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

NOVIEMBRE, 2024

TABLA DE CONTENIDO

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

Fecha	Versión	Descripción	Responsables
			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. Cabe indicar que estas normas corresponden a buenas prácticas para los procesos establecidos en el Marco Normativo de Gobierno y Gestión de TI.	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
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

Fecha	Versión	Descripción	Responsables
			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 Garcia Vargas, 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 Rebeca Granados Vargas,

Fecha	Versión	Descripción	Responsables
			Departamento Redes y Telecomunicaciones Daniel Josué Delgado Leandro. Oficina de Ciberseguridad Juan Carlos Rodríguez Valerio. Oficina de Ciberseguridad

2 INTRODUCCIÓN

La Ley General de Control Interno, Ley N° 8292, Artículo 12 del 31 de julio del 2002, establece para los jerarcas 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 .

6 AUTOR (ES):

Jefaturas de la DIG.

7 ACTUALIZADO POR

Lic. Alban Antonio Garcia Vargas, Departamento Sistemas de Información, noviembre 2024.

Licda. Jenny Navarro Blanco, Departamento Base de Datos, noviembre 2024.

Lic. Marlon Vásquez Vásquez, Departamento Soporte Técnico, noviembre 2024.

Lic. José Martín Sanchún Macín, Departamento Gestión y Control Informático, noviembre 2024.

Lic. Máximo Varela Castro, Departamento Adquisición Tecnológica, noviembre 2024.

Licda. Rebeca Granados Vargas, Departamento Redes y Telecomunicaciones, noviembre 2024.

Ing. Daniel Josué Delgado Leandro. Oficina de Ciberseguridad, noviembre 2024.

Lic. Juan Carlos Rodríguez Valerio. Oficina de Ciberseguridad, noviembre 2024.

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 "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, MICITT, Dirección Jurídica, 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."

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 más preciado 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.

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 conexa.

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 Normas técnicas emitidas por el MICITT que aplican

A continuación, se indican las Normas Técnicas emitidas por el MICITT que, según nuestro análisis, aplican de manera parcial o total a este manual:

- EDM01 - Asegurar el establecimiento y el mantenimiento del Marco de Gobierno;
  - 01 - Evaluar el sistema de Gobierno;
    - Actividades 3 y 5;
  - 02 - Dirigir el sistema de Gobierno;
    - Actividades 2 y 6;
  - 03 - Monitorear el sistema de gobierno;
    - Actividad 6;

- EDM02 - Asegurar la Obtención de Beneficios;
  - 01 - Establecer el objetivo de la combinación en la inversión;
    - Actividad 3;
  - 02 - Evaluar la optimización del valor;
    - Actividad 2;
- EDM03 - Asegurar la Optimización del Riesgo;
  - 01 - Evaluar la gestión de riesgos;
    - Actividades 1, 2, 3, 4, 5, 6 y 7;
  - 02 - Dirigir la gestión de riesgos;
    - Actividades 4;
- EDM04 - Asegurar la optimización de los recursos;
  - 02 - Dirigir la gestión de recursos;
    - Actividades 1 y 2;
- EDM05 - Asegurar el compromiso de las partes interesadas;
  - 01 - Evaluar el compromiso y los requisitos de reportes de las partes interesadas;
    - Actividad 2;
- APO01 - Gestionar el marco de gestión de I&T;
  - 01 - Diseñar el sistema de gestión para la I&T de la Institución;
    - Actividades 2 y 3;
  - 02 - Gestionar la comunicación de objetivos, dirección y decisiones tomadas;
    - Actividades 2, 3 y 4;
  - 04 - Definir e implementar las estructuras organizativas;
    - Actividades 3, 4, 6 y 7;
  - 05 - Establecer roles y responsabilidades;
    - Actividades 1, 4, 5, 6 y 7;
  - 07 - Definir la propiedad de la información (datos) y del sistema de información;
    - Actividades 2 y 3;
  - 09 - Definir y comunicar políticas y procedimientos;
    - Actividades 1, 2 y 3;
  - 10 - Definir e implementar la infraestructura, servicios y aplicaciones para respaldar el sistema de gobierno y gestión;
    - Actividad 2

- 11 - Gestionar la mejora continua del sistema de gestión de I&T;
  - Actividad 4 y 6;

- APO02 - Gestionar la estrategia;
  - 02 - Evaluar las capacidades, rendimiento y madurez digital actual de la empresa;
    - Actividad 2;
  - 06 - Comunicar la dirección y estrategia de I&T;
    - Actividades 1 y 3;
- APO03 - Gestionar la Arquitectura Empresarial;
  - 05 - Proporcionar servicios de arquitectura empresarial;
    - Actividad 1;
- APO04 - Gestionar la innovación;
  - 01 - Crear un entorno favorable que conduzca a la innovación;
    - Actividades 2, 3 y 4;
  - 03 - Monitorizar explorar el entorno tecnológico;
    - Actividad 1, 2 y 3;
- APO05 - Gestionar el portafolio;
  - 05 - Gestionar el logro de beneficios;
    - Actividad 3;
- APO07 - Gestionar los recursos humanos;
  - 04 - Evaluar y reconocer/recompensar el rendimiento laboral de los empleados;
    - Actividad 4;
  - 06 - Gestionar al personal contratado;
    - Actividades 2 y 3;
- APO08 - Gestionar las relaciones;
  - 01 - Entender las expectativas del negocio;
    - Actividad 7;
  - 02 - Alinear la estrategia de I&T con las expectativas empresariales e identificar oportunidades para que TI mejore el negocio;
    - Actividad 1;
  - 03 - Gestionar la relación con el negocio;
    - Actividades 3 y 4;
  - 05 - Proporcionar aportes para la mejora continua de los servicios;

        - Actividades 1, 2 y 3;
- APO09 - Gestionar los acuerdos de servicio;
    - 03 - Definir y preparar acuerdos de servicio;
        - Actividad 1;
    - 05 - Revisar los acuerdos y los contratos de servicio;
        - Actividades 1 y 2;
- APO10 - Gestionar los proveedores;
    - 02 - Seleccionar proveedores;
        - Actividades 4 y 7;
    - 03 - Gestionar los contratos y las relaciones con los proveedores;
        - Actividad 3;
- APO11 - Gestionar la calidad;
    - 02 - Enfocar la gestión de la calidad en los clientes;
        - Actividad 4;
    - 03 - Gestionar los estándares, prácticas y procedimientos de calidad e integrar la gestión de la calidad en los procesos y soluciones clave;
        - Actividad 1 y 2;
- APO13 - Gestionar la seguridad;
    - 01 - Establecer y mantener un sistema de gestión de seguridad de la información (SGSI);
        - Actividad 6;
    - 02 - Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad;
        - Actividades 5 y 6;
- APO14 - Gestionar los datos;
    - 01 - Definir y comunicar la estrategia y los roles y responsabilidades de la gestión de datos de la organización;
        - Actividades 2, 3, 4, 8 y 9;
    - 02 - Definir y mantener un glosario empresarial consistente;
        - Actividades 1, 2 y 3;
    - 04 - Definir una estrategia de calidad de los datos;
        - Actividades 2 y 3;
    - 09 - Soportar el archivo y retención de datos;
        - Actividad 1;

- 10 - Gestionar los acuerdos de toma de copia de seguridad y restauración de datos;
  - Actividades 1, 2 y 3;
- BAI02 - Gestionar la definición de requisitos;
  - 01 - Definir y mantener los requisitos funcionales y técnicos del negocio;
    - Actividades 4, 5 y 6;
  - 04 - Adquirir los componentes de la solución;
    - Actividad 5;
- BAI03 - Gestionar la identificación y construcción de soluciones;
  - 11 - Definir productos y servicios de TI y mantener el portafolio de servicios;
    - Actividad 2;
- BAI04 - Gestionar la disponibilidad y la capacidad;
  - 04 - Monitorizar y revisar la disponibilidad y la capacidad;
    - Actividad 2;
  - 05 - Investigar y resolver los problemas de disponibilidad, rendimiento y capacidad;
    - Actividades 3 y 4;
- BAI05 - Gestionar el cambio organizativo;
  - 01 - Establecer el deseo de cambiar;
    - Actividad 4;
  - 02 - Formar un equipo de implementación eficaz;
    - Actividad 1;
  - 06 - Incorporar nuevos enfoques;
    - Actividades 1, 2, 3 y 4;
- BAI07 - Gestionar la aceptación y la transición de los cambios de TI;
  - 03 - Plan de pruebas de aceptación;
    - Actividad 4;
  - 07 - Proporcionar soporte oportuno en producción;
    - Actividades 1 y 2;
- BAI09 - Gestionar los activos;
  - 01 - Identificar y registrar los activos actuales;
    - Actividad 1 y 2;
  - 02 - Gestionar activos críticos;

        - Actividades 5, 6, 7 y 8;
    - 03 - Gestionar el ciclo de vida del activo;
        - Actividades 5 y 8;
    - 05 - Gestionar las licencias;
        - Actividades 1, 2 y 3;
- BAI10 - Gestionar la configuración;
    - 01 - Establecer y mantener un modelo de configuración;
        - Actividad 1;
- DSS01 -Gestionar las operaciones;
    - 03 - Monitorizar la infraestructura de I&T;
        - Actividades 5 y 6;
    - 04 - Gestionar el medioambiente;
        - Actividades 1, 2, 3, 4 y 7;
- DSS02 - Gestionar las peticiones y los incidentes de servicio;
    - 06 - Cerrar las peticiones de servicio y los incidentes;
        - Actividades 1 y 2;
- DSS03 - Gestionar los problemas;
    - 01 - Identificar y clasificar los problemas;
        - Actividades 5 y 6;
    - 04 - Resolver y cerrar los problemas;
        - Actividades 1 y 2;
- DSS04 - Gestionar la continuidad;
    - 01 - Definir la política de continuidad del negocio, sus objetivos y alcance;
        - Actividades 1, 2, 3 y 4;
    - 02 - Mantener la resiliencia del negocio;
        - Actividades 1, 2, 3, 4, 5, 6, 7 y 8;
    - 03 - Desarrollar e implementar una respuesta de continuidad del negocio;
        - Actividades 1, 2, 3, 4, 5, 6, 7 y 8;
    - 04 - Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP);
        - Actividades 1, 2, 3, 4, 5 y 6;
    - 05 - Revisar, mantener y mejorar los planes de continuidad;

- Actividades 1, 2, 3 y 4;
- 06 - Realizar formación sobre el plan de continuidad;
  - Actividades 1, 2, 3 y 4;
- 07 - Administrar los acuerdos de respaldo;
  - Actividades 1, 2 y 3;

1. 08 - Realizar revisiones post-reanudación;
   - Actividades 1, 2 y 3;

- DSS05 - Gestionar los servicios de seguridad;
  - 01 - Proteger contra software malicioso;
    - Actividades 1, 2, 3, 4 y 5;
- DSS06 - Gestionar los controles de procesos de negocio;
  - 03 - Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad;
    - Actividad 1 y 5;
  - 06 - Asegurar los activos de información;
    - Actividades 2, 3 y 5.

11.2 Generales

11.2.1. 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.".

11.2.2. 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."

11.2.3. 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.

11.2.4. El incumplimiento de las normas establecidas en este manual podrá acarrear responsabilidad administrativa, disciplinaria, civil y penal.

11.3 Al usuario que tiene asignados los bienes informáticos

11.3.1. Utilizar los bienes informáticos 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, sitos 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. 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).

11.3.5. 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.

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

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

11.3.8. Verificar con el *software* antivirus los medios de almacenamiento externo usados para el resguardo de información.

11.3.9. Es deber de cada funcionario realizar el respaldo de su información laboral que se encuentra en sus unidades de almacenamiento 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* o *OneDrive* empresarial.

11.3.10. Queda bajo la responsabilidad del usuario, el almacenamiento de la información institucional en la nube (*Dropbox*, *Onedrive* personal, *GoogleDocs* 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.

11.3.11. No se deben almacenar en las carpetas compartidas, *OneDrive* empresarial y/o los discos duros de las computadoras institucionales, archivos de música (*mp3*, *wma*, *wav*, entre otros), archivos de video (*vob*, *avi*, *mpg*, *swf,* entre otros) o archivos de imágenes (*jpg*, *bmp*, entre otros), 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.

11.3.12. 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.

11.3.13. 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.

11.3.14. 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.

11.3.15. 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.

11.3.16. 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*).

11.3.17. 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.

11.3.18. No conectar en los puertos USB del equipo institucional celulares, tabletas, reproductores mp3 o mp4, así como dispositivos de almacenamiento USB, entre otros. Y en caso de hacerlo, retirarlo del equipo mediante la opción "Quitar *hardware* de forma segura y expulsar el medio".

11.3.19. En caso de abandonar el área de trabajo, bloquear el equipo empleando la combinación de teclas *Windows* + L ().

11.3.20. Para los funcionarios con labores no teletrabajables o en tiempos de vacaciones colectivas, deberán dejar los equipos apagados.

11.3.21. Para los funcionarios con labores teletrabajables se les recomienda cerrar sesión de los sistemas de información, *software* y/o bases de datos.

11.3.22. Procurar el óptimo y adecuado uso de los bienes o recursos informáticos a su cargo.

11.3.23. Será responsable del bien o recurso informático, de su uso, resguardo y cuido.

11.3.24. 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.

11.3.25. Cuando el funcionario se encuentre en algún edificio del MEP, 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. Esta regla no aplica si el dispositivo es proporcionado por la Institución.

11.3.26. Debe custodiar los medios de almacenamiento (*CD*s o memorias *USB*) que le fueron entregados con equipo de cómputo.

11.3.27. 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.

11.3.28. 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.

11.3.29. 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.

11.3.30. 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.

11.3.31. 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.

11.3.32. 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.

11.3.33. Acatar ***obligatoriamente*** con lo estipulado por la DIG en relación a las mejores prácticas de seguridad informática.

11.3.34. Acatar lo indicado en los ítems 11.2, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11, 11.12, 11.13, 11.14, 11.15, 11.16, 11.17, 11.18 y 12, según corresponda.

11.4 Al usuario que hace uso de los bienes informáticos

11.4.1. Utilizar los bienes informáticos únicamente para el cumplimiento de las funciones asignadas según su clase de puesto y especialidad.

11.4.2. 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.

11.4.3. 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, sitos 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".*

11.4.4. 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.

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

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

11.4.7. Verificar con el *software* antivirus los medios de almacenamiento externo usados para el resguardo de información.

11.4.8. 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* o *OneDrive* empresarial.

11.4.9. Queda bajo la responsabilidad del usuario, el almacenamiento de la información institucional en la nube (*Dropbox*, *Onedrive* personal, *GoogleDocs* 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.

11.4.10. No se deben almacenar en las carpetas compartidas, *OneDrive* empresarial y/o los discos duros de las computadoras institucionales, archivos de música (*mp3*, *wma*, *wav*, entre otros), archivos de video (*vob*, *avi*, *mpg*, *swf*, entre otros) o archivos de imágenes (*jpg*, *bmp*, entre otros), 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

11.4.11. 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.

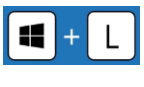
11.4.12. No conectar en los puertos USB del equipo institucional celulares, tabletas, reproductores mp3 o mp4, así como dispositivos de almacenamiento USB, entre otros. Y en caso de hacerlo, retirarlo del equipo mediante la opción "Quitar *hardware* de forma segura y expulsar el medio".

11.4.13. 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.

11.4.14. 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.

11.4.15. 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*).

11.4.16. 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.

11.4.17. En caso de abandonar el área de trabajo, bloquear el equipo empleando la combinación de teclas *Windows* + L ().

11.4.18. Para los funcionarios con labores no teletrabajables o en tiempos de vacaciones colectivas, deberán dejar los equipos apagados.

11.4.19. Para los funcionarios con labores teletrabajables se les recomienda cerrar sesión de los sistemas de información, *software* y/o bases de datos.

11.4.20. Procurar el óptimo y adecuado uso de los bienes o recursos informáticos que tiene a su disposición para efectuar sus labores.

11.4.21. Será responsable del uso, resguardo y cuido, del bien o recurso informático.

11.4.22. 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.

11.4.23. Cuando el funcionario se encuentre en algún edificio del MEP, 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. Esta regla no aplica si el dispositivo es proporcionado por la Institución.

11.4.24. Debe custodiar los medios de almacenamiento (*CD*s o memorias *USB*) que le fueron entregados con equipo de cómputo.

11.4.25. Reportar a los funcionarios del Proyecto de Arrendamiento 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.

11.4.26. 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.

11.4.27. 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.

11.4.28. 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.

11.4.29. 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.

11.4.30. Todo funcionario que utiliza el recurso informático es responsable de velar por un adecuado uso, previamente aceptados mediante formulario u oficio respectivo.

11.4.31. 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.

11.4.32. Acatar ***obligatoriamente*** con lo estipulado por la DIG en relación a las mejores prácticas de seguridad informática.

11.4.33. Acatar lo indicado en los ítems 11.2, 11.3, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11, 11.12, 11.13, 11.14, 11.15, 11.16, 11.17, 11.18 y 12 según corresponda.

11.5 A las jefaturas

11.5.1. 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.

11.5.2. Informar inmediatamente a la DIG mediante oficio el cese de cada funcionario para cerrar la cuenta del correo Ministerial asignada a este.

11.5.3. 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.

11.5.4. 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.

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

11.5.6. Es deber de las jefaturas velar, gestionar, instruir que los procedimientos de asignación, traslado, devolución y control de inventario de los bienes informáticos que tiene su dependencia sean ejecutados correctamente y mantener los mismos actualizados.

11.5.7. Gestionar la asignación del bien informático mediante el uso de los formularios correspondientes. Equipo propiedad del MEP → "Formulario de Asignación de Bienes de la Proveeduría Institucional" (SICAMEP) y/o Equipo de cómputo/impresoras arrendadas → "Formulario Control de Activos en Arrendamiento" (Unidad de Control de Contratos).

11.5.8. 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.

11.5.9. Velar por que los funcionarios que se encuentran en algún edificio del MEP, no compartan Internet a las computadoras institucionales, mediante dispositivos de uso personal, tales como teléfonos celulares, tabletas, *MiFi*, *routers* portátiles, *datacards*, entre otros. Esta regla no aplica si el dispositivo es proporcionado por la Institución.

11.5.10. Velar por que los funcionarios utilicen la función examinar del *software* antivirus a los medios de almacenamiento externo usados para el resguardo de información antes de su uso.

11.5.11. 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.

11.5.12. 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.

11.5.13. 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.

11.5.14. Velar por que sus colaboradores empleen los bienes informáticos únicamente para el cumplimiento de las funciones asignadas según su clase de puesto y especialidad.

11.5.15. 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.

11.5.16. Crear cultura en sus colaboradores para que realicen los respaldos de la información almacenada en el disco duro y que considere crítica o de suma importancia, esto como medida de contingencia ante un eventual daño en su computador. Se recomienda emplear

un medio de almacenamiento masivo, ya sea dispositivos *USB* o *OneDrive* empresarial.

11.5.17. Velar porque los colaboradores no almacenen información institucional en la nube (*Dropbox*, *Onedrive* personal, *GoogleDocs* 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.

11.5.18. Crear cultura en sus colaboradores para que no almacenen en las carpetas compartidas, *OneDrive* empresarial y/o los discos duros de las computadoras institucionales, archivos de música (*mp3*, *wma*, *wav*, entre otros), archivos de video (*vob*, *avi, mpg*, *swf*, entre otros) o archivos de imágenes (*jpg*, *bmp*, entre otros), 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.

11.5.19. 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.

11.5.20. 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*).

11.5.21. 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**.** Y en caso de hacerlo, retirarlo del equipo mediante la opción "Quitar *hardware* de forma segura y expulsar el medio".

11.5.22. Concientizar a los colaboradores que emplean bienes y recursos informáticos institucionales, en el óptimo y adecuado uso, resguardo y cuido de estos.

11.5.23. Velar porque sus colaboradores participen activamente en el proceso de capacitación dispuesto por las Autoridades Superiores.

11.5.24. Velar porque sus colaboradores cumplan con lo estipulado por la DIG en relación a las mejores prácticas de seguridad informática.

11.5.25. Acatar lo indicado en los ítems 11.2, 11.3, 11.4, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11, 11.12, 11.13, 11.14, 11.15, 11.16, 11.17, 11.18 y 12 según corresponda.

11.6 A la DIG

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

11.6.2. 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.

11.6.3. 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.

11.6.4. Asegurar la continuidad del servicio brindado por el recurso informático arrendado a los usuarios, con el fin de no entorpecer sus labores cotidianas.

11.6.5. Apoyar la labor de la Oficina de Ciberseguridad, brindando los insumos requeridos.

11.6.6. Promover como lineamiento y concientizar sobre la importancia de examinar dispositivos de almacenamiento con el antivirus antes de su uso.

11.6.7. Concientizar a todos los funcionarios del Ministerio por el resguardo de información institucional en el *OneDrive* empresarial.

11.6.8. Promover que los funcionarios del Ministerio no conecten en los puertos USB del equipo institucional celulares, tabletas, reproductores *mp3* o *mp4*, así como dispositivos de almacenamiento *USB*, entre otros. Y en caso de hacerlo, retirarlo del equipo mediante la opción "Quitar *hardware* de forma segura y expulsar el medio".

11.6.9. Concientizar frecuentemente mediante los canales de difusión masiva oficiales, a las Jefaturas para lleven a cabo lo indicado en el ítem 11.5.122.

11.6.10. Velar porque los funcionarios participen activamente en el proceso de capacitación dispuesto por las Autoridades Superiores.

11.6.11. 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.

11.6.12. Establecer lineamientos para la correcta gestión de actualizaciones para garantizar que todos los sistemas y aplicaciones estén actualizados.

11.6.13. Vigilar porque el *software* antivirus se encuentre debidamente configurado y actualizado, así como, una solución antimalware en todos los dispositivos, buscando siempre una mejora continua.

11.6.14. 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.

11.6.15. Acatar lo indicado en los ítems 11.2, 11.3, 11.4, 11.5, 11.7, 11.8, 11.9, 11.10, 11.11, 11.12, 11.13, 11.14, 11.15, 11.16, 11.17, 11.18 y 12, según corresponda.

11.7 Autoridades superiores

11.7.1. 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.

11.7.2. 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.

11.7.3. Concientizar al personal del ministerio en el uso **obligatorio** de este manual al realizar sus labores diarias.

11.7.4. Gestionar alianzas con empresas privadas o del sector gobierno en la búsqueda de capacitación para el personal del ministerio.

11.7.5. Establecer política enfocada a la capacitación, aprendizaje de destrezas, relacionada con temas relevantes de nuestra actualidad, tales como Ciberseguridad, resguardo de la información, 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 WiFi públicas y como protegerse, entre otros.

11.7.6. Concientizar al personal del ministerio en la participación activa en el proceso de capacitación.

11.7.7. Buscar la creación de alianzas y/o convenios con instituciones públicas y privadas para recibir la capacitación requerida.

11.7.8. 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.

11.7.9. Acatar lo indicado en los ítems 11.2, 11.3, 11.4, 11.5, 11.6,11.8, 11.9, 11.10, 11.11, 11.12, 11.13, 11.14, 11.15, 11.16, 11.17, 11.18 y 12, según corresponda.

11.8 Relacionados a instalaciones/desinstalaciones de software

11.8.1. 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.

11.8.2. Todo *software* que no cuente con la licencia respectiva será removido del equipo inmediatamente sin previo aviso.

11.8.3. Se prohíbe la instalación de *software* no autorizado por la DST o bien que no cuente con su respectiva licencia.

11.8.4. 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 a las funciones institucionales.

11.8.5. 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

11.8.6. Únicamente el personal del DST de la DIG está facultado para la instalación y/o desinstalación de *software* que no cuente con una licencia.

11.8.7. 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."*

11.8.8. 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.

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.

11.8.9. 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".

11.8.10. 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.

11.9 A la atención de solicitudes de Recursos Informáticos

11.9.1. Remitir a las cuentas de correo electrónico (basededatos@mep.go.cr, secretariasistemas@mep.go.cr y 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).

11.9.2. 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.

11.9.3. 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. 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.

11.9.4. 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 conexa, 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.

11.9.5. 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.

11.9.6. 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.

11.9.7. 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).

11.9.8. 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.

11.9.9. 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.

11.10 Manejo de cuentas de usuario y contraseñas de acceso

11.10.1. 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.

11.10.2. Es terminantemente prohibido el uso de cuentas y contraseñas de otros usuarios.

11.10.3. El uso de la contraseña es personal, confidencial e intransferible (a otros usuarios y/o su jefatura).

11.10.4. No debe almacenar las contraseñas en agendas, libretas, *post-it*, entre otros.

11.10.5. 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.

11.10.6. 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 esta queda bajo la responsabilidad del usuario, así como el uso correcto.

11.10.7. El usuario debe acatar las características establecidas por la DIG para el establecimiento de contraseñas robustas y seguras. El resguardo de esta queda bajo la responsabilidad del usuario, así como el uso correcto.

11.10.8. Se recomienda que la contraseña sea robusta y segura. Que cumpla con las siguientes características: longitud de 10 a 30 caracteres, combinar de letras mayúsculas, minúsculas, caracteres especiales y al menos un número.

11.10.9. 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).

11.10.10. 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.

11.10.11. **Es obligatorio** el uso del doble factor de autenticación (MFA), para aplicar una capa adicional al acceso debidamente definido por la DIG.

11.11 Respaldo de datos

11.11.1. 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 del computador, 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 de eléctrico. Utilizando para ello cualquier medio de almacenamiento masivo con que se cuente, por ejemplo, dispositivos USB.

11.11.2. Queda bajo la responsabilidad del usuario, el almacenamiento de la información institucional en la nube (*Dropbox*, *Onedrive* personal,

GoogleDocs 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.

11.11.3. No se deben almacenar en las carpetas compartidas, *OneDrive* empresarial 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 la DIG si se determina con un informe técnico/auditoría y/o denuncia que respalde tal accionar.

11.11.4. 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.

11.11.5. Se prohíbe el uso de dispositivos que permiten el acceso a Internet en las computadoras institucionales, cuando este en cualquier dependencia ministerial conectado a la red institucional.

11.11.6. No conectar en los puertos *USB* del equipo institucional, dispositivos de almacenamiento *USB*. Y en caso de hacerlo, retirarlo del equipo mediante la opción "Quitar *hardware* de forma segura y expulsar el medio".

11.11.7. 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.

11.12 Uso de servicios en red

11.12.1. 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.

11.13 Uso de telefonía IP

11.13.1. 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.

11.13.2. 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.

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

11.13.4. 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.

11.13.5. Se autoriza la instalación de este servicio en computadoras personales, siempre y cuando sea el equipo destinado para realizar las labores de teletrabajo.

Cabe indicar que los funcionarios del DST no brindan soporte en las computadoras personales, por lo que la instalación debe ser asumida por el funcionario, siguiendo la guía de instalación suministrada por la DIG.

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 planteando la solicitud.

11.13.6. Se **prohíbe** la instalación de los aplicativos de la telefonía IP en dispositivos móviles como celulares y tabletas.

11.13.7. 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.

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

11.14 Permisos especiales a servicios institucionales

11.14.1. En casos especiales, corresponderá a la DIG 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, funcionarios 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.

11.15 Uso del correo electrónico

11.15.1. Cada funcionario será responsable del uso adecuado de su cuenta de correo electrónico y de la información que remita.

11.15.2. La DIG sólo brindará ayuda y soporte a las cuentas @mep.go.cr

11.15.3. Los servicios de correo electrónico y accesos a Internet son puestos a disposición de los funcionarios para asuntos **estrictamente** laborales.

11.15.4. Para la utilización de programas de mensajería y chat para fines laborales, debe utilizarse *Microsoft Teams* con la cuenta oficial del MEP.

11.15.5. **Es obligatorio** el uso del doble factor de autenticación (MFA), para aplicar una capa adicional al acceso debidamente definido por la DIG.

11.15.6. 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.

11.15.7. Si el funcionario se siente ofendido por un mensaje de correo electrónico que recibió, favor de reenviarlo a su jefatura inmediata para lo correspondiente.

11.15.8. 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.

11.15.9. 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.

11.15.10. Si se desea mantener un mensaje en forma permanente, este se debe almacenar en una carpeta personal en el equipo del usuario.

11.15.11. 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.

11.15.12. 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.

11.15.13. 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.

11.15.14. 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.

11.16 Uso de mensajes de correo electrónico masivos

11.16.1. 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.

11.16.2. 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.

11.16.3. 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.

11.16.4. 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.

11.16.5. Si se desea mantener un mensaje en forma permanente, este se debe almacenar en una carpeta personal en el equipo del usuario.

11.16.6. 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.

11.16.7. 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.

11.16.8. 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.

11.17 Uso del equipo arrendado (Computadoras e impresoras)

11.17.1. 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 de equipo de cómputo e impresión de la DIG.

11.17.2. Para la consulta en la tramitología, procedimientos vigentes de los equipos arrendados por los contratos de la DIG, pueden solicitarse a los siguientes correos arrendamientoecdig@mep.go.cr / arrendamientoimpresora@mep.go.cr / arrendamiento.control.activos@mep.go.cr

11.18 Uso de la firma digital

11.18.1. El usuario es responsable de establecer y resguardar el PIN de acceso de la firma digital.

11.18.2. El PIN de la firma digital es personal, confidencial e intransferible (a otros usuarios, jefatura y/o colaboradores).

11.18.3. Es **terminantemente prohibido** el uso de firmas digitales de otros usuarios.

11.18.4. No debe almacenar el PIN de la firma digital en agendas, libretas, *post-it*, entre otros.

11.18.5. Retirar la firma digital del lector en caso de abandonar temporalmente su espacio laboral.

11.18.6. Al retirar la firma digital del puerto USB del equipo institucional, debe emplearse la opción "Quitar *hardware* de forma segura y expulsar el medio".

11.18.7. 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.

11.18.8. En caso de olvidar el PIN, deberá presentarse en la institución emisora que le brindó la firma digital para cambiarla.

11.18.9. Ser consciente que cada acción firmada con la firma digital no es repudiable.

12 RECOMENDACIONES EMANADAS POR LA OFICINA DE CIBERSEGURIDAD

12.1. 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.

12.2. 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". Se recomienda a la DIG inhabilitar los puertos USB.

12.3. 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.

12.4. 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, Nº 8968.

12.5. Concientizar a los funcionarios con charlas, **videos**, circulares para educarlos sobre cómo detectar correos electrónicos sospechosos, spam y phishing.

12.6. Se recomienda a la oficina de Ciberseguridad 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.

12.7. 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.

12.8. 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.

13 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 Nº 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 emitidas por el MICITT aplicándolas de manera parcial o total en este documento.
- Así como cualquier otra normativa vigente relacionada.

14 ANEXOS:

No cuenta con anexos.

15 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 Dpto. Base de Datos y Seguridad	JENNY MARIA NAVARRO BLANCO (FIRMA) Firmado digitalmente por JENNY MARIA NAVARRO BLANCO (FIRMA) Fecha: 2024.11.27 12:11:23 -06'00'
José Martín Sanchún Macín Dpto. de Control y Gestion Informático	JOSE MARTIN SANCHUN MACIN (FIRMA) Firmado digitalmente por JOSE MARTIN SANCHUN MACIN (FIRMA) Fecha: 2024.11.27 11:25:25 -06'00'
Alban A. Garcia Vargas Dpto. Sistemas de Información	ALBAN ANTONIO GARCIA VARGAS (FIRMA) Firmado digitalmente por ALBAN ANTONIO GARCIA VARGAS (FIRMA) Fecha: 2024.11.27 13:15:43 -06'00'
Juan Carlos Rodríguez Oficina de Ciberseguridad	JUAN CARLOS RODRIGUEZ VALERIO (FIRMA) Firmado digitalmente por JUAN CARLOS RODRIGUEZ VALERIO (FIRMA) Fecha: 2024.11.27 13:22:53 -06'00'
Daniel Josué Delgado Oficina de Ciberseguridad	DANIEL JOSUE DELGADO LEANDRO (FIRMA) Firmado digitalmente por DANIEL JOSUE DELGADO LEANDRO (FIRMA) Fecha: 2024.11.27 14:02:02 -06'00'
Marlon Vásquez Vásquez Dpto. de Soporte Técnico	MARLON ALEXANDER VASQUEZ VASQUEZ (FIRMA) Firmado digitalmente por MARLON ALEXANDER VASQUEZ VASQUEZ (FIRMA) Fecha: 2024.12.02 07:39:04 -06'00'
Rebeca Granados Vargas Dpto. de Redes y Telecomunicaciones	PAULA REBECA GRANADOS VARGAS (FIRMA) Firmado digitalmente por PAULA REBECA GRANADOS VARGAS (FIRMA) Fecha: 2024.11.27 12:19:54 -06'00'

Noviembre, 2024

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
Dpto. de Base de datos y Seguridad

IVAN LEONEL ROJAS ALVAREZ (FIRMA)
Firmado digitalmente por IVAN LEONEL ROJAS ALVAREZ (FIRMA)
Fecha: 2024.12.02 12:14:11 -06'00'

Lic. Berny Salazar Rojas
Dpto. de Redes y Telecomunicaciones

BERNI SALAZAR ROJAS (FIRMA)
Firmado digitalmente por BERNI SALAZAR ROJAS (FIRMA)
Fecha: 2024.12.05 13:30:28 -06'00'

Lic. John Mehlbaum Ucanan
Dpto. de Soporte Técnico

JOHN MEHLBAUM UCAÑAN (FIRMA)
Firmado digitalmente por JOHN MEHLBAUM UCAÑAN (FIRMA)
Motivo: Estoy aprobando este documento
Ubicación: DIG, Departamento de Soporte Técnico, Jefe de Soporte Técnico, cédula 1-587-536
Fecha: 2024.12.11 09:39:57 -06'00'

Licda. Kattia Paniagua Alfaro
Dpto. de Gestión y Control Informático

KATTIA MARCELA PANIAGUA ALFARO (FIRMA)
Firmado digitalmente por KATTIA MARCELA PANIAGUA ALFARO (FIRMA)
Fecha: 2024.12.11 09:37:46 -06'00'

Lic. Randy Valverde Valverde
Dpto. de Sistemas de Información

RANDY ALEXANDER VALVERDE VALVERDE (FIRMA)
Firmado digitalmente por RANDY ALEXANDER VALVERDE VALVERDE (FIRMA)
Motivo: He revisado este documento
Ubicación: Jefe, Depto de Sistemas de Información. MEP. Randy Valverde Valverde, Ced: 1-1143-0122
Fecha: 2024.12.11 10:11:13 -06'00'

Noviembre, 2024

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

GABRIEL ANTONIO DENIS DENIS (FIRMA)
Firmado digitalmente por GABRIEL ANTONIO DENIS DENIS (FIRMA)
Fecha: 2024.12.12 10:02:43 -06'00'

Esteban Arroyo Pacheco
Director de Informática de Gestión

ESTEBAN ARROYO PACHECO (FIRMA)
Digitally signed by ESTEBAN ARROYO PACHECO (FIRMA)
Reason: Visado
Location: Lic Esteban arroyo Pacheco ced 109080209
Date: 2024.12.13 09:28:09 -06'00'

Noviembre, 2024