



# POLITICAS Y NORMAS GENERALES DE TI

UNIDAD DE INFORMATICA-2022



Ministerio de  
**Agricultura y  
Ganadería**  
DE COSTA RICA



Contenido

Presentación..... 2

Marco Jurídico..... 3

    Ámbito de aplicación..... 3

    Actualizaciones de este manual ..... 3

Marco Filosófico..... 4

    Del establecimiento de políticas ..... 4

    Objetivos ..... 4

        Objetivo General ..... 4

        Objetivos Específicos..... 4

    Supervisión de políticas..... 5

    Violación a las políticas ..... 5

    Generalidades ..... 5

Definición de Políticas ..... 7

    Normas de aplicación General ..... 7

        Marco estratégico de TI ..... 7

        Gestión de la Calidad..... 7

        Gestión de Riesgos de TI ..... 8

        Gestión de la Seguridad en TI..... 8

        Consideraciones generales de la implementación de las Tecnologías de Información..... 25

Implementación de las Tecnologías de Información ..... 27

Prestación de servicios y ..... 29



## Presentación

---

Para el Ministerio de Agricultura y Ganadería, es importante disponer y poner al servicio del Sector Agropecuario novedosas herramientas tecnológicas, que le permita cumplir con mayor eficiencia, las funciones que le corresponde.

La Unidad Informática en su rol como director de las actividades de tecnología de la información y comunicación, propicia el mejoramiento de los procesos técnicos y administrativos de la Institución, en beneficio de los usuarios del Ministerio, productores agropecuarios y de la ciudadanía en general que hace uso de los servicios, y por medio de este documento presenta, las normas y políticas institucionales en materia de TI que deben seguirse para propiciar un mejor aseguramiento de los activos que pertenecen al MAG tanto físicos como lógicos y un mejor aseguramiento y disponibilidad de los servicios que presta.



## Marco Jurídico

---

La Contraloría General de la República ha emitido leyes y normativas para el control y la administración en materia de tecnologías de información y comunicación, así como la Ley General de Control Interno y otras normativas relacionadas sobre este tema.

Para este caso el Ministerio de Ciencia, Innovación, Tecnologías y Comunicaciones (MICITT), emitió el 11 de noviembre del 2021, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, normas que llegan a sustituir las implementadas por la Contraloría General de la República en el 2007.

Esta nueva versión emitida por el MICITT, en todas las instituciones del Estado debe existir manuales de políticas internas relativas a la administración de Tecnologías de Información; por lo que, para su cumplimiento, se definen en este documento las políticas que, en esta materia, deben aplicarse para el Ministerio de Agricultura y Ganadería.

### Ámbito de aplicación

Las políticas definidas en este documento son de aplicación para todo el Ministerio, incluyendo las direcciones nacionales, regionales y todas las organizaciones adscritas al MAG, cuyas actividades se apoyan en instrumentos informáticos.

### Actualizaciones de este manual

Este instrumento rige una vez que el jerarca institucional lo apruebe y haya ordenado su puesta en marcha a través de una directriz ministerial. Deberá ser revisado y actualizado formalmente por lo menos una vez cada año, siendo responsabilidad de la jefatura de la instancia administrativa de Tecnologías de Información, en adelante denominado Unidad de Informática, realizar este proceso.

Durante el proceso de implementación cualquier usuario podrá hacer observaciones, con el objetivo de mejorar y/o modificar cláusulas o políticas, las cuales se harán llegar a la jefatura de la Unidad de Informática.



## Marco Filosófico

---

### Del establecimiento de políticas

El término política se define como la guía o principios generales, con que se conduce un asunto o se emplean los medios para alcanzar un fin. De esta manera, las políticas se pueden entender como las orientaciones o directrices que rigen la actuación de una persona o una entidad en un asunto o campo determinado.

El Ministerio de Agricultura y Ganadería define periódicamente el conjunto de políticas generales y normas para la Institución, por lo que las políticas que se definen en este documento pasan a formar parte de este conjunto, como complemento para orientar las actividades apoyadas en tecnologías de información.

### Objetivos

#### Objetivo General

Mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, que son propiedad o se encuentran a disposición del Ministerio de Agricultura y Ganadería, para alcanzar la misión institucional.

#### Objetivos Específicos

1. Utilizar los recursos tecnológicos de información y comunicación en forma responsable y apropiada, de conformidad con las disposiciones dadas en este manual y otras de carácter institucional, legal o emitido por otros órganos del Estado Costarricense, que guarden relación con normativas aplicables a la materia.
2. Minimizar las interrupciones de los servicios asociadas a los sistemas informáticos y comunicaciones, ocasionados por uso inapropiado o por daños causados en forma accidental o intencional.



## Supervisión de políticas

La supervisión del cumplimiento de las “Políticas Generales sobre Tecnologías de Información”, queda a cargo de la Unidad de Informática; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estas políticas y las normativas vigentes en materias de tecnologías de información y comunicación.

## Violación a las políticas

La infracción o incumplimiento de las políticas sobre tecnologías de información y comunicación, será notificado a la Unidad Administrativa correspondiente a fin de que ésta proceda según corresponda. Durante el proceso de implementación se estará revisando el tema de cumplimiento y sanción con el Departamento de Recursos Humanos.

Este documento se estará revisando y/o actualizando por parte de la instancia administrativa de tecnologías de información en la Sede Central, con la finalidad de estarlo mejorando. Estas modificaciones serán comunicadas a través del Despacho Ministerial con apoyo del departamento de Prensa.

## Generalidades

- La Unidad de Informática no será responsable de ningún recurso o servicio informático que esté por fuera de los parámetros establecidos en las políticas establecidas.
- Cada funcionario del Ministerio tendrá asignado máximo un (1) equipo de cómputo para el desarrollo de sus funciones, cualquier excepción a lo anterior deber ser aprobado formalmente y por escrito por la Dirección Administrativa y Financiera y la Unidad de Informática.
- Toda adquisición, donación o proyecto que se realice en el Ministerio comprenda un bien o servicio tecnológico debe contar con la aprobación formal de la Unidad de informática, el cual es el único de manera que le permita dimensionar el impacto o afectación en los servicios actuales como internet, servicios en nube, telefonía IP, impresión.
- La Unidad de Informática, en compañía de Auditoría, tendrán la potestad de realizar revisiones periódicas con el fin verificar el cumplimiento de las presentes políticas, además de reportar a Gestión Institucional de Recursos Humanos cualquier anomalía detectada para su valoración y eventual sanción por incumplimiento
- Toda solicitud de servicio debe estar soportada por una solicitud a del sistema de soporte técnico oficial, tal y como se establece ~~se indica~~ en el procedimiento llamado



**“6P02-02 Solicitud de Servicios en Tecnologías de Información”**, del sistema de Gestión de la Calidad Institucional.

- Los recursos y servicios informáticos que provee el ministerio en materia de TI son para uso exclusivo de actividades propias de la institución y para el desarrollo de las funciones propias de cada funcionario.
- Se prohíbe el uso del equipo Institucional por personas externas a la institución (hijos, cónyuges, familiares, etc.) y para funciones ajenas a las labores propias de los funcionarios, cuando se determine que el equipo es usado por otras personas o para otras funciones, se reportara a Gestión Institucional de Recursos Humanos cualquier anomalía detectada para su valoración y eventual sanción por incumplimiento.
- Cualquier situación no prevista en las presentes políticas será resuelta por la Unidad de Informática del MAG.
- En ninguna circunstancia se instalarán licencias propiedad del Ministerio de Agricultura y Ganadería en equipos personales (por ejemplo, Windows, Office, Antivirus, otros).



## Definición de Políticas

---

### Normas de aplicación General

#### Marco estratégico de TI

1. La Unidad de informática (UI), será la encargada de ejecutar los procesos de planeación, coordinación, ejecución y supervisión estratégica de los proyectos e inversiones en materia de Tecnología de Información y Comunicación a nivel institucional. Para ello tendrá una dependencia jerárquica adecuada a este propósito, que en el caso de la Sede Central la tendrá con el Despacho del/la Oficialía Mayor, quien cuidará de este tema a nivel institucional.
2. Las políticas de tecnologías de información serán aprobadas por el jerarca del Ministerio y divulgadas adecuadamente a través de los/las directores(as) nacionales, regionales y sitios web institucionales.
3. El jerarca liderará el proceso continuo de promulgación y divulgación de las presentes políticas y la inclusión de estas como materia obligada en los procesos de inducción a los nuevos funcionarios de la institución.
4. La Unidad de Informática se encargará de la ejecución y actualización del Plan Estratégico en Tecnologías de Información y Comunicación (PETIC), del cual deriva el Plan Anual Estratégico con el cual se orientarán las actividades de la Unidad.
5. Todo proyecto en materia de TI deberá ser desarrollado bajo la metodología de Administración y control de los proyectos de TI, utilizada en dicho Departamento.

#### Gestión de la Calidad

##### *Políticas de la calidad de los servicios y proyectos de TI*

1. La Unidad de Informática elaborará y divulgará el catálogo de servicios de la UI, el cual deberá oficializar y divulgar a los funcionarios del Ministerio.
2. Cada vez que un funcionario requiera un servicio por parte de la Unidad de Informática no solo debe crear la solicitud en el Sistema de Soporte Técnico, vía web; sino que además debe concluir la boleta e indicar si quedó o no conforme con el servicio técnico recibido, tomando en cuenta su solución, tiempo empleado y procedimiento ejecutado. Esta información será utilizada por la Unidad de Informática, para la toma de decisiones que ayuden al mejoramiento continuo de los servicios brindados.
3. La Unidad de Informática elaborará e implementará un proceso para la gestión y aseguramiento de la calidad de las TI el cual permita que los servicios sean brindados con resultados satisfactorios.
4. Las jefaturas departamentales deben solicitar formalmente el desarrollo de un proyecto de TI, mediante la metodología establecida y participar activamente en el desarrollo y prueba de las soluciones tecnológicas. Según lo establecido en el procedimiento **“6P02-02 Solicitud de Servicios en Tecnologías de Información”**, del sistema de Gestión de la Calidad Institucional.



## Gestión de Riesgos de TI

### *Política de evaluación del riesgo*

1. La Unidad de Informática será el encargado de definir el proceso de gestión de riesgos en materia de TI y de mantener actualizado dicho proceso. Así como alimentar el Sistema de Valoración del Riesgo Institucional con los riesgos identificados al menos una vez al año.

## Gestión de la Seguridad en TI

### *Marco de la seguridad de la información*

#### *Políticas de seguridad de la Información*

2. El/la jerarca institucional será el encargado de oficializar y divulgar el marco de seguridad de la información que incluyan las directrices sobre seguridad y utilización de las tecnologías de información y comunicaciones elaboradas por la Unidad de informática. El Marco de seguridad será un proceso incluido durante las inducciones a los nuevos funcionarios y que la violación comprobada a las normas establecidas se pueda tipificar como falta leve o grave según sea el caso, y se imponga la sanción disciplinaria correspondiente.
3. La Unidad de Informática será el responsable de mantener actualizado el marco de seguridad de la información y velar porque se cumpla a nivel institucional.

### *Compromiso del personal con la seguridad de la información*

#### *Políticas de uso de recursos y servicios informáticos*

La Unidad de Informática es la dependencia encargada de establecer los lineamientos necesarios para el uso de los recursos y servicios informáticos.

#### *Software*

##### *Responsabilidades de los usuarios:*

1. Toda persona que haga uso de los equipos de cómputo del MAG utilizará los programas de software solo en virtud de los acuerdos establecidos por los términos de licenciamiento y será responsable por el uso correcto de este.
2. Toda persona que se entere de cualquier uso indebido o no autorizado de software o la documentación vinculada a estos, deberán comunicarlo a la Unidad de Informática.
3. El software, siempre, deberá ajustarse a los términos de uso y licenciamiento establecidos por el fabricante, incluidas las versiones de prueba.
4. Toda persona que requiera el uso de una licencia de software deberá realizar la solicitud de manera anticipada ante la Unidad de Informática a través del sistema de soporte técnico.

##### *Restricciones de los usuarios*

1. Está prohibido hacer uso de cualquier software no autorizado por la Unidad de Informática en los computadores y servidores de la institución.



2. Está prohibido realizar la instalación de software en los equipos de cómputo del MAG por parte de personal diferente a la Unidad de Informática.
3. Solo está autorizado el uso de software de terceros, siempre y cuando, previamente se realice el proceso de licenciamiento respectivo a cargo de la Dirección de Informática.
4. No está autorizada la reproducción de programas de software y la documentación vinculada a éste, excepto con fines de respaldo.
5. Ningún funcionario, estudiante, o contratista podrá realizar instalaciones, desinstalaciones, renovaciones o actualizaciones de software por ningún medio (Internet, CD, USB, entre otros) en los equipos de cómputo de la institución. La unidad de Informática es la única dependencia del Ministerio autorizada para instalar, renovar o actualizar programas de software.
6. Ningún funcionario, contratista o estudiante podrá tener usuario con perfil administrador que le permita realizar instalaciones de software, a menos que tenga una excepción explícitamente aprobada por la Unidad Informática.
7. Ninguna persona externa al Ministerio sin previa autorización de la Unidad de Informática podrá realizar la instalación, desinstalación formateo, revisión o cambio de componentes de equipos institucionales

#### *Políticas sobre inventario de software*

1. La Unidad de Informática deberá mantener un inventario de software y programas instalados en cada una de las computadoras. Este inventario deberá revisarse y actualizarse dos veces al año. Ver políticas para instalación de software.
2. La Unidad de Informática, es la dependencia designada por el jerarca institucional, para que confeccione un informe anual de inventario de los programas instalados en los equipos, el cual debe hacerlo llegar al Registro Nacional de Derechos de Autor y Derechos Conexos a efectos de hacer constar que el Ministerio cumple con la protección de los derechos de autor relativos a los programas de cómputo, en observancia al Decreto de Legalización de Software en el Gobierno Central, número 3015-J.

#### *Monitoreo de licenciamiento*

La Unidad de Informática en compañía de la Unidad de Auditoría, realizará revisiones periódicas a las diferentes dependencias con el fin de identificar el correcto licenciamiento de las instalaciones de software en los equipos de cómputo de la Institución. Si se encuentran copias de software sin licencia, estas serán desinstaladas y el incidente reportado a nombre del usuario responsable por el equipo de cómputo relacionado.

#### *Competencias de la Unidad de Informática sobre el software*

1. Cualquier duda referente a los términos de licenciamiento o legalidad de un software puede consultarse con la jefatura de la Unidad de Informática.
2. Las licencias de software estarán bajo el dominio y custodia del Departamento de Servicios de TI de la Dirección de Informática. No se hará entrega o copia de los medios físicos o medios digitales de las licencias a los usuarios.



3. La Unidad de Informática, estará en la facultad de desinstalar o desactivar las licencias que hayan caducado, ya sea porque finalizó el periodo de licenciamiento asignado y no fue aprobada su prórroga de uso, o porque sus características no se ajustan a las necesidades o requerimientos de la institución, o por cualquier otra situación que impida su instalación o uso.
4. La Unidad de Informática, definirá teniendo en cuenta las necesidades Institucionales, la infraestructura de TI, el presupuesto y las condiciones de licenciamiento, cuál es la versión del software requerido que será utilizado en Ministerio para fines comunicación, ofimática, capacitación, protección.

### Equipos de cómputo y periféricos

#### *Responsabilidades de los usuarios*

1. Los funcionarios del MAG usarán el equipo de cómputo en labores exclusivamente de trabajo y serán responsables por el uso adecuado de las herramientas de hardware (tales como el PC, impresoras, escáner, medios de almacenamiento como discos externos, tabletas, portátiles, llaves "maya" USB, otros) y el software (programas) instalado.
2. El usuario tendrá la responsabilidad de informar y entregar a la Unidad de Informática de forma expedita los recursos y servicios informáticos que no estén siendo utilizados.
3. En caso de robo o hurto de cualquier recurso informático, es responsabilidad del usuario proceder trámite de denuncia ante el Organismo de Investigación Judicial y la copia de la denuncia deberá entregarla a la Unidad de Informática; la cual debe incorporar la marca, modelo, serie y placa del recurso informático, de lo contrario se procederá a iniciar el proceso disciplinario correspondiente.
4. Es prohibido a todo el personal de cualquier nivel, utilizar el equipo de la oficina para descargar de internet y/o ejecutar: juegos, música, videos, fotos, "screensavers" y todo archivo que provenga de fuentes no confiables; así como todo tipo de material pornográfico, que atente contra el trabajo o el honor de las personas.
5. Todo computador del Ministerio en su sede Central y direcciones Regionales debe estar registrado dentro del dominio MAG y configurado con su respectivo usuario.
6. Ningún funcionario del MAG deberá utilizar los equipos de otros sin la debida autorización de la persona responsable del bien y además no podrá hacer uso de equipos con usuarios de otros funcionarios, debe de utilizar el usuario de dominio que se le haya asignado.
7. Se prohíbe ingerir cualquier tipo de alimento o bebida cerca de los equipos, por lo que las jefaturas o coordinadores de cada departamento deben velar que esta disposición sea acatada.
8. Se prohíbe colocar cerca o sobre los equipos, artículos que perjudiquen el funcionamiento correcto de estos (líquidos, alcohol, plantas, peceras, imanes, entre otros)
9. No se debe evitar ubicar equipos de cómputo cerca de ventanas, debido a la posibilidad de que sufran daños en caso de que ocurra un terremoto o algún evento que produzca que éstas caigan sobre los equipos; además para evitar acciones de robo por ser fácilmente visibles y alcanzables.
10. Los equipos de cómputo deben mantenerse anclados o asegurados con cables de acero al escritorio para evitar acciones de robo, cada Agencia, Región o Departamento deberá



- coordinar con el área de Almacén y Distribución de la Proveduría Institucional para que realicen la perforación de los escritorios que permitan la colocación del candado o cable de acero.
11. Se prohíbe adherir sticker o adhesivos a los equipos a todos los equipos del Ministerio o arrendados.
  12. Los funcionarios deben velar porque su equipo de cómputo tenga la debida protección contra fallas en el suministro eléctrico. Para ello La Unidad de Informática contará con la información actualizada del parque computacional, en el caso de que se requiera de UPS, el Departamento que lo requiera le solicita a la jefatura de la UI la compra o alquiler de los dispositivos de seguridad.
  13. Los equipos de los usuarios deben apagarse y desconectarse durante tormentas eléctricas para evitar los daños que pueden ocasionar los rayos o las variaciones en el voltaje de la corriente eléctrica. También deben desconectarse durante los fines de semana o periodos no laborales prolongados.
  14. Se debe evitar colocar equipos en áreas de alto tráfico de personas, en sitios en donde puedan ser fácilmente accedidos, en lugares donde no puedan ser vigilados o que puedan sufrir daños por factores ambientales.
  15. Los equipos de cómputo (tabletas, portátiles, CPU) deben contar con el antivirus oficial del MAG. El antivirus debe estar debidamente actualizado por lo que, si éste presenta problemas de actualización o el equipo no dispone de antivirus, el usuario deberá notificarlo a la Unidad de Informática por medio del sistema de soporte.
  16. Está prohibido conectar cualquier dispositivo de red (switch, router) a la red institucional sin la autorización correspondiente de la Unidad de Informática, si se requiere la instalación de alguno de ellos, el servicio deberá ser solicitado mediante el sistema de soporte técnico.

#### *Políticas para uso de impresoras en red*

1. El usuario que requiere utilizar las impresoras en red disponibles en el edificio Central deberá hacer la solicitud respectiva en la Unidad de Informática.
2. La Unidad de Informática, le asignará una contraseña de acceso a las impresoras al cada funcionario, por lo que queda bajo responsabilidad del usuario mantener bajo seguridad dicho acceso.
3. Queda prohibido la impresión de archivos personales, ni de terceras personas.
4. La Unidad de Informática mensualmente hará entrega vía correo a las jefaturas Departamentales el informe de impresión de sus funcionarios, para que se tomen las medidas respectivas.

#### *Políticas de responsabilidad y mantenimiento del hardware*

1. El hardware que se encuentra en el área de servidores y los gabinetes de comunicaciones es responsabilidad directa del personal del área de infraestructura de la Unidad de Informática, y velaran uso apropiado y cuidado.
2. Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de



- reportarlo inmediatamente a través del sistema de soporte a la Unidad de Informática para que se proceda a su revisión.
3. Los usuarios tienen el deber de informar sobre el rendimiento de cada equipo, para que sea valorado y de ser necesario mejorado.
  4. Las computadoras, impresoras y otros dispositivos del MAG serán sometidos a un mantenimiento preventivo por lo menos una vez al año (salvo aquellas que se encuentren en garantía), con la finalidad de aumentar su vida útil, mejorar el rendimiento, detectar a tiempo posibles causas de fallas y determinar su necesidad de mejora o reemplazo.
  5. El mantenimiento preventivo del equipo de telecomunicaciones se realizará por lo menos una vez al año, por el encargado de Infraestructura, quien deberá establecer un programa de trabajo y llevar los respectivos controles.
  6. Es responsabilidad de la Unidad de Informática hacer cumplir las garantías respectivas de cada uno de los equipos; para tal razón se deberán respetar los sellos de garantía que vienen adheridos a los equipos, y velar porque el usuario final no los desprenda en caso de que el proveedor utilice ese mecanismo.
  7. Es responsabilidad de la Unidad de Informática valorar la necesidad de sustituir algún equipo cuando ya éste no garantice la funcionalidad y operatividad adecuada.
  8. Solamente se les dará el servicio de soporte técnico a los equipos computacionales que pertenezcan a la institución. Dichos equipos deben poseer el patrimonio respectivo y en el caso de que no cuente con patrimonio deberá presentar la documentación respectiva del Departamento de Bienes y Servicios en la que se compruebe que se encuentra bajo su tutela y que pertenece a la institución.
  9. Los funcionarios que opten por la modalidad de Teletrabajo, si el equipo utilizado es arrendado o propiedad del MAG, se le brindará soporte una vez realizada la solicitud y solamente en las herramientas establecidas por la UI para la realización de labores. La UI no dará soporte aquellos equipos personales, donde se requiera la instalación de software no perteneciente al ministerio. **en ninguna circunstancia se autorizan las reparaciones en las viviendas de la persona teletrabajadora o por terceros ajenos al Ministerio, en caso de que esto suceda se abrirá el proceso disciplinario correspondiente.**

#### *Políticas relacionadas al teletrabajo*

1. Todos los funcionarios que utilicen equipos (portátiles) propiedad del Ministerio de Agricultura y Ganadería (MAG/SFE/SENASA/INTA/CONAC/SEPSA), deben completar el formulario de Solicitud de autorización de salida de equipo Institucional previo al retiro del equipo, ubicado en la dirección XXX de lo contrario el funcionario **NO** podrá retirar el equipo de su centro de trabajo.
2. Así, las características mínimas con cuales debe contar el cómputo personal o Institucional, con el que se compromete la persona teletrabajadora a realizar sus tareas son las siguientes:



- a. Procesador: Intel Core i3, AMD Ryzen 3, similar o superior
  - b. Memoria RAM 8 Gigas
  - c. Disco Duro 250 Gigas con al menos 50 GB libres
  - d. Monitores o pantallas de 14" (pulgadas), es decir no se permiten monitores o pantallas menores a 13 pulgadas
  - e. Cámara Web con resolución de: 720p/30 fps
  - f. Micrófono (puede estar incluido en la webcam, o bien, ser sustituido por un headset)
  - g. Parlantes (puede estar incluido en las portátiles, o bien, ser sustituido por un headset)
  - h. Sistema Operativo Windows 8.1 o superior con su respectiva licencia (se aceptará hasta el 10 de enero de 2023 cuando finaliza el soporte por parte del fabricante, posterior a esa fecha debe contar con Windows 10), macOS Big Sur 11.6 o superior con su respectiva licencia (se aceptará hasta el noviembre de 2023 cuando finaliza el soporte por parte del fabricante, posterior a esa fecha debe contar con al menos macOS Big Sur 11.7), Ubuntu 20.04 LTS.  
<https://computing.cs.cmu.edu/desktop/os-lifecycle>
  - i. Herramientas de Ofimática (Procesador texto (Word), hoja electrónica (Excel), presentaciones (PowerPoint), correo electrónico (Outlook)), con su respectiva licencia o las herramientas de ofimática libres, la institución no brindará licencias de office para equipos personales
  - j. Navegadores web (Internet Explorer, Google Chrome, Edge) en su última versión
  - k. Antivirus activo y con sus actualizaciones al día con licencia si la requiere (la institución no brindara licencias para equipos personales)
  - l. Herramientas de almacenamiento en la nube (OneDrive / Google Drive)
3. Software autorizado para teletrabajo:
    - a. Microsoft Teams / GSuite
    - b. OneDrive / Google Drive
    - c. Acrobat reader y Firma digital
    - d. Configuración del cliente Outlook (MAG/SEPSA/CONAC/INTA/SENASA)
    - e. MicroSIP (MAG/SEPSA/CONAC/INTA)
    - f. Sistemas institucionales WEB
  4. La velocidad mínima de Internet será de **15 Mbps** fijo (hogar), no se permite la conexión por celular en forma permanente.
  5. Debe contar con la herramienta Microsoft Teams (MAG / SEPSA / CONAC / INTA / SENASA) o Gsuite (Google Suite para el SFE) instalada y activa en el equipo de cómputo durante el teletrabajo de manera que permita la comunicación con la persona teletrabajadora
  6. El equipo utilizado por la persona teletrabajadora deberá contar con las herramientas instaladas para el soporte remoto (TeamViewer, asistencia rápida de Microsoft, Microsoft Teams, Chrome Remote Desktop) o cualquier otra herramienta que defina y oficialice cada área de TI. Cuando se acceda al equipo de forma remota, la persona teletrabajadora deberá estar presente en todo momento verificando el accionar el



- funcionario del área de TI, en caso contrario el funcionario del área de TI cerrará la sesión remota.
7. Cuando la Institución le facilite a la persona teletrabajadora un equipo de cómputo para que realice sus funciones y en caso de que se presente algún inconveniente o falla en el equipo, deberá reportarlo por los medios establecidos por cada área de TI y deberá trasladarlo a su centro de trabajo para ser atendido por la empresa contratada o funcionarios de la Institución, **bajo ninguna circunstancia se autorizan las reparaciones en las viviendas de la persona teletrabajadora o por terceros ajenos al Ministerio, en caso que esto suceda se abrirá el proceso disciplinario correspondiente.**
  8. Los equipos personales no recibirán ningún mantenimiento preventivo o soporte correctivo en los componentes físicos del mismo o bien en software de uso personal o no designado para el teletrabajo por parte de las áreas de TI, en caso de falla el funcionario es responsable de su equipo y estará en la obligación de contratar el soporte técnico necesario para la reparación de este, posterior a esa reparación deberá solicitar una nueva valoración por parte del área de TI correspondiente.
  9. En caso de falla del equipo personal o institucional utilizado para el teletrabajo, donde la reparación supere las 8 horas laborales el funcionario deberá retomar sus labores presenciales.
  10. En ninguna circunstancia se instalarán licencias propiedad del Ministerio de Agricultura y Ganadería (comprende Servicio Nacional de Salud Animal, Servicio Fitosanitario del Estado, Instituto Nacional de Tecnología Agropecuaria, Consejo Nacional de Clubes 4S, Secretaría Ejecutiva de Planificación Sectorial Agropecuaria), en equipos personales (por ejemplo, Windows, Office, Antivirus, otros).
  11. Se prohíbe la instalación de programas no autorizados por las áreas de TI o bien la instalación de licencias personales en los equipos Institucionales
  12. Cuando se presente una suspensión de servicios (electricidad o internet) que dificulte la comunicación o las labores de la persona teletrabajadora, deberá notificar de forma inmediata su jefatura para tomar las acciones pertinentes, entre ellas el retorno presencial al centro de trabajo.
  13. Es responsabilidad de todos los funcionarios realizar y mantener un respaldo periódico de la información contenida en los equipos y en la herramienta de almacenamiento en nube (al menos una vez a la semana, en el OneDrive o Google Drive) provisto en su cuenta de correo Institucional.
  14. Se prohíbe el uso del equipo Institucional por personas externas a la institución (hijos, cónyuges, familiares, etc.) y para funciones ajenas a las labores propias de la persona teletrabajadora, cuando se determine que el equipo es usado por otras personas o para otras funciones, el equipo será retirado de forma inmediata.



15. Las áreas de TI no suministran ningún dispositivo periférico (mouse, teclado, parlantes, impresoras, entre otros), a la persona teletrabajadora para ser empleado en el equipo personal o adicional al equipo Institucional.

#### *Políticas sobre inventario de equipos*

1. La Unidad de Informática mantendrá un inventario del parque computacional (hardware) con las características de cada uno de ellos, tanto de la sede central como de las direcciones regionales y sus agencias.  
La Unidad de Informática deberá revisar el inventario del equipo por lo menos dos veces al año, realizando los cambios que sean necesarios. Hará un informe a la Administración sobre las diferencias y/o deficiencias encontradas.

#### *Políticas sobre la reparación de equipos*

1. Todos los usuarios deben acatar el procedimiento que La Unidad de Informática implemente para controlar los servicios de reparación y la calidad de estos.
2. La obtención de fondos presupuestarios para la adquisición de repuestos y accesorios será responsabilidad de la jefatura departamental.
3. La Unidad de Informática tendrá un control de las garantías de los equipos adquiridos para hacer cumplir los compromisos contractuales. Los equipos no cubiertos se procederán a ser reparados en el sitio mismo o en el taller.
4. En lo posible se formalizarán y se dará seguimiento a contratos de reparación y mantenimiento de equipos, alquiler de impresoras y equipos, tanto de la Sede Central del MAG, como de las oficinas regionales. La Unidad de Informática, es el encargado de coordinar la realización efectiva del mantenimiento y evaluar el cumplimiento y la calidad de los servicios brindados por las empresas contratadas.

#### *Información*

##### *Responsabilidades de los usuarios*

1. La unidad de informática le asignará a cada funcionario sus credenciales de acceso a la Plataforma de servicios TI, el cual incluye su usuario de dominio, contraseña y correo institucional.
2. Todo el personal debe mantener las claves de acceso que le hayan asignado en forma confidencial.
3. Cada funcionario/a debe asegurarse de cerrar apropiadamente sesiones abiertas en sistemas internos o aplicaciones externas, sobre todo en sitios accedidos vía internet.
4. **El funcionario será el responsable de realizar los respaldos de su información** (incluido el correo electrónico, nube/onedrive, equipos de Microsoft Teams y cualquier otro medio donde almacene Información) y mantenerlos resguardados en los medios adecuados que les permita una recuperación segura en caso de algún daño al equipo. En caso de las aplicaciones cliente-servidor el responsable de realizar los respaldos será el administrador o encargado de las bases de datos de la Unidad informática.
5. Los funcionarios darán autorización por escrito con la boleta respectiva, al personal de la Unidad de Informática, cada vez que soliciten o se requiera formatear el equipo a su



- cargo, asumiendo la responsabilidad de cualquier pérdida de datos si no cuentan con los respaldos de su información.
6. Para permitir el acceso a usuarios externos sobre los recursos y servicios informáticos de la institución, la jefatura de cada departamento /dirección debe realizar la solicitud de activación e inactivación de una cuenta de usuario para tal fin a la Unidad de Informática a través del sistema de soporte quien evaluará dicha solicitud.
  7. La definición de los parámetro y procedimientos de las contraseñas será responsabilidad de la Unidad de Informática, por lo que todo usuario deberá acatar dichas disposiciones.
  8. El titular del usuario institucional es la única persona autorizada para solicitar cambios de contraseña de su usuario institucional.
  9. Es obligación de cada funcionario realizar el cambio de contraseñas para el ingreso a los sistemas institucionales y correo electrónico cada 3 meses
  10. La Unidad de Informática es la responsable de la seguridad de acceso a los sistemas operativos (SO), sistemas de información (SI), bases de datos (BD), y redes que operen en los equipos de cómputo institucionales.
  11. Las jefaturas deben solicitar formalmente la apertura, modificación o cierre de las cuentas de usuario (acceso a sistemas y herramientas de ofimática, Active Directory o correo electrónico institucional).
  12. El acceso a las computadoras, sistemas de información, impresoras en red, correo electrónico, bases de datos; estará determinado por un usuario y una contraseña que le será dada al usuario en la Unidad de Informática. El funcionario podrá cambiar la contraseña si La Unidad de Informática le permite y capacita para hacerlo.
  13. Las contraseñas de los usuarios deben tener alta o mediana seguridad, no se deben permitir *contraseñas* genéricas. Es responsabilidad de cada usuario resguardar su clave y no facilitársela a terceros por ningún motivo
  14. Una vez finalizada la relación laboral entre el funcionario y el Ministerio, se desactivarán o bloquearán las cuentas de usuario a aquellos funcionarios que no laboren para el Ministerio. Los roles o privilegios se modificarán por solicitud de las jefaturas departamentales o por decisión de la Unidad de Informática si se evidencia un riesgo para la seguridad de la información.
  15. El Departamento de Recursos Humanos deberá notificar a la Unidad de Informática, toda vez que una persona suspenda temporalmente su servicio para el MAG o traslado temporal a otra institución; para realizar las gestiones pertinentes al usuario asignado al funcionario.

*Una vez que se presente ante el Departamento de Recursos Humanos permisos y traslados a otras instituciones (incluyendo órganos adscritos del MAG) por períodos mayores a un mes, la licencia de correo será retirada cumplido el primer mes, en los casos en que se tramiten renuncias, la licencia será retirada 3 días después, ambos tomando como base la fecha en que rige, razones por las cuales cada funcionario será responsable de realizar el respaldo de correo electrónico y los archivos que almacena en la nube (OneDrive) previo a la fecha en que rige el movimiento.*

#### *Políticas de seguridad de bases de datos*

1. Todo acceso a las bases de datos del Ministerio debe contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.



2. La Unidad de Informática velará porque toda base de datos que sea instalada cuente con los controles de seguridad que garanticen la confiabilidad de la información.
3. Las jefaturas departamentales podrán solicitar formalmente el acceso a la información de las bases de datos para los funcionarios a su cargo, indicando el nivel de acceso con el que ingresarán a los sistemas.
4. Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos del Ministerio, con el fin de garantizar su conservación. Queda bajo la responsabilidad del Administrador de la Base de Datos de la Unidad de Informática dichos respaldos.
5. La Unidad de Informática establecerá planes de recuperación de la información de las bases de datos, para garantizar la continuidad del servicio que se presta por medio de los sistemas de información.
6. Las dependencias, “dueñas” de la información, deberán participar junto con la Unidad de Informática, para verificar si la información de los respaldos o la restauración de la base de datos fue exitosa.
7. La Unidad de Informática implementará controles para que todos los respaldos de información de las bases de datos se encuentren almacenados en medios externos.

#### *Políticas de seguridad de acceso a sistemas operativos*

1. La activación y desactivación de usuarios de sistemas operativos estará a cargo del personal técnico de la Unidad de Informática.
2. En la activación de usuarios de sistemas operativos, se crearán identificadores de usuario utilizando el estándar de la letra inicial del nombre seguida del primer apellido. En caso de que se repitan dichos datos, es decir coincidan con 2 o más funcionarios, se utilizará letra inicial del nombre, seguida del primer apellido y letra inicial del segundo apellido.
3. Siempre que los sistemas operativos utilizados lo permitan, deberá controlarse el número de intentos de ingreso fallidos: luego de tres intentos, deberá bloquearse la cuenta del usuario y no permitir su ingreso al sistema. El funcionario deberá comunicarse con la Unidad de Informática, para solicitar el desbloqueo de la cuenta.

#### *Políticas de seguridad de acceso a sistemas de información (SI)*

1. La Unidad de Informática tiene establecidos tres ambientes para los sistemas de información: área de desarrollo y mantenimiento de aplicaciones, pruebas de esta, capacitación a los usuarios y ambiente de producción.
2. El acceso a los programas fuente de los sistemas implementados, es sólo para el personal del Área de Informática, específicamente del personal desarrollador y analista.
3. La activación y desactivación de usuarios de los sistemas de información estará a cargo del personal técnico de la Unidad de Informática.
4. Las jefaturas departamentales son las que deben definir los roles y privilegios que sus funcionarios pueden tener para acceder a determinada aplicación, ya sea un sistema



interno (Por ejemplo, Expediente Personal, Sistema Financiero Contable, otros.) o externo (Certificaciones, SIGAF del Ministerio de Hacienda, otros). La jefatura debe realizar solicitud formal ante la Unidad de Informática para que se apliquen estas asignaciones al personal a cargo.

5. Las jefaturas departamentales deberán solicitar a la UI cualquier cambio en los roles y privilegios de acceso a los Sistemas Internos o Externos (como los del Ministerio de Hacienda), o el cese de privilegios a dichas aplicaciones, tales son los casos de cambio de funciones de la persona traslado a otra oficina, o decisión de suspender el privilegio.
6. En toda transacción que se realice en los sistemas informáticos deberá quedar grabado el nombre del usuario, la fecha y la hora en que se realizó, para pistas de auditoría.

### *Retención de la información*

Las políticas de retención establecidas para los elementos eliminados con posibilidad de recuperarlos para los funcionarios terminan su periodo laboral con la institución, son los siguientes:

1. One Drive: 30 días.
2. Sharepoint Online: 30 días.
3. Correo: 30 días

Cuando se presente ante GIRH permisos y traslados a otras instituciones (incluye órganos adscritos del MAG) por periodos mayores a un mes, la licencia de correo será retirada cumplido el primer mes, en los casos en que se tramiten renuncias, la licencia de correo será retirada 3 días después, ambos tomando como base la fecha en que rige; razones por las cuales cada funcionario será responsable de realizar el respaldo de correo electrónico y los archivos que almacena en la nube (OneDrive) previo a la fecha en que rige el movimiento. Definido en la circular UI-004-2021.

### *Correo electrónico*

El correo electrónico es un medio de comunicación oficial de la institución, administrado y soportado por la Unidad de Informática.

El contenido del correo electrónico se considera confidencial y sólo perderá este carácter en casos de investigaciones administrativas, judiciales o en incidentes relacionados con la seguridad de la información y la ciberseguridad, cumpliendo a cabalidad con el debido tratamiento y la ley costarricense.

### *Responsabilidades de los usuarios*

1. La cuenta de correo electrónico institucional es personal e intransferible.
2. Los correos de la institución sólo se deben utilizar para atender asuntos institucionales.
3. La Unidad de Informática asignará las cuentas de correo de acuerdo con las licencias disponibles. Se asignará con la prioridad establecida por la Administración Superior.
4. Cuando una jefatura requiera la creación de un grupo o lista de distribución, para enviar correos a varios destinatarios a la vez, debe realizar solicitud formal ante la Unidad de Informática, justificando el motivo por el cual lo requiere.



5. Para la utilización del correo institucional fuera del país, el usuario deberá realizar la debida solicitud por medio del sistema de soporte.
6. Para la comunicación oficial del Ministerio debe utilizarse la cuenta de correo institucional.
7. El acceso a los servicios de Internet y correo electrónico estarán disponibles para todos los usuarios del Ministerio, si las condiciones de infraestructura tecnológica y administrativa lo permiten.
8. El uso de los servicios de Internet, correo electrónico y mensajería teams, deberán ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.
9. No está permitido facilitar u ofrecer las cuentas de correo a terceras personas. En este punto también se debe acatar las normas sobre seguridad y confiabilidad de la información
10. Se prohíbe a los funcionarios formar parte de cadenas de mensajes o SPAM, ya que esto contribuye a la saturación de las redes de telecomunicación y facilita la divulgación de su cuenta de correo y la proliferación de virus en la red.
11. Se prohíbe a los funcionarios que tengan acceso al servicio de correo electrónico abrir mensajes de procedencia desconocida.
12. El funcionario que tenga acceso a servicios de correo electrónico institucional debe evitar divulgar su cuenta a personas o entes desconocidos.
13. Ningún equipo que esté designado como servidor debe tener asociada una cuenta de correo electrónica.
14. Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
15. Los funcionarios deben realizar revisiones periódicas de los mensajes almacenados con el fin de no mantener información innecesaria.
16. Las jefaturas deberán notificar a la Unidad de Informática se deba cerrar o inhabilitar una cuenta de correo electrónico.
17. El personal usuario debe atender a los avisos de actualización automática del programa de detección de virus e informar a la Unidad de Informática, cuando la actualización no se realice satisfactoriamente.
18. Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o buscadores (browser) no deberán ser cambiados, excepto por indicaciones de la Unidad de Informática.
19. Está prohibida la utilización abusiva del correo electrónico y de las listas o grupos de distribución incluyendo la realización de prácticas tales como:
  - a. Si se requiere un envío masivo de correo se recomienda usar las listas de distribución o usar el campo de "copia oculta" (Bcc ó Cco) para poner la lista de destinatarios, o bien ponerse en contacto con la Unidad de Informática.
  - b. Actividades comerciales privadas:
    - i. Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.
    - ii. El insulto, la amenaza o la difamación a cualquier persona.



- iii. Suscribirse a periódicos, revistas, semanarios, buscadores de parejas, chats ni a ningún otro tipo de actividades o boletines electrónicos que no sea el estrictamente relacionado con el área profesional de trabajo del funcionario.
  - iv. Descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional del funcionario. La Unidad de Informática procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados.
20. Está prohibido la transmisión y/o, descarga de material obsceno o pornográfico, que contenga amenazas o cualquier tipo de información que atente contra la moral o buenas costumbres.

### Gestión de impresión

La Unidad de Informática será la encargada de gestionar los servicios de impresión de acuerdo con las necesidades indicadas por el departamento /Dirección, definiendo el tipo de impresora requerido y su ubicación.

La Unidad de informática hará monitoreo al uso y consumo de impresión regularmente.

### *Solicitud del servicio de impresión*

1. Toda persona hará uso del servicio de impresión con el usuario asignado. No se asignarán usuarios genéricos.
2. Los traslados de las impresoras a otra área o dependencia deberán solicitarse por medio del sistema de soporte técnico. No está permitido realizar el traslado sin previa autorización.
3. Los documentos que se impriman deben ser de carácter institucional, No podrán imprimir documentos personales, ni a terceras personas en los equipos de la institución.

### *Responsabilidades de los usuarios*

1. Velar porque el servicio de impresión sea utilizado para actividades laborales y uso exclusivo de la institución.
2. Propender por el buen uso de la impresora por parte de otros usuarios y reportar las solicitudes, requerimientos e incidentes correspondientes al servicio de impresión a la Unidad de Informática.
3. Realizar un uso adecuado del papel e imprimir siempre y cuando sea estrictamente necesario.
4. No realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la Unidad de Informática.
5. Limitarse a usar el papel de impresión con las características definidas por la Unidad de Informática.
6. Abstenerse de utilizar impresoras no avaladas por la Unidad de Informática.



## Servicios de Telefonía IP y videoconferencias

La Unidad de Informática es la única dependencia del MAG autorizada para instalar, trasladar, modificar o retirar teléfonos IP o equipos de Videoconferencia.

### *Responsabilidades de los usuarios*

El teléfono IP quedará bajo la responsabilidad del usuario a quien le fue asignado para sus actividades laborales en el MAG.

1. Todos los funcionarios que requieran para el cumplimiento de sus funciones un servicio de telefonía deben de tener asignado un teléfono IP o un Softphone (software en el computador), asignado por el MAG.
2. Toda persona que haga uso de los teléfonos IP o salas de videoconferencia de la institución, utilizará estos solo en virtud de los acuerdos establecidos por los términos de licencia y será responsable por el correcto uso de éste.
3. Las asignaciones de permisos especiales para llamadas, será responsabilidad solamente de la Unidad de Informática, por lo que el usuario que requiera dicho permiso, deberá solicitarlo mediante el sistema de soporte técnico con la debida justificación. Queda a criterio de la Unidad de Informática su aprobación o no.
4. Los teléfonos IP quedan asociados y bajo la responsabilidad del centro de costos del área o departamento, lo que indica que éstos no pueden ser trasladados a otra área o departamento sin previa autorización de la Dirección de Informática. Cada área o departamento debe hacer sus solicitudes de manera independiente.
5. Cuando se requiera la colaboración de la Unidad de Informática en el soporte para la realización de videoconferencias, deberá solicitarse el soporte con dos días de anticipación para realizar las pruebas correspondientes antes de la actividad (equipo, conectividad) ante la jefatura de la UI.

### *Restricciones*

1. Los teléfonos IP y equipos de videoconferencia suministrados por la Unidad de Informática son los únicos que pueden ser usados dentro de la Institución. Ningún otro dispositivo podrá instalarse sin previo consentimiento por parte de la Unidad de Informática.
2. Ningún funcionario está autorizado para retirar, trasladar o modificar estos equipos sin previo consentimiento por parte de la Unidad de Informática.

## Políticas de seguridad de acceso a redes

1. La Unidad de Informática será la responsable de documentar y aplicar los procedimientos para nombrar los equipos dentro del dominio.
2. Los funcionarios, deben reportar a la Unidad de Informática, cuando se le asigna una PC a fin de que el equipo pueda ser identificado correctamente dentro de la red institucional. Para ello utilizarán la Boleta de Traslado de Equipo, diseñada por el área Almacén y Distribución / Proveeduría Institucional o cualquier otro medio documental



establecido para indicar un traslado de equipo. El mismo medio documental será usado por la persona funcionaria para notificar a la Unidad de Informática, si un equipo a su nombre fue reasignado a otro empleado. Esto con el fin de que la Unidad de Informática pueda renombrar los equipos acordes a la persona responsable del activo y mantener actualizado el registro y estatus de los equipos institucionales.

3. La Unidad de Informática, asignará las claves de acceso a los usuarios, además procederá conforme con los procedimientos para la activación y desactivación de usuarios en el servidor de Acceso de dominio (AD).
4. Para otorgarle acceso a las redes de datos, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá enviar la solicitud formal a la UI. Puede solicitarlo a través del Sistema de Soporte Técnico vía internet.
5. Cada jefatura debe notificar a la UI cuándo un(a) usuario (a) debe tener acceso exclusivo o dedicado para un Sistema Externo del Ministerio de Hacienda u otra instancia, a fin de reservar la IP para uso de la persona. De igual forma, la jefatura debe notificar si se da un cambio en la situación laboral que amerita que el uso exclusivo de la dirección IP, sea traslado a otro/a funcionario, se congele o cese el uso exclusivo de la IP reservada.

### ***Seguridad Física y Ambiental***

#### **Políticas para el acceso físico a la Unidad de Informática**

1. Los funcionarios del MAG y personas ajenas a la institución deberán identificarse con su respectivo gafete del MAG o de visitante ante la recepción de la UI, para efectos de solicitar servicios o realizar consultas. Asimismo, podrán ingresar a lo interno de la Unidad siempre que haya un funcionario de la UI que los atienda personalmente.
2. Los funcionarios de la UI deberán portar siempre su identificación institucional.
3. Ningún equipo del MAG será ingresado en la Unidad de Informática, sin tener la debida documentación en papel o en electrónico (solicitud de servicio, boleta de traslado de equipo, otro) mediante el cual se pueda determinar la persona responsable del bien y el motivo por el cual ingresa al Departamento.
4. Toda empresa que requiera realizar labores de mantenimiento en los equipos de la sala de servidores de la Unidad de Informática deberá coordinar con anticipación la visita con el personal de la UI para verificar su disponibilidad.

#### **Políticas de ubicación y ambiente de la Unidad de Informática**

1. Las estaciones de trabajo deben estar dotadas con las condiciones ambientales necesarias para garantizar un entorno físico conveniente para su funcionamiento.
2. El espacio de la Unidad de Informática deberá estar climatizado a una temperatura constante de 23° para garantizar el mejor rendimiento de los componentes electrónicos y alargar la vida útil de los mismos.
3. La puerta de acceso a las áreas de La Unidad de Informática debe estar completamente cerrada para impedir el acceso de personas no autorizadas
4. Todo el cableado eléctrico que sea utilizado en los equipos de la Unidad de Informática deberá ser distribuido correctamente para el centro de datos y servidores. Con sus respectivas cargas de distribución, polarizado y carga eléctrica correcta



5. Para efectos de cableado de datos se utilizarán las normas de cableado que se fundamenten en las mejores prácticas utilizadas en el mercado. Deberá utilizarse para el cableado de red la certificación vigente en el momento que se instalen nuevas conexiones.

#### Políticas para el manejo de desechos de los medios tecnológicos

1. La institución deberá definir y establecer procedimientos para proteger la información en cualquier medio fijo o removible (papel, cintas, discos flexibles, discos duros de la PC o externos, otros), y el manejo y desecho de dichos medios.
2. El MAG procurará la entrega de sus desechos tecnológicos a empresas recicladoras que cumplan con las normativas vigentes de Políticas de Gestión Ambiental Institucional.
3. Cada dispositivo de cómputo que desea desechar de la institución o donarlo, deberá contar con el diagnóstico técnico emitido por la Unidad de Informática.

#### *Continuidad de los servicios de TI*

La UI deberá desarrollar e implementar un Sistema para la continuidad de los servicios de TI (SCS), que permita el registro y la actualización de eventos que afecten los servicios, su solución, su criticidad y su impacto, recursos, escalabilidad, procedimientos de recuperación y responsables.

#### Administración y operación de la plataforma tecnológica

1. El objetivo es mantener la plataforma tecnológica en óptimas condiciones y minimizar el riesgo de fallas.
2. La administración debe establecer y documentar los procedimientos y responsabilidades asociados con la operación de la plataforma y vigilar constantemente la capacidad desempeño y uso, asegurando su correcta operación y manejo de fallas
3. La Unidad de Informática debe identificar requerimientos presentes y futuros y gestionar la adquisición de recursos de TI por contingencias, cargas de trabajo, obsolescencia de la plataforma y tendencias tecnológicas.
4. La UI se encargará de realizar inventario de hardware y software, y realizar las verificaciones correspondientes en forma periódica.
5. El Área de Salud Ocupacional Institucional es la encargada de emitir las recomendaciones para la adquisición de mobiliario ergonómico para uso de los equipos de cómputo en armonía con la salud física del personal que los usa.

#### *Modelo de Arquitectura de Información*

1. Se debe optimizar la integración, uso y estandarización de los sistemas de información. Por lo que el desarrollo de sistemas de información interno o externo de la institución debe estar definido bajo la arquitectura empresarial de información.



2. Las jefaturas interesadas en adquirir un sistema o aplicación deben presentar solicitud formal ante la Unidad de Informática, siguiendo la metodología ya establecida.
3. Las jefaturas departamentales no deben adquirir o implementar sistemas, (ya sea por donación, práctica estudiantil, contrato a terceros), sin la debida aprobación de la Unidad de Informática.
4. Las aplicaciones adquiridas por el MAG deben ser compatible con la plataforma tecnológica institucional (sistemas operativos, sistema de bases de datos, ambiente web, etc.)

#### Políticas para la creación de Base de Datos

1. La Unidad de Informática será la encargada de diseñar física y lógicamente las bases de datos, que utilizarán los sistemas de información que se desarrollen internamente.
2. La Unidad de Informática permitirá la creación de bases de datos a empresas contratadas para este fin o para el desarrollo de sistemas de información, siempre que entreguen, en forma completa, toda la documentación técnica de dichas bases de datos que permita su fácil comprensión.
3. En la creación de nuevas bases de datos se deberá generar la documentación necesaria y suficiente, que permita comprender su estructura física y lógica, así como su contenido.
4. En la definición de nomenclatura para las bases de datos, debe respetarse el Manual de Estándares de bases de datos correspondiente utilizado por La Unidad de Informática.
5. La Unidad de Informática hará uso de una herramienta para el modelaje de datos, creación y generación de base de datos, para lo cual debe adquirirse la respectiva licencia y la capacitación para su manejo.

#### Políticas para la migración de Base de Datos

1. Toda migración de base de datos deberá ser realizada por encargado de las bases de datos de la Unidad de Informática o personal externo del ministerio que corresponda bajo la supervisión de la Unidad de Informática.
2. Antes de cualquier proceso de migración se deberán realizar los respaldos respectivos, así como realizar previamente una prueba de la migración en un servidor de pruebas, para garantizar que el proceso de migración funciona correctamente.
3. En las actividades de migración de información a bases de datos, se deberá seguir el procedimiento definido por la Unidad de Informática para evitar atrasos y complicaciones, así como dejar documentado en una bitácora todo lo realizado para futuras migraciones.

#### Políticas sobre la instalación de Base de Datos



1. Toda instalación de base de datos deberá ser realizada por el encargado de las bases de datos de la UI, o en su defecto por personal de empresas contratadas para estos efectos, bajo la supervisión de la Unidad de Informática.
2. Antes de cualquier instalación deberá realizarse los respaldos respectivos para evitar accidentes y garantizar la recuperación de la base de datos.
3. Para la instalación se deberá seguir el procedimiento definido por La Unidad de Informática para prevenir que se den atrasos o complicaciones, así como dejar documentado en una bitácora todo lo realizado.

#### Políticas sobre administración y mantenimiento de bases de datos

1. Todo mantenimiento a las bases de datos deberá ser realizado por encargado de las bases de datos de TI interno. En el caso de bases de datos que darán mantenimientos profesionales externos, deberán ser supervisados por el profesional responsable de esa tarea de la Unidad de Informática.
2. Antes de cualquier proceso de mantenimiento a la base de datos, se deberán realizar los respaldos respectivos para estar prevenidos contra cualquier accidente que se pudiera presentar.
3. Todo cambio o ajuste hecho en el proceso de mantenimiento, se deberá dejar documentado en una bitácora para efectos de control y seguimiento.

### **Consideraciones generales de la implementación de las Tecnologías de Información**

#### ***Políticas para el desarrollo interno de sistemas de información Infraestructura Tecnológica***

##### Políticas para la adquisición de nuevas tecnologías

1. Se deberá buscar la adquisición de infraestructura (red, software, hardware, servicios), con la debida justificación y que esté alineada al plan estratégico de TI.
2. Todos los procesos institucionales de adquisición de recursos informáticos deben ser valorados y aprobados previamente por La Unidad de Informática.
3. Para la adquisición de nuevos recursos de hardware, software y otros dispositivos tecnológicos, será política de la Unidad de Informática recomendar aquellos que ofrezcan calidad comprobada y sean referentes en el mercado nacional.
4. Para el trámite de adquisición de nuevos recursos informáticos, La Unidad de Informática asesorará y apoyará a la Proveduría Institucional, en la definición de las características tecnológicas y evaluación de ofertas mediante recomendaciones técnicas.
5. Para la adquisición de nuevos recursos, La Unidad de Informática se fundamentará en los reglamentos y normativas de compras definidos para la Institución.
6. La Unidad de Informática velará porque los recursos informáticos adquiridos sean enviados y utilizados por el mismo sitio en que surgió la necesidad de compra.





## Implementación de las Tecnologías de Información

1. La Unidad de Informática desarrollará los sistemas de información que la organización requiera, de acuerdo con los recursos humanos y tecnológicos que tenga a su disposición para este fin.
2. El desarrollo de aplicaciones o sistemas se hará bajo el concepto de tecnología web y siguiendo el procedimiento para el desarrollo de sistemas.
3. Las solicitudes de nuevos sistemas de información, solicitadas por las diferentes dependencias del Ministerio, serán evaluadas y aprobadas por La Unidad de Informática de acuerdo con las prioridades que éstos determinen.
4. Las pruebas de los nuevos sistemas de información deberán hacerse en servidores y ambiente de pruebas y con la utilización de bases de datos de prueba antes de ser puestos en producción.
5. Ningún sistema será puesto en producción si no se cuenta con la debida aprobación del stakeholder (patrocinador del proyecto) del sistema.

### ***Contratación de terceros para la implementación y mantenimiento de software e infraestructura***

#### Políticas para soluciones de terceros

1. La Unidad de Informática podrá recurrir al desarrollo sistemas de información por “outsourcing”, cuando no cuente con el recurso humano y/o tecnológico necesario, para llevar a cabo los desarrollos de forma interna.
2. Las solicitudes de nuevos sistemas de información a desarrollar en la modalidad de “outsourcing”, deberán ser formalmente presentadas por las Jefaturas, en forma escrita e indicando en éstas los requerimientos generales por cubrir y la constancia de la existencia de los fondos presupuestarios emitida por el Departamento Financiero. Además, serán evaluados y aprobados por la Comisión Gerencial de Control Interno y La Unidad de Informática, de acuerdo con las prioridades que la Administración determine.
3. Para los proyectos de desarrollo de sistemas de información por “outsourcing”, deberá establecerse un contrato formal entre el Ministerio y la empresa proveedora del servicio, en donde se definan las condiciones de la contratación, el uso de los programas fuente y la reutilización del sistema en el MAG.
4. El control y monitoreo del avance de proyectos de sistemas de información por “outsourcing” estará a cargo de la Unidad de Informática.
5. Para el desarrollo de proyectos de sistemas de información por “outsourcing”, deberán existir uno o más funcionarios que cumplan las funciones de “contraparte” de la Institución, quienes deberán ser preferiblemente profesionales de la Unidad de Informática y del área usuaria.
6. La Unidad de Informática estará pendiente de que las empresas contratadas para el desarrollo de sistemas de información brinden la capacitación a sus funcionarios en



administración, uso y mantenimiento del nuevo sistema de información, para minimizar la dependencia que se genere del MAG hacia la empresa.

7. Los sistemas de información desarrollados por empresas externas deberán ser entregados por éstas, de manera formal y debidamente documentados, incluyendo en dicha documentación al menos: código fuente, el manual técnico del sistema de información y el manual de los usuarios.
8. Los programas desarrollados o adquiridos externamente serán de uso exclusivo del MAG, y no se permite el uso para funciones que no correspondan a las operaciones normales del MAG.
9. Se deberá implementar un proceso de transferencia tecnológica para minimizar la dependencia del ministerio de las empresas contratadas una vez que termina el contrato, que faculte para que los funcionarios de TI absorban los conocimientos y mantengan la solución operando cuando termina el contrato.



## Prestación de servicios y mantenimiento

### Definición y administración de acuerdos de servicio

1. La Unidad de Informática creará un registro de los servicios que ofrece a las dependencias del Ministerio y los informará a través de la web. Entre los servicios podrían estar; acceso a web privado y público, contrato de terceros, capacitación, red, apoyo en formación virtual, soporte a la gestión de la DNEA, soporte técnico, entre otros.
2. Para cada servicio el jerarca institucional y la Unidad de Informática, documentarán sus atributos, definirán responsabilidades de las partes y su sujeción a las condiciones establecidas y evaluarán su cumplimiento. Se deberá tener claro qué es exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.