

**MANUAL DE LINEAMIENTOS DEL USO DE LOS
RECURSOS INFORMÁTICOS INSTITUCIONALES**

CÓDIGO: DVM-A-DIG-MAN-02

OCTUBRE, 2021

TABLA DE CONTENIDO

| | | |
|-----------|---|-----------|
| 1 | HISTORIAL DE REVISIONES | 4 |
| 2 | INTRODUCCIÓN | 5 |
| 3 | OBJETIVOS..... | 5 |
| 3.1 | Objetivo General | 5 |
| 3.2 | Objetivos Específicos | 5 |
| 4 | ALCANCE | 6 |
| 5 | ABREVIATURAS Y DEFINICIONES..... | 6 |
| 5.1 | Abreviaturas..... | 6 |
| 5.2 | Definiciones | 6 |
| 6 | AUTOR: | 9 |
| 7 | ACTUALIZADO POR: | 9 |
| 8 | DIRECTRICES..... | 9 |
| 9 | RESPONSABILIDAD | 9 |
| 10 | DESCRIPCIÓN DEL MANUAL | 10 |
| 11 | DESCRIPCIÓN DE LINEAMIENTOS..... | 10 |
| 11.1 | Generales..... | 11 |
| 11.2 | Al usuario que tiene asignados los bienes informáticos..... | 12 |
| 11.3 | Al usuario que hace uso de los bienes informáticos | 15 |
| 11.4 | A las jefaturas..... | 17 |
| 11.5 | A la Administración | 17 |
| 11.6 | Relacionados a instalaciones de software..... | 18 |
| 11.7 | A la atención de solicitudes de Recursos Informáticos | 19 |
| 11.8 | Manejo de cuentas de usuario y contraseñas de acceso..... | 20 |
| 11.9 | Respaldo de datos | 21 |
| 11.10 | Uso de servicios en red | 22 |
| 11.11 | Permisos especiales a servicios del MEP | 22 |
| 11.12 | Uso del correo electrónico | 22 |
| 11.13 | Uso de correos masivos | 23 |



**VICEMINISTERIO ADMINISTRATIVO
DIRECCIÓN DE INFORMÁTICA DE GESTIÓN**

**MANUAL DE LINEAMIENTOS DEL USO DE LOS RECURSOS
INFORMÁTICOS INSTITUCIONALES**

| | | |
|-------|---|----|
| 11.14 | Uso del equipo de cómputo arrendado | 24 |
| 11.15 | Uso de impresoras arrendadas..... | 24 |
| 12 | <i>DOCUMENTOS DE REFERENCIA</i> | 25 |
| 13 | <i>HOJA DE FIRMAS</i> | 26 |

1 HISTORIAL DE REVISIONES

| Fecha | Versión | Descripción | Responsables |
|-----------------|---------|--|--|
| Marzo, 2008 | 1 | Documento inicial | Jefaturas de la DIG |
| Julio, 2009 | 2 | Se modifica tanto en forma como en fondo, de acuerdo a la reestructuración de la DIG. | Jefaturas de la DIG |
| Febrero, 2012 | 3 | Se modifica en su mayoría, pero su publicación no se llevó a cabo por diversas gestiones propias de la DIG. | Jefaturas de la DIG |
| Setiembre, 2017 | 4 | Se actualiza en su mayoría debido a la nueva forma de realizar las labores propias del área de acción de cada uno de los departamentos de la DIG | Kattia Paniagua Alfaro |
| Junio, 2019 | 5 | Se actualiza con el tema de arrendamiento de equipo de cómputo. | Kattia Paniagua Alfaro |
| Octubre, 2021 | 6 | <p>Se actualiza a nivel de redacción, basado en los siguientes documentos: Políticas Generales del Código Nacional de Tecnologías Digitales, Plan Estratégico Tecnología Información (PETI) y Política en Tecnologías de la Información del Ministerio de Educación Pública.</p> <p>Esto debido a la derogación de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de República a partir del 31 de diciembre del 2021, según resolución N° R-CO-26-2007, y modificación de las Normas de Control Interno para el sector público.</p> | <p>Fulton Hernández Espinoza, Departamento Sistemas de Información</p> <p>Jenny Navarro Blanco, Departamento Base de Datos</p> <p>Marlon Vásquez Vásquez, Departamento Soporte Técnico</p> <p>Tahyli Mondragón Fonseca, Departamento Soporte Técnico</p> <p>José Martín Sanchún Macín, Departamento Gestión y Control Informático</p> <p>Máximo Varela Castro, Departamento Adquisición Tecnológica</p> <p>Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones</p> |

2 INTRODUCCIÓN

La Ley General de Control Interno, Ley N° 8292, Artículo 12 del 31 de julio del 2002, establece para los jefes y los titulares subordinados los deberes de velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.

Así el Artículo 15 de esta Ley, estipula el deber de esos funcionarios de proteger y conservar todos los activos institucionales, ejerciendo los controles generales a todos los sistemas de información computarizados y de aplicación para el procesamiento de datos con *software*.

Dado que el Ministerio de Educación Pública (MEP) en su proceso de modernización, ha dotado de equipo informático y otros recursos tecnológicos a las Oficinas Centrales (OC) y Direcciones Regionales de Educación (DRE), lo cual actualmente es fundamental en el cumplimiento del servicio público que el Ministerio presta a toda la comunidad costarricense.

En el presente manual se establecen las reglas y procedimientos para la administración y buen uso de los recursos informáticos, así como los lineamientos técnicos establecidos por la Dirección de Informática de Gestión (DIG), constituyéndolos como complemento de la normativa oficial para el uso idóneo de los recursos informáticos a nivel de Oficinas Centrales y Direcciones Regionales de Educación.

3 OBJETIVOS

3.1 Objetivo General

Asegurar el uso eficiente de los recursos informáticos (*hardware* y *software*) empleando para ello buenas prácticas de seguridad y una adecuada administración, esto garantiza el máximo aprovechamiento y eficiencia posible en las Oficinas Centrales y Direcciones Regionales de Educación.

3.2 Objetivos Específicos

- Uniformar criterios sobre lineamientos técnicos para el adecuado e idóneo uso de los recursos informáticos del Ministerio.
- Aumentar la eficiencia en las labores cotidianas de los funcionarios que laboran en las dependencias del Ministerio.
- Promover medidas de seguridad para el *hardware* y *software* en Oficinas Centrales y Direcciones Regionales de Educación.
- Fiscalizar la administración de la plataforma informática y telemática del Ministerio a nivel de *hardware* y *software*, en relación con los sistemas, bases de datos y los servicios en red, como también los recursos informáticos asignados individualmente a los funcionarios de las Oficinas Centrales y Direcciones Regionales de Educación, para garantizar su máximo aprovechamiento y eficiencia permisible.

- Asegurar el cumplimiento de las disposiciones contenidas en el presente manual.

4 ALCANCE

Establece los lineamientos y políticas a seguir en el uso de los recursos informáticos en el Ministerio de Educación Pública, entiéndase para estos efectos Oficinas Centrales y Direcciones Regionales de Educación.

5 ABREVIATURAS Y DEFINICIONES

5.1 Abreviaturas

DIEE: Dirección de Infraestructura y Equipamiento Educativo.

DIG: Dirección de Informática de Gestión.

DRE: Direcciones Regionales de Educación.

MEP: Ministerio de Educación Pública.

OC: Oficinas Centrales.

5.2 Definiciones

Administración de bienes o servicios informáticos: Función que consiste en controlar, autorizar y administrar la utilización de los recursos y bienes informáticos disponibles en el Ministerio. Esta labor recae sobre las Unidades de Informática, a nivel de Dirección o Centros de Tecnologías de Información

Áreas Informáticas: Lugar donde se concentran bienes informáticos con alto grado de sensibilidad (servidores, equipos de comunicaciones, entre otros).

Arrendamiento: Alquiler de un bien o servicio por un tiempo y precio definidos.

Bienes Informáticos: Todos los recursos materiales o productos *hardware*, *software* (estaciones de trabajo, servidores, impresoras, accesorios, equipos de comunicaciones, conmutadores (*switches*), concentradores (*hubs*), enrutadores, módems, *firewall* (muro de fuego), cableado, programas de computación, sistemas de información, paquetes, utilitarios, entre otros), servicios informáticos y en general cualquier otro producto informático propiedad del MEP o que bajo su autorización se tenga derecho de uso en la Institución.

Computador: Máquina electrónica que recibe y procesa datos para convertirlos en información conveniente y útil, que posteriormente se envían a las unidades de salida. Tiene tamaño mediano y es utilizado por un usuario a la vez.

Contraseña: Combinación de letras (mayúsculas y/o minúsculas), números y caracteres especiales que debe teclearse para obtener acceso a un programa o partes de un sistema, terminal u ordenador personal, punto en la red, entre otros. Muchas veces se utiliza la terminología inglesa (*password*) para referirse a la clave de acceso.

Contrato de arrendamiento: Relación entre dos partes, mediante la cual se obligan de manera recíproca y por un tiempo determinado la cesión de un bien o servicio, quedando obligada la parte que aprovecha la posesión a pagar un precio determinado, ya sea en un solo desembolso o en forma periódica.

Correo electrónico: Forma de comunicarse mediante mensajes enviados y recibidos a través de Internet.

Cuentas de usuario: Colección de información que indica al sistema operativo, los archivos y carpetas a los que puede obtener acceso. Permite que se comparta el mismo equipo entre varias personas, cada una de las cuales tiene sus propios archivos, configuraciones y acceso a ella con un nombre y contraseña.

Freeware: Tipo de *software* que se distribuye sin costo, disponible para su uso y por tiempo ilimitado

Funcionario público: Persona encargada de ejercer las funciones atribuidas al Estado en virtud de un mandato constitucional y/o legal.

El Numeral 111 de la Ley General de la Administración Pública define al “funcionario público” del siguiente modo:

“Artículo 111.- 1. Es servidor público la persona que presta servicios a la Administración o a nombre y por cuenta de ésta, como parte de su organización, en virtud de un acto válido y eficaz de investidura, con entera independencia del carácter imperativo, representativo, remunerado, permanente o público de la actividad respectiva.”

En concordancia con el Artículo 111 de la Ley General de la Administración Pública, No. 6227 y el Artículo 2° de la Ley contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública, No. 8422, los términos “funcionario”, “servidor” y “empleado” público serán equivalentes.

“Artículo 2°—Servidor público. Para los efectos de esta Ley, se considerará servidor público toda persona que presta sus servicios en los órganos y en los entes de la Administración Pública, estatal y no estatal, a nombre y por cuenta de esta y como parte de su organización, en virtud de un acto de investidura y con entera independencia del carácter imperativo, representativo, remunerado, permanente o público de la actividad respectiva. Los términos funcionario, servidor y empleado público serán equivalentes para los efectos de esta Ley.../.”

Hardware: Todas las partes tangibles de un sistema informático y cuyos componentes pueden ser eléctricos, electrónicos, electromecánicos y mecánicos.

Internet: Gran comunidad de computadoras conectadas entre sí, por medio de líneas de comunicaciones especiales, agrupando una gran cantidad de asociaciones y empresas.

Lineamientos Generales Informáticos: Conjunto de instrucciones o normas generales que rigen la utilización y tenencia de los bienes y servicios informáticos.

Navegador Web: Programa que provee una interface para acceder y ver archivos en Internet.

Nube (Cloud): Tendencia tecnológica que brinda un servicio que funciona a través de Internet, permite a los usuarios guardar información de cualquier tipo, teniéndolos alojados en servidores dedicados 24/7/365 y pudiéndolos acceder desde cualquier lugar del mundo. Conocido como computación en la nube, servicios en la nube, informática en la nube, nube de cómputo (del inglés *cloud computing*).

Recurso informático: Todos aquellos componentes de *hardware* y *software* que son necesarios para el buen funcionamiento y optimización del trabajo con computadores y sus periféricos, tanto a nivel Individual, colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos. Los recursos son las aplicaciones, herramientas, dispositivos (periféricos) y capacidades con los que cuenta una computadora.

Red de datos institucional: Infraestructura de comunicaciones por medio de la cual se proveen los servicios asociados a ella. Entiéndase por datos, cualquier formato en el que los mismos puedan ser representados (texto, voz, imagen, entre otros).

Servicios Informáticos: Define las actividades relacionadas con el soporte técnico a la función informática; como pueden ser el desarrollo de sistemas informáticos, asesorías en el uso de los sistemas automatizados institucionales, utilización de los servicios de red (correo electrónico, Internet, entre otros), conexión de equipos a la red y otros; consultorías tanto a nivel del *software* como del *hardware* que posee la Institución, mantenimiento de servidores, computadores personales y/o distintos dispositivos que constituyen la infraestructura de red, capacitación en el uso de las diferentes herramientas tecnológicas; y otras, las cuales están orientadas a la satisfacción de los requerimientos de los usuarios y los del Ministerio, como tal.

Sistemas Informáticos: Equipo informático que junto con el *software* base, herramientas y elementos conexos prestan un determinado servicio informático, que el usuario utiliza para el procesamiento de la información generada por su actividad laboral, sean estas aplicaciones funcionales a la medida, corporativas, departamentales o locales al puesto, desarrolladas o adquiridas para la gestión administrativa de la institución.

Software: Equipamiento lógico o soporte lógico de un sistema informático; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

UPS: Dispositivo de alimentación eléctrica ininterrumpida.

Usuario externo: Persona(s) física(s) o jurídica(s) ajena(s) a la Institución que utilizan bienes o servicios informáticos que el MEP provee.

Usuario interno: Persona que labora en la estructura administrativa sea esta Dirección, Departamento o Unidad Administrativa en el MEP y que utiliza o accede a cualquier bien o servicio informático.

World Wide Web: Servicio de Internet ampliamente difundido. Muchas personas piensan en el web como un sinónimo de Internet, y no se dan cuenta que "la web" es una entidad que corre

en el Internet. La característica más importante de los documentos WWW es que están enlazados con otros documentos por medio de hipertexto. Conocida como WWW o simplemente "la web".

6 AUTOR:

Jefaturas de la DIG.

7 ACTUALIZADO POR:

Lic. Fulton Hernández Espinoza, Departamento Sistemas de Información, octubre 2021.

Licda. Jenny Navarro Blanco, Departamento Base de Datos, octubre 2021.

Licda. Tahyli Mondragón Fonseca, Departamento Soporte Técnico, octubre 2021.

Lic. Marlon Vásquez Vásquez, Departamento Soporte Técnico, octubre 2021.

Lic. Martín Sanchún Macín, Departamento Gestión y Control Informático, octubre 2021.

Lic. Máximo Varela Castro, Departamento Adquisición Tecnológica, octubre 2021.

Licda. Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones, octubre 2021.

8 DIRECTRICES

El presente documento es de conocimiento y aplicación obligatoria para todos los funcionarios del Ministerio de Educación Pública.

9 RESPONSABILIDAD

Los funcionarios del MEP, son responsables de cumplir a cabalidad con los lineamientos indicados en este documento. Así mismo, los jefes tienen la responsabilidad de velar por el cumplimiento de estos lineamientos.

10 DESCRIPCIÓN DEL MANUAL

En este manual se describen aspectos generales, reglas y procedimientos para la administración y buen uso de los recursos informáticos; así como las responsabilidades que conllevan, esto con la finalidad de unificar criterios y términos relacionados a los lineamientos técnicos establecidos por la DIG, constituyéndolos como complemento de la normativa oficial para el uso idóneo de los recursos informáticos a nivel de Oficinas Centrales y Direcciones Regionales de Educación. Adicionalmente, se establece el uso correcto de los servicios en la Intranet e Internet, con el objetivo de enmarcar las prohibiciones, los controles y la adecuada y/o eficiente administración.

De acuerdo con los Artículos 28 Inciso a) y 102 Inciso a) de la Ley General de la Administración Pública, es de acatamiento obligatorio para todos los funcionarios del Ministerio de Educación Pública, una vez que se haya cumplido con los requisitos de publicidad establecidos en el Artículo 125 de la Ley General de la Administración Pública. Adicionalmente, deberán cumplir con lo que se relacione a los bienes y servicios informáticos que dicta este documento, independientemente de su clase de puesto y especialidad.

11 DESCRIPCIÓN DE LINEAMIENTOS

El Ministerio de Educación Pública cuenta con una red y recursos informáticos institucionales para el uso de sus colaboradores, tanto en Oficinas Centrales como en Direcciones Regionales de Educación, los cuales fortalecen el flujo de información interna y externa. A su vez, apoyan las diferentes tareas que desarrolla la Institución en el mejoramiento de los procesos de gestión.

Los bienes y servicios informáticos ministeriales son herramientas de trabajo que, por uso distinto a lo regulado en el presente manual, puede implicar responsabilidades disciplinarias al funcionario, establecidas en los siguientes documentos: Ley de Derecho de Autor y Derechos Conexos, Ley de Delitos Informáticos, Reglamento Interno de Trabajo del MEP, Ley General de Administración Pública y demás normativa conexas.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) rigen hasta el 31 de diciembre del 2021, según resolución N° R-CO-26-2007, y modifica las Normas de Control Interno para el sector público, en la cual la Contraloría General de la República las deroga a partir del 1 de enero del 2022.

Es por ello, que este documento se ajusta para que cumpla a cabalidad con lo establecido en el ítem Políticas Generales del Código Nacional de Tecnologías Digitales, Plan Estratégico Tecnología Información (PETI) y Política en Tecnologías de la Información del Ministerio de Educación Pública. Los siguientes ítems responden a los objetivos estratégicos del Eje 5 del documento Políticas TIC del Ministerio de Educación Pública.

11.1 Generales

- Los funcionarios de Oficinas Centrales y Direcciones Regionales de Educación están obligados a acatar la normativa que a continuación se cita (REGLAMENTO INTERIOR DE TRABAJO DEL MINISTERIO DE EDUCACIÓN PÚBLICA (Decretos Ejecutivos: 5771-E del 21 de abril de 1976, Alcance No 65 y 10137-E del 30 de mayo de 1979, Gaceta No. 116)), relacionados al adecuado uso de los bienes y/o servicios informáticos, así como del deber de vigilancia.

“Artículo 42, además de lo dispuesto en este reglamento, son obligaciones de los servidores del Ministerio:

Inciso H. Responder por los objetos, máquinas, útiles o herramientas del Ministerio que tengan en uso y reponer o pagar aquellos cuyo deterioro, destrucción o pérdida les sea imputable.

Inciso I. Cuidar las máquinas, el mobiliario, equipo y útiles de propiedad o al servicio de las Institución y no usarlos para fines distintos de aquellos a que están destinados, velar porque no sufran más deterioro que el que exige el trabajo.”

“Artículo 43, además de las contempladas en el artículo anterior y en otros del presente Reglamento, los Directores, Jefes de Departamento, de Sección o de Unidad, tendrán las siguientes obligaciones:

Inciso A. Supervisar las labores de todos los servidores subalternos, tanto en el aspecto técnico como en el administrativo.

Inciso C. Cuidar la disciplina y la buena asistencia de los servidores subalternos bajo su responsabilidad, reportando lo correspondiente al Departamento de Personal, para que determinen las sanciones que correspondan.”

“Artículo 46, además de lo dispuesto en el Código de Trabajo, Estatuto de Servicio Civil y su Reglamento y otras normas del presente Reglamento, queda absolutamente prohibido a los empleados:

Inciso A. Ocupar tiempo dentro de las horas de trabajo, para asuntos ajenos a las labores que les han sido encomendadas.

Inciso B. Recibir visitas o hacer uso del teléfono para asuntos personales en horas de trabajo, salvo casos de urgencia.

Inciso F. Hacer dentro del ministerio o en desempeño de sus funciones demostraciones manifiestas de carácter político, electoral, divulgar asuntos que puedan entorpecer las labores del ministerio, así como ejercer actividades o hacer propaganda en cualquier forma, contrarias al orden público o al régimen democrático que establece la constitución política.

Inciso H. Salvo los casos que conlleven fines benéficos y otros debidamente autorizados por la Oficina de Personal, hacer colectas, rifas o

ventas de objetos dentro de los locales en donde presten sus servicios en horas de trabajo.

Inciso Q. Cualquier otro proceder contrario a la moral y buen nombre que necesariamente debe poseer todo empleado del Ministerio.”.

- Los funcionarios de Oficinas Centrales y Direcciones Regionales de Educación que incumplan con cualquiera de las obligaciones establecidas, podrán ser sujetos de eventuales responsabilidades disciplinarias, de conformidad con la normativa que rige su relación de servicio, y la norma que a continuación se cita del REGLAMENTO INTERIOR DE TRABAJO DEL MINISTERIO DE EDUCACIÓN PÚBLICA (Decretos Ejecutivos: 5771-E del 21 de abril de 1976, Alcance No 65 y 10137-E del 30 de mayo de 1979, Gaceta No. 116))

“Artículo 54. Las contravenciones al presente reglamento y las faltas en que incurran los servidores serán sancionadas con las siguientes medidas disciplinarias:

Amonestación verbal, Apercibimiento escrito, Suspensión del trabajo sin goce de salario hasta por 15 días y Despido sin responsabilidad patronal.”

- Es responsabilidad de cada jefatura, velar por el cumplimiento de las normas establecidas, y a la vez notificar a la Dirección de Informática de Gestión, los cambios o movimientos del personal que autoriza, ya sea por traslados a otra dependencia, despido, renuncia, entre otros.
- El incumplimiento de las normas establecidas en este manual podrá acarrear responsabilidad administrativa, disciplinaria, civil y penal.

11.2 Al usuario que tiene asignados los bienes informáticos

Este punto, hace cumplimiento al capítulo I, Normas de aplicación general, inciso 1.4 Gestión de la Seguridad de la Información, inciso 1.4.2 Compromiso del personal con la seguridad de la información, 1.4.5 Control de acceso

- Utilizar los bienes informáticos únicamente para el cumplimiento de las funciones asignadas según su clase de puesto y especialidad.
- Se prohíbe a todos los funcionarios utilizar el equipo de cómputo y los servicios de comunicación de la Institución para acceder y/o exhibir material pornográfico. De acuerdo con la Directriz de la Presidencia N° 30, publicada en el Diario Oficial La Gaceta N° 160 del miércoles 22 de agosto del 2001, dirigida a los Jerarcas de los Ministerios e Instituciones Autónomas.
- Todo funcionario está en la obligación de denunciar ante la Contraloría de Servicios o bien Auditoría interna, el uso indebido del equipo de cómputo, sobre todo en el caso de pedofilia, sitios de pornografía, acoso sexual y trata de personas. Como se indica en el documento denominado Política Ética Institucional se debe aplicar los valores éticos en el ejercicio de los deberes y hacer uso correcto de los recursos informáticos:

“La Política, además responde a lo establecido en el artículo 13 inciso a) de la Ley General de Control Interno, el cual indica que es deber del jerarca y los titulares subordinados “Mantener y demostrar integridad y valores éticos en el ejercicio de sus deberes y obligaciones, así como contribuir con su liderazgo y sus acciones a promoverlos en el resto de la organización, para el cumplimiento efectivo por parte de los demás funcionarios”.

- Todo funcionario es responsable de velar por los bienes informáticos asignados a él y previamente aceptados en la “Boleta de Asignación de Bienes de la Proveeduría Institucional”.
- Todos los usuarios deben tener conocimiento y estar conscientes de los compromisos, normas y reglamentos que han adquirido para el uso de los servicios informáticos.
- Acatar e implementar las medidas de seguridad establecidas que garanticen el resguardo necesario.
- No debe fumar o consumir alimentos y/o bebidas mientras realiza sus labores.
- Revisar en los equipos que se active diariamente la rutina de verificación del *software* antivirus autorizado por la Institución.
- Verificar con el *software* antivirus los medios de almacenamiento externo usados para el resguardo de información.
- Deberá hacer respaldos de la información que se encuentra almacenada en el disco duro y que considere crítica o de suma importancia. Esto de manera regular, como medida de contingencia ante un eventual daño en su computador. Utilizando para ello cualquier medio de almacenamiento masivo con que se cuente, por ejemplo, dispositivos USB.
- Queda bajo la responsabilidad del usuario, el almacenamiento de la información institucional en la nube (*Dropbox, Onedrive, GoogleDocs*, entre otros), las implicaciones en cuanto confidencialidad de la información y responsabilidad de la misma, así como su uso. Con la finalidad de que el uso de estas herramientas no afecte el tráfico en las comunicaciones en la red de datos del MEP, el ancho de banda disponible será administrado por la DIG.
- No se deben almacenar en las carpetas compartidas y/o los discos duros de las computadoras del Ministerio archivos de música (mp3, wma, wav, o cualquier otro), archivos de video (vob, avi, mpg, swf o cualquier otro) o archivos de imágenes (jpg, bmp o cualquier otro), que no sean propias de las labores realizadas para la Institución. Los archivos no autorizados pudieran ser borrados por el personal técnico de forma inmediata.
- Los fondos y/o refrescamientos de pantallas serán definidos por el Departamento de Gestión de Producción de la Dirección de Recursos Tecnológicos del MEP. Estos serán instalados por los funcionarios del Departamento de Redes y Telecomunicaciones de la Dirección de Informática de Gestión.

- Mantener el bien informático en un entorno adecuado para este, asegurándose que el mismo no corra riesgos físicos, tales como: exposición a la humedad, polvo, altas temperaturas, agua, alimentos, bebidas y otros elementos que atenten contra el correcto funcionamiento del bien.
- Conectar el bien informático únicamente en los sitios de alimentación eléctrica designados para este fin. Preferiblemente a un regulador de voltaje o unidad de energía ininterrumpida con regulador de voltaje (UPS).
- No conectar en tomacorrientes destinados para los bienes informáticos, los siguientes artículos fotocopiadoras, hornos de microondas, percoladores/*coffemaker*, abanicos, cargadores de teléfonos y otros artefactos electrónicos.
- Debe apagar el equipo mientras no lo use durante un período prolongado (horas de almuerzo, reuniones fuera de la oficina, entre otros).
- Cerrar sesión de los sistemas de información, *software*, bases de datos y/o servicio de red; cuando abandone el área de trabajo y/o no esté usando el equipo, para luego proceder a apagarlo.
- Procurar el óptimo y adecuado uso de los bienes informáticos a su cargo.
- Será responsable del bien informático, de su uso, resguardo y cuidado.
- Debe mantener la configuración que permite que los equipos ingresen a la red.
- Se prohíbe el uso de *DATACARDS* o dispositivos que permiten el acceso a Internet en las computadoras institucionales.
- Debe custodiar los medios de almacenamiento (CDs o memorias USB) que le fueron entregados con equipo de cómputo.
- Reportar a los funcionarios del Proyecto de Arrendamiento del Departamento de Soporte Técnico de la Dirección de Informática de Gestión y al Departamento de Control de Bienes de la Dirección de Proveduría Institucional, la movilización de los bienes informáticos (computadoras y/o impresoras) que tiene bajo su responsabilidad, mediante el sistema creado para este fin.
- Deberá comunicar inmediatamente a su superior sobre cualquier inconveniente que se presente, en especial si algún bien ha sido sustraído o reporta fallas de funcionamiento.
- Al devolver el equipo, este debe contar con el *software* preinstalado, así como todos los componentes (teclado, mouse, *docking*, maletín, entre otros). Cabe indicar que el equipo entregado, debe ser verificado por el funcionario que recibe.
- El funcionario que requiera desinstalar *software* en su equipo, deberá hacer la solicitud al Departamento de Soporte Técnico mediante el Sistema de atención de incidencias.
- La oficina a la que se le asigne el equipo informático, deberá resguardar todos sus componentes y/o programas de cómputo autorizados, con su respectiva licencia.

- Todo funcionario es responsable de velar por los bienes informáticos asignados a él y previamente aceptados en la “Boleta de Asignación de Bienes de la Proveeduría Institucional”.
- Todos los usuarios deben tener conocimiento y estar conscientes de los compromisos, normas y reglamentos que han adquirido para el uso de los servicios informáticos.

11.3 Al usuario que hace uso de los bienes informáticos

Este punto, hace cumplimiento al capítulo I, Normas de aplicación general, inciso 1.4 Gestión de la Seguridad de la Información, inciso 1.4.2 Compromiso del personal con la seguridad de la información, 1.4.5 Control de acceso

- Utilizar los bienes informáticos únicamente para el cumplimiento de las funciones asignadas según su clase de puesto y especialidad.
- Se prohíbe a todos los funcionarios utilizar el equipo de cómputo y los servicios de comunicación de la Institución para acceder y/o exhibir material pornográfico. De acuerdo con la Directriz de la Presidencia N° 30, publicada en el Diario Oficial La Gaceta N° 160 del miércoles 22 de agosto del 2001, dirigida a los Jerarcas de los Ministerios e Instituciones Autónomas.
- Todo funcionario está en la obligación de denunciar ante la Contraloría de Servicios o bien Auditoría interna, el uso indebido del equipo de cómputo, sobre todo en el caso de pedofilia, sitios de pornografía, acoso sexual y trata de personas. Como se indica en el documento denominado Política Ética Institucional se debe aplicar los valores éticos en el ejercicio de los deberes y hacer uso correcto de los recursos informáticos:

“La Política, además responde a lo establecido en el artículo 13 inciso a) de la Ley General de Control Interno, el cual indica que es deber del jerarca y los titulares subordinados “Mantener y demostrar integridad y valores éticos en el ejercicio de sus deberes y obligaciones, así como contribuir con su liderazgo y sus acciones a promoverlos en el resto de la organización, para el cumplimiento efectivo por parte de los demás funcionarios”.

- Todos los usuarios deben tener conocimiento y estar conscientes de los compromisos, normas y reglamentos que han adquirido para el uso de los servicios informáticos.
- Acatar e implementar las medidas de seguridad establecidas que garanticen el resguardo necesario.
- No debe fumar o consumir alimentos y/o bebidas mientras realiza sus labores.
- Revisar en los equipos que se active diariamente la rutina de verificación del *software* antivirus autorizado por la Institución.
- Verificar con el *software* antivirus los medios de almacenamiento externo usados para el resguardo de información.

- Deberá hacer respaldos de la información que se encuentra almacenada en el disco duro y que considere crítica o de suma importancia. Esto de manera regular, como medida de contingencia ante un eventual daño en su computador. Utilizando para ello cualquier medio de almacenamiento masivo con que se cuente, por ejemplo, dispositivos USB.
- Queda bajo la responsabilidad del usuario, el almacenamiento de la información institucional en la nube (*Dropbox, Onedrive, GoogleDocs*, entre otros), las implicaciones en cuanto confidencialidad de la información y responsabilidad de la misma, así como su uso. Con la finalidad de que el uso de estas herramientas no afecte el tráfico en las comunicaciones en la red de datos del MEP, el ancho de banda disponible será administrado por la DIG.
- No se deben almacenar en las carpetas compartidas y/o los discos duros de las computadoras del Ministerio archivos de música (mp3, wma, wav, o cualquier otro), archivos de video (vob, avi, mpg, swf o cualquier otro) o archivos de imágenes (jpg, bmp o cualquier otro), que no sean propias de las labores realizadas para la Institución. Los archivos no autorizados pudieran ser borrados por el personal técnico de forma inmediata.
- Los fondos y/o refrescamientos de pantallas serán definidos por el Departamento de Gestión de Producción de la Dirección de Recursos Tecnológicos del MEP. Estos serán instalados por los funcionarios del Departamento de Redes y Telecomunicaciones de la Dirección de Informática de Gestión.
- Mantener el bien informático en un entorno adecuado para este, asegurándose que el mismo no corra riesgos físicos, tales como: exposición a la humedad, polvo, altas temperaturas, agua, alimentos, bebidas y otros elementos que atenten contra el correcto funcionamiento del bien.
- Conectar el bien informático únicamente en los sitios de alimentación eléctrica designados para este fin. Preferiblemente a un regulador de voltaje o unidad de energía ininterrumpida con regulador de voltaje (UPS).
- No conectar en tomacorrientes destinados para los bienes informáticos, los siguientes artículos fotocopiadoras, hornos de microondas, percoladores/*coffemaker*, abanicos, cargadores de teléfonos y otros artefactos electrónicos.
- Debe apagar el equipo mientras no lo use durante un período prolongado (horas de almuerzo, reuniones fuera de la oficina, entre otros).
- Cerrar sesión de los sistemas de información, *software*, bases de datos y/o servicio de red; cuando abandone el área de trabajo y/o no esté usando el equipo, para luego proceder a apagarlo.
- Procurar el óptimo y adecuado uso de los bienes informáticos que tiene a su disposición para efectuar sus labores.
- Debe mantener la configuración que permite que los equipos ingresen a la red.

- Se prohíbe el uso de *DATACARDS* o dispositivos que permiten el acceso a Internet en las computadoras institucionales.
- Deberá comunicar inmediatamente a su superior sobre cualquier inconveniente que se presente, en especial si algún bien ha sido sustraído o reporta fallas de funcionamiento.
- Todos los usuarios deben tener conocimiento y estar conscientes de los compromisos, normas y reglamentos que han adquirido para el uso de los servicios informáticos.

11.4 A las jefaturas

Este punto, hace cumplimiento al capítulo I, Normas de aplicación general, inciso 1.4 Gestión de la Seguridad de la Información, inciso 1.4.2 Compromiso del personal con la seguridad de la información, 1.4.5 Control de acceso

- Informar inmediatamente a la DIG cuando un colaborador deja de laborar para su dependencia, esto con el fin de deshabilitar los accesos a los recursos informáticos otorgados y evitar usos indebidos.
- Informar a la Dirección de Informática de Gestión el cese de cada funcionario para cerrar la cuenta del correo Ministerial asignada a este.
- Solicitar por escrito a la Dirección de Informática de Gestión los recursos de red, acceso a los sistemas de información, instalación de *software* y cualquier otro servicio que se brinda en la DIG. Además, deben indicar las calidades de la persona y el detalle de la labor a realizar.
- En caso de requerir la instalación de bienes informáticos, reconfiguración de estos o de accesorios que no forman parte de la configuración original, debe coordinar la respectiva colaboración a la DIG. Así mismo, debe comunicar de dichos cambios al Departamento de Control de Bienes de la Dirección de Proveduría Institucional.
- Vigilar por la implementación de las medidas de seguridad dispuestas en este Manual o cualquier lineamiento informático dictado por autoridad competente.
- Comunicar a sus colaboradores cuando el equipo es arrendado.

11.5 A la Administración

Este punto, hace cumplimiento al capítulo I, Normas de aplicación general, inciso 1.4 Gestión de la Seguridad de la Información, inciso 1.4.2 Compromiso del personal con la seguridad de la información, 1.4.5 Control de acceso

- Vigilar por la implementación de las medidas de seguridad dispuestas en este Manual o cualquier lineamiento informático dictado por autoridad competente.

- Planificar y presupuestar todo lo relacionado para la adquisición de los consumibles requeridos para el adecuado/eficiente funcionamiento del o los bienes/servicios informáticos arrendados.
- La Administración cuenta con herramientas adecuadas para la verificación del cumplimiento de las restricciones, con las limitantes según sea el caso del servicio que se brinda.
- Asegurar la continuidad del servicio brindado por el recurso informático arrendado (computadoras y/o impresoras) a los usuarios, con el fin de no entorpecer sus labores cotidianas.

11.6 Relacionados a instalaciones de software

- La instalación del *software* especializado de uso no común debe ser aprobada por su jefatura inmediata; y su instalación será realizada solo por personal autorizado del Departamento de Soporte Técnico de la Dirección de Informática de Gestión.
- Todo *software* que no cuente con la licencia respectiva será removido del equipo inmediatamente sin previo aviso.
- Se prohíbe la instalación de *software* no autorizado por la Dirección de Informática de Gestión o bien que no cuente con su respectiva licencia.
- En todos los bienes informáticos de la entidad o arrendados, queda prohibida la instalación y uso de *software* o programas que no cuenten con la licencia correspondiente y/o que su utilización no sea afín a las funciones institucionales.
- No se debe instalar o utilizar *software* o programas de entretenimiento (juegos, chats, música, programas para escuchar música o sintonizar radioemisoras vía Internet) en los bienes informáticos de la entidad o arrendados.
- Únicamente el personal del Departamento de Soporte Técnico de la Dirección de Informática de Gestión, está facultado para la instalación y/o desinstalación de *software* que no cuente con una licencia.
- En el Decreto 37549 del Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central, se indica lo siguiente:

“Artículo 2º—Cada Ministerio e Instituciones adscritas al Gobierno Central, tendrán las siguientes obligaciones:

Establecer sistemas y controles para garantizar la utilización en sus computadoras, única y exclusivamente, de aquellos programas de cómputo que cumplan con los derechos de autor correspondientes. Cualquier programa que exceda el número autorizado o que no cuente con la licencia correspondiente deberá removerse inmediatamente.”
- La Dirección de Informática de Gestión llevará el inventario y control de las licencias de *software* adquiridas y solicitará a las diferentes dependencias del MEP que adquieran

licencias para el desempeño de labores, que informen sobre las mismas. Por ejemplo: el DIEE con AutoCad.

- En el Código Nacional de Tecnologías Digitales, en el apartado Políticas Generales, Inventario y control de activos de *software*, se indica lo siguiente:

“Contar con un inventario de software oficial y actualizado periódicamente, que promueva el aseguramiento de software actualizado y soportado por el fabricante.

Listas de software aprobado para el uso dentro de la organización

- Contar con listas de software permitido para la instalación y uso, que promueva la seguridad de la información y no comprometa la plataforma tecnológica”.
- Toda instalación de bienes informáticos (hardware y/o software), reconfiguración de los mismos o de accesorios que no forman parte de la configuración original, debe ser solicitada por medio del Sistema de atención de incidencias para ser autorizado e instalado por el Departamento de Soporte Técnico de la Dirección de Informática de Gestión.

11.7 A la atención de solicitudes de Recursos Informáticos

Este punto, hace cumplimiento al capítulo I, Normas de aplicación general, inciso 1.4 Gestión de la Seguridad de la Información, inciso 1.4.2 Compromiso del personal con la seguridad de la información, 1.4.5 Control de acceso

- Solicitar por escrito a la Dirección de Informática de Gestión los recursos de red, acceso a los sistemas de información, instalación de *software* y cualquier otro servicio que se brinda en la DIG. Además, deben indicar las calidades de la persona y el detalle de la labor a realizar.
- La DIG evaluará la solicitud y recomendará la provisión de bienes y/o servicios informáticos necesarios para suplir los requerimientos de automatización de las distintas unidades administrativas del Ministerio.

Además, debe cumplir lo dispuesto en el Decreto No. 38170, el cual contempla la Organización Administrativa de las Oficinas Centrales del Ministerio de Educación Pública, siendo reguladas las funciones de la DIG de conformidad a los artículos 153 al 162.

De manera conexas, la DIG actuará de conformidad a las posibilidades que le faculta la Ley General de la Administración Pública con sustento en el artículo No. 4 y demás normativa relacionada.

- La DIG garantiza la seguridad informática y el uso adecuado de los recursos informáticos, debe controlar y limitar el acceso al funcionario que viole los lineamientos establecidos en este manual o interfiera con los derechos de otros usuarios. También

tiene la responsabilidad de notificar a las personas que se vean afectadas por las decisiones tomadas.

- Cuando sea solicitado por la parte interesada, autoridad superior, o bien reguladora; la Dirección de Informática de Gestión entregará el informe técnico necesario, en aquellos casos en que se ha producido el uso no autorizado o indebido del bien y/o servicio informático, el cual se sugiere elevar al Departamento de Régimen Disciplinario para el debido proceso.
- En caso de requerirse como insumo para un debido proceso disciplinario, la DIG o una entidad externa al MEP con índole de seguridad; se encargará del embalaje del bien informático (con su debida solicitud).
- Establecerá las prioridades cuando la demanda de servicios pueda ocasionalmente exceder la disponibilidad, dando la más alta prioridad a las actividades consideradas más esenciales para llevar a cabo la gestión del Ministerio.
- Toda instalación de bienes informáticos (*hardware* y/o *software*), reconfiguración de los mismos o de accesorios que no forman parte de la configuración original, debe ser solicitada por medio del Sistema de atención de incidencias para ser autorizado e instalado por el Departamento de Soporte Técnico de la Dirección de Informática de Gestión.

11.8 Manejo de cuentas de usuario y contraseñas de acceso

- El usuario es responsable de establecer y salvaguardar la(s) contraseñas de acceso al correo electrónico, red institucional y/o aplicaciones informáticas referentes a sus labores cotidianas.
- Es terminantemente prohibido el uso de cuentas y contraseñas de otros usuarios.
- El uso de la contraseña es personal, confidencial e intransferible (a otros usuarios y/o su jefatura).
- No debe almacenar las contraseñas en agendas, libretas, *post-it*, entre otros.
- El usuario es responsable de cambiar periódicamente las contraseñas de acceso al correo electrónico, red institucional y/o aplicaciones informáticas referentes a sus labores cotidianas, antes de su vencimiento. El resguardo de ésta queda bajo la responsabilidad del usuario así como el uso correcto.
- El usuario es responsable de cambiar inmediatamente la contraseña genérica (temporal) que se le brinda cuando ingresa por primera vez a la dependencia, cuando se vence o se olvida. El resguardo de ésta queda bajo la responsabilidad del usuario así como el uso correcto.
- Se recomienda que la contraseña sea robusta y segura. Que cumpla con las siguientes características: longitud de 6 a 30 caracteres, combinar de letras mayúsculas, minúsculas, caracteres especiales y al menos un número.

- Es prohibido para el usuario, establecer contraseñas para ingresar al BIOS y al encendido del equipo (no son las claves para ingresar al dominio de la institución).
- Toda acción realizada con la contraseña de un usuario, será responsabilidad directa de este. No podrá aducir desconocimiento y deberá asumir todo proceso administrativo y/o judicial.

11.9 Respaldo de datos

- El usuario que tiene asignado bienes informáticos, así como, el que los usa, deberá hacer respaldos de la información que se encuentra almacenada en el disco duro y que considere crítica o de suma importancia. Esto de manera regular, en el momento que se jubile, renuncie, se cambie de dependencia o se ausente por incapacidad prolongada, como medida de contingencia ante un eventual daño en su computador. Utilizando para ello cualquier medio de almacenamiento masivo con que se cuente, por ejemplo, dispositivos USB.
- Queda bajo la responsabilidad del usuario, el almacenamiento de la información institucional en la nube (*Dropbox, Onedrive, GoogleDocs*, entre otros), las implicaciones en cuanto confidencialidad de la información y responsabilidad de la misma, así como su uso. Con la finalidad de que el uso de estas herramientas no afecte el tráfico en las comunicaciones en la red de datos del MEP, el ancho de banda disponible será administrado por la DIG.
- No se deben almacenar en las carpetas compartidas y/o los discos duros de las computadoras del Ministerio archivos de música (mp3, wma, wav, o cualquier otro), archivos de video (vob, avi, mpg, swf o cualquier otro) o archivos de imágenes (jpg, bmp o cualquier otro), que no sean propias de las labores realizadas para la Institución. Los archivos no autorizados pudieran ser borrados por el personal técnico de forma inmediata.
- El Departamento de Soporte Técnico de la Dirección de Informática de Gestión deberá alertar al usuario y/o su jefatura inmediata mediante un reporte, para que el usuario proceda a borrar todos los archivos, carpetas, música, *software* y otros que no sean parte de las labores ministeriales. Para ello, en cada revisión programada, de equipo de cómputo se verificará el contenido de los mismos y procederán como corresponda.
- Se prohíbe el uso de *DATA CARDS* o dispositivos que permiten el acceso a Internet en las computadoras institucionales.

11.10 Uso de servicios en red

- El uso de la infraestructura o servicios de la red de datos institucional debe responder a los objetivos, fines y beneficios que establezca la Institución sobre la base de sus requerimientos. Para ello, la Dirección de Informática de Gestión será la responsable de:
 - a) Administrar los servicios de la red de datos institucional de manera exclusiva, con el personal del área responsable de esta función y en los casos necesarios, con la participación de los proveedores autorizados.
 - b) Administrar las diferentes cuentas de usuarios (correo electrónico institucional y de acceso a servidores) y mantendrá registros en línea o almacenados sobre el uso de las mismas, con las limitantes según sea el caso del servicio que se brinda.
 - c) Realizar las gestiones de instalación y/o desinstalación de las líneas de acceso a Internet y transmisión de datos, según corresponda para las Oficinas Centrales, Direcciones Regionales de Educación y circuitos educativos.
 - d) Monitorear el volumen y consumo del flujo de datos de cada usuario, así como los sitios visitados.

11.11 Permisos especiales a servicios del MEP

- En casos especiales, corresponderá a la Dirección de Informática de Gestión otorgar cuentas de usuarios a personas ajenas a la Institución (personal externo) siendo aprobado por el Director o autoridad competente, relacionada con el área donde trabajará la persona solicitante, completando el respectivo formulario. Ejemplo: Auditorías, miembros de la Contraloría General de la República, entes reguladores del sector público o bien personas que asisten a reuniones y que por diferentes razones necesitan conectarse a la red inalámbrica.

11.12 Uso del correo electrónico

- Cada funcionario será responsable del uso adecuado de su cuenta de correo y de la información que remita.
- La Dirección de Informática de Gestión sólo brindará ayuda y soporte a las cuentas @mep.go.cr
- Los servicios de correo electrónico y accesos a Internet son puestos a disposición de los funcionarios para asuntos estrictamente laborales.
- Para la utilización de programas de mensajería y chat para fines laborales, debe utilizarse *Microsoft Teams* con la cuenta oficial del MEP.

- El funcionario no debe suscribirse a listas de amigos por Internet, ya que esto provoca una gran cantidad de mensajes en su casilla de correo provocando saturación.
- Si el funcionario se siente ofendido por un mensaje de correo que recibió, favor de reenviarlo a la jefatura inmediata para lo correspondiente.
- Completar el espacio de asunto al enviar un mensaje de correo electrónico, ya que esto corresponde a una regla de cortesía y de cultura organizacional.
- El funcionario debe desconfiar de todos los correos que procedan de remitentes desconocidos o de dudosa procedencia; ya que estos podrían estar infectados con virus, asimismo, evitar abrir los archivos adjuntos de estos correos, en tal caso debe eliminarlos.
- Si se desea mantener un mensaje en forma permanente, este se debe almacenar en una carpeta personal en el equipo del usuario.
- El uso de letras en mayúsculas y en color rojo en las frases y/u oraciones se considera un grito y una descortesía. Los funcionarios deben ser corteses al momento de generar y enviar un mensaje de correo electrónico.
- El funcionario tiene el deber de depurar su buzón de correo electrónico borrando la información innecesaria, para minimizar inconvenientes cuando se acabe el límite de almacenamiento.
- El Departamento de Soporte Técnico dará una única inducción al usuario de como respaldar la información de correo mediante un archivo de extensión PST, con el fin de que este último pueda generar regularmente el respaldo de su buzón correo.
- La administración de la red, no da garantías de ningún tipo, sea expresa o implícitamente, para el servicio del correo que se provee, por cualquier daño que el usuario sufra causado por negligencia propia, errores, omisiones o el mal uso del servicio.

11.13 Uso de correos masivos

- La comunicación masiva a los funcionarios del MEP mediante el correo electrónico sólo será posible para aquellas instancias o funcionarios que, de acuerdo a sus responsabilidades, requieran realizar comunicados de índole informativo y que efectivamente sean de interés de los funcionarios del Ministerio. Para lo cual, deben solicitar dicho permiso de uso de este recurso, de forma escrita ante la Dirección de Informática de Gestión.
- Los funcionarios autorizados serán responsables por el contenido de los mensajes, a efecto que cumplan la característica de ser mensajes oficiales y de carácter laboral.
- Completar el espacio de asunto al enviar un mensaje de correo electrónico, ya que esto corresponde a una regla de cortesía y de cultura organizacional.

- El funcionario debe desconfiar de todos los correos que procedan de remitentes desconocidos o de dudosa procedencia; ya que estos podrían estar infectados con virus, asimismo, evitar abrir los archivos adjuntos de estos correos, en tal caso debe eliminarlos.
- Si se desea mantener un mensaje en forma permanente, este se debe almacenar en una carpeta personal en el equipo del usuario.
- El uso de letras en mayúsculas y en color rojo en las frases y/u oraciones se considera un grito y una descortesía. Los funcionarios deben ser corteses al momento de generar y enviar un mensaje de correo electrónico.
- La administración de la red, no da garantías de ningún tipo, sea expresa o implícitamente, para el servicio del correo que se provee, por cualquier daño que el usuario sufra causado por negligencia propia, errores, omisiones o el mal uso del servicio.

11.14 Uso del equipo de cómputo arrendado

- Se referencia a una serie de documentos relacionados con la tramitología de los equipos arrendados. Los siguientes documentos regulan el uso y administración del equipo de cómputo arrendado se pueden ver en la **página oficial del MEP en la sección de compras-contrataciones**:

| Documento |
|---|
| Manual Políticas Equipo Cómputo Arrendado |
| Formulario Activos Arrendamiento Junio 2018 |

- El formulario denominado Activos Arrendamiento Junio 2018, debe ser actualizado cada vez que el equipo arrendado se traslade entre edificios de forma permanente y enviado al proyecto de arrendamiento arrendamientoecdig@mep.go.cr.
- Los aspectos indicados en el ítem 11 de este manual se aplican para el equipo de cómputo arrendado.

11.15 Uso de impresoras arrendadas

- El documento referente al arrendamiento de impresoras aún se encuentra en la etapa de elaboración, en cual se detallará su uso y administración.
- En el momento de la actualización de este manual no se cuenta con los documentos oficiales del arrendamiento de impresoras.

- Cualquier trámite referente a las impresoras arrendadas se debe de notificar a la siguiente cuenta de correo: arrendamientoimpresora@mep.go.cr.
- Los aspectos indicados en el ítem 11 de este manual se aplican para las impresoras arrendadas.

12 DOCUMENTOS DE REFERENCIA

- Normas que regulan el uso adecuado de los servicios tecnológicos.
- Capítulo IX Prohibiciones, Artículo 23 del Reglamento Autónomo de Servicio y Organización de la Dirección General de Servicio Civil, Decreto N° 25813-MP, publicado en La Gaceta N° 36 del jueves 20 de febrero de 1997, inciso s).
- Artículo 111 Delito Informático.

“Cometerán delito informático, sancionando con prisión de 1 a 3 años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:

 - *Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder datos de uso restringido.*
 - *Causar daño dolosamente a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.*
 - *Facilitar a terceras personas el uso del código personal y la clave de acceso a acceder a los sistemas.*
 - *Utilizar las facilidades del sistema para beneficio propio o de terceros...”*
- Código Nacional de Tecnologías Digitales en el apartado de Políticas Generales.
 - *“Inventario y control de activos de software.*
 - *Contar con un inventario de software oficial y actualizarlo periódicamente. Con el fin de asegurar que el software esté actualizado y soportado por el fabricante.*
 - *Listas de software cuyo uso este aprobado en la Institución.*
 - *Contar con listas de software permitido para la instalación y uso, que promueva la seguridad de la información y no comprometa la plataforma tecnológica.”*
- Plan Estratégico de Tecnología de la Información (PETI)
- Política en Tecnologías de la Información del Ministerio de Educación Pública, en el apartado Objetivos estratégicos del Eje 5.
- Política Ética Institucional

“La Política, además responde a lo establecido en el artículo 13 inciso a) de la Ley General de Control Interno, el cual indica que es deber del jerarca y los titulares subordinados “Mantener y demostrar integridad y valores éticos en el ejercicio de sus deberes y obligaciones, así como contribuir con su liderazgo y sus acciones a promoverlos en el resto de la organización, para el cumplimiento efectivo por parte de los demás funcionarios”.

- Decreto 37549 Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central

“Artículo 2º—Cada Ministerio e Instituciones adscritas al Gobierno Central, tendrán las siguientes obligaciones:

a) Establecer sistemas y controles para garantizar la utilización en sus computadoras, única y exclusivamente, de aquellos programas de cómputo que cumplan con los derechos de autor correspondientes.”

- Normas de control interno para el sector público de la Contraloría General de la República, los siguientes puntos:
 - Capítulo IV: Normas sobre actividades de Control, puntos 4.3
 - Capítulo V: Normas sobre sistemas de información.
- Normas Técnicas para la gestión y el control de las tecnologías de la Información de la Contraloría General de la República.
- Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de República a partir del 31 de diciembre del 2021, según resolución N° R-CO-26-2007, y modificación de las Normas de Control Interno para el sector público.

13 HOJA DE FIRMAS

----- INTENCIONALMENTE DEJADO EN BLANCO -----

HOJA DE REVISIÓN Y ACEPTACIÓN
MANUAL DE LINEAMIENTOS DEL USO DE LOS
RECURSOS INFORMÁTICOS INSTITUCIONALES

CÓDIGO: DVM-A-DIG-MAN-02

ACTUALIZADO POR:

Fulton Hernández Espinoza

Jenny Navarro Blanco

Marlon Vásquez Vásquez

José Martín Sanchún Macín

Máximo Varela Castro

Rebeca Granados Vargas

Tahyli Mondragón Fonseca

REVISADO POR:

José Sandí Zúñiga

NOMBRE

FIRMA

APROBADO POR:

José Sandí Zúñiga

NOMBRE

FIRMA

FECHA: Octubre, 2021