las diversas herramientas posibles, los salones de chat son las más usadas por estos depredadores. Normalmente adoptan una identidad falsa como miembro de un salón de chat específico. Por ejemplo, si el salón pertenece sólo a menores, un depredador podría adoptar fácilmente la identidad de un niño con el fin de participar en él.

Tema: Instrucciones para proteger a toda la familia de los depredadores en línea

Los miembros de su familia pueden convertirse en víctimas de los depredadores en línea. Estos depredadores pueden intentar establecer contacto con ellos para aprovecharse económicamente. También pueden intentar implicarles en relaciones inapropiadas.

En la siguiente tabla, se enumeran algunas instrucciones que puede seguir para proteger a toda su familia de los depredadores en línea.

Instrucciones	Descripción
Conocer el comportamiento de los depredadores	Los depredadores en línea tienen algunos comportamientos previsibles que pueden ayudarle a identificarlos fácilmente. Los depredadores en línea tienden a intimar con gran rapidez. Suelen expresar mucho interés y afecto hacia sus víctimas. Debe asegurarse de que los miembros de su familia puedan detectar este comportamiento para evitar el contacto con posibles depredadores en línea.
Sospeche de los regalos que le ofrezcan a través de Internet	Los depredadores en línea suelen atraer a sus víctimas con regalos u otras ofertas tentadoras. Debe tener cuidado con estos regalos u ofertas. Indique a los miembros de su familia que deben sospechar de los regalos que le ofrezcan a través de Internet.
Informe a su familia sobre las medidas de seguridad en línea	Infórmeles acerca del comportamiento adecuado en los salones de chat para evitar que se conviertan en víctimas de los depredadores en línea. Indíqueles que usen nombres de pantalla neutros y que no sean sugerentes. Los nombres de pantalla no deben revelar nunca el nombre, la edad, el sexo ni la información de contacto real, ya que se podría hacer un mal uso de estos datos.
Indique a su familia que no revele información personal	Algunos sitios Web intentan obtener información con el pretexto de que están recopilando opiniones o que se trata de una encuesta. Indique a su familia que no revele ninguna información personal en estos sitios Web sin su permiso. Asegúrese también de que su familia no proporcione ningún detalle personal (nombre, apellidos, dirección, número de teléfono) en los salones de chat y tableros de anuncios. Los miembros de su familia no deben compartir su nombre de usuario y contraseña con ninguna persona, ni siquiera los amigos.


Es aconsejable seguir algunas instrucciones más para proteger a sus hijos de los depredadores en línea. En la siguiente tabla se enumeran estas instrucciones adicionales.

Instrucciones	Descripción
Oriente a los menores cuando visiten sitios Web	Los padres deben restringir las visitas de los más jóvenes a los sitios Web que no sean apropiados para ellos, o aquellos que les pongan en contacto con posibles depredadores en línea. Es recomendable que orienten a sus hijos más pequeños cuando visiten un sitio Web.

<p>Conozca los sitios Web que visitan sus hijos</p>	<p>Es importante que los padres comprueben con regularidad el tipo de sitios Web que visitan sus hijos. Puede realizar un seguimiento de los sitios Web visitados anteriormente si consulta el historial del explorador o usa un software que le ayude a realizar un seguimiento de la actividad en línea de una computadora.</p>
<p>Bloquee el acceso a sitios Web inapropiados</p>	<p>Puede habilitar la característica Asesor de contenido del explorador para controlar el tipo de sitios Web que visitan los miembros de su familia al navegar por Internet. Con ella, puede restringir el acceso de menores de edad a sitios Web con contenido para adultos. También puede instalar ciertos programas de software que le ayuden a bloquear determinados sitios Web.</p>
<p>Controle las conversaciones por chat mantenidas en su computadora</p>	<p>Con un software especializado se pueden controlar las conversaciones por chat y marcar el intercambio de información inapropiada en su computadora. Puede instalar este tipo de software para realizar un seguimiento de las conversaciones por chat de sus hijos.</p>
<p>Indique a sus hijos que salgan de los sitios Web que sean desagradables</p>	<p>Los padres deben indicar a sus hijos que salgan de un sitio Web si les hace sentirse incómodos o si contiene algún tipo de contenido desagradable. Indíqueles también que lo hagan si en el sitio Web se les pide demasiada información personal.</p>

Cada pareja de frases contiene una verdadera y una falsa. Para cada pareja de frases, indique cuál es verdadera colocando una marca en la columna Verdadero de la derecha.

	Frase	Verdadero	Falso
1	NO ES SEGURO compartir información en un salón de chat.		
2	ES SEGURO compartir información en un salón de chat.		
3	Los depredadores en línea NO INTIMAN con gran rapidez.		
4	Los depredadores en línea INTIMAN con gran rapidez.		
5	Los padres NO NECESITAN conocer los sitios Web que sus hijos visitan.		
6	Los padres NECESITAN conocer los sitios Web que sus hijos visitan.		
7	Las conversaciones por chat SE PUEDEN controlar.		
8	Las conversaciones por chat NO SE PUEDEN controlar.		
9	Los sitios Web que los menores visitan SE PUEDEN restringir.		
10	Los sitios Web que los menores visitan NO SE PUEDEN restringir.		
11	Los depredadores en línea SE DIRIGEN a los menores.		
12	Los depredadores en línea NO SE DIRIGEN a los menores.		
13	Los menores NO DEBEN tener permiso para visitar sitios Web en solitario.		
14	Los menores DEBEN tener permiso para visitar sitios Web en solitario.		
15	Los depredadores en línea NO ATRAEN a sus víctimas con regalos.		
16	Los depredadores en línea ATRAEN a sus víctimas con regalos.		
17	NO ES SEGURO que un menor entre en un área de chat privada.		
18	ES SEGURO que un menor entre en un área de chat privada.		



Nota: las respuestas correctas se muestran en la siguiente página.

	Frase	Verdadero	Falso
1	NO ES SEGURO compartir información en un salón de chat.		
2	ES SEGURO compartir información en un salón de chat.		
3	Los depredadores en línea NO INTIMAN con gran rapidez.		
4	Los depredadores en línea INTIMAN con gran rapidez.		
5	Los padres NO NECESITAN conocer los sitios Web que sus hijos visitan.		
6	Los padres NECESITAN conocer los sitios Web que sus hijos visitan.		
7	Las conversaciones por chat SE PUEDEN controlar.		
8	Las conversaciones por chat NO SE PUEDEN controlar.		
9	Los sitios Web que los menores visitan SE PUEDEN restringir.		
10	Los sitios Web que los menores visitan NO SE PUEDEN restringir.		
11	Los depredadores en línea SE DIRIGEN a los menores.		
12	Los depredadores en línea NO SE DIRIGEN a los menores.		
13	Los menores NO DEBEN tener permiso para visitar sitios Web en solitario.		
14	Los menores DEBEN tener permiso para visitar sitios Web en solitario.		
15	Los depredadores en línea NO ATRAEN a sus víctimas con regalos.		
16	Los depredadores en línea ATRAEN a sus víctimas con regalos.		
17	NO ES SEGURO que un menor entre en un área de chat privada.		
18	ES SEGURO que un menor entre en un área de chat privada.		

Pregunta 1

¿Cuál de las siguientes medidas puede ayudarle a garantizar la privacidad en línea?

Seleccione la respuesta correcta.

<input type="checkbox"/>	En lugar de chats, usar mensajes de correo electrónico para compartir información personal.
<input type="checkbox"/>	Usar contraseñas seguras para tener acceso a las cuentas de correo electrónico.
<input type="checkbox"/>	Ejecutar una detección de virus siempre que crea que un virus infectó la computadora.
<input type="checkbox"/>	Abrir todos los mensajes de correo electrónico no solicitado para identificar a los remitentes antes de responder.

Pregunta 2

¿Cuál de las siguientes afirmaciones describe el modo en que operan los depredadores en línea?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Ofrecen a los menores más atención y afecto.
<input type="checkbox"/>	Intentan infectar su computadora con virus.
<input type="checkbox"/>	Atraen a los menores para mantener relaciones inapropiadas.
<input type="checkbox"/>	Atraen a los menores para que compren un producto.

Pregunta 3

¿Cuáles son algunas de las medidas que los padres pueden tomar para proteger a sus hijos de los depredadores en línea?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Evitar discutir con ellos sobre su uso y experiencias de Internet.
<input type="checkbox"/>	Controlar sus conversaciones de los salones de chat.
<input type="checkbox"/>	Confiar en los menores para que decidan qué sitios Web son seguros para visitar.

	Educar a los menores para que eviten compartir información personal en Internet.
--	----------------------------------------------------------------------------------

Nota: las respuestas correctas se muestran en la siguiente página.

Respuesta 1

¿Cuál de las siguientes medidas puede ayudarle a garantizar la privacidad en línea?

Seleccione la respuesta correcta.

<input type="checkbox"/>	En lugar de chats, usar mensajes de correo electrónico para compartir información personal.
<input type="checkbox"/>	Usar contraseñas seguras para tener acceso a las cuentas de correo electrónico.
<input type="checkbox"/>	Ejecutar una detección de virus siempre que crea que un virus infectó la computadora.
<input type="checkbox"/>	Abrir todos los mensajes de correo electrónico no solicitado para identificar a los remitentes antes de responder.

Respuesta 2

¿Cuál de las siguientes afirmaciones describe el modo en que operan los depredadores en línea?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Ofrecen a los menores más atención y afecto.
<input type="checkbox"/>	Intentan infectar su computadora con virus.
<input type="checkbox"/>	Atraen a los menores para mantener relaciones inapropiadas.
<input type="checkbox"/>	Atraen a los menores para que compren un producto.

Respuesta 3

¿Cuáles son algunas de las medidas que los padres pueden tomar para proteger a sus hijos de los depredadores en línea?

Seleccione todas las respuestas que puedan considerarse correctas.

<input type="checkbox"/>	Evitar discutir con ellos sobre su uso y experiencias de Internet.
<input type="checkbox"/>	Controlar sus conversaciones de los salones de chat.
<input type="checkbox"/>	Confiar en los menores para que decidan qué sitios Web son seguros para visitar.
<input type="checkbox"/>	Educar a los menores para que eviten compartir información personal en Internet.

Lección 4

Mantenimiento de la computadora segura y actualizada

Contenido de la lección

	Configuración de la seguridad de la computadora
	Mantenimiento de la computadora actualizada
	Autoevaluación

Introducción a la lección

Cuando conecta la computadora a Internet, el resto del mundo puede obtener acceso al software y los datos que contiene. La conexión a Internet aumenta la amenaza para su computadora de virus, spyware y piratas informáticos. Sin embargo, puede minimizar estas amenazas de seguridad si configura las opciones de seguridad de la computadora y mantiene el software de seguridad actualizado.

En esta lección, aprenderá a aprovechar al máximo la seguridad de su computadora mediante la configuración de las opciones de seguridad del sistema operativo. En ella también se describe cómo configurar la computadora para que actualice automáticamente su software de seguridad.

Objetivos de la lección

Cuando haya completado esta lección, será capaz de:

- Describir la finalidad de los distintos valores de configuración de seguridad de la computadora.
- Identificar las opciones disponibles para mantener la computadora actualizada.

Las mayores amenazas de seguridad para su computadora a través de Internet proceden de los piratas informáticos y los virus. Estas amenazas se producen casi siempre porque la configuración de seguridad de la computadora no está definida correctamente o el software de seguridad no está presente o quedó obsoleto. La configuración de seguridad se define en la computadora cuando se instala el sistema operativo. Sin embargo, se puede modificar según sus requisitos.

Por ejemplo, en Windows XP Service Pack 2, la configuración de seguridad se puede consultar y modificar por medio del Centro de seguridad de Windows. En el Centro de seguridad puede:

- Usar las opciones de seguridad de Internet para especificar los niveles de seguridad y privacidad de los sitios Web que se visitan.
- Modificar la configuración del firewall para proteger mejor la computadora del acceso no autorizado a través de Internet.
- Configurar la computadora para que descargue e instale automáticamente el software de seguridad actualizado para proteger mejor la computadora de nuevos virus.

En esta demostración, aprenderá a definir la configuración de seguridad de una computadora que se ejecuta en Windows XP Service Pack 2.

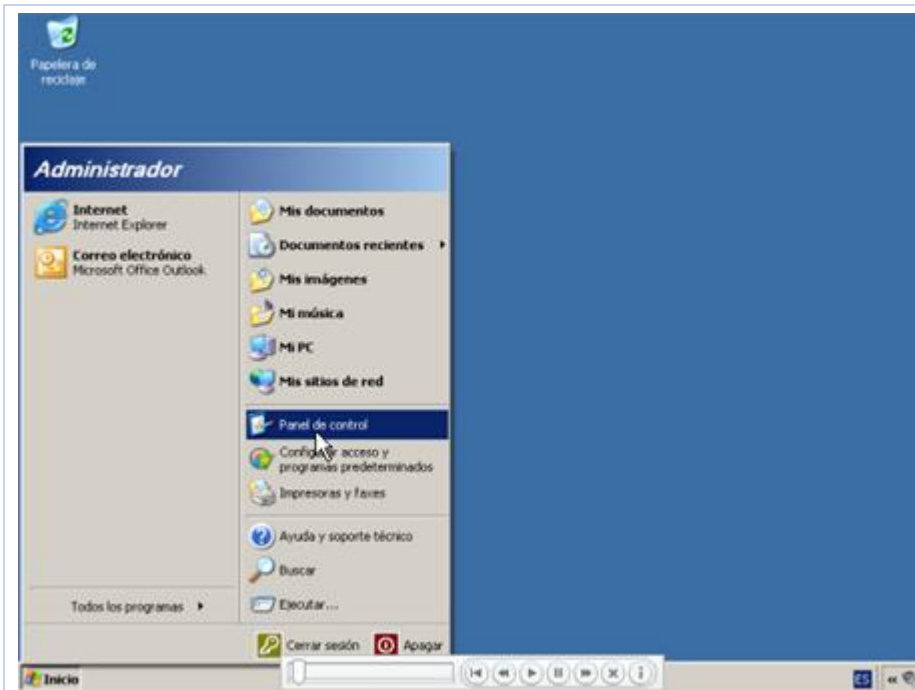
La siguiente tabla contiene los pasos y la transcripción de una demostración en línea.

Lista de pasos

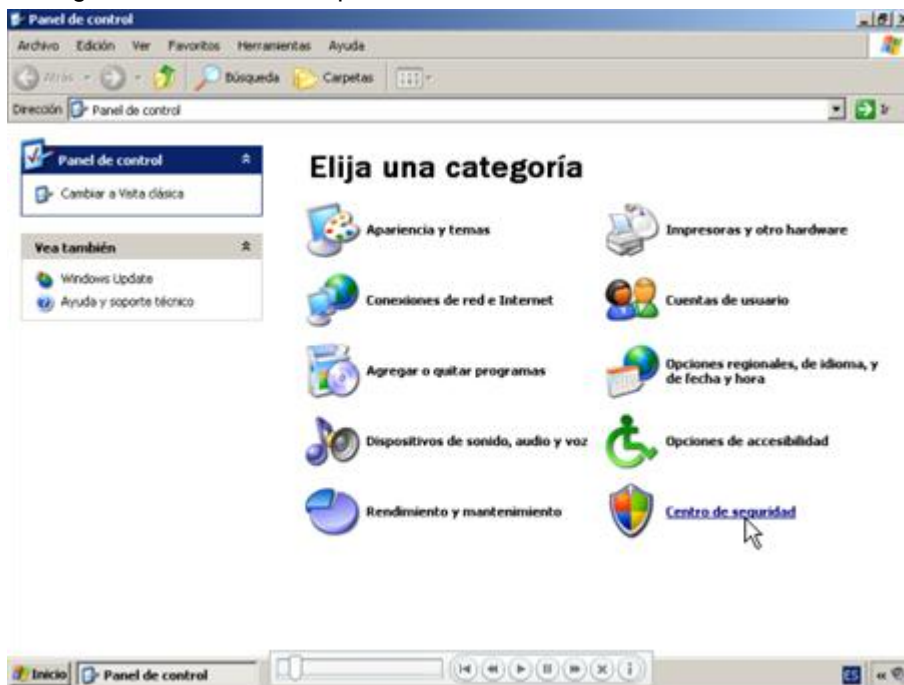
1	Demostración: Configuración de la seguridad de la computadora
2	Para que se muestre el Panel de control, haga clic en Inicio y, a continuación, en Panel de control
3	Para abrir el Centro de seguridad de Windows, haga doble clic en Centro de seguridad en el Panel de control.
4	Observe que hay tres vínculos disponibles en el Centro de seguridad de Windows.
5	Para ver las opciones de Internet, haga clic en el vínculo Opciones de Internet .
6	Observe que el cuadro de diálogo Propiedades de Internet contiene siete fichas.
7	Haga clic en la ficha General para ver las opciones.

8	Haga clic en la ficha Seguridad para ver las opciones.
9	Haga clic en la ficha Privacidad para ver las opciones.
10	Haga clic en la ficha Contenido para ver las opciones.
11	Haga clic en la ficha Conexiones para ver las opciones.
12	Haga clic en la ficha Programas para ver las opciones.
13	Haga clic en la ficha Opciones avanzadas para ver las opciones.
14	Haga clic en Aceptar para cerrar el cuadro de diálogo Propiedades de Internet .
15	Para ver la configuración del firewall de la computadora, haga clic en el vínculo Firewall de Windows .
16	Observe que el cuadro de diálogo Firewall de Windows contiene tres fichas.
17	Observe las opciones de la ficha General .
18	Haga clic en la ficha Excepciones para ver las opciones.
19	Haga clic en la ficha Opciones avanzadas para ver las opciones.
20	Haga clic en Aceptar para cerrar el cuadro de diálogo Firewall de Windows .
21	Haga clic en el vínculo Actualizaciones automáticas para descargar e instalar automáticamente en la computadora las actualizaciones de seguridad.
22	Haga clic en Aceptar para cerrar el cuadro de diálogo Actualizaciones automáticas .

Transcripción

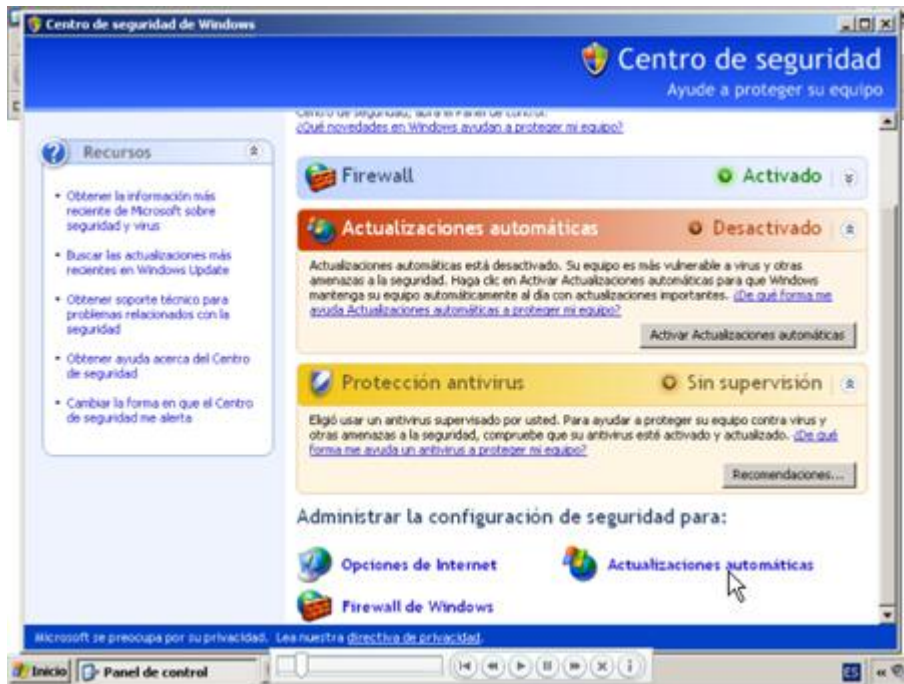


Cuando se instala Windows XP Service Pack 2, se establece automáticamente la configuración de seguridad en la computadora. Esta configuración se puede consultar y modificar por medio del Centro de seguridad de Windows, que se abre desde el Panel de control.



El Panel de control incluye elementos que permiten modificar la configuración de una computadora. Por ejemplo, el Panel de control permite agregar nuevos dispositivos de hardware, agregar o quitar software y cambiar la fecha y hora del sistema. También contiene elementos diseñados para configurar

la seguridad de la computadora en el Centro de seguridad de Windows.



El Centro de seguridad de Windows ofrece tres opciones para establecer la configuración de privacidad y seguridad de la computadora: Opciones de Internet, Firewall de Windows y Actualizaciones automáticas. Cuando se abre el Centro de seguridad de Windows, se indica si estas tres opciones se encuentran activadas.

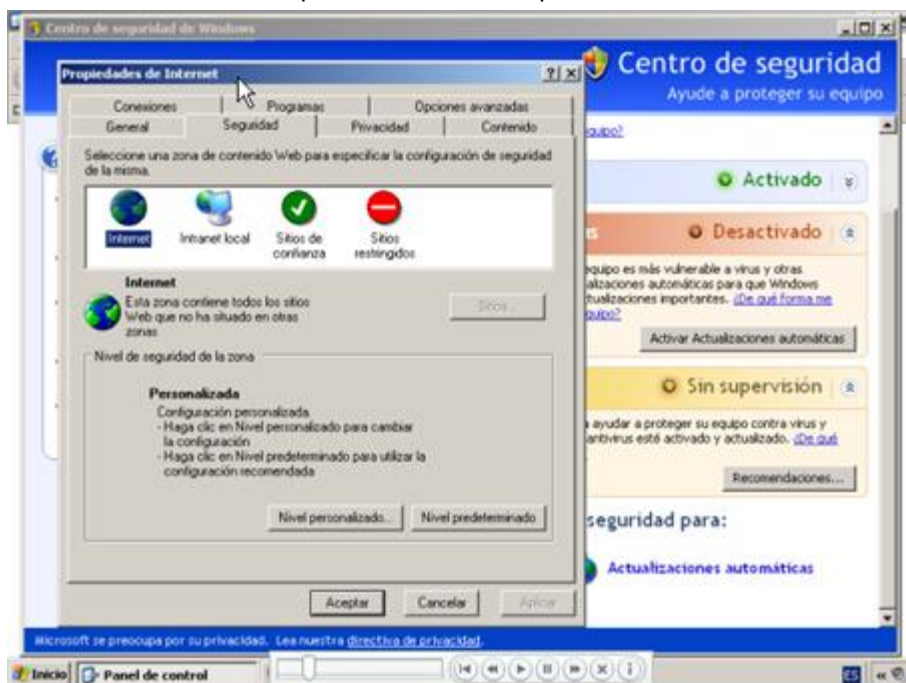


La primera opción disponible es el vínculo Opciones de Internet. Si hace clic en él, se abrirá el cuadro de diálogo Propiedades de Internet, donde podrá especificar la configuración de Internet.



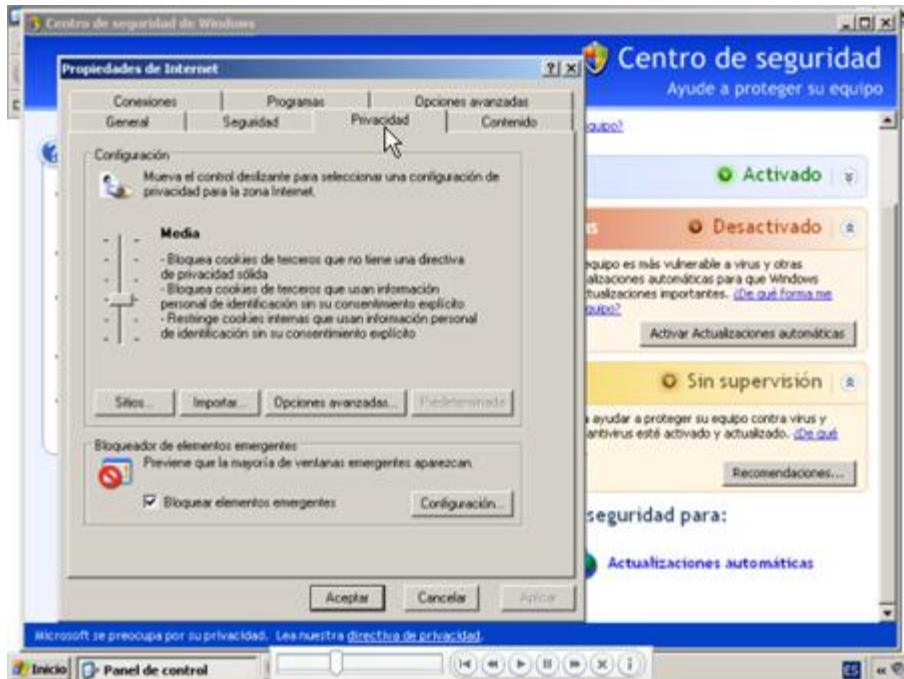
El cuadro de diálogo Propiedades de Internet presenta siete fichas que contienen opciones para modificar la configuración de seguridad de la computadora. Estas fichas son General, Seguridad, Privacidad, Contenido, Conexiones, Programas y Opciones avanzadas.

La primera ficha del cuadro de diálogo Propiedades de Internet es General, e incluye opciones para especificar la página Web que desea que se muestre en primer lugar cuando abre un explorador Web. Asimismo, puede indicar si desea realizar un seguimiento de las páginas Web que visita y si quiere eliminar los archivos temporales de Internet que se almacenan cuando visita diferentes sitios Web.

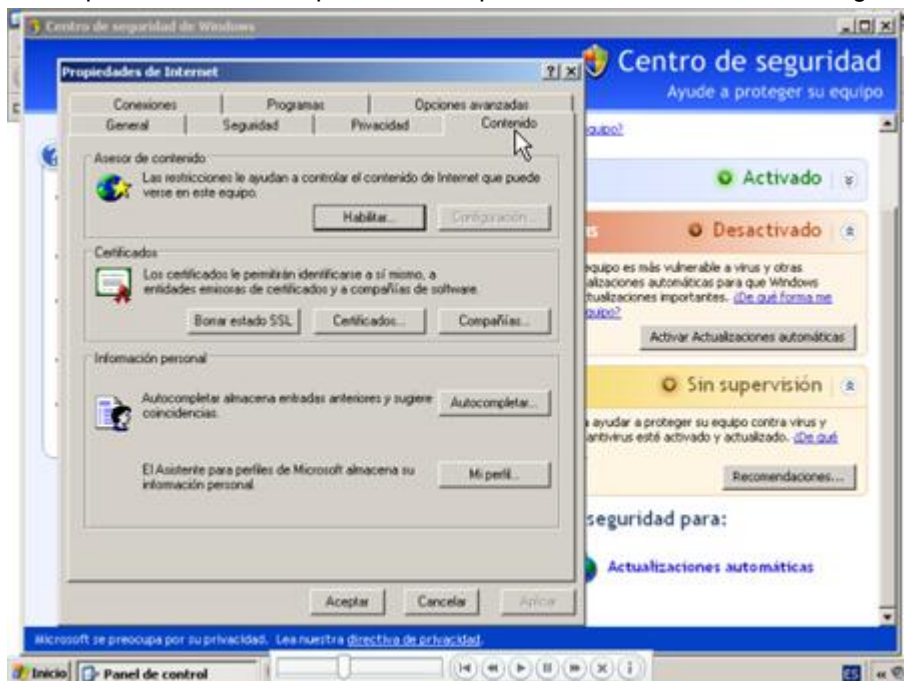


La segunda ficha es Seguridad y permite clasificar los sitios Web en función del riesgo de seguridad que entrañan. En ella también podrá especificar si un sitio Web es confiable o no. Además, puede

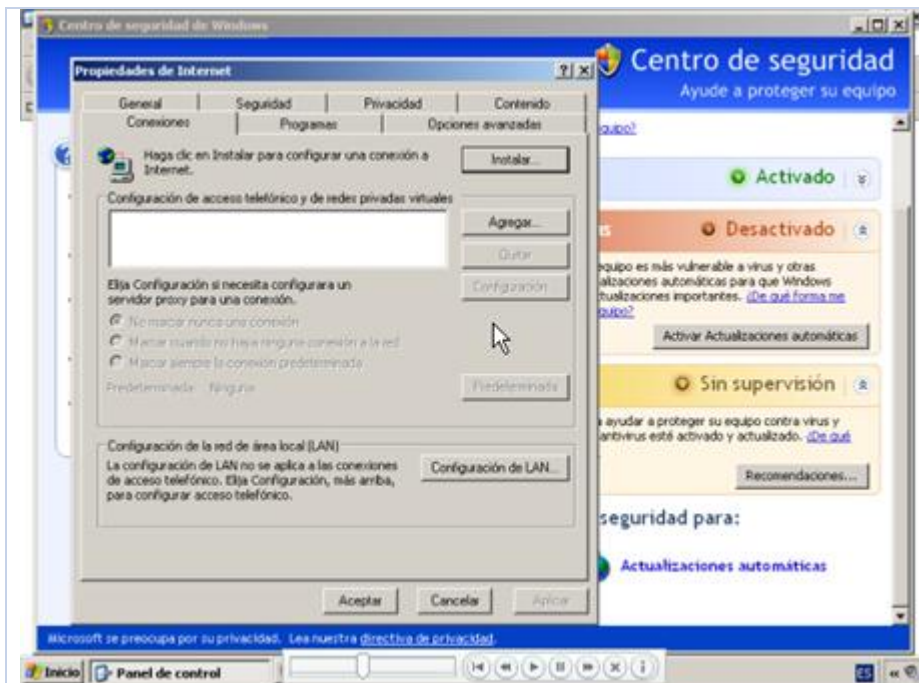
establecer un nivel de seguridad mayor en el caso de los sitios Web no confiables para asegurar una mayor protección de la computadora.



La tercera ficha del cuadro de diálogo Propiedades de Internet es Privacidad, que contiene valores de configuración para bloquear sitios Web de forma que no se guarden archivos temporales de Internet en la computadora. También puede evitar que se muestren ventanas emergentes al navegar por Internet.



La cuarta ficha es Contenido. Con los valores de configuración de esta ficha se pueden controlar los tipos de contenido a los que se puede tener acceso desde la computadora. Por ejemplo, puede hacer que los menores de edad no puedan visitar sitios Web con contenido para adultos.



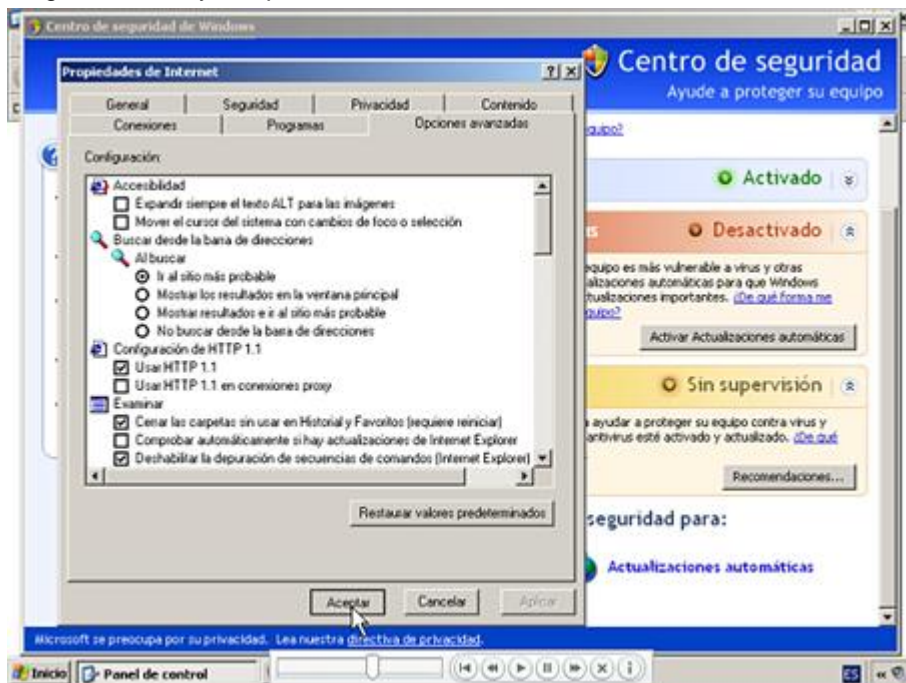
La quinta ficha de este cuadro de diálogo es Conexiones, donde se configura la conexión a Internet. Asimismo, puede especificar la configuración de red de área local o LAN de la computadora.



La sexta ficha es Programas, que sirve para especificar los programas que Windows usa automáticamente para los servicios de Internet, como el correo electrónico, los grupos de noticias, el calendario y las llamadas por Internet. También puede usar esta ficha para restaurar la configuración original del explorador Web.



La última ficha del cuadro de diálogo Propiedades de Internet es Opciones avanzadas. Esta ficha contiene características avanzadas que puede usar para definir con mayor precisión el explorador Web, como Internet Explorer. Por ejemplo, puede configurar el explorador Web para que sea más accesible para personas con discapacidad. Además, puede desactivar los gráficos para que las páginas Web se carguen con mayor rapidez.



Cuando establezca la configuración en el cuadro de diálogo Propiedades de Internet, deberá guardar los cambios haciendo clic en Aceptar.



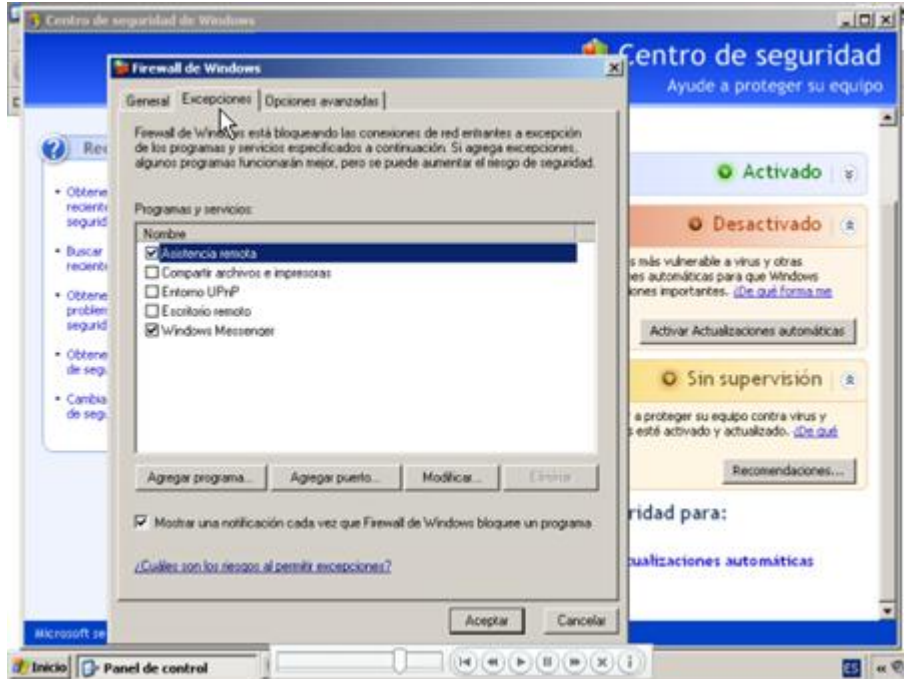
La segunda opción disponible en el Centro de seguridad de Windows es el vínculo Firewall de Windows. Si hace clic en este vínculo, se abrirá el cuadro de diálogo Firewall de Windows. Tenga en cuenta que es posible que esta opción no esté disponible en versiones anteriores de Windows XP.



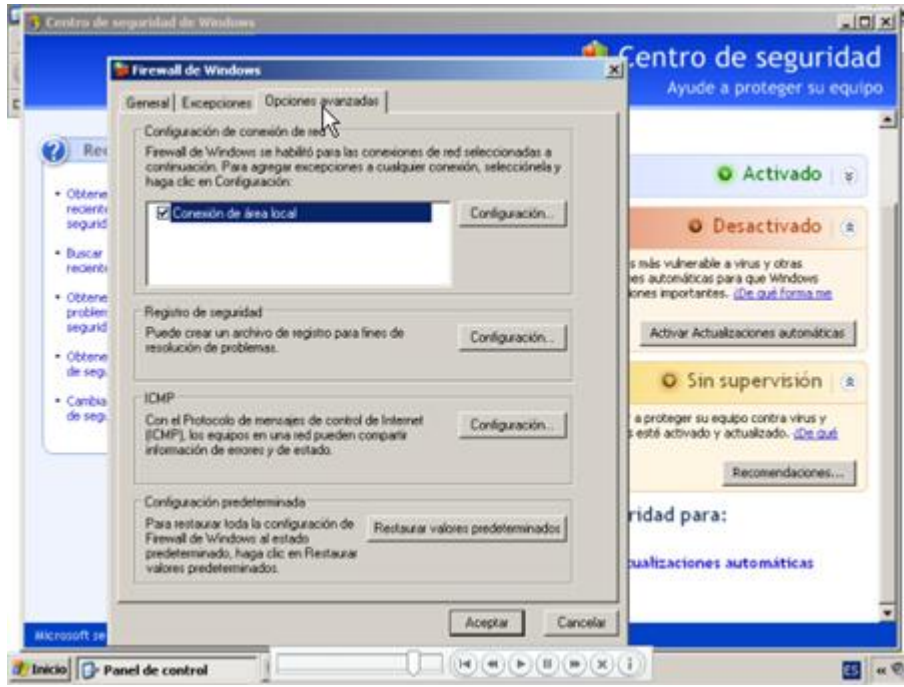
El cuadro de diálogo Firewall de Windows contiene tres fichas donde encontrará opciones para proteger la computadora del acceso no autorizado a través de Internet y, asimismo, para bloquear la información con respecto a fuentes no confiables.

La primera ficha del cuadro de diálogo Firewall de Windows es General. En ella, se activa y desactiva el Firewall de Windows. No obstante, se recomienda no desactivarlo con el fin de evitar que la computadora quede expuesta a ataques de virus y spyware. También puede usar los valores de

configuración de esta ficha para bloquear todas las solicitudes no deseadas para establecer una conexión con la computadora.



La segunda ficha del cuadro de diálogo Firewall de Windows es Excepciones, que se puede utilizar para permitir que un programa se comunice a través del Firewall de Windows. Por ejemplo, para que una persona pueda enviar un archivo a través de un programa de chat, deberá especificar el programa en esta ficha. Solamente así el firewall permitirá el envío del archivo por medio del programa de chat. No olvide que con estas excepciones la computadora es más vulnerable a ataques de seguridad. Por lo tanto, sólo haga una excepción con un programa cuando realmente lo precise y elimine la excepción tan pronto como deje de ser necesario.



La última ficha del cuadro de diálogo Firewall de Windows es Opciones avanzadas. Úsela para especificar la configuración de seguridad para una conexión de red individual. En esta ficha también se puede restaurar la configuración original del firewall.



Cuando establezca la configuración en el cuadro de diálogo Firewall de Windows, debe guardarla haciendo clic en Aceptar.



La tercera opción disponible en el Centro de seguridad de Windows es el vínculo Actualizaciones automáticas. Use la configuración del cuadro de diálogo Actualizaciones automáticas para descargar e instalar automáticamente en la computadora las actualizaciones de seguridad. Asimismo, puede especificar la hora y la frecuencia con la que descarga e instalación de actualizaciones deben

producirse.



Cuando establezca la configuración en el cuadro de diálogo Actualizaciones automáticas, deberá guardar los cambios haciendo clic en Aceptar. En esta demostración, conoció las diversas configuraciones de privacidad y seguridad que existen para proteger la computadora de virus, accesos no autorizados y demás amenazas de seguridad.

Todos vemos cómo se crean continuamente nuevos medicamentos para tratar nuevas enfermedades. Del mismo modo, la industria informática actualiza continuamente las versiones de software antivirus y productos similares para hacer frente a nuevos virus, gusanos y spyware. Es necesario mantener la computadora actualizada con las últimas versiones de software de seguridad para garantizar una mayor protección.

El sitio Web de Microsoft Windows Update ofrece las actualizaciones de seguridad necesarias para proteger el sistema operativo de la computadora. También permite descargar estas actualizaciones de seguridad e instalarlas en la computadora. Si le resulta complicado realizar un seguimiento del software de seguridad que necesita actualizar, puede configurar la computadora para que automatice este proceso de actualización.

En esta demostración, conocerá las distintas opciones que puede usar para mantener actualizado el software de seguridad de la computadora de forma automática.

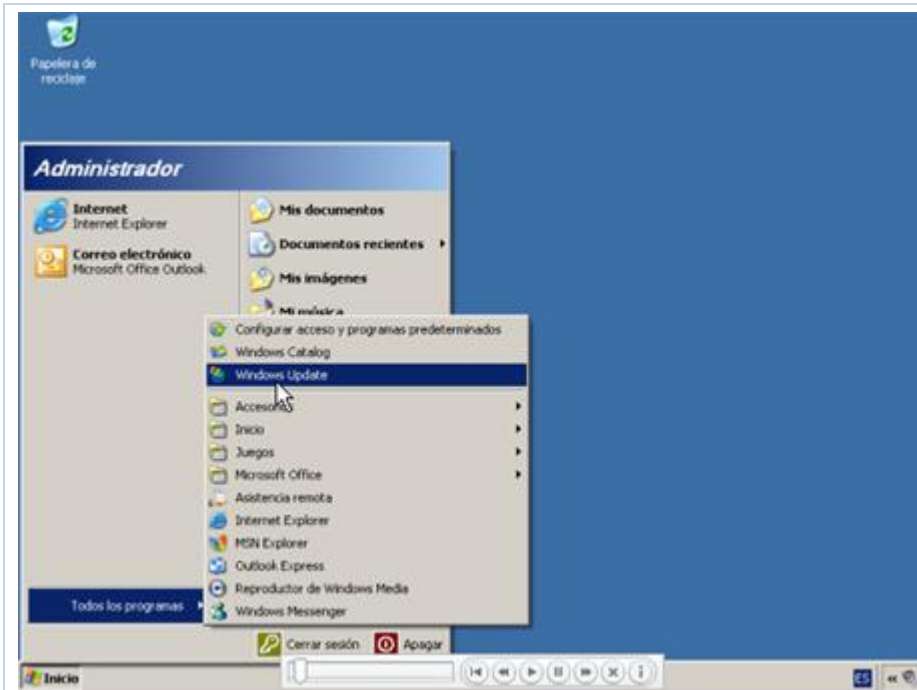
La siguiente tabla contiene los pasos y la transcripción de una demostración en línea.

Lista de pasos

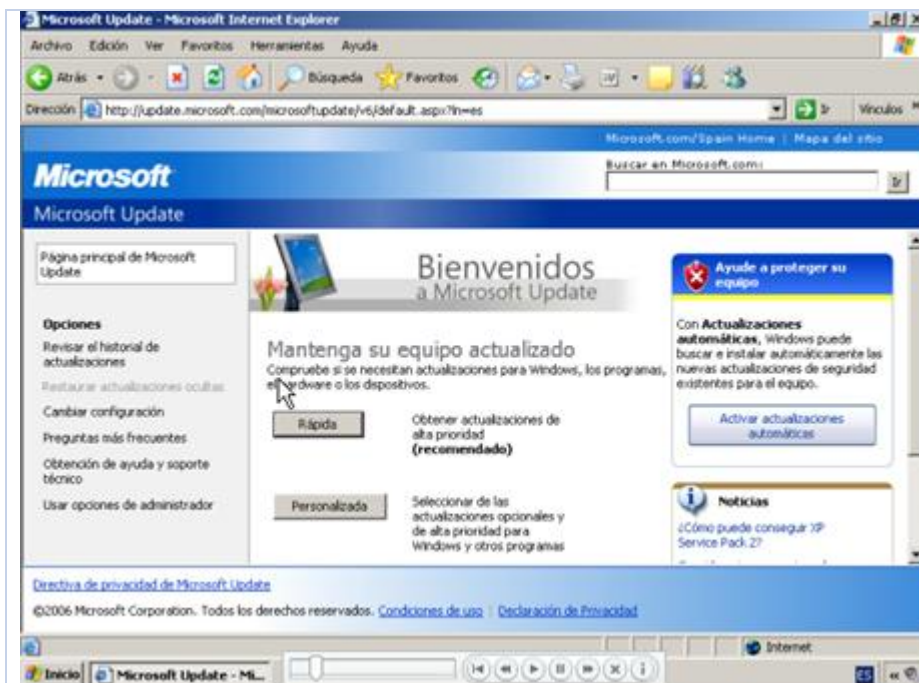
1	Demostración: Mantenimiento de la computadora actualizada
2	Para abrir el sitio Web de Microsoft Windows Update, haga clic en Inicio , seleccione Todos los programas y, a continuación, haga clic en Windows Update .
3	Observe los vínculos que aparecen bajo Opciones.
4	El Centro de seguridad de Windows se abrió automáticamente. Haga clic en el vínculo Actualizaciones automáticas para descargar e instalar automáticamente en la computadora las actualizaciones de seguridad. Se abrirá el cuadro de diálogo Actualizaciones automáticas .
5	Observe las cuatro opciones del cuadro de diálogo Actualizaciones automáticas .
6	Haga clic en Automático (recomendado) para descargar e instalar automáticamente en la computadora las actualizaciones de seguridad a una hora y con una frecuencia predeterminadas.
7	Haga clic en Descargar actualizaciones por mí, pero permitirme elegir cuándo instalarlas para recibir una alerta cuando se hayan descargado automáticamente las actualizaciones de seguridad.
8	Haga clic en Notificarme, pero no descargarlas automáticamente ni instalarlas para recibir una alerta cuando las actualizaciones de seguridad estén listas para descargar.

9	Haga clic en Desactivar Actualizaciones automáticas para desactivarlas.
10	Observe que el vínculo del sitio Web de Windows Update está disponible en el cuadro de diálogo Actualizaciones automáticas .
11	Haga clic en Aceptar para cerrar el cuadro de diálogo Actualizaciones automáticas .

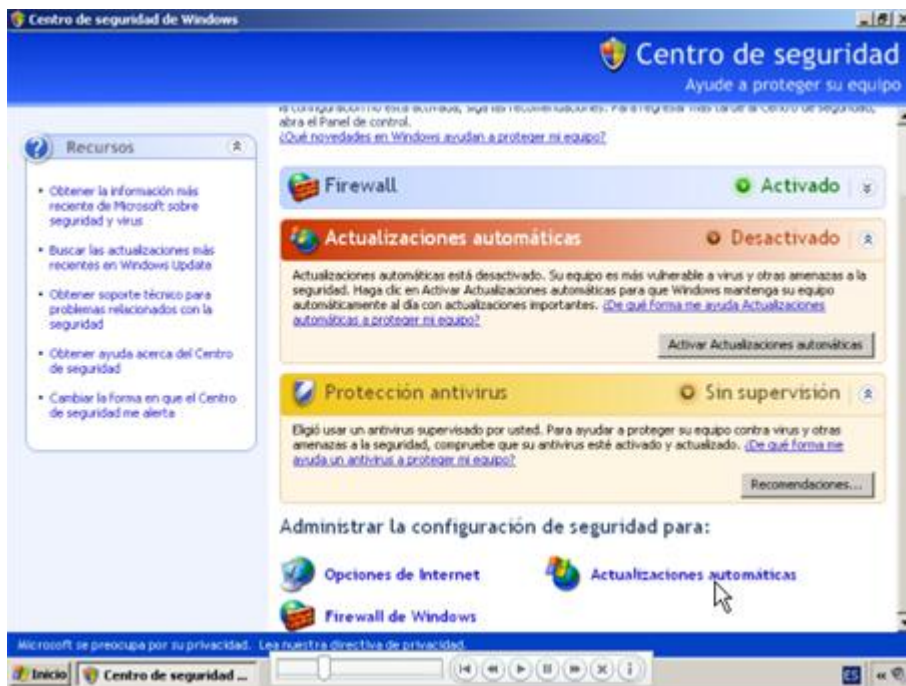
Transcripción



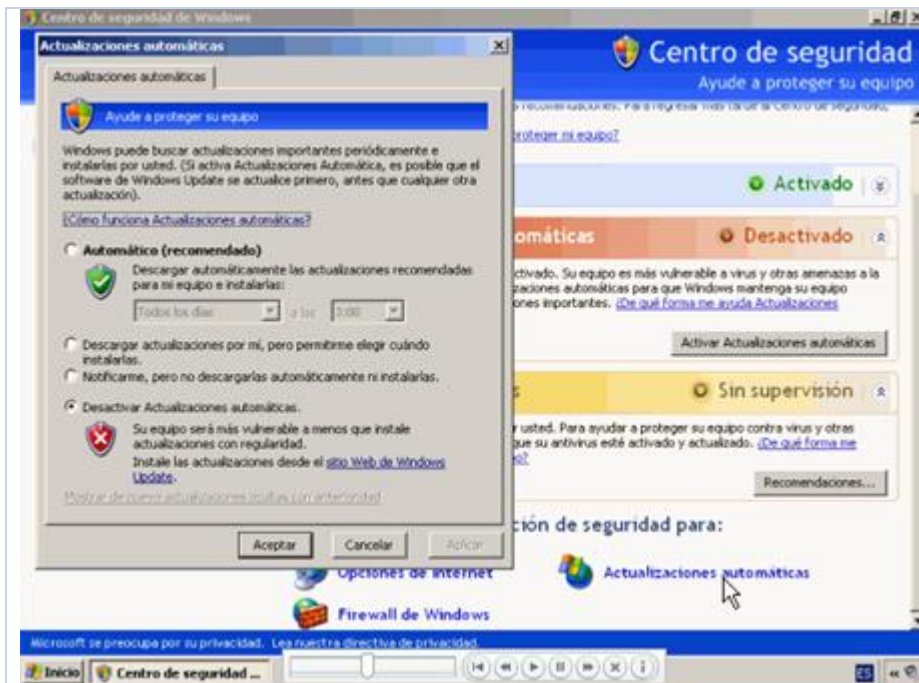
Puede mantener la computadora actualizada si descarga las actualizaciones del sistema y otro software de seguridad disponible desde el sitio Web de Microsoft Windows Update.



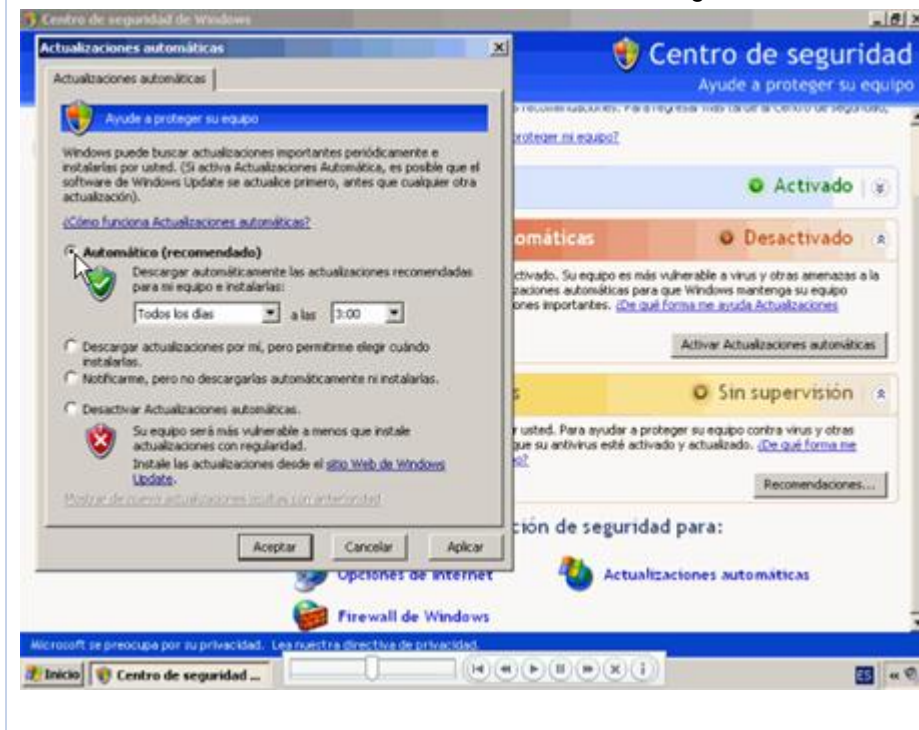
Este sitio Web ofrece las actualizaciones de seguridad necesarias para que la computadora permanezca protegida frente a las amenazas de seguridad. Cuando visite este sitio, Windows Update explorará la computadora e informará de las actualizaciones que se pueden descargar e instalar en ella.



En el sitio Web de Microsoft Windows Update podrá consultar una lista donde se incluyen las actualizaciones que ya descargó e instaló en la computadora. Este sitio ofrece también respuestas a las preguntas más frecuentes, y la ayuda y soporte necesarios para resolver los problemas relacionados con las actualizaciones de Windows.



Para aprovechar las actualizaciones de seguridad más recientes del sitio Web de Microsoft Windows Update, deberá visitar este sitio regularmente. Este proceso se puede automatizar estableciendo una configuración determinada en el Centro de seguridad de Windows. La opción Actualizaciones automáticas permite que la computadora descargue e instale automáticamente las actualizaciones de seguridad desde el sitio Web de Microsoft Windows Update. Este proceso de descarga no interfiere en la descarga de otros archivos y no interrumpe el trabajo. No obstante, es posible que se muestre un mensaje en caso de que una actualización requiera reiniciar la computadora. Si hace clic en el vínculo Actualizaciones automáticas, se abrirá el cuadro de diálogo Actualizaciones automáticas.

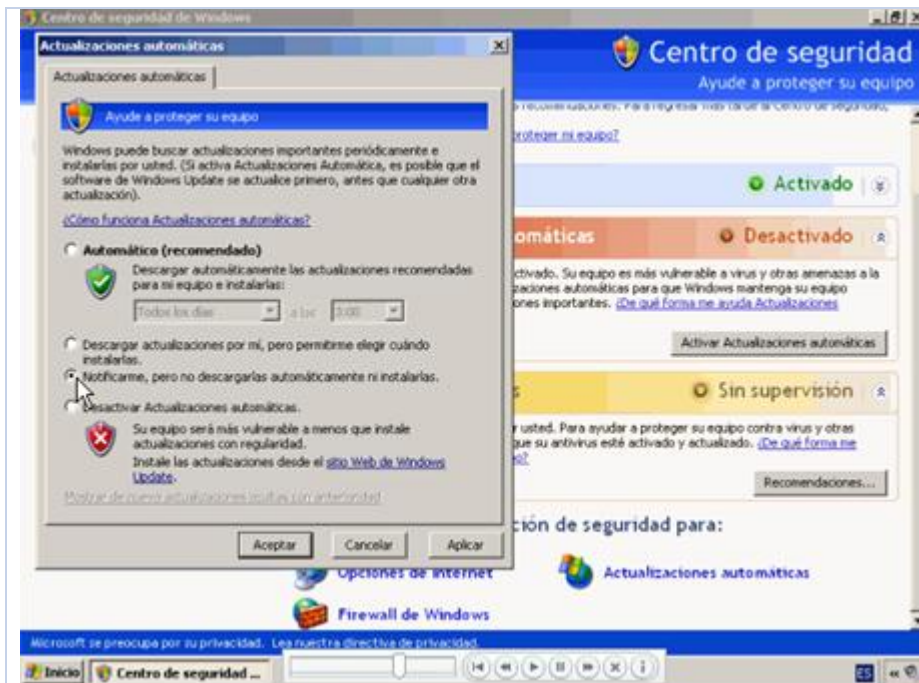


Puede elegir entre las cuatro opciones de este cuadro de diálogo para decidir cuándo desea descargar e instalar las actualizaciones de seguridad.

Si elige la primera opción, las actualizaciones automáticas se descargarán e instalarán automáticamente en la computadora a las 3:00 a. m. cada día. La hora y la frecuencia se pueden modificar, pero no olvide que la computadora debe estar conectada a Internet a la hora especificada para que el proceso de actualización funcione.



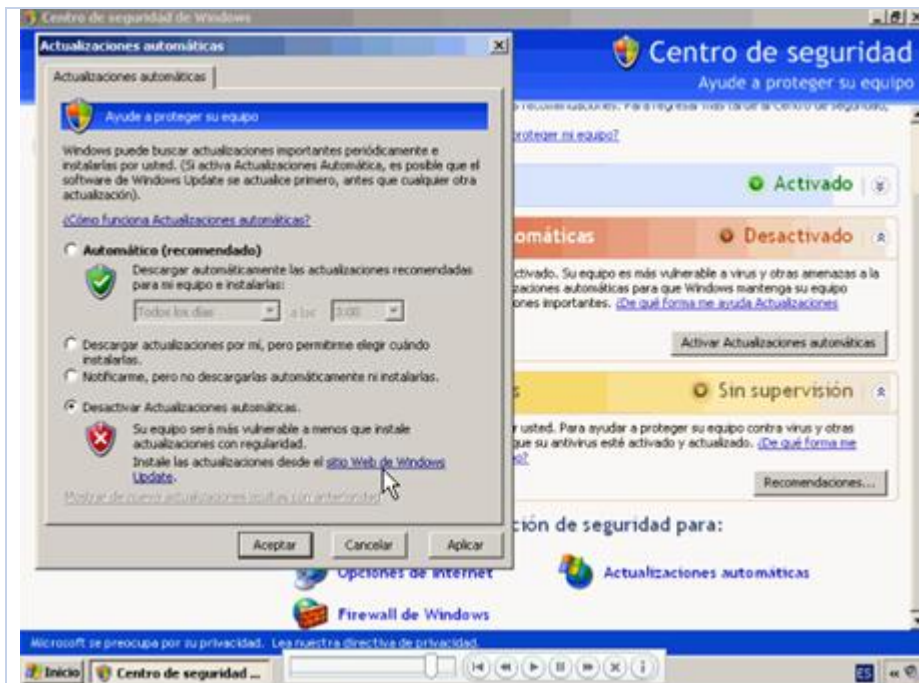
Si usa la segunda opción, la computadora descargará las actualizaciones automáticamente pero no las instalará en la computadora, sino que recibirá un aviso cuando las actualizaciones se descarguen por completo. Así, podrá instalar las actualizaciones que desee en cuanto reciba el aviso o cuando lo considere más oportuno.



Si usa la tercera opción, la computadora no descargará ni instalará las actualizaciones de seguridad automáticamente. En su lugar, cada vez que haya una actualización disponible recibirá una alerta. Así, podrá descargar e instalar las actualizaciones que desee cuando más le convenga.



Por último, si selecciona la cuarta opción, las actualizaciones no se descargarán ni instalarán en la computadora, ni tampoco recibirá ningún aviso cuando estén disponibles. Se recomienda no usar esta opción, ya que podría hacer que la computadora sea vulnerable a las amenazas de seguridad.



El cuadro de diálogo Actualizaciones automáticas sirve además para visitar el sitio Web de Microsoft Windows Update. Para ello, haga clic en el vínculo del sitio Web de Windows Update.



Cuando establezca la configuración en el cuadro de diálogo Actualizaciones automáticas, deberá guardar los cambios haciendo clic en Aceptar. En caso de que la computadora tenga instalado otro software de seguridad, como un antivirus o un programa anti spyware, no olvide seguir los procedimientos para mantenerlo actualizado. En esta demostración, conoció las distintas opciones disponibles para mantener la computadora actualizada automáticamente con el software de seguridad más reciente.

Ordene los tipos de soluciones en sus categorías correspondientes escribiendo el número de frase en el cuadro de opción pertinente.

Frase	
1	Mostrar contenido selectivo
2	Especificar configuración de LAN
3	Bloquear ventanas emergentes
4	Ver respuestas a las preguntas más frecuentes
5	Permite realizar descargas automáticas
6	Bloquear una solicitud no deseada
7	Realizar una excepción para un programa
8	Recibir una alerta para las descargas

Opción 1	Opción 2	Opción 3
Opciones de Internet	Firewall de Windows	Actualizaciones automáticas

Nota: las respuestas correctas se muestran en la siguiente página.

Opción 1		Opción 2		Opción 3
Opciones de Internet		Firewall de Windows		Actualizaciones automáticas
3, 2, 1		7, 6		8, 5, 4

Lección 5

Ética informática

Contenido de la lección

	Acerca de la propiedad intelectual
	Prevención e infracción de las leyes de derechos de autor
	Problemas legales de intercambio de información
	Juego de los paneles: Conocimiento de la ética informática
	Autoevaluación

Introducción a la lección

En Internet se puede encontrar gran cantidad de información, como noticias, artículos, imágenes, canciones, películas y software. La búsqueda en Internet suele ser la forma más rápida y sencilla de recopilar información en cualquier momento. Por ejemplo, puede usar Internet para buscar información para los deberes del colegio, o bien ideas que se puedan incluir en una presentación de trabajo. También es posible descargar canciones y películas desde distintos sitios Web.

En la mayoría de los sitios, la descarga de información es gratuita. Pero estas descargas gratuitas pueden no serlo realmente. La información de un sitio Web es propiedad legal del autor que la creó o del sitio Web que la publicó. Por lo tanto, puede que necesite el permiso del autor o del propietario del sitio Web para usar su contenido. Debe conocer los derechos o permisos que tiene respecto al contenido disponible en un sitio Web antes de descargarlo.

En esta lección se describe el significado de la propiedad intelectual en el campo de la informática y cómo un uso no autorizado de ella puede suponer una infracción de las leyes de derechos de autor. Asimismo, conocerá los distintos problemas legales asociados con el intercambio de información.

Objetivos de la lección

Cuando haya completado esta lección, será capaz de:

- Explicar el significado del término propiedad intelectual con respecto a la informática.
- Identificar las distintas infracciones de las leyes de derechos de autor y las medidas preventivas posibles.
- Identificar los distintos problemas legales asociados con el intercambio de información.

Arturo López trabaja para una agencia de noticias. Tiene que escribir un artículo sobre tecnología informática. Arturo copia algunos datos de un sitio Web y los usa en su artículo. Sin embargo, no menciona la fuente de donde copió la información. Después de publicar el artículo, se acusa a Arturo de infringir las leyes de derechos de autor. El motivo es que usó una propiedad intelectual sin permiso de su propietario.

Cualquier información disponible en Internet es una propiedad intelectual, cuyo propietario legal es la persona que la creó. Por ejemplo, si publica un artículo en un sitio Web, el artículo será su propiedad intelectual. Como propietario de una propiedad intelectual, tiene derechos exclusivos para controlar el uso del material para:

- Copiar, reproducir o distribuir la propiedad.
- Compartir o vender los derechos de la propiedad.
- Ceder los derechos de la propiedad de forma gratuita.

Nota:

Los derechos reales de una propiedad intelectual pueden variar en función del permiso que otorgue el propietario.

No tiene derecho a usar la propiedad intelectual sin el permiso de su propietario. Existen leyes que protegen los derechos de una persona respecto a una propiedad intelectual. Estas leyes se denominan leyes de *derechos de autor*. La infracción de estas leyes puede causar problemas legales.

Tema: Prevención e infracción de las leyes de derechos de autor

El uso de una propiedad intelectual con derechos de autor sin el consentimiento de su propietario puede suponer una infracción de las leyes de derechos de autor. Los motivos de esta infracción y las medidas que se pueden tomar para evitarla se describen a continuación.

Plagio

El hecho de copiar el trabajo de alguien y usarlo como si fuera propio, sin mencionar la fuente, se conoce como *plagio*. Imaginemos que crea una copia exacta de un gráfico que aparece en un sitio Web. Después lo incluye en otro sitio Web que crea usted, pero sin mencionar de dónde lo copió. Este hecho se considera plagio.

En muchos países, parafrasear un trabajo existente y hacerlo pasar como original también se considera plagio.

Mal uso de material con derechos de autor

En la siguiente tabla se describen algunos casos comunes de mal uso de material con derechos de autor que debe tener en cuenta y evitar.

Mal uso de derechos de autor	Descripción
Copiar música	<p>Hay muchos sitios Web que permiten descargar y compartir canciones. Sin embargo, algunos de estos sitios Web no tienen autorización legal para ofrecer la descarga gratuita de las canciones. La descarga de canciones desde estos sitios Web supone un mal uso de la música con derechos de autor.</p> <p>Se hace un mal uso de la música con derechos de autor cuando:</p> <ul style="list-style-type: none">• Se descarga música con derechos de autor desde un sitio Web sin el permiso del propietario o sin pagar una tasa por derechos de autor.• Se descarga música con derechos de autor desde un sitio Web y se crean CDs y DVDs con la música descargada.• Se crean copias de CDs o DVDs con derechos de autor y se comparten con otras personas.• Se comparten canciones con derechos de autor en Internet a través de sitios Web que facilitan el uso compartido de

	canciones.	
Usar software sin licencia ni permiso	<p>La copia no autorizada de software con derechos de autor sin obtener la licencia o el permiso de su propietario de derechos de autor se considera piratería de software.</p> <p>Tenga en cuenta las siguientes situaciones para evitar la piratería de software:</p> <ul style="list-style-type: none"> • Si descarga software con derechos de autor desde un sitio Web sin el permiso del propietario o sin pagar una tasa, se considerará piratería de software. • Si compra una copia legal de software, crea copias del mismo y las distribuye a otras personas, también se considerará piratería de software. • Algunos proveedores de computadoras instalan copias de software sin licencia en las computadoras que venden. Lo hacen para ahorrar los costos de las tasas de las licencias. Sin embargo, la adquisición de computadoras con software sin licencia se considera piratería de software. Por lo tanto, a la hora de adquirir una computadora, asegúrese de que tiene los documentos de la licencia del software que viene instalado en ella o que se vende con ella. 	
Copiar logotipos	<p>Un logotipo es un material con derechos de autor que usa su propietario como un identificador. Es ilegal copiar o usar un logotipo sin el permiso de su autor. Por ejemplo, usar el logotipo de Microsoft en su tarjeta de visita sin obtener el permiso de Microsoft se considera una infracción de las leyes de derechos de autor.</p> <p>En ocasiones, una persona puede tener permiso para usar un logotipo, pero con ciertas limitaciones. Por ejemplo, una persona puede tener permiso para usar el logotipo de Microsoft sólo cuando está haciendo negocios en nombre de Microsoft. Si la persona usa el logotipo de Microsoft para hacer negocios para beneficio personal, entonces se considera un mal uso del logotipo con derechos de autor.</p>	

Con el uso extendido de Internet, es posible que se vea implicado en actividades ilegales o poco éticas, como los juegos de azar o las difamaciones. Debe tener cuidado y ser consciente de este tipo de actividades. No olvide tampoco que estos problemas pueden variar de un país a otro, e incluso en las distintas zonas de un mismo país.

En la siguiente tabla, se describen algunos usos ilegales y poco éticos del intercambio de información.

Actividad ilegal	Descripción
<p>Difamaciones sobre la reputación de una persona</p>	<p>Cuando se comunique con otras personas a través del correo electrónico, chat o foros públicos en línea, asegúrese de no realizar ninguna afirmación en la que pueda difamar a alguien. La difamación consiste en realizar afirmaciones falsas sobre una persona que pueden afectar negativamente a su reputación. Por ejemplo, imaginemos que escribe un mensaje en un foro en línea donde afirma falsamente que su vecino, que es una persona famosa, tiene algunas propiedades ilegales. Este hecho puede considerarse una difamación, ya que está expresando una información falsa que puede afectar a la credibilidad de su vecino.</p> <div style="border: 1px solid orange; padding: 5px; margin: 10px 0;"> <p>Nota: Una afirmación falsa puede considerarse difamatoria incluso si no es despectiva. En ocasiones, incluso las afirmaciones verdaderas pueden considerarse difamatorias si dañan la reputación de una persona.</p> </div> <p>Las <i>injurias</i> y <i>calumnias</i> son dos formas de difamación. Las calumnias son difamaciones escritas que se publicaron, mientras que las injurias son difamaciones verbales.</p> <p>El sistema legal de casi todos los países considera estas dos difamaciones como delitos castigados por la ley. Puede enfrentarse a sanciones civiles o penales, según el sistema legal de su país. La pena puede abarcar desde una sanción económica hasta castigos más severos, como penas de cárcel. En ocasiones, la gravedad de la infracción depende de la situación. Por ejemplo, en algunos países, un insulto al Presidente se considera un acto delictivo. Sin embargo, en otros países, los cargos públicos tienen menos protección que cualquier ciudadano normal. Por lo tanto, tenga en cuenta las leyes locales antes de realizar cualquier afirmación difamatoria.</p>
<p>Visitar sitios Web inapropiados</p>	<p>Internet ofrece acceso libre a todo tipo de sitios Web, algunos de los cuales podrían fomentar actividades ilegales. Algunos sitios Web ofrecen servicios que esconden otras actividades prohibidas por el sistema legal de su estado o país, y es posible tener acceso a ellos a través de Internet, ya que allí no existen límites ni controles. Por ejemplo, puede tener acceso a un sitio de juegos de azar, incluso si la ley de su país los prohíbe. Sin embargo, podría causarle problemas legales.</p>

	<p>También debe tener en cuenta que el sistema legal es diferente según los estados y los países. Por ejemplo, los productos que puede comprar o vender legalmente en un país pueden suponer una compra o venta ilegal en otro. Por lo tanto, aunque en un sitio Web no se le prohíba comprar un artículo que sea ilegal en su país, puede que sea acusado de algún delito por ello.</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tema: Juego de los paneles: Conocimiento de la ética informática

Cada pareja de frases contiene una verdadera y una falsa. Para cada pareja de frases, indique cuál es verdadera colocando una marca en la columna Verdadero de la derecha.

	Frase	Verdadero	Falso
1	El uso no autorizado de la propiedad intelectual es ILEGAL.		
2	El uso no autorizado de la propiedad intelectual es LEGAL.		
3	Una pintura ES propiedad legal de su autor.		
4	Una pintura NO ES propiedad legal de su autor.		
5	El autor de un libro NO PUEDE controlar el uso del libro.		
6	El autor de un libro PUEDE controlar el uso del libro.		
7	Un propietario de derechos de autor NO PUEDE venderlos.		
8	Un propietario de derechos de autor PUEDE venderlos.		
9	La infracción de las leyes de derechos de autor NO PUEDE causar problemas legales.		
10	La infracción de las leyes de derechos de autor PUEDE causar problemas legales.		
11	Compartir una canción con derechos de autor NO ES una infracción de las leyes de derechos de autor.		
12	Compartir una canción con derechos de autor ES una infracción de las leyes de derechos de autor.		
13	Las calumnias son difamaciones VERBALES.		
14	Las calumnias son difamaciones ESCRITAS.		
15	Las injurias son difamaciones VERBALES.		
16	Las injurias son difamaciones ESCRITAS.		
17	Los juegos de azar en línea PUEDEN causar problemas legales.		

18	Los juegos de azar en línea NO PUEDEN causar problemas legales.		
----	-----------------------------------------------------------------	--	--

Nota: las respuestas correctas se muestran en la siguiente página.

	Frase	Verdadero	Falso
1	El uso no autorizado de la propiedad intelectual es ILEGAL.		
2	El uso no autorizado de la propiedad intelectual es LEGAL.		
3	Una pintura ES propiedad legal de su autor.		
4	Una pintura NO ES propiedad legal de su autor.		
5	El autor de un libro NO PUEDE controlar el uso del libro.		
6	El autor de un libro PUEDE controlar el uso del libro.		
7	Un propietario de derechos de autor NO PUEDE venderlos.		
8	Un propietario de derechos de autor PUEDE venderlos.		
9	La infracción de las leyes de derechos de autor NO PUEDE causar problemas legales.		
10	La infracción de las leyes de derechos de autor PUEDE causar problemas legales.		
11	Compartir una canción con derechos de autor NO ES una infracción de las leyes de derechos de autor.		
12	Compartir una canción con derechos de autor ES una infracción de las leyes de derechos de autor.		
13	Las calumnias son difamaciones VERBALES.		
14	Las calumnias son difamaciones ESCRITAS.		
15	Las injurias son difamaciones VERBALES.		
16	Las injurias son difamaciones ESCRITAS.		
17	Los juegos de azar en línea PUEDEN causar problemas legales.		
18	Los juegos de azar en línea NO PUEDEN causar problemas legales.		

Pregunta 1

¿Cuáles de los siguientes usos de material con derechos de autor son legítimos?

Seleccione la respuesta correcta.

<input type="checkbox"/>	Copiar contenido de un sitio Web y usarlo tal cual en su propio sitio Web.
<input type="checkbox"/>	Crear copias de CDs comprados en línea y venderlas.
<input type="checkbox"/>	Usar párrafos de un artículo en línea y citar la fuente.
<input type="checkbox"/>	Crear copias de software con licencia y distribuir las entre sus amigos.

Pregunta 2

Está muy enfadado con su supervisor y escribe un mensaje en un foro en línea donde afirma que no es una persona honesta. ¿Qué tipo de delito está cometiendo?

Seleccione la respuesta correcta.

<input type="checkbox"/>	Calumnia
<input type="checkbox"/>	Infracción de las leyes de derechos de autor
<input type="checkbox"/>	Injuria
<input type="checkbox"/>	Plagio

Nota: las respuestas correctas se muestran en la siguiente página.

Respuesta 1

¿Cuáles de los siguientes usos de material con derechos de autor son legítimos?

Seleccione la respuesta correcta.

<input type="checkbox"/>	Copiar contenido de un sitio Web y usarlo tal cual en su propio sitio Web.
<input type="checkbox"/>	Crear copias de CDs comprados en línea y venderlas.
<input type="checkbox"/>	Usar párrafos de un artículo en línea y citar la fuente.
<input type="checkbox"/>	Crear copias de software con licencia y distribuir las entre sus amigos.

Respuesta 2

Está muy enfadado con su supervisor y escribe un mensaje en un foro en línea donde afirma que no es una persona honesta. ¿Qué tipo de delito está cometiendo?

Seleccione la respuesta correcta.

<input type="checkbox"/>	Calumnia
<input type="checkbox"/>	Infracción de las leyes de derechos de autor
<input type="checkbox"/>	Injuria
<input type="checkbox"/>	Plagio

Lecciones

<p>Descripción general de la seguridad y la privacidad de la computadora</p>	<p>Las computadoras deben protegerse de las distintas amenazas que afectan a su seguridad y privacidad. Estas amenazas pueden ser:</p> <ul style="list-style-type: none"> • Desastres naturales • Errores humanos o accidentes • Actos malintencionados como el robo, el acceso no autorizado por piratas informáticos o los ataques de virus <p>Tanto las computadoras independientes como las que están en una red se enfrentan a estas amenazas, por lo que es necesario tomar algunas medidas de seguridad para proteger el hardware, el software y los datos que contienen.</p>	
<p>Protección de la computadora y los datos</p>	<p>Es necesario proteger la computadora y los datos almacenados en ella de las distintas amenazas de seguridad y privacidad. Tome las siguientes medidas para proteger el sistema operativo, el software y los datos de su computadora:</p> <ul style="list-style-type: none"> • Implementar la identificación de usuario. • Establecer un nombre de usuario y una contraseña. • Mantener las contraseñas seguras. • Usar una combinación de bloqueo. • Cifrar los datos para evitar el acceso no autorizado. • Realizar copias de seguridad en otro dispositivo de almacenamiento. • Actualizar el sistema y el software vulnerable. <p>Las computadoras conectadas a una red o a Internet requieren más medidas de seguridad que las computadoras independientes. Para las computadoras conectadas a una red, se recomienda lo siguiente:</p> <ul style="list-style-type: none"> • Usar un software de seguridad actualizado. • Proteger la computadora de los piratas informáticos y spyware. • Borrar el historial y la memoria caché 	

	<p>regularmente.</p> <ul style="list-style-type: none"> • Eliminar cookies regularmente. • Realizar las transacciones en línea sólo en sitios seguros. • No revelar nunca información personal en un sitio Web. • Habilitar y configurar los componentes de seguridad en el Centro de seguridad de Windows. • Deshabilitar el contenido activo. • Usar la ayuda de seguridad que le ofrece su ISP. <p>Los archivos adjuntos de correo electrónico pueden ser portadores de virus o gusanos. Estas son algunas medidas de seguridad que puede tomar al usar el correo electrónico o chat:</p> <ul style="list-style-type: none"> • Usar un software de seguridad actualizado. • Evitar abrir mensajes de correo electrónico con archivos adjuntos. • Eliminar los mensajes de correo no deseado. • Eliminar los mensajes de correo comercial no solicitado. • Protegerse de la suplantación de identidad. • Restringir las conversaciones por chat sólo a personas que conozca. 	
<p>Protección de toda la familia ante las amenazas de seguridad</p>	<p>Para proteger la privacidad de su computadora, puede tomar medidas de seguridad como:</p> <ul style="list-style-type: none"> • Proteger su identidad. • Comprobar el estado de seguridad de su computadora con regularidad. • Ejecutar detecciones de virus a diario. • Usar un software anti spyware. • Realizar las transacciones en línea en sitios Web seguros con proveedores acreditados. • Comunicar cualquier abuso al ISP. • Eliminar o reducir el correo no deseado. • Cifrar el correo electrónico confidencial para evitar el acceso no autorizado. 	

<p>Mantenimiento de la computadora segura y actualizada</p>	<p>Una configuración de seguridad adecuada en la computadora puede evitar y detectar el acceso no autorizado a ella través de Internet. El Centro de seguridad de Windows ofrece las siguientes opciones de seguridad:</p> <ul style="list-style-type: none"> • Opciones de Internet • Firewall de Windows • Actualizaciones automáticas <p>Para mejorar la seguridad de su computadora, compruebe las opciones de seguridad y modifíquelas si es necesario.</p> <p>Estas son las medidas que puede tomar para mantener su computadora actualizada:</p> <ul style="list-style-type: none"> • Mantener la computadora actualizada mediante la descarga de las actualizaciones de seguridad necesarias desde el sitio Web de Microsoft Windows Update. • Configurar Actualizaciones automáticas para que su computadora pueda descargar e instalar automáticamente las actualizaciones de seguridad. 	
<p>Ética informática</p>	<p>El propietario de una propiedad intelectual tiene derechos exclusivos para usar la propiedad. Las leyes de derechos de autor protegen los derechos de las propiedades intelectuales. Las infracciones de estas leyes pueden ser las siguientes:</p> <ul style="list-style-type: none"> • Plagio • Piratería de software • Descarga no autorizada de material con derechos de autor desde sitios Web <p>Hay algunas formas legales de usar materiales con derechos de autor. Para usar legalmente material con derechos de autor:</p> <ul style="list-style-type: none"> • Haga un uso limitado del material con fines educativos y mencione la fuente. • Proporcione referencias o vínculos al material, en lugar de copiarlo. • Busque y obtenga el permiso del propietario de los derechos de autor para usar el material. <p>En Internet es posible verse implicado en actividades ilegales o poco éticas, como difamar a una persona,</p>	

	<p>participar en juegos de azar o adquirir artículos cuya compra o venta no es legal en su país. Por lo tanto, tenga en cuenta las leyes locales e internacionales antes de involucrarse en una actividad de este tipo.</p>	
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Caballo de Troya

Programa informático destructivo que se camufla como un juego, una herramienta o un software. Cuando se ejecuta, un caballo de Troya provoca algún tipo de daño a la computadora aunque parezca que esté haciendo algo útil.

Calumnia

Difamación escrita que ha sido publicada. La calumnia constituye un delito castigado por la ley.

Capa de sockets seguros (SSL)

Protocolo de seguridad de Internet que garantiza una comunicación de datos segura mediante el cifrado de la información transmitida. El protocolo SSL certifica que un sitio Web es genuino y garantiza que no se hará un mal uso de los datos proporcionados en él.

Cifrado

Proceso de convertir datos en un formato ilegible y que no se pueda usar. El cifrado se realiza para evitar el acceso no autorizado a los datos, especialmente durante la transmisión de datos a través de Internet.

Contenido activo

Programa pequeño que se instala en una computadora mientras se navega por Internet. Su función principal es ofrecer una experiencia de Internet interactiva a través de vídeos y barras de herramientas. En ocasiones se usa para obtener acceso no autorizado a una computadora y dañar sus datos o instalar software malintencionado en ella.

Contraseña

Cadena de caracteres única que escribe un usuario como código de identificación. Se trata de una medida de seguridad para restringir el acceso a las computadoras y archivos confidenciales.

Cookie

Archivo pequeño que se crea cuando un usuario visita un sitio Web. Los sitios Web usan cookies para identificar a los usuarios que los visitan y también realizan un seguimiento de sus preferencias.

Correo no deseado

Mensaje de correo electrónico irrelevante y no solicitado enviado por un remitente desconocido. El correo no deseado se envía para distribuir un mismo mensaje a muchos destinatarios al mismo tiempo.

Depredador en línea

Persona que establece contacto con usuarios de Internet a través de salones de chat, foros en línea o correo electrónico con el fin de aprovecharse de ellos económicamente o implicarlos en relaciones peligrosas.

Derechos de autor

Método de protección legal de los derechos del creador original de un trabajo creativo, como puede ser un texto, una pieza musical, una pintura o un programa informático.

Descifrado

Proceso de volver a convertir los datos cifrados en un formato legible y que se pueda usar.

Firewall

Filtro que bloquea información no confiable de Internet antes de que llegue a una computadora o una red privada. Ofrece asimismo protección adicional contra amenazas, tales como piratas informáticos y virus. Un firewall ayuda además a garantizar la privacidad de la computadora, ya que restringe el acceso externo por parte de algún usuario no autorizado.

Gusano

Programa informático que se propaga por las computadoras, normalmente replicándose en la memoria de cada una de ellas. Un gusano puede duplicarse con tanta frecuencia en una computadora que puede bloquear la computadora.

Injuria

Difamación verbal. La injuria constituye un delito castigado por la ley.

Memoria caché

Memoria temporal de la computadora que en ocasiones se usa para almacenar copias locales de archivos abiertos al navegar por Internet.

Nombre de usuario

Nombre con el que se identifica un usuario en una computadora o una red. Para tener acceso a una computadora protegida con nombre de usuario y contraseña, es necesario escribir la combinación correcta de nombre de usuario y contraseña.

Pirata informático

Persona que usa sus conocimientos informáticos para obtener acceso no autorizado a una computadora y después alterar o hacer un mal uso de los programas y datos almacenados en ella.

Piratería de software

Copia no autorizada de software con derechos de autor sin obtener la licencia o el permiso de su propietario de derechos de autor.

Plagio

Acto por el cual se copia el trabajo de alguien y se usa como si fuera propio sin mencionar la fuente.

Privacidad de la computadora

Mantener los datos de un usuario, incluidos los mensajes de correo electrónico y archivos personales, de tal manera que no pueda tener acceso a ellos ninguna persona que no cuente con el permiso adecuado.

Propiedad intelectual

Cualquier información disponible en Internet es una propiedad intelectual, cuyo propietario legal es la persona que la creó. El propietario de una propiedad intelectual tiene derechos exclusivos para controlar el uso de esta información.

Proveedor de servicios Internet (ISP)

Compañía que permite que personas, empresas y organizaciones se conecten a Internet.

Realizar una copia de seguridad

Hacer un duplicado de un programa, un disco o datos. El duplicado se denomina copia de seguridad.

Seguridad de la computadora

Proteger una computadora y sus datos ante posibles pérdidas y alteraciones, ya sean accidentales o intencionadas.

Sobrevoltaje

Un aumento repentino del voltaje de la línea que puede ocasionar daños en los dispositivos electrónicos, como las computadoras.

Spyware

Programa informático que se instala en su computadora sin su conocimiento. El spyware puede enviar en secreto información sobre sus hábitos de exploración del Web u otros detalles personales a otras computadoras a través de la red.

Suplantación de identidad

Acto por el cual se obtiene información personal, como contraseñas y detalles de tarjetas de crédito, de los usuarios de computadoras con el fin de usarla posteriormente con fines malintencionados.

Virus

Programa informático diseñado para causar el mal funcionamiento de una computadora o dañar los datos almacenados en ella.