



**MINISTERIO DE  
EDUCACIÓN PÚBLICA**

**GOBIERNO  
DE COSTA RICA**

**VICEMINISTERIO ADMINISTRATIVO  
DIRECCIÓN DE INFORMÁTICA DE GESTIÓN**

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



**DVM-A-DIG-MAN-02**

**Marzo, 2026**



## **TABLA DE CONTENIDO**

<b>1. HISTORIAL DE REVISIONES.....</b>	<b>4</b>
<b>2. INTRODUCCIÓN .....</b>	<b>7</b>
<b>3. OBJETIVOS .....</b>	<b>7</b>
<b>3.1. Objetivo General.....</b>	<b>7</b>
<b>3.2. Objetivos Específicos .....</b>	<b>7</b>
<b>4. ALCANCE .....</b>	<b>8</b>
<b>5. ABREVIATURAS Y DEFINICIONES.....</b>	<b>8</b>
<b>5.1. Abreviaturas .....</b>	<b>8</b>
<b>5.2. Definiciones .....</b>	<b>9</b>
<b>6. AUTOR (ES).....</b>	<b>9</b>
<b>7. ACTUALIZADO POR.....</b>	<b>9</b>
<b>8. DIRECTRICES .....</b>	<b>9</b>
<b>9. RESPONSABILIDAD .....</b>	<b>10</b>
<b>10. DESCRIPCIÓN DEL MANUAL.....</b>	<b>10</b>
<b>11. DESCRIPCIÓN DE LINEAMIENTOS .....</b>	<b>11</b>
<b>11.1. Generales .....</b>	<b>11</b>
<b>11.2. Al usuario que tiene asignados los bienes informáticos .....</b>	<b>13</b>
<b>11.3. Al usuario que hace uso de los bienes informáticos .....</b>	<b>16</b>
<b>11.4. A las jefaturas .....</b>	<b>19</b>
<b>11.5. A la DIG .....</b>	<b>21</b>
<b>11.6. Autoridades superiores.....</b>	<b>22</b>
<b>11.7. Relacionados a instalaciones/desinstalaciones de software.....</b>	<b>23</b>
<b>11.8. A la atención de solicitudes de Recursos Informáticos .....</b>	<b>24</b>
<b>11.9. Manejo de cuentas de usuario y contraseñas de acceso.....</b>	<b>26</b>
<b>11.10. Respaldo de datos .....</b>	<b>26</b>
<b>11.11. Uso de servicios en red.....</b>	<b>27</b>
<b>11.12. Uso de telefonía IP .....</b>	<b>28</b>
<b>11.13. Permisos especiales a servicios institucionales .....</b>	<b>28</b>
<b>11.14. Uso del correo electrónico .....</b>	<b>29</b>
<b>11.15. Uso de mensajes de correo electrónico masivos .....</b>	<b>30</b>
<b>11.16. Uso del equipo arrendado (Computadoras e impresoras) .....</b>	<b>30</b>
<b>11.17. Uso de la firma digital .....</b>	<b>31</b>



11.18. Recomendaciones emanadas por la Oficina de Ciberseguridad .....	<b>31</b>
<b>12. DOCUMENTOS DE REFERENCIA .....</b>	<b>32</b>
<b>13. ANEXOS .....</b>	<b>35</b>
13.1. Anexo 1. Norma Técnica para la gestión y el control de las Tecnologías de Información. ....	35
<b>14. HOJA DE FIRMAS .....</b>	<b>35</b>





## 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 con 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	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. 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.	Fulton Hernández Espinoza, Departamento Sistemas de Información Jenny Navarro Blanco, Departamento Base de Datos Marlon Vásquez Vásquez, Departamento Soporte Técnico Tahyli Mondragón Fonseca, Departamento Soporte Técnico José Martín Sanchún Macín, Departamento Gestión y Control Informático Máximo Varela Castro, Departamento Adquisición Tecnológica Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones
Noviembre, 2022	7	Se actualiza con el fin de implementar las Normas Técnicas emitidas por el MICITT, que consideramos aplican según el enfoque de este manual.	Fulton Hernández Espinoza, Departamento Sistemas de Información Jenny Navarro Blanco, Departamento Base de Datos



Fecha	Versión	Descripción	Responsables
		Cabe indicar que estas normas corresponden a buenas prácticas para los procesos establecidos en el Marco Normativo de Gobierno y Gestión de TI.	Marlon Vásquez Vásquez, Departamento Soporte Técnico José Martín Sanchún Macín, Departamento Gestión y Control Informático Máximo Varela Castro, Departamento Adquisición Tecnológica Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones
Junio, 2023	8	Se actualiza con el fin de implementar aspectos relacionados con Ciberseguridad apegados a las normas técnicas emitidas por el MICITT, que consideramos aplican según el enfoque de este manual.	Fulton Hernández Espinoza, Departamento Sistemas de Información Jenny Navarro Blanco, Departamento Base de Datos Marlon Vásquez Vásquez, Departamento Soporte Técnico José Martín Sanchún Macín, Departamento Gestión y Control Informático Máximo Varela Castro, Departamento Adquisición Tecnológica Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones Daniel Josué Delgado Leandro, Oficina de Ciberseguridad Juan Carlos Rodríguez Valerio, Oficina de Ciberseguridad
Noviembre, 2024	9	Se actualizan encabezados, cambios en las definiciones. Se incluye referencia a la Política de seguridad de información del Ministerio de Educación Pública, se modifican los textos relacionados con soporte Técnico y Equipo Arrendamiento.	Alban Antonio García Vargas, Departamento Sistemas de Información Jenny Navarro Blanco, Departamento Base de Datos Marlon Vásquez Vásquez, Departamento Soporte Técnico



Fecha	Versión	Descripción	Responsables
			<p>José Martín Sanchún Macín, Departamento Gestión y Control Informático</p> <p>Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones</p> <p>Daniel Josué Delgado Leandro, Oficina de Ciberseguridad</p> <p>Juan Carlos Rodríguez Valerio, Oficina de Ciberseguridad</p>
Marzo, 2026	10	<p>Se actualiza con el fin de implementar aspectos relacionados con Ciberseguridad apegados a las normas técnicas emitidas por el MICITT, que consideramos aplican según el enfoque de este manual.</p>	<p>Alban Antonio Garcia Vargas, Departamento Sistemas de Información</p> <p>Jenny Navarro Blanco, Departamento Base de Datos</p> <p>Marlon Vásquez Vásquez, Departamento Soporte Técnico</p> <p>José Martín Sanchún Macín, Departamento Gestión y Control Informático</p> <p>Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones</p> <p>Gabriela Artavia Jiménez, Oficina de Ciberseguridad</p> <p>Daniel Josué Delgado Leandro, Oficina de Ciberseguridad</p> <p>Juan Carlos Rodríguez Valerio, Oficina de Ciberseguridad</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), Direcciones Regionales de Educación (DRE) y Circuitos Escolares, 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 aplicando el resguardo y la seguridad de la información, procurando la confidencialidad, integridad y disponibilidad de ésta, 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, Direcciones Regionales de Educación y Circuitos Escolares. Lo anterior, con procesos de gestión basados en las mejores prácticas establecidas en las Normas Técnicas emitidas por el MICITT aplicándolas de manera parcial o total, para los procesos establecidos en el Marco Normativo de Gobierno y Gestión de las TI.

## 3. OBJETIVOS

### 3.1. Objetivo General

Asegurar el uso eficiente de los recursos informáticos (*hardware* y *software*) empleando para ello buenas prácticas de seguridad, procurando la confidencialidad, integridad y disponibilidad de la información y una adecuada administración, esto garantiza el máximo aprovechamiento y eficiencia posible en las OC, DRE y Circuitos Escolares, basados en las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por el MICITT.

### 3.2. Objetivos Específicos

- Uniformar criterios sobre lineamientos técnicos para el adecuado e idóneo uso de los recursos informáticos del Ministerio, basados en las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por el MICITT.
- Aumentar la eficiencia en las labores cotidianas de los funcionarios que laboran en las dependencias del Ministerio (OC, DRE y Circuitos Escolares).



- Promover medidas de seguridad para el *hardware* y *software* en OC, DRE y Circuitos Escolares.
- 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 OC, DRE y Circuitos Escolares, para garantizar su máximo aprovechamiento y eficiencia permisible, aplicando las mejores prácticas en Ciberseguridad que emita el Ente rector en conjunto con la DIG.
- Asegurar el cumplimiento obligatorio de las disposiciones contenidas en el presente manual.

## 4. ALCANCE

Establece los lineamientos y directrices a seguir en el uso de los recursos y bienes informáticos en el MEP, entiéndase para estos efectos, los servicios informáticos y en general cualquier otro producto informático propiedad del MEP, activo institucional adquirido y donado o que bajo su autorización se tenga derecho de uso en la Institución, incluyendo todo equipo en arrendamiento vigente con el MEP en OC, DRE y Circuitos Escolares.

Se aplicará en este manual las mejores prácticas para la gestión de los recursos tecnológicos, así como las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por el MICITT.

## 5. ABREVIATURAS Y DEFINICIONES

### 5.1. Abreviaturas

**DAI:** Dirección de Auditoría Interna.

**DDoS** (*Denial of Service*): Ataque de Denegación de Servicio.

**DIEE:** Dirección de Infraestructura y Equipamiento Educativo.

**DIG:** Dirección de Informática de Gestión.

**DPI:** Dirección de Proveeduría Institucional.

**DRE:** Direcciones Regionales de Educación.

**DRT:** Departamento de Redes y Telecomunicaciones.

**DRTE:** Dirección de Recursos Tecnológicos en Educación.

**DST:** Departamento de Soporte Técnico.

**MEP:** Ministerio de Educación Pública.

**MFA** (*Multi-Factor Authentication*): Multi Factor de Autenticación.

**MICITT:** Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.



**OC:** Oficinas Centrales.

**TIC:** Comisión de Tecnologías de Información.

## 5.2. Definiciones

Refiérase al Glosario de términos para la DIG, ubicado en la dirección electrónica: [\\dominiomep\compartidas\Manuales\\_y\\_Estandares\Vigente\Glosario de términos DIG](\\dominiomep\compartidas\Manuales_y_Estandares\Vigente\Glosario_de_términos DIG).

## 6. AUTOR (ES)

Jefaturas de la DIG.

## 7. ACTUALIZADO POR

Lic. Alban Antonio García Vargas, Departamento Sistemas de Información, marzo 2026.

Licda. Jenny Navarro Blanco, Departamento Base de Datos y Seguridad, marzo 2026.

Lic. Marlon Vásquez Vásquez, Departamento Soporte Técnico, marzo 2026.

Lic. José Martín Sanchún Macín, Departamento Gestión y Control Informático, marzo 2026.

Licda. Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones, marzo 2026.

Tecn. Gabriela Artavia Jiménez, Oficina de Ciberseguridad, marzo 2026.

Ing. Daniel Josué Delgado Leandro, Oficina de Ciberseguridad, marzo 2026.

Lic. Juan Carlos Rodríguez Valerio, Oficina de Ciberseguridad, marzo 2026.

## 8. DIRECTRICES

El presente documento es de conocimiento y aplicación **obligatoria** para todos los funcionarios del MEP, entiéndase para estos efectos OC, DRE y Circuitos Escolares.

Es obligación de todos los funcionarios acatar las normativas establecidas en la Política de seguridad de información del Ministerio de Educación Pública avalada mediante el oficio DM-0472-03-2024, y oficializada y divulgada el 22 de marzo del 2024 mediante el oficio DVM-A-DIG-0135-2024 y el oficio de divulgación de este manual del periodo vigente

*“Se insta a las direcciones como objetivo común, a considerar en sus procesos internos, el uso de dicha política e implementar la misma a corto y mediano plazo, promoviendo la implementación de esta en todas sus dimensiones. Es importante recalcar que dicha política fue avalada por la señora ministra de*



*Educación, en su momento, en conjunto con el MICITT, Dirección de Asuntos Jurídicos, Dirección de Planificación y Comisión TIC del Ministerio de Educación. Se instruye a los funcionarios del Ministerio de Educación Pública para que participen en las gestiones generadas por dicha política.”*

actualmente se mantiene vigente dicho aval.

## 9. RESPONSABILIDAD

Los funcionarios del MEP (OC, DRE y Circuitos Escolares) 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, asegurando un comportamiento ético y profesional de sus colaboradores sin comprometer el recurso máspreciado de la Institución la información.

## 10. DESCRIPCIÓN DEL MANUAL

En este manual se describen aspectos generales, reglas y procedimientos para la adecuada administración y buen uso de los recursos informáticos; procurando la seguridad, el resguardo, confidencialidad, integridad y disponibilidad de la información, 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 OC, DRE y Circuitos Escolares. 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 para todos los funcionarios del MEP, 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 **obligatoriamente** con lo que se relacione a los bienes y servicios informáticos que dicta este documento, independientemente de su clase de puesto y especialidad.

Aunado a lo anterior, con el fin de proteger los recursos informáticos institucionales, para brindar acceso a terceras personas, se debe cumplir a cabalidad con lo dispuesto en el PROTOCOLO PARA BRINDAR ACCESO A RECURSOS INTERNOS A TERCEROS.

La DIG se ha dado a la tarea de actualizar el Manual de Lineamientos en el uso de los recursos informáticos, en el cumplimiento de las recomendaciones establecidas y mejores prácticas de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por el MICITT, aplicándolas de manera parcial o total según corresponda.



## 11. DESCRIPCIÓN DE LINEAMIENTOS

El MEP cuenta con una red y recursos informáticos institucionales para el uso de sus colaboradores, tanto en OC, DRE y Circuitos Escolares; 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, así como las mejores prácticas para la gestión de los recursos tecnológicos y las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por el MICITT. Los siguientes ítems responden a los objetivos estratégicos del Eje 5 del documento Políticas TIC del Ministerio de Educación Pública.

### 11.1. Generales

- 11.1.1. Los funcionarios de OC, DRE y Circuitos Escolares 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.”.*

- 11.1.2. Los funcionarios de OC, DRE y Circuitos Escolares 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.”*

- 11.1.3. Es responsabilidad de cada jefatura, velar por el cumplimiento de las normas establecidas, y a la vez notificar a la DIG, los cambios o movimientos del personal que autoriza, ya sea por traslados a otra dependencia, despido, renuncia, entre otros.



- 11.1.4. 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

- 11.2.1. Utilizar los bienes informáticos tangibles e intangibles (*software*) únicamente para el cumplimiento de las funciones asignadas según su clase de puesto, especialidad y/o las asignadas por su jefatura.
- 11.2.2. 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.
- 11.2.3. Todo funcionario está en la obligación de denunciar ante la Contraloría de Servicios o bien DAI, 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”.*
- 11.2.4. Todo funcionario es responsable de velar por los bienes informáticos asignados a él y sean previamente aceptados en la “Formulario de Asignación de Bienes de la Proveeduría Institucional” (SICAMEP) y/o “Formulario Control de Activos en Arrendamiento” (Unidad de Control de Contratos).
- 11.2.5. Todos los usuarios deben tener conocimiento y estar conscientes de los compromisos, normas y reglamentos que han adquirido para el uso de los recursos/servicios informáticos. Usar correctamente los sistemas que acceden con la cuenta de usuario asignada y su respectiva contraseña, al realizar acciones tales como extraer, modificar, eliminar datos, que puedan causar daño a la institución. Modificar configuraciones en consolas de *software* de seguridad, correos electrónicos, *Intune*, *Azure*, otros. Ingreso a carpetas compartidas y borrar información laboral, información compartida en *OneDrive*, otros.
- 11.2.6. Aquellos usuarios que requieran usar el equipo informático asignado para atender alguna eventualidad en horario de lunes a viernes entre 8:00 p.m. y las 6:00 a.m. y/o fin de semana, deberán informar a la Oficina de Ciberseguridad en el momento en que se encienden este, a la cuenta de correo electrónico [seguridadinformaticadiq@mep.go.cr](mailto:seguridadinformaticadiq@mep.go.cr), con copia a su jefatura inmediata.

En caso de requerir laborar durante el fin de semana, semana santa y/o vacaciones colectivas, las jefaturas deberán informar mediante formulario



generado por la Oficina de Ciberseguridad para dicho fin, a la cuenta de correo electrónico, de manera oportuna.

- 11.2.7. Acatar e implementar las medidas de seguridad establecidas que garanticen el resguardo necesario.

Para hacer uso de equipos informáticos asignados fuera del país, para atender actividades oficiales y/o eventos especiales, deben de indicar por medio de oficio el nombre del funcionario, usuario de dominio, placa del equipo, el detalle de los países destino, motivo del viaje, fecha de salida y regreso del país.

Se recomienda no acceder a redes inalámbricas públicas, no protegidas o vulnerables, como las empleadas en los parques, aeropuertos, restaurantes entre otros, donde se solicite correos electrónicos o usuarios de dominio.

- 11.2.8. No debe fumar o consumir alimentos y/o bebidas mientras realiza sus labores.

- 11.2.9. Es deber de cada funcionario realizar el respaldo de su información laboral que se encuentra en su equipo de cómputo asignado por la institución 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 el *OneDrive* empresarial, ya que es la herramienta oficial en la institución para resguardar información laboral en la nube, y debe estar configurada en el equipo, esto con la finalidad de que el uso de estas herramientas no afecte el tráfico en las comunicaciones en la red de datos del MEP.

- 11.2.10. No se deben almacenar en las carpetas compartidas ubicadas en los servidores, *OneDrive* empresarial y/o el almacenamiento interno de los equipos informáticos asignados, archivos de música, de video o archivos de imágenes que no sean propias de las labores realizadas para la Institución. Los archivos no autorizados pudieran ser borrados por el personal técnico de la DIG si se determina con un informe técnico/auditoría y/o denuncia que respalde tal accionar.



- 11.2.11. Cuando se utilizan dispositivos tecnológicos propios (computadoras, tabletas, celulares, cámaras fotográficas, entre otros), el funcionario debe velar de no sincronizar información no laboral en el espacio en el *OneDrive* empresarial o en el equipo, ambos asignados por la Institución.

- 11.2.12. Cada usuario debe guardar sus documentos frecuentemente, en especial si el mismo no cuenta con una *UPS* que resguarde su equipo en caso de una avería eléctrica.

- 11.2.13. Los fondos y/o refrescamientos de pantallas serán definidos por el Departamento de Gestión de Producción de la DRTE del MEP. Estos serán instalados por los funcionarios del DRT de la DIG.

- 11.2.14. 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. De igual forma es deber de cada funcionario informar a su jefatura inmediata si las condiciones donde labora no poseen un entorno adecuado para el bien informático que fue asignado a él.



- 11.2.15. 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*).
- 11.2.16. No conectar en tomacorrientes destinados para los bienes informáticos, los siguientes artículos: fotocopiadoras, hornos de microondas, percoladores/*coffeemaker*, abanicos, cargadores de teléfonos y otros artefactos electrónicos.
- 11.2.17. No conectar en los puertos *USB* del equipo institucional celulares, tabletas, reproductores *mp3* o *mp4*, así como dispositivos de almacenamiento *USB*, entre otros.
- 11.2.18. En caso de abandonar el área de trabajo, bloquear el equipo empleando la combinación de teclas *Windows* + L ( + ).
- 11.2.19. Para los funcionarios con labores no teletrabajables o en tiempos de vacaciones colectivas, deberán dejar los equipos apagados.
- 11.2.20. Para los funcionarios con labores teletrabajables deben cerrar sesión de los sistemas de información, *software* y/o bases de datos, cuando se va a retirar del equipo.
- 11.2.21. Procurar el óptimo y adecuado uso de los bienes o recursos informáticos a su cargo.
- 11.2.22. Será responsable del bien o recurso informático, de su uso, resguardo y cuidado.
- 11.2.23. No alterar las configuraciones del equipo, de manera tal que pueda afectar el uso normal de este, tanto en oficinas o en modalidad de teletrabajo, ni alterará los dispositivos de seguridad del equipo, tales como sellos, etiquetas, candados u otros que poseen. Solo el personal informático que posee autorización puede abrir los equipos de cómputo o cambiar la configuración.
- 11.2.24. Cuando el funcionario se encuentre en algún edificio del MEP, para realizar sus labores, debe conectar el equipo asignado (arrendado o adquirido por el Ministerio) a la red institucional proporcionada (red cableada, *WiFi*) del edificio. Se le prohíbe compartir Internet a las computadoras institucionales, mediante dispositivos de uso personal, tales como teléfonos celulares, tabletas, *MiFi*, *routers* portátiles, *datacards*, entre otros.
- 11.2.25. Reportar a los funcionarios de la Unidad de Control de Contratos del DST de la DIG y al Departamento de Control de Bienes de la DPI, la movilización de los bienes informáticos (computadoras y/o impresoras entre otros equipos informáticos) que tiene bajo su responsabilidad, mediante el sistema creado para este fin. Deberá comunicar inmediatamente a su superior sobre cualquier inconveniente que se presente, ya sea sobre eventos de robo, hurto, daño físico y fallas en su funcionamiento.
- 11.2.26. Es deber de cada funcionario de OC, DRE y Supervisiones Educativas reportar fallas en su funcionamiento de sus bienes informáticos que le fueron asignado a él, que se encuentren a su cargo, bajo su administración, custodia o concesión, por medio del Sistema dispuesto por el Departamento de Soporte Técnico. Cabe indicar que los funcionarios del DST no brindan soporte al equipo que es propiedad de los funcionarios.



- 11.2.27. Al devolver el equipo, este debe contar con el *software* preinstalado, así como todos los componentes que les fue entregado para su resguardo (tal como teclado, *mouse*, *docking*, maletín, cables, entre otros). Cabe indicar que el equipo que se entrega debe ser verificado por el funcionario que recibe.
- 11.2.28. Cuando el funcionario tenga fecha de finalización de relación laboral con la oficina, departamento, dirección u oficina adscrita en la que labora, sean ceses interinos, ascensos, descensos, traslados o préstamo a hacia otra oficinas en el MEP entre otros; es deber del funcionario realizar previo a su movimiento de personal, los procedimientos vigentes de devolución de los bienes informáticos a su jefe inmediato, bienes que le fueron asignado a él, que se encuentren a su cargo, bajo su administración, custodia o concesión. Se excluyen de este proceso ceses laborales por defunción por no ser de control del funcionario.
- 11.2.29. El funcionario que requiera instalar/desinstalar *software* en su equipo deberá hacer la solicitud al DST, mediante el Sistema de atención de incidencias oficial del MEP, con el visto bueno de los encargados de Normalización de Licencias y Oficina Ciberseguridad.
- 11.2.30. El funcionario al que se asigne el equipo informático deberá velar por el resguardo de todos sus componentes y/o programas de cómputo autorizados, con su respectiva licencia.
- 11.2.31. Acatar ***obligatoriamente*** con lo estipulado por la DIG en relación con las mejores prácticas de seguridad informática.
- 11.2.32. Acatar lo indicado en este manual según corresponda.

### 11.3. Al usuario que hace uso de los bienes informáticos

- 11.3.1. Utilizar los bienes informáticos tangibles e intangibles (*software*), únicamente para el cumplimiento de las funciones asignadas según su clase de puesto y especialidad.
- 11.3.2. 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.
- 11.3.3. Todo funcionario está en la obligación de denunciar ante la Contraloría de Servicios o bien DAI, 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”.*

- 11.3.4. Todos los usuarios deben tener conocimiento y estar conscientes de los compromisos, normas, reglamentos y lineamientos que han adquirido para el uso de los servicios informáticos.
- 11.3.5. Acatar e implementar las medidas de seguridad establecidas que garanticen el resguardo necesario.
- 11.3.6. No debe fumar o consumir alimentos y/o bebidas mientras realiza sus labores.
- 11.3.7. Deberá hacer respaldos de la información que se encuentra en el almacenamiento interno de la computadora 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 oficial *OneDrive* empresarial.
- 11.3.8. No se debe almacenar la información que sea propia de las labores realizadas para la Institución en almacenamiento en la nube personal (*OneDrive* personal o en cualquier otro servicio de almacenamiento en la nube), las implicaciones en cuanto confidencialidad de la información y responsabilidad de ésta, 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.
- 11.3.9. No se deben almacenar en las carpetas compartidas ubicadas en los servidores, *OneDrive* empresarial y/o el almacenamiento interno de los equipos informáticos asignados, archivos de música, de video o archivos de imágenes que no sean propias de las labores realizadas para la Institución. Los archivos no autorizados pudieran ser borrados por el personal técnico de la DIG si se determina con un informe técnico/auditoría y/o denuncia que respalde tal accionar.
- 11.3.10. Cuando se utilizan dispositivos tecnológicos propios (computadoras, tabletas, celulares, cámaras fotográficas, entre otros), el funcionario debe de tener cuidado de no sincronizar información no laboral en el espacio en el *OneDrive* empresarial o en el equipo, ambos asignados por la Institución.
- 11.3.11. No conectar en los puertos *USB* del equipo institucional celulares, tabletas, reproductores *mp3* o *mp4*, así como dispositivos de almacenamiento *USB*, entre otros.
- 11.3.12. Los fondos y/o refrescamientos de pantallas serán definidos por el Departamento de Gestión de Producción de la DRTE del MEP. Estos serán instalados por los funcionarios del DRT de la DIG.
- 11.3.13. 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.
- 11.3.14. 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*).



- 11.3.15. 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.
- 11.3.16. En caso de abandonar el área de trabajo, bloquear el equipo empleando la combinación de teclas *Windows* + L ( + ).
- 11.3.17. Para los funcionarios con labores no teletrabajables o en tiempos de vacaciones colectivas, deberán dejar los equipos apagados.
- 11.3.18. Para los funcionarios con labores teletrabajables se les recomienda cerrar sesión de los sistemas de información, *software* y/o bases de datos, cuando se va a retirar del equipo.
- 11.3.19. Procurar el óptimo y adecuado uso de los bienes o recursos informáticos que tiene a su disposición para efectuar sus labores.
- 11.3.20. Será responsable del uso, resguardo y cuidado, del bien o recurso informático.
- 11.3.21. No alterar las configuraciones del equipo, de manera tal que pueda afectar el uso normal de este, tanto en oficinas o en modalidad de teletrabajo.
- 11.3.22. Cuando el funcionario se encuentre en algún edificio del MEP y haga uso de los bienes informáticos, para realizar sus labores, debe conectar el equipo asignado (arrendado o adquirido por el Ministerio) a la red institucional proporcionada (red cableada, *WiFi*) del edificio. Se le prohíbe compartir Internet a las computadoras institucionales, mediante dispositivos de uso personal, tales como teléfonos celulares, tabletas, *MiFi*, *routers* portátiles, *datacards*, entre otros.
- 11.3.23. Restricción de conexión de equipos no autorizados a la red institucional del MEP.

Dentro de la red institucional existe una configuración base estandarizada y administrada por la DIG, diseñada para garantizar la seguridad, disponibilidad, desempeño y estabilidad de los servicios de telecomunicaciones.

Queda estrictamente prohibido que los funcionarios conecten a la red institucional cualquier equipo de telecomunicaciones no autorizado a puntos de acceso inalámbricos o por cable de red cómo: *switches* domésticos (AP), *routers*, repetidores, extensores de red u otros dispositivos similares, con el objetivo de extender, modificar o redistribuir la conectividad de red.

La conexión de este tipo de equipos puede generar tormentas de *broadcast* (Difusión masiva de información o paquetes de datos a través de redes informáticas. En el caso de la informática, *broadcast* o difusión es la transferencia de información desde un nodo emisor a una multitud de nodos receptores), bucles de red, conflictos de direccionamiento *IP*, degradación del rendimiento, interrupciones del servicio y vulnerabilidades de seguridad, afectando de manera directa la operación normal de la red institucional y de los sistemas críticos que dependen de ella.

Cualquier requerimiento de ampliación, mejora o modificación de la conectividad de red deberá ser canalizado y aprobado previamente por la DIG, quien evaluará la necesidad.



El incumplimiento de esta disposición podrá derivar en la desconexión inmediata del equipo, así como en la aplicación de las medidas administrativas correspondientes, de acuerdo con las disposiciones internas del MEP.

- 11.3.24. Reportar a los funcionarios de Control de Contratos del DST de la DIG y al Departamento de Control de Bienes de la DPI, la movilización de los bienes informáticos (computadoras y/o entre otros equipos informáticos) que tiene bajo su responsabilidad, mediante el sistema creado para este fin.
- 11.3.25. Deberá comunicar inmediatamente a su superior sobre cualquier inconveniente que se presente, en especial si algún bien ha sido sustraído, reporta fallas en su funcionamiento o sufra un daño físico.
- 11.3.26. Cada usuario debe guardar sus documentos frecuentemente, en especial si el mismo no cuenta con una *UPS* que resguarde su equipo en caso de una avería eléctrica.
- 11.3.27. El funcionario que requiera instalar/desinstalar *software* en su equipo deberá hacer la solicitud al DST, mediante el Sistema de atención de incidencias oficial del MEP, con el visto bueno de los encargados de Normalización de Licencias y Oficina Ciberseguridad.
- 11.3.28. El funcionario que hace uso del equipo informático deberá velar por el resguardo de todos sus componentes y/o programas de cómputo autorizados, con su respectiva licencia.
- 11.3.29. Todo funcionario que utiliza el recurso informático es responsable de velar por un adecuado uso, previamente aceptados mediante formulario u oficio respectivo.
- 11.3.30. Al devolver el equipo, este debe contar con el *software* preinstalado, así como todos los componentes (teclado, *mouse*, *docking*, maletín, cables, entre otros). Cabe indicar que el equipo entregado, debe ser verificado por el funcionario que recibe.
- 11.3.31. Acatar **obligatoriamente** con lo estipulado por la DIG en relación con las mejores prácticas de seguridad informática.
- 11.3.32. Acatar lo indicado en este manual según corresponda.

#### 11.4. A las jefaturas

- 11.4.1. Informar inmediatamente a la DIG mediante oficio 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, así como pérdida de información.
- 11.4.2. Solicitar por escrito (oficio y formulario debidamente firmado) a la DIG 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.
- 11.4.3. En caso de requerir la instalación de bienes informáticos, reconfiguración de estos o de accesorios que no forman parte de la configuración original, deben coordinar la respectiva colaboración a la DIG, mediante el Sistema de atención de incidencias oficial del MEP, para su respectivo análisis.



- 11.4.4. Vigilar por la implementación de las medidas de seguridad dispuestas en este Manual o cualquier lineamiento informático dictado por autoridad competente.
- 11.4.5. Informar inmediatamente a la DIG mediante oficio el cese de cada funcionario para cerrar la cuenta del correo Ministerial asignada a este.
- 11.4.6. Es deber de las jefaturas velar, gestionar, instruir que los procedimientos de asignación, traslado, devolución, salidas del país y control de inventario de los bienes informáticos que tiene su dependencia sean ejecutados correctamente y mantener los mismos actualizados.
- 11.4.7. Gestionar la asignación del bien informático mediante el uso de los formularios correspondientes. Equipo propiedad del MEP “Formulario de Asignación de Bienes de la Proveduría Institucional” (SICAMEP) y/o Equipo de cómputo/impresoras arrendadas a “Formulario Control de Activos en Arrendamiento” (Unidad de Control de Contratos).
- 11.4.8. Si la jefatura cuenta con equipos disponibles para asignarlos a sus colaboradores, la asignación se debe de realizar mediante el Formulario control de activos en arrendamiento.
- 11.4.9. Velar cuando sus colaboradores se encuentren en algún edificio del MEP y haga uso de los bienes informáticos, para realizar sus labores, debe conectar el equipo asignado (arrendado o adquirido por el Ministerio) a la red institucional proporcionada (red cableada, *WiFi*) del edificio. Se le prohíbe compartir Internet a las computadoras institucionales, mediante dispositivos de uso personal, tales como teléfonos celulares, tabletas, *MiFi*, *routers* portátiles, *datacards*, entre otros.
- 11.4.10. Concientizar a los colaboradores en su actuar en caso de que su equipo presente cualquier inconveniente, en especial si algún bien ha sido sustraído, reporta fallas en su funcionamiento o sufra un daño físico.
- 11.4.11. Crear la cultura en sus colaboradores para que cuando requieran instalar/desinstalar *software* en su equipo deberá hacer la solicitud al DST, mediante el Sistema de atención de incidencias oficial del MEP.
- 11.4.12. Velar por el resguardo de todos los componentes y programas de cómputo autorizados, así como su respectiva licencia del equipo informático (entiéndase este como equipo propiedad del MEP o arrendado), que se designa a los colaboradores mediante el formulario correspondiente. En este documento debe indicarse el detalle del equipo/bien informático designado, como mínimo el número de activo, descripción, serie, marca.
- 11.4.13. Velar por que sus colaboradores empleen los bienes informáticos únicamente para el cumplimiento de las funciones asignadas según su clase de puesto y especialidad.
- 11.4.14. Concientizar a los colaboradores en tener conocimiento y estar conscientes de los compromisos, normas y reglamentos que han adquirido para el uso de los recursos/servicios informáticos.
- 11.4.15. Crear cultura en sus colaboradores para que realicen los respaldos de la información que se encuentra en el almacenamiento interno de la computadora 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 oficial *OneDrive* empresarial.

- 11.4.16. Velar porque los colaboradores no deben almacenar información institucional en la nube (*OneDrive* personal o en cualquier otro servicio de almacenamiento en la nube) y en caso de que lo hagan, queda bajo la responsabilidad del usuario, así como las implicaciones en cuanto confidencialidad de la información y responsabilidad de ésta, así como su uso. Esto con la finalidad de no afectar el tráfico en las comunicaciones en la red de datos del MEP, el ancho de banda disponible será administrado por la DIG.
- 11.4.17. Crear cultura en sus colaboradores para que no almacenen en las carpetas compartidas, ubicadas en los servidores, *OneDrive* empresarial y/o el almacenamiento interno de los equipos informáticos asignados, archivos de música, de video o archivos de imágenes que no sean propias de las labores realizadas para la Institución. Los archivos no autorizados pudieran ser borrados por el personal técnico de la DIG si se determina con un informe técnico/auditoría y/o denuncia que respalde tal accionar.
- 11.4.18. Crear cultura para que sus colaboradores guarden sus documentos frecuentemente, en especial si el mismo no cuenta con una *UPS* que resguarde su equipo en caso de una avería eléctrica.
- 11.4.19. Velar porque sus colaboradores conecten 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*).
- 11.4.20. Velar porque sus colaboradores no conecten en los puertos *USB* del equipo institucional celulares, tabletas, reproductores *mp3* o *mp4*, así como dispositivos de almacenamiento *USB*, entre otros.
- 11.4.21. Concientizar a los colaboradores que emplean bienes y recursos informáticos institucionales, en el óptimo y adecuado uso, resguardo y cuidado de estos.
- 11.4.22. Velar porque sus colaboradores participen activamente en el proceso de capacitación dispuesto por las Autoridades Superiores.
- 11.4.23. Velar porque sus colaboradores cumplan con lo estipulado por la DIG en relación con las mejores prácticas de seguridad informática.
- 11.4.24. Acatar lo indicado en este manual según corresponda.

## 11.5. A la DIG

- 11.5.1. Vigilar por la implementación de las medidas de seguridad dispuestas en este Manual o cualquier lineamiento informático dictado por autoridad competente.
- 11.5.2. 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.
- 11.5.3. Contar con las herramientas adecuadas para la verificación del cumplimiento de las restricciones, con las limitantes según sea el caso del servicio que se brinda.



- 11.5.4. Asegurar la continuidad del servicio brindado por el recurso informático arrendado a los usuarios, con el fin de no entorpecer sus labores cotidianas.
- 11.5.5. Apoyar la labor de la Oficina de Ciberseguridad, brindando los insumos requeridos.
- 11.5.6. Concientizar a todos los funcionarios del Ministerio por el resguardo de información institucional en el *OneDrive* empresarial.
- 11.5.7. Concientizar a todos los funcionarios del Ministerio no deben conectar en los puertos *USB* del equipo institucional celulares, tabletas, reproductores *mp3* o *mp4*, así como dispositivos de almacenamiento *USB*, entre otros.
- 11.5.8. Concientizar frecuentemente mediante los canales de difusión masiva oficiales, a las Jefaturas para crear la cultura en sus colaboradores para que cuando requieran instalar/desinstalar *software* en su equipo deberá hacer la solicitud al DST, mediante el Sistema de atención de incidencias oficial del MEP.
- 11.5.9. Velar porque los funcionarios participen activamente en el proceso de capacitación dispuesto por las Autoridades Superiores.
- 11.5.10. Velar porque se cumpla una correcta configuración/actualización y las mejores prácticas en la solución del *firewall* para proteger la red y los dispositivos institucionales.
- 11.5.11. Establecer lineamientos para la correcta gestión de actualizaciones, para garantizar que todos los sistemas y aplicaciones estén actualizados.
- 11.5.12. Vigilar porque el *software* de seguridad se encuentre debidamente configurado y actualizado, así como, una solución *antimalware* en todos los dispositivos, buscando siempre una mejora continua.
- 11.5.13. Realizar el comunicado para que los colaboradores realicen **el acatamiento obligatorio** de las mejores prácticas de seguridad informática, que sean generadas por la DIG, o algún ente especializado/regulador.
- 11.5.14. Crear cultura y velar por que las jefaturas de los funcionarios que van a salir del país tramiten el oficio correspondiente con anticipación y en caso de presentarse durante el viaje algún incidente repórtalo a las autoridades del país donde se presentó este, remitir reporte a los siguientes correos los sucedido [seguridadinformaticadig@mep.go.cr](mailto:seguridadinformaticadig@mep.go.cr) y [arrendamientoecdig@mep.go.cr](mailto:arrendamientoecdig@mep.go.cr), para iniciar el trámite de la gestión.
- 11.5.15. Acatar lo indicado en este manual según corresponda.

## 11.6. Autoridades superiores

- 11.6.1. Apoyar a la DIG y a la Oficina de Ciberseguridad en la implementación de las medidas de seguridad dispuestas en este Manual o cualquier lineamiento informático dictado por autoridad competente.
- 11.6.2. Aprobar el proceso para asegurar la continuidad del servicio brindado por el recurso informático arrendado a los usuarios, con el fin de no entorpecer sus labores cotidianas.



- 11.6.3. Concientizar al personal del ministerio en el uso **obligatorio** de este manual al realizar sus labores diarias.
- 11.6.4. Gestionar alianzas con empresas privadas o del sector gobierno en la búsqueda de capacitación para el personal del ministerio.
- 11.6.5. Establecer política enfocada a la capacitación, aprendizaje de destrezas, relacionada con temas relevantes de nuestra actualidad, tales como Ciberseguridad, resguardo de la información que se encuentra en la unidad de almacenamiento interno de la computadora, uso del *OneDrive* empresarial, importancia de la seguridad física de los dispositivos de almacenamiento, su protección contra robo y/o pérdida, así como el transporte de estos, ¿cómo detectar correos electrónicos sospechosos?, *spam* y *phishing*, no hacer clic en los enlaces cortos que provengan de remitente desconocido y cómo verificar la seguridad de un sitio *web* antes de visitarlo, riesgos de conectarse a redes inalámbricas públicas, no protegidas o vulnerables, como las empleadas en los parques, aeropuertos, restaurantes entre otros, donde se solicite correos electrónicos o usuarios de dominio y como protegerse y otros temas relevantes.
- 11.6.6. Concientizar al personal del ministerio en la participación activa en el proceso de capacitación.
- 11.6.7. Buscar la creación de alianzas y/o convenios con instituciones públicas y privadas para recibir la capacitación requerida.
- 11.6.8. Solicitar a sus colaboradores su anuencia **al acatamiento obligatorio** de las mejores prácticas de seguridad informática, que sean generadas por la DIG, o algún ente especializado/regulador.
- 11.6.9. Acatar lo indicado en este manual según corresponda.

## 11.7. Relacionados a instalaciones/desinstalaciones de *software*

- 11.7.1. La instalación/desinstalación del *software* especializado de uso no común debe ser aprobada por su jefatura inmediata; y su instalación será realizada solo por personal autorizado del DST de la DIG, debe ser solicitada por medio del Sistema de atención de incidencias para ser autorizado e instalado, con el visto bueno de los encargados de Normalización de Licencias y Oficina Ciberseguridad.
- 11.7.2. Todo *software* que no cuente con la licencia respectiva será removido del equipo inmediatamente sin previo aviso.
- 11.7.3. Se prohíbe la instalación de *software* no autorizado por el DST o bien que no cuente con su respectiva licencia.
- 11.7.4. En todos los bienes informáticos institucionales, 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 para el cumplimiento de las funciones asignadas al funcionario según su clase de puesto y especialidad.
- 11.7.5. 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 institucionales



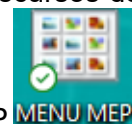
- 11.7.6. Únicamente el personal del DST de la DIG está facultado para la instalación y/o desinstalación de *software* que no cuente con una licencia.
- 11.7.7. En el decreto 45167-MICITT-J-COMEX, Reglamento para garantizar la observancia de los Derechos de Autor en el uso de los programas de Cómputo por parte de los Ministerios e Instituciones Adscritas al Gobierno Central, en el Capítulo III Gestión de los programas de cómputo en las instituciones cubiertas, se indica lo siguiente:
- “Artículo 8.- Los programas de cómputo a ser instalados en los equipos de los Ministerios e Instituciones adscritas al Gobierno Central, deben ser debidamente autorizados por los departamentos de tecnología de la información, y solamente podrán ser instalados por el experto en informática autorizado o por quien este determine para el buen desempeño de las funciones designadas.*
- Artículo 9.- Ante cualquier violación a las normas de derechos de autor por parte de los funcionarios de los Ministerios e Instituciones adscritas al Gobierno Central, se procederá con la apertura de un procedimiento administrativo, con el fin de aplicar la sanción de carácter administrativo disciplinario que corresponda.”*
- 11.7.8. La DIG llevará el inventario de las licencias de *software* adquiridas y solicitará a las Unidades Gestoras o Administradoras de *software* información sobre las mismas.
- 11.7.9. La DIG no controla ni administra licencias, es cada Unidad Gestora o Administradora de *software* la que realiza esa labor. Por ejemplo: el DIEE con AutoCad.
- 11.7.10. Toda instalación de bienes informáticos (*hardware* y/o *software*), reconfiguración de estos 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 DST de la DIG.

## 11.8. A la atención de solicitudes de Recursos Informáticos

- 11.8.1. Remitir a las cuentas de correo electrónico ([basededatos@mep.go.cr](mailto:basededatos@mep.go.cr), [secretariasistemas@mep.go.cr](mailto:secretariasistemas@mep.go.cr) y [correspondencia.redes@mep.go.cr](mailto:correspondencia.redes@mep.go.cr)) oficio con el formulario creado para tal fin. Estos documentos deben ser firmados de forma digital.

El formulario para solicitar la creación de usuario y acceso a los recursos de

red y sistemas de información, lo pueden encontrar en el Menú MEP



en el icono



Si el sistema no se encuentra en el formulario, se debe indicar en el oficio el nombre del sistema y los permisos que requiere, así como las calidades de los funcionarios (número de identificación y nombre completo).



- 11.8.2. En caso de requerirse la instalación de *software* y cualquier otro servicio que se brinda en la DIG, se debe plantear la solicitud mediante el Sistema de atención de incidencias oficial del MEP.
- 11.8.3. Si requieren el servicio de telefonía *IP*, la solicitud deben plantearla mediante oficio firmado de manera digital y enviarlo a la cuenta de correo electrónico [correspondencia.redes@mep.go.cr](mailto:correspondencia.redes@mep.go.cr). En dicho documento deben indicar las calidades de los funcionarios (número de identificación y nombre completo), y en caso de contar con usuario de red y cuenta de correo electrónico ministerial, deben suministrar dicha información en el oficio.
- 11.8.4. 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 del 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.
- 11.8.5. La DIG garantiza la seguridad informática y el uso adecuado de los recursos informáticos, así como, 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.
- 11.8.6. Cuando sea solicitado por la parte interesada, autoridad superior, o bien reguladora; la DIG entregará el informe técnico necesario, en aquellos casos en que se ha producido el uso no autorizado o indebido del bien/recurso y/o servicio informático, el cual se sugiere elevar al Departamento de Régimen Disciplinario para el debido proceso.
- 11.8.7. 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/recurso informático (con su debida solicitud).
- 11.8.8. 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.
- 11.8.9. Toda instalación/desinstalación de bienes/recursos informáticos (*hardware* y/o *software*), reconfiguración de estos o de accesorios que no forman parte de la configuración original, debe ser solicitada por medio del Sistema de atención de incidencias oficial del MEP para ser autorizado e instalado por el DST de la DIG, con el visto bueno de los encargados de Normalización de Licencias y Oficina Ciberseguridad.



### 11.9. Manejo de cuentas de usuario y contraseñas de acceso

- 11.9.1. 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.
- 11.9.2. Es terminantemente prohibido el uso de cuentas y contraseñas de otros usuarios.
- 11.9.3. El uso de la contraseña es personal, confidencial e intransferible (a otros usuarios y/o su jefatura).
- 11.9.4. No debe almacenar las contraseñas en agendas, libretas, *post-it*, entre otros.
- 11.9.5. 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 esta queda bajo la responsabilidad del usuario, así como el uso correcto.
- 11.9.6. 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.
- 11.9.7. El usuario debe acatar las características establecidas por la DIG para el establecimiento de contraseñas robustas y seguras. El resguardo de ésta queda bajo la responsabilidad del usuario, así como el uso correcto.
- 11.9.8. Se recomienda que la contraseña sea robusta y segura. Que cumpla con las siguientes características: longitud mínima de 14 caracteres, combinación de letras mayúsculas, minúsculas, caracteres especiales y al menos un número.
- 11.9.9. 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).
- 11.9.10. 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.
- 11.9.11. **Es obligatorio** el uso del doble factor de autenticación (*MFA*), para aplicar una capa adicional al acceso debidamente definido por la DIG.

### 11.10. Respaldo de datos

- 11.10.1. El usuario que tiene asignado bienes informáticos, así como, el que los usa, deberá hacer respaldos de la información ubicada en su unidad de almacenamiento interno de la computadora, información laboral que considere crítica o de suma importancia.

Debe realizarse de manera regular, como medida de contingencia, en el momento que se jubile, renuncie, se cambie de dependencia o se ausente por incapacidad prolongada ante un eventual daño en su computador o corte de fluido eléctrico, utilizando para ello el *OneDrive* empresarial.



- 11.10.2. No se debe almacenar la información que sea propia de las labores realizadas para la Institución en almacenamiento en la nube personal (*OneDrive* personal o en cualquier otro servicio de almacenamiento en la nube), las implicaciones en cuanto confidencialidad de la información y responsabilidad de ésta, 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.
- 11.10.3. No se deben almacenar en las carpetas compartidas ubicadas en los servidores, *OneDrive* empresarial y/o el almacenamiento interno de los equipos informáticos asignados, archivos de música, de video o archivos de imágenes que no sean propias de las labores realizadas para la Institución. Los archivos no autorizados pudieran ser borrados por el personal técnico de la DIG si se determina con un informe técnico/auditoría y/o denuncia que respalde tal accionar.
- 11.10.4. El DST de la DIG 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 estos y procederán como corresponda.
- 11.10.5. Se prohíbe el uso de dispositivos que permiten el acceso a Internet en las computadoras institucionales, cuando esté en cualquier dependencia ministerial conectado a la red institucional.
- 11.10.6. No conectar en los puertos *USB* del equipo institucional, dispositivos de almacenamiento *USB*.
- 11.10.7. Cada usuario debe guardar sus documentos frecuentemente, en especial si el mismo no cuenta con una *UPS* que resguarde su equipo en caso de una avería eléctrica.

#### **11.11. Uso de servicios en red**

- 11.11.1. 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 DIG 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 éstas, 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 OC, DRE y Circuitos Escolares.
  - d) Monitorear el volumen y consumo del flujo de datos de cada usuario, así como los sitios visitados.



### 11.12. Uso de telefonía IP

- 11.12.1. El uso de la telefonía *IP* es **único** y **exclusivo** para usuarios destacados y que desempeñan labores en OC, DRE y Circuitos Escolares.

Ante alguna solicitud especial, se puede extender el servicio a programas especiales, así como Centros Educativos que por situaciones del proveedor de servicios (robo de cable, no disponibilidad de telefonía convencional) se les puede asignar extensiones, esto avalado por los Despachos.

- 11.12.2. Los usuarios deben emplear el servicio de telefonía *IP* para asuntos **exclusivamente** relacionados con sus labores y en horario de oficina o para atender algún imprevisto.

- 11.12.3. Queda prohibido el uso de este servicio para asuntos personales o cualquier otro uso distinto al indicado anteriormente.

- 11.12.4. Es responsabilidad del funcionario y su jefatura reiterar y velar por el adecuado uso de este servicio; cualquier mal uso de este acarreará la responsabilidad correspondiente.

- 11.12.5. No se autoriza la instalación de este servicio en computadoras personales, al ser este exclusivo para equipos propios del MEP o arrendados.

Los funcionarios del DST tienen instrucciones para atender solicitudes de instalación de los aplicativos de la telefonía *IP* en equipos institucionales. El funcionario debe registrar la solicitud en el Sistema de atención de incidencias oficial del MEP y en caso de no contar con dicho acceso, enviar mensaje de correo electrónico a la cuenta [mesaserviciosmep@mep.go.cr](mailto:mesaserviciosmep@mep.go.cr) planteando la solicitud.

- 11.12.6. Se **prohíbe** la instalación de los aplicativos de la telefonía *IP* en dispositivos móviles como celulares, tabletas, así como computadoras personales.

- 11.12.7. El aplicativo del servicio de telefonía *IP* basado en el principio de la privacidad y las telecomunicaciones **NO** graba ni almacena las llamadas telefónicas. Únicamente, registra las estadísticas del servicio de llamadas entrantes o salientes, tales como fecha, hora, origen, destino, estado y duración; esto como parte de la administración del servicio, basado en la Ley de Control Interno.

- 11.12.8. Las estadísticas del servicio de llamadas entrantes o salientes pueden ser solicitado por el dueño de la extensión o por su jefatura.

### 11.13. Permisos especiales a servicios institucionales

- 11.13.1. En casos especiales, corresponderá a la DIG otorgar cuentas de usuarios a personas externas a la Institución el cual será analizado y aprobado por el director o autoridad competente, relacionada con el área donde trabajará la persona solicitante.

Se debe generar un oficio haciendo la solicitud, posteriormente la DIG responderá con las instrucciones que debe seguir para el respectivo análisis,



con base en este se determinará si la solicitud puede ser aprobado o no.  
Ejemplos:

- Todas las unidades y dependencias del MEP que requieran la conexión a la red institucional de empresas externas con contratos o convenios vigentes.
- Empresas consultoras, proveedores de servicios tecnológicos, empresas con convenios vigentes y cualquier otro que utilice dispositivos propios para consulta autorizada, soporte o mantenimiento a los sistemas internos del MEP.

#### 11.14. Uso del correo electrónico

- 11.14.1. Cada funcionario será responsable del uso adecuado de su cuenta de correo electrónico y de la información que remita.
- 11.14.2. La DIG sólo brindará ayuda y soporte a las cuentas @mep.go.cr
- 11.14.3. Los servicios de correo electrónico y accesos a Internet son puestos a disposición de los funcionarios para asuntos **estrictamente** laborales. Esta cuenta de correo electrónico no debe ser utilizada para fines personales, por ejemplo, bancos, Uber, registros de páginas en línea como CANVA y redes sociales, entre otros, para esto debe utilizarse el correo personal.
- 11.14.4. Para la utilización de programas de mensajería y chat para fines laborales, debe utilizarse *Microsoft Teams* con la cuenta oficial del MEP.
- 11.14.5. **Es obligatorio** el uso del doble factor de autenticación (*MFA*), para aplicar una capa adicional al acceso debidamente definido por la DIG.
- 11.14.6. 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 electrónico provocando saturación.
- 11.14.7. Si el funcionario se siente ofendido por un mensaje de correo electrónico que recibió, favor de reenviarlo a su jefatura inmediata para lo correspondiente.
- 11.14.8. 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.
- 11.14.9. El funcionario debe desconfiar de todos los mensajes de correo electrónico que procedan de remitentes desconocidos o de dudosa procedencia; ya que estos podrían estar infectados con *malware*, asimismo, evitar abrir los archivos adjuntos, en tal caso proceder a eliminar los mensajes.
- 11.14.10. Si se desea mantener un mensaje en forma permanente, este se debe almacenar en una carpeta personal en el equipo del usuario.
- 11.14.11. 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.
- 11.14.12. 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.



- 11.14.13. El DST dará una única inducción al usuario de como respaldar la información de correo electrónico mediante un archivo de extensión PST, con el fin de que este último pueda generar regularmente el respaldo de su buzón correo.
- 11.14.14. La administración de la red no da garantías de ningún tipo, sea expresa o implícitamente, para el servicio del correo electrónico que se provee, por cualquier daño que el usuario sufra causado por negligencia propia, errores, omisiones o el mal uso del servicio.

### **11.15. Uso de mensajes de correo electrónico masivos**

- 11.15.1. La comunicación masiva a los funcionarios institucionales mediante el correo electrónico sólo será posible para aquellas instancias o funcionarios que, de acuerdo con 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 DIG.
- 11.15.2. 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.
- 11.15.3. 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.
- 11.15.4. El funcionario debe desconfiar de todos los mensajes de correo electrónico que procedan de remitentes desconocidos o de dudosa procedencia; ya que estos podrían estar infectados con *malware*, asimismo, evitar abrir los archivos adjuntos, en tal caso proceder a eliminar los mensajes.
- 11.15.5. Si se desea mantener un mensaje en forma permanente, este se debe almacenar en una carpeta personal en el equipo del usuario.
- 11.15.6. 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.
- 11.15.7. 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.
- 11.15.8. La administración de la red no da garantías de ningún tipo, sea expresa o implícitamente, para el servicio del correo electrónico que se provee, por cualquier daño que el usuario sufra causado por negligencia propia, errores, omisiones o el mal uso del servicio.

### **11.16. Uso del equipo arrendado (Computadoras e impresoras)**

- 11.16.1. Los lineamientos documentados en el presente manual, para funcionarios, jefaturas y leyes generales vinculantes al uso de equipo, aplican para el equipo arrendado de los contratos vigentes de equipo de cómputo e impresión de la DIG.



- 11.16.2. Para la consulta sobre trámites relacionados por ejemplo con la atención de incidentes de reportes de garantía, por daños físicos y/o robo; tipos de movimientos de los equipos arrendados tales como asignación, devolución y traslado; reporte de salidas de equipos de cómputo fuera del país, además de procedimientos vigentes de los equipos arrendados por los contratos gestionados por el Departamento de Soporte Técnico de la DIG, pueden solicitarse a las siguientes cuentas de correo electrónico [arrendamientoecdig@mep.go.cr](mailto:arrendamientoecdig@mep.go.cr) y [arrendamientoimpresora@mep.go.cr](mailto:arrendamientoimpresora@mep.go.cr).

### 11.17. Uso de la firma digital

- 11.17.1. El usuario es responsable de establecer y resguardar el PIN de acceso de la firma digital.
- 11.17.2. El PIN de la firma digital es personal, confidencial e intransferible (a otros usuarios, jefatura y/o colaboradores).
- 11.17.3. Es **terminantemente prohibido** el uso de firmas digitales de otros usuarios.
- 11.17.4. No debe almacenar el PIN de la firma digital en agendas, libretas, *post-it*, entre otros.
- 11.17.5. Retirar la firma digital del lector en caso de abandonar temporalmente su espacio laboral.
- 11.17.6. Al retirar la firma digital del puerto *USB* del equipo institucional, debe emplearse la opción "Quitar *hardware* de forma segura y expulsar el medio".
- 11.17.7. Renovar con anticipación la firma digital antes de su expiración, de igual manera solicitar al DST mediante el Sistema de atención de incidencias oficial del MEP, la colaboración requerida para la actualización del certificado digital en el equipo.
- 11.17.8. En caso de olvidar el PIN, deberá presentarse en la institución emisora que le brindó la firma digital para cambiarla.
- 11.17.9. Ser consciente que cada acción firmada con la firma digital no es repudiable.
- 11.17.10. Independientemente del firmador que se utilice, se debe de validar estrictamente con el validador agente GAUDI validar. (G Agente GAUDI Validar )

### 11.18. Recomendaciones emanadas por la Oficina de Ciberseguridad

- 11.18.1. Se recomienda a la DIG la implementación de un sistema de gestión de seguridad de la información, solicitando el apoyo/compromiso de las autoridades superiores del MEP.
- 11.18.2. Se recomienda limitar el uso de dispositivos *USB* en computadoras institucionales con la finalidad de evitar la infección de archivos maliciosos en la red y/o equipos institucionales. Y en caso de hacerlo, concientizar que para retirarlo del equipo empleen la opción "Quitar *hardware* de forma segura y expulsar el medio".



- 11.18.3. Se recomienda a la DIG, gestionar al DSI que realice la investigación, análisis e implementación del MFA a nivel de aplicativos en aquellos que lo permitan según su arquitectura de programación o de desarrollo.
- 11.18.4. Se recomienda establecer lineamientos de privacidad y seguridad de datos que aborde el manejo de información personal y confidencial, relacionado a la categorización de datos, según lo dispuesto en la Ley de Protección de la Persona frente al tratamiento de sus datos personales, N° 8968.
- 11.18.5. Concientizar a los funcionarios con charlas, videos, circulares para educarlos sobre cómo detectar correos electrónicos sospechosos, *spam* y *phishing*.
- 11.18.6. Se recomienda a la DIG gestionar oportunamente el presupuesto para adquirir herramientas/servicios externos, con el objetivo de realizar evaluaciones de vulnerabilidades para identificar posibles brechas de seguridad y minimizar la afectación en los servicios brindados.
- 11.18.7. Se recomienda a la DIG, velar porque las soluciones de monitoreo de seguridad para detectar amenazas y anomalías se utilicen diariamente y con frecuencia; y que se encuentren debidamente actualizadas.
- 11.18.8. Se recomienda a la DIG, configurar una solución de protección contra ataques de denegación de servicio (DDoS), para garantizar que los sitios *web* y los servicios en línea no se interrumpan, y que se encuentren debidamente actualizadas.

## 12. DOCUMENTOS DE REFERENCIA

1. 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).

2. 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...”*

3. Plan Estratégico de Tecnología de la Información (PETI)



4. 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”.*

5. En el decreto N° 45167-MICITT-J-COMEX, Reglamento para Garantizar la Observancia de los Derechos de Autor en el uso de los Programas de Cómputo por parte de los Ministerios e Instituciones Adscritas al Gobierno Central, en el Capítulo I, Disposiciones Generales, artículo 3, inciso e) se indica lo siguiente:

*“e) Implementar los controles para garantizar la utilización en sus equipos, única y exclusivamente, de aquellos programas de cómputo que respeten plenamente los derechos de autor correspondientes. Cualquier programa que exceda el número autorizado o que no cumpla con los términos y condiciones de uso correspondientes, deberá removerse inmediatamente.”*

6. 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.

7. Normas Técnicas emitidas por el MICITT aplicándolas de manera parcial o total en este documento.

Ley N° 8968 del 07 de julio de 2011, denominada Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales

*“ARTÍCULO 1.- Objetivo y fin. Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.*

*ARTÍCULO 7.- Derechos que le asisten a la persona. Se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos. La persona responsable de la base de datos debe cumplir lo solicitado por la persona, de manera gratuita, y resolver en el sentido que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud.*

#### *1.- Acceso a la información*

*La información deberá ser almacenada en forma tal que se garantice plenamente el derecho de acceso por la persona interesada.*



*El derecho de acceso a la información personal garantiza las siguientes facultades del interesado:*

*a) Obtener en intervalos razonables, según se disponga por reglamento, sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.*

*b) Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen.*

*c) Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.*

*d) Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.*

*El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, le corresponderá a sus sucesores o herederos.*

## **2.- Derecho de rectificación**

*Se garantiza el derecho de obtener, llegado el caso, la rectificación de los datos personales y su actualización o la eliminación de estos cuando se hayan tratado con infracción a las disposiciones de la presente ley, en particular a causa del carácter incompleto o inexacto de los datos, o hayan sido recopilados sin autorización del titular.*

*Todo titular puede solicitar y obtener de la persona responsable de la base de datos, la rectificación, la actualización, la cancelación o la eliminación y el cumplimiento de la garantía de confidencialidad respecto de sus datos personales.*

*El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, le corresponderá a sus sucesores o herederos.*

**ARTÍCULO 8.- Excepciones a la autodeterminación informativa del ciudadano**



*Los principios, los derechos y las garantías aquí establecidos podrán ser limitados de manera justa, razonable y acorde con el principio de transparencia administrativa, cuando se persigan los siguientes fines:*

- a) La seguridad del Estado.*
- b) La seguridad y el ejercicio de la autoridad pública.”*

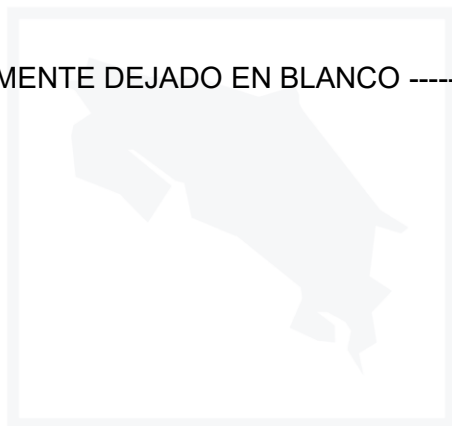
8. Así como cualquier otra normativa vigente relacionada.

## 13. ANEXOS

13.1. Anexo 1. Norma Técnica para la gestión y el control de las Tecnologías de Información.

## 14. HOJA DE FIRMAS

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





# HOJA DE REVISIÓN Y ACEPTACIÓN

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

### DVM-A-DIG-MAN-02

ACTUALIZADO POR:

Jenny Navarro Blanco

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

José Martín Sanchún Macín

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Alban A. García Vargas

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Juan Carlos Rodríguez

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Daniel Josué Delgado

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Marlon Vásquez Vásquez

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Rebeca Granados Vargas

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

**Marzo, 2026**



# HOJA DE REVISIÓN Y ACEPTACIÓN

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

### DVM-A-DIG-MAN-02

#### REVISADO POR:

**Lic. Iván Rojas Álvarez**

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Departamento Base de Datos y Seguridad

**Lic. Berni Salazar Rojas**

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Departamento Redes y Telecomunicaciones

**Lic. John Mehlbaum Ucanan**

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Departamento Soporte Técnico

**Licda. Kattia Paniagua Alfaro**

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Departamento Gestión y Control Informático

**Lic. Randy Valverde Valverde**

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

Departamento Sistemas de Información

**Marzo, 2026**



# HOJA DE REVISIÓN Y ACEPTACIÓN

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

**DVM-A-DIG-MAN-02**

### APROBADO POR:

**Gabriel Denis Denis**

Subdirector

Dirección de Informática de Gestión

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

**Danelia Ramírez Vargas**

Directora

Dirección de Informática de Gestión

FIRMADO DIGITALMENTE CON GAUDI  
ley 8454 de certificados y firmas digitales

**Marzo, 2026**