Resolución de Secretaría General

Lima, 13 JUL. 2016

N° 023-2016-PCM/SG

VISTOS: Los Memorandos N° 1043-2015-PCM/OS, N° 166-2016-PCM/OS y N° 227-2016-PCM/OS e Informe N° 005-2016-PCM/OS-JMOSyR de la Oficina de Sistemas; Memorando N° 245-2016-PCM/OGA de la Oficina General de Administración; el Memorando N° 536-2016-PCM/OGPP e Informe N° 017-2016-PCM/OGPP/GABS de la Oficina General de Planeamiento y Presupuesto; y el Informe N° 075-2016-PCM/OGAJ-CMV de la Oficina General de Asesoría Jurídica; y,

CONSIDERANDO:

Que, de conformidad con el artículo 22 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante el Decreto Supremo N° 063-2007-PCM, y modificatorias, la Oficina General de Administración es el órgano responsable de la gestión de los sistemas de recursos humanos, materiales, económicos y financieros, así como la prestación de servicios para el normal funcionamiento de los órganos de la Presidencia del Consejo de Ministros;

Que, el numeral 23.7 del artículo 23 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, establece como una de las funciones de la Oficina General de Administración, el proponer resoluciones, normas y directivas, así como celebrar contratos y convenios, sobre asuntos de su competencia;

Que, asimismo, de acuerdo al artículo 28 del citado Reglamento de Organización y Funciones, la Oficina de Sistemas es la unidad orgánica, que depende jerárquicamente de la Oficina General de Administración, encargada de realizar las actividades relacionadas con el desarrollo, implementación, operación, mantenimiento y seguimiento de los sistemas informáticos y de brindar soporte técnico a los usuarios. Asimismo, es responsable del trámite documentario y el archivo de la Entidad;

Que, mediante la Resolución Ministerial N° 053-2015-PCM, se aprobó la Directiva N° 001-2015-PCM "Normas para la formulación, modificación y aprobación de directivas en la Presidencia del Consejo de Ministros", que tiene como objetivo normar y establecer los lineamientos para la formulación, modificación y aprobación de directivas que se expidan en la Presidencia del Consejo de Ministros;

Que, de acuerdo al numeral 5.3 de la Directiva General N° 001-2015-PCM/SG, los titulares de los órganos, comisiones, programas y proyectos especiales de la Presidencia del Consejo de Ministros, son responsables de evaluar las directivas bajo su ámbito, cuya vigencia sea mayor a los dos años, con el fin de proceder a su actualización y/o iniciar los trámites de aprobación de nuevas directivas que las reemplacen, de ser el caso;

Que, mediante Resolución del Secretario General N° 005-2004-PCM se aprueba la Directiva N° 005-2004-PCM/SG "Directiva de Seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros";

Que, mediante Memorandos N° 1043-2015-PCM/OS, N° 166-2016-PCM/OS, N° 277-2016-PCM/OS e Informe Técnico N° 005-2016-PCM/OS-JMOSyR, la Oficina de Sistemas propone la actualización de la Directiva N° 005-2004-PCM/SG señalando que tiene una vigencia mayor a dos años; que existen normativas en vigencia que deben incluirse, así también es necesario excluir las normas derogadas; y, que la entidad requiere cumplir con la implementación de la NTP ISO/IEC 27001:2014;

Que, conforme a lo dispuesto en el numeral 7.2.3 de la Directiva General N° 001-2015-PCM/SG, las directivas quedan sin efecto por declaración expresa, cuando las disposiciones de la que emanan pierden vigencia o cuando su materia es integrante o regulada por otra directiva;

Que, en dicho sentido, atendiendo a las sustanciales modificaciones que contiene la propuesta de Directiva "Medidas de Protección contra virus informáticos y software malicioso en la Presidencia del Consejo de Ministros"; corresponde aprobar una nueva Directiva y dejar sin efecto la Directiva N° 005-2004-PCM/SG "Directiva de Seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros" aprobada mediante la Resolución del Secretario General N° 005-2004-PCM de fecha 23 de junio de 2004;

Que, de conformidad con lo dispuesto en el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 063-2007-PCM, y sus modificatorias; y, a la delegación efectuada en el numeral 1.1 del artículo 1 de la Resolución Ministerial N° 298-2015-PCM, rectificada por Fe de Erratas publicada en el Diario Oficial El Peruano el 9 de enero de 2016;

Con los vistos de la Oficina General de Administración; de la Oficina General de Planeamiento y Presupuesto; y de la Oficina General de Asesoría Jurídica;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva N° 006 -2016-PCM/SG "Medidas de Protección contra virus informáticos y software malicioso en la Presidencia del Consejo de Ministros", cuyo texto forma parte integrante de la presente Resolución de Secretaría General.

Artículo 2.- Dejar sin efecto la Directiva N° 005-2004-PCM/SG "Directiva de Seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros" aprobada mediante la Resolución del Secretario General N° 005-2004-PCM de fecha 23 de junio de 2004;

Artículo 3.- Disponer la publicación de la presente Resolución de Secretaría General y de la Directiva a que hace referencia el artículo 1, en el Portal Institucional de la Presidencia del Consejo de Ministros (www.pcm.gob.pe).

Regístrese y comuníquese

ABOG. MANUEL MESONES CASTELO
Secretario General
Presidencia del Consejo de Ministros

Directiva006-2016-PCM/SG

Medidas de Protección contra virus informáticos y software malicioso en la Presidencia del Consejo de Ministros

2016

HOJA DE INFORMACIÓN GENERAL

CONTROL DOCUMENTAL:

PROYECTO:	Directiva "Medidas de Protección contra virus informáticos y software malicioso en la Presidencia del Consejo de Ministros"
ENTIDAD:	Presidencia del Consejo de Ministros.
VERSIÓN:	2.0
FECHA EDICIÓN:	Febrero 2016
DOCUMENTOS RELACIONADOS:	Directiva N° 005-2004-PCM/SG "Directiva de seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros"

DERECHOS DE USO:

La presente documentación es de uso interno de la Presidencia del Consejo de Ministros.

ESTADO FORMAL:

Preparado por:	Revisado por:	Aprobado por:
Nombre: Julia Milagros Olea Sal y Rosas Oficina : Oficina de Sistemas Cargo : Oficial de Seguridad de la Información Entidad: PCM Fecha: Nov 2015	Nombre: Jorge Calderón Sánchez Oficina : Oficina de Sistemas Cargo : Coordinador de Soporte Entidad: PCM Fecha: Nov 2015 Nombre: María Angélica Castillo Cargo: Jefe de la Oficina de Sistemas Entidad: PCM Fecha: Nov 2015	Nombre: Manuel Gustavo Mesones Castelo Oficina: Secretaría General Cargo: Secretario General Entidad: PCM Fecha: Feb 2016

Control de Versiones

Versión	Fecha de aprobación	Elaboración	Revisión	Aprobación	Breve descripción
1.0	2004	Oficina de Desarrollo y Sistemas de PCM con el apoyo ONGEI	Nombre: Rafael Parra Erkel Cargo: Jefe (e) Oficina de Desarrollo y Sistemas Jefe de la Oficina Nacional de Gobierno Electrónico e Informática Entidad: PCM Fecha: Junio 2004	Resolución de SA Nº 005-2004-PCM Directiva 005-2004-PCM/SG	Documento que presenta la directiva para la seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros

NOTAS

- La presente versión sustituye completamente a todas las precedentes de manera que este sea el único documento válido.

- El propietario de los documentos de Seguridad de la Información es el personal que haga las veces de Oficial de Seguridad de la Información

CONTENIDO

"Medidas de Protección contra virus informáticos y software malicioso en la Presidencia del Consejo de Ministros"

Directiva -2016-PCM/SG

I. OBJETIVO

Establecer normas de protección de los Sistemas de Información, Red Institucional, equipos de cómputo y servicios informáticos asignados a los usuarios de la Presidencia del Consejo de Ministros ante la presencia de virus informáticos y software malicioso.

II. FINALIDAD

Proporcionar procedimientos y conceptos básicos para evitar y mitigar los riesgos de una infección por virus informáticos y software malicioso en los Sistemas de Información, Red Institucional, equipos de cómputo y servicios informáticos asignados a los usuarios en la Presidencia del Consejo de Ministros.

III. BASE LEGAL

- Ley N° 27444- Ley del Procedimiento Administrativo General.
- Decreto Supremo N° 063-2007-PCM que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Resolución Ministerial N° 053-2015-PCM, que aprueba la Directiva N° 001-2015-PCM/SG "Norma para la formulación, modificación y aprobación de Directivas en la PCM".
- Resolución Jefatural 088-2003 INEI, que aprueba la Directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública"
- Resolución de Contraloría N° 320-2006-CG, que aprueba "Normas de Control Interno"
- Resolución Ministerial N° 004-2016-PCM, Aprueba el uso obligatorio de la "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática
- Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales no arancelarias N° 129-2014/CNB-INDECOPI, que aprueba como Norma Técnica Peruana la "NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA

INFORMACIÓN. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requisitos. 2ª Edición. Reemplaza a la NTP-ISO/IEC 27001:2008"

IV. ALCANCE

El cumplimiento de lo dispuesto en la presente Directiva es de aplicación a todos los órganos y unidades orgánicas, proyectos, programas y comisiones adscritas de la Presidencia del Consejo de Ministros.

V. RESPONSABILIDAD

5.1 La Oficina de Sistemas de la Presidencia del Consejo de Ministros es responsable de lo siguiente:

a) Aplicar, hacer el seguimiento y la evaluación del cumplimiento de la presente directiva

b) Administrar y supervisar el buen funcionamiento de los sistemas informáticos, servicios informáticos y red de la institución.

c) Administrar y asignar los recursos informáticos de la Presidencia del Consejo de Ministros.

d) Concientizar, asesorar y capacitar al personal de la Institución, sobre el buen uso de los recursos y servicios informáticos, las normas, procedimientos vigentes y los compromisos que han adquirido para el acceso a los sistemas informáticos, equipos de cómputo, servicios y red de la Institución.

e) Gestionar y controlar el uso y la instalación de software y hardware en los equipos informáticos de la institución.

f) Instalar las soluciones antivirus y antimalware que permita mantener en buen funcionamiento a los equipos de cómputo de los usuarios y del Centro de Datos.

5.2 Los usuarios son responsables de lo siguiente:

a) Realizar adecuado uso de los equipos de cómputo que les han sido asignados.

b) Colaborar con la seguridad de la información de la Red Institucional, de los sistemas y servicios informáticos a los que tenga acceso.

c) Revisar los medios de almacenamiento externos con la solución antivirus/ antimalware instalada en los equipos de cómputo asignados, para asegurarse que los archivos contenidos estén libres de infección.

d) Cautelar la apertura y contestación de correos electrónicos que provengan de remitentes desconocidos o dudosos, ni acceder a los enlaces y/o archivos adjuntos sospechosos, debiendo reportar los eventos de este tipo a la Oficina de Sistemas.

VI. DISPOSICIONES GENERALES

6.1 La Oficina de Sistemas de la Presidencia del Consejo de Ministros, es la única oficina autorizada para realizar la instalación de software y hardware en los equipos informáticos de la institución.

6.2 Los equipos informáticos del usuario y del Centro de Datos deben tener instalado una solución de software antivirus/antimalware confiable y con licencia vigente, que permita establecer filtros significativos que detecten correos electrónicos con contenido malicioso, como puede ser: el remitente, el asunto, el cuerpo del mensaje y el anexo.

6.3 La Oficina de Sistemas debe realizar la entrega de equipos Informáticos a los usuarios que se incorporen a laborar en la Presidencia del Consejo de Ministros, con la versión actualizada de la solución antivirus / antimalware con que se cuente.

6.4 La Oficina de Sistemas debe instalar la solución antivirus / antimalware con que se cuente, solo a los equipos informáticos de la Presidencia del Consejo de Ministros.

6.5 La Oficina de Sistemas mantendrá actualizada la protección antivirus en la Presidencia del Consejo de Ministros, sin mediar la intervención del usuario final, mediante actualizaciones automáticas y calendarizadas. En caso de alerta, las actualizaciones deberán ser frecuentes, como mínimo cada 3 horas.

6.6 La Oficina de Sistemas debe mantener actualizada la instalación de mejoras y correcciones de software que publiquen las compañías fabricantes, a fin de mitigar las vulnerabilidades de estos softwares. De esta manera se puede controlar eficazmente los efectos que podría provocar la ejecución de archivos con código malicioso.

6.7 Los equipos de cómputo asignados a los usuarios son exclusivamente para uso oficial, por tanto debe cumplirse con las medidas de protección señaladas en la

presente directiva, bajo responsabilidad directa del usuario.

6.8 La Oficina de Sistemas debe realizar el mantenimiento técnico correctivo a los recursos informáticos de la Institución que sean afectados por la infección de un virus informático o malware, de forma inmediata.

6.9 La Oficina de Sistemas debe realizar periódicamente el mantenimiento técnico preventivo a los equipos informáticos para actualizar las bases de datos de virus/ malware y las versiones de las soluciones de software correspondientes.

6.10 Para comunicar una alerta de virus, el usuario debe enviar un correo electrónico a: soporte@pcm.gob.pe, con el asunto: [VIRUS], sustentando la razón del envío de la alerta

6.11 La Oficina de Sistemas debe mantener un registro de las alertas por infección de virus recibidas de los usuarios, estaciones de trabajo y servidores, adjuntándolos al Reporte de Incidencias mensual, para su análisis posterior. Este registro es de uso interno de la Oficina de Sistemas.

6.12 La Oficina de Sistemas debe efectuar a la brevedad los procedimientos de limpieza de virus y malware, al detectar infecciones de equipos informáticos por el reporte de los agentes instalados, para lo cual los usuarios deben otorgar todas las facilidades del caso.

6.13 Los usuarios son pasibles de sanción de comprobarse que provocan deliberadamente el mal funcionamiento de computadoras, componentes periféricos de redes y sistemas o al ejecutar software malicioso.

VII. DISPOSICIONES ESPECÍFICAS

7.1 Correo Electrónico

7.1.1 El servicio de correo electrónico institucional es para uso exclusivo de envío y recepción de información relacionada al desarrollo de las funciones y actividades, que el usuario cumple para la Presidencia del Consejo de Ministros.

7.1.2 La cuenta de correo electrónico institucional que se asigna a cada usuario no debe usarse para el envío de ningún archivo que contenga algún tipo de software malicioso.

7.1.3 En caso de que un usuario reciba correos de procedencia dudosa o

sospeche que podría ser malicioso, deberá notificar el hecho a la Oficina de Sistemas, al correo electrónico: soporte@pcm.gob.pe con el asunto: [CORREO SOSPECHOSO], para que la Oficina de Sistemas tome las acciones pertinentes ante dicha alerta. Por ningún motivo se debe dar respuesta directa a estos correos.

7.1.4 Los usuarios deben tener especial cuidado con los archivos o enlaces que pueden estar incluidos en los mensajes recibidos, porque pueden desencadenar la descarga de software malicioso que afecte negativamente al equipo de cómputo y a la red institucional. Por lo tanto, no debe abrir archivos que provengan de usuarios desconocidos ni acceder a los enlaces adjuntos.

7.1.5 Los usuarios deben evitar abrir los archivos adjuntos a un mensaje de correo electrónico cuya extensión sea ".exe", ".vbs", ".pif", ".bat" o ".bak" o que tengan doble extensión (Por ejemplo: informe.doc.exe)

7.1.6 La configuración de la solución antivirus/antimalware que la entidad utilice debe contemplar el análisis automático del correo electrónico, tanto entrante como saliente y que no permita la instalación de ningún programa que haga que los archivos adjuntos se descarguen de forma automática.

7.1.7 Ante la violación de cualquier política definida en el servidor, al recibir un correo electrónico infectado, el personal de Soporte de la Oficina de Sistemas debe acudir a ejecutar procedimientos de limpieza y desinfección, así como configurar acciones de procesamiento tales como eliminar el correo electrónico o eliminar los archivos adjuntos, notificando las acciones tomadas al usuario receptor. Asimismo, se informará al Administrador de Redes de la Oficina de Sistemas, a fin de que actualice las reglas de bloqueo y filtrado, las cuales pueden ser:

- Bloqueo de correos electrónicos por el campo FROM o DE.
- Bloqueo de correos electrónicos por el campo SUBJECT o ASUNTO.
- Bloqueo de correos electrónicos por el campo CC o Con Copia.
- Bloqueo de correos electrónicos por el campo DOMAIN o DOMINIO.
- Bloqueo de correos electrónicos por el campo TO o PARA.
- Bloqueo de correos electrónicos por tipos de extensión del adjunto.
- Bloqueo de correos electrónicos por tipos el nombre del adjunto.
- Bloqueo de correos electrónicos por tamaño del adjunto.
- Bloqueo de código o scripts HTML.

- Análisis de contenidos en archivos de la gama MS Office.

7.2 Internet

7.2.1 La Oficina de Sistemas debe implementar políticas de prevención de ataques configurando los equipos de la Infraestructura Tecnológica del Centro de Datos, a fin de detectar códigos contaminados introducidos por los protocolos SMTP, HTTP y FTP, códigos Java, VB Script y Active X. De esta manera, el sistema del usuario quedará protegido al entrar a Internet (a una página Web o al bajar información de la misma).

7.2.2 Los usuarios deben evitar descargar programas y aplicaciones desde sitios de Internet de prestigio dudoso o desconocido o del que se advierta sospechas de contener archivos con código contaminado o malicioso.

7.3 Red LAN

7.3.1 La Oficina de Sistemas debe establecer y mantener un cronograma para las actividades de limpieza de virus y código malicioso en la institución, debiendo ejecutarlo efectivamente.

7.3.2 Toda alerta recibida por infección de virus debe ser registrada para su análisis y control.

7.4 Equipos Informáticos

7.4.1 Los usuarios no deben instalar por sus propios medios, software en sus equipos de cómputo. Para proceder con la instalación de software, el usuario debe solicitar la intervención de la Oficina de Sistemas, quien debe efectuar la revisión e instalación del software; para ello el usuario previamente debe contar con la autorización de su jefe inmediato.

7.4.2 Los usuarios que ejecuten algún software no proporcionado por la Oficina de Sistemas en los equipos de cómputo asignados, sin la revisión previa por parte de esta oficina y no cuenten con la autorización del jefe inmediato, son responsables de los problemas que podrían ocasionar en dichos equipos y en los demás equipos conectados a la Red Institucional, así como de las licencias del software instalado que se invaliden por dicha causa.

7.4.3 El usuario deberá revisar los dispositivos de almacenamiento portátil USB (pendrive), disco duros externos o cualquier medio de

almacenamiento externo que se inserte en el equipo de cómputo asignado, a través del programa antivirus instalado, para evitar un posible contagio por virus o malware.

7.4.4 El usuario no debe acceder a contenidos web que puedan estar relacionados con servidores generadores de VIRUS o que puedan contener programas que permitan romper las claves de acceso u otros que puedan utilizarse con fines ilícitos, no autorizados y dañinos tanto para la entidad como para terceros.

7.5 Seguridad de la Información

7.5.1 El usuario que encuentre alguna irregularidad en los equipos de cómputo y/o servicios informáticos asignados, debe comunicarlo inmediatamente a la Oficina de Sistemas mediante correo electrónico a: soporte@pcm.gob.pe, a fin de que esta oficina tome las medidas correctivas correspondientes.

7.5.2 Los usuarios deben efectuar periódicamente una copia de seguridad de los datos relevantes de la información de su equipo de cómputo, guardando el mismo en la red o en medios portátiles como cds o dvds. De esta forma, si se produce un ataque vírico, se reduce el impacto en la pérdida de archivos que podría ocasionar esta situación.

7.5.3 Los usuarios que sospechen que su equipo de cómputo pueda estar infectado, debe informarlo a la Oficina de Sistemas mediante el correo electrónico: soporte@pcm.gob.pe, para que esta oficina tome las medidas inmediatas que correspondan ante dicha alerta.

VIII. DISPOSICIONES COMPLEMENTARIAS

8.1 Déjese sin efecto las normas internas en la parte que se opongan a la presente Directiva.

8.3 La presente versión sustituye completamente a todas las precedentes.

IX. GLOSARIO

1. **ACCESO:** Acción de poder ingresar a cualquier equipo de la entidad por parte del personal autorizado de la Oficina de Sistemas de manera local o remota.

2. **CHAT:** Comunicación escrita en tiempo real ("en vivo") a través de Internet entre dos o más personas.

3. **CORREO ELECTRÓNICO:** El correo electrónico, o e-mail, es el medio por el cual se pueden intercambiar mensajes utilizando un dispositivo electrónico.

4. **EQUIPO DE COMPUTO:** Conjunto (Kit) compuesto por una pantalla, teclado, mouse, impresora, UPS, estabilizador, cables, supresor de pico y/o estabilizador de corriente, CPU y protector de pantalla.

   También se denomina equipos de cómputo a las unidades de cinta (Tape Backup), lectora o lectora grabadora de CD, unidades DVD, módems externos, scanner, unidades de almacenamiento de información, debidamente identificados, que funcionan de manera sincronizada con otros componentes, pero con relativa autonomía para su operatividad.

5. **INTERNET:** Red de ordenadores a nivel mundial. Ofrece distintos servicios, como el envío y recepción de correo electrónico, la posibilidad de ver información en las páginas web, de participar en foros de discusión, de enviar y recibir ficheros mediante, de charlar en tiempo real, etc.

6. **LAN:** (Local Área Network), nombrado así a la interconexión de 2 o más computadoras que comparten servicios y recursos en común. La Red LAN es el conjunto de componentes que permite la interconexión de los equipos de cómputo a fin de que los usuarios puedan compartir y utilizar los recursos informáticos implementados. Está compuesto por los servidores (donde se almacena toda la información de los sistemas y servicios informáticos), medios de conexión (cable o medio, tarjetas de red y distribuidores de conexiones), y las estaciones de trabajo (equipo de cómputo del usuario).

7. **MANTENIMIENTO CORRECTIVO:** Acción que se realiza cuando un equipo de cómputo presenta una falla. El mantenimiento correctivo incluye el diagnóstico sobre la falla del equipo.

8. **MANTENIMIENTO PREVENTIVO:** Acción que permite detectar fallas repetitivas, disminuir los puntos muertos por paradas, aumentar la vida útil de los equipos, disminuir costos de reparación, detectar puntos débiles en la instalación, entre otras ventajas.

9. **SISTEMA DE INFORMACIÓN:** Todo aquel programa o software informático que se ha confeccionado para brindar un servicio de manejo de información, el mismo que puede haber sido creado por personal de la PCM o se haya adquirido.

10. **SISTEMA FIREWALL:** Un Sistema Firewall consta de un conjunto de mecanismos, filtros de protocolo y dispositivos de control de accesos que manejan de forma segura la conexión entre redes.
    Este sistema protege las comunicaciones entre un usuario y una red externa, de la forma más transparente posible para el usuario, facilitándole al máximo los servicios que dicha red ofrece. La mayoría de los sistemas firewall están diseñados para asegurar el tráfico con la red Internet, debido a que representa la mayor fuente de información y de medios de comunicación con terceros, incluyendo:

11. **SOFTWARE:** Cada uno de los programas que, una vez ejecutados, permiten trabajar con la computadora. Por ejemplo los procesadores de textos (Microsoft Word), hojas de cálculo (Microsoft Excel), bases de datos (SQL Server), programas de dibujo (Corel Draw), paquetes estadísticos (S-Plus), etc.

12. **USB:** Universal Serial Bus (bus universal en serie). El USB es utilizado como estándar de conexión de periféricos como: teclados, ratones, memorias USB, joysticks, escáneres, cámaras digitales, teléfonos móviles, reproductores multimedia, impresoras, dispositivos multifuncionales, sistemas de adquisición de datos, módems, tarjetas de red, tarjetas de sonido, tarjetas sintonizadoras de televisión y grabadoras de DVD externa, discos duros externos y disqueteras externas.

13. **DISCO DURO EXTERNO:** Es una unidad de disco duro que es fácil de instalar y transportar de una computadora a otra, sin necesidad de consumir constantemente energía eléctrica o batería.