Política DI-PO-09

Sobre el uso de recursos de tecnología de la información

Fecha de envío:
Enero, 2014

Política sobre el uso de recursos de tecnología de la Información

1. Objetivo

La presente norma tiene como objeto proveer una guía básica sobre el uso adecuado que deberá brindársele a los Recursos de Información del Ministerio de Cultura y Juventud.

2. Alcance

Estas políticas son aplicables al Usuario que utilice los Recursos Informáticos del Ministerio de Cultura y Juventud, en lo que a cada uno de ellos les corresponda.

3. Definiciones

Estas políticas son parte de la Política Integral de Seguridad del MCJ y por tanto, aplica en general la misma tabla de definiciones allí incluida, así como en específico, las siguientes:

3.1. Debido Proceso:

Es aquel proceso que ha sido debidamente aprobado por el Ministerio o que se encuentra vigente por ley, y que debe aplicarse de previo al establecimiento de una sanción.

3.2. Responsable Asignado:

Es en última instancia la persona a quien el Ministerio de Cultura y Juventud ha encargado la responsabilidad del cuido y resguardo de los Recursos Informáticos a su cargo.

4. Responsabilidades de los puestos involucrados

Las responsabilidades de los puestos involucrados se definen en el cuerpo mismo de cada una de las normas aquí incluidas, según corresponda.

5. Descripción

En plena conformidad con lo estipulado por Ley de Administración Financiera de la República, por la Ley General de Control Interno y por las Normas para la Gestión y Control de las Tecnologías de la Información, las instituciones del Estado tendrán la obligación irrefutable de velar por el uso que se les da a sus Recursos Informáticos, de manera que éste sea un uso responsable, eficiente y seguro.

Cada funcionario que reciba y tenga bajo su custodia bienes del Estado, será responsable de ellos y de cualesquier daño, pérdida o abuso, empleo ilegal que le sea imputable por falta al deber de cuidado, negligencia o dolo.

Se debe rendir cuentas por todos los Recursos Informáticos del Ministerio.

Ejemplos de los Recursos Informáticos del Ministerio son los siguientes:

a) **Recursos de información:** Documentación de sistemas, archivos y bases de datos, manuales técnicos de usuario, material de capacitación, procedimientos operativos y de soporte, disposiciones relativas a sistemas de emergencia para la reposición de información, planes de continuidad, diagramas de red, información archivada.

b) **Equipo informático:** Activos físicos (equipos reproductores, procesadores, monitores, computadores de todo tipo, tablets, dispositivos electrónicos, equipos de comunicaciones (routers, centrales telefónicas, máquinas de fax, teléfonos de todo tipo, contestadores automáticos, redes y enlaces de comunicaciones), medios magnéticos y ópticos; otros equipos técnicos (suministro de electricidad, sistemas de aire acondicionado), mobiliario;

c) **Recursos de software:** Software de todo tipo (e.g, de sistemas, de aplicaciones, operativos), herramientas de desarrollo, y demás utilitarios;

d) **Servicios:** Servicios informáticos y de comunicaciones (correo electrónico, Intranet, Internet, entre otros), utilitarios generales (iluminación, energía eléctrica, aire acondicionado)[1].

6. Fecha de creación

El presente documento fue creado en Enero de 2014, y se encuentra en plena vigencia desde esa fecha.

7. Lista de distribución

Las presentes políticas se distribuirán al Usuario directamente involucrado con su cumplimiento, únicamente en lo que a cada uno corresponda.

8. Referencia a otros documentos y Anexos

a) Estándar en materia de Seguridad de la Información ISO/IEC 27002:2013;
b) Estándar para la implementación de Sistemas de Administración de la Seguridad Informática ISO /IEC 27001:2013;
c) Legislación costarricense aplicable a la materia (incluyendo la Ley General de Control Interno -No. 8292 de 31 de julio de 2002-, y Las Normas Técnicas para la Gestión y Control de las Tecnologías de la Información –No. R-CO-26-2007 del 7 de junio, 2007, entre otras);
d) COBIT v. 4.1. en lo referente a seguridad de la información.

[1] ISO 27002:2005, Control 7.1.1.

9. Asignación de responsabilidades por Recursos Tecnológicos

9.1. Designación de un responsable por activo

Las jefaturas de las distintas áreas o unidades del Ministerio se encargarán de que cada activo bajo su tutela sea asignado a la responsabilidad de un funcionario (en adelante el "Responsable Asignado"). Este Responsable Asignado será quien en última instancia, mantendrá la responsabilidad directa por el cuido y resguardo de los activos bajo su cargo. Lo anterior, sin perjuicio alguno de las responsabilidades que sobre estos mismos activos, correspondan además a otros funcionarios, ya sea por mandato de Ley o por directriz interna del MCJ.

Se aclara que la denominación de "Responsable", le es conferida al funcionario *únicamente en virtud* de la protección que le debe brindar a los bienes, y no implica en ningún sentido, derecho alguno de propiedad o relacionados sobre los mismos. Todos los derechos de propiedad o relacionados, corresponden única y exclusivamente al Ministerio de Cultura y Juventud.

9.2. Responsabilidades generales del Responsable Asignado

Aunadas a todas las responsabilidades que directamente les apliquen, ya sean las incluidas en este documento y/o en otras disposiciones que en materia de uso de activos sean debidamente aprobadas por el Ministerio, los Responsables Asignados rendirán cuentas por todos los activos bajo su protección y velarán además, porque se instauren sobre los mismos, los controles de seguridad formalmente aprobados por el Ministerio de Cultura y Juventud.

9.3. Prohibición de fumar, comer o beber

Está estrictamente prohibido fumar, comer o beber cerca de los Recursos Informáticos del Ministerio; y en aquellas áreas que hayan sido delimitadas con tal prohibición.

Cualesquier daño que provenga de cualesquier omisión o violación a lo aquí estipulado, debe ser personalmente asumido por su causante hasta sus últimas consecuencias.

9.4. Limpieza de los equipos de cómputo

Los usuarios deben asegurarse que en los equipos de cómputo que les son asignados, se implementen los procedimientos de limpieza (incluyendo soplado contra el polvo), que el Ministerio formalmente emita para esos efectos, según las instrucciones vertidas por la Institución. Es responsabilidad de cada usuario proteger el equipo que le ha sido asignado.

9.5. Utilización de Recursos Informáticos únicamente para usos previstos

Los Recursos Informáticos del Ministerio, serán utilizados única y exclusivamente para los efectos provistos por éste, es decir, para la realización de las labores del usuario para con la Institución. No se permitirá, ni el Ministerio tolerará ningún tipo de uso ni ubicación no autorizado.

10. Monitoreo del uso de los sistemas y Recursos Informáticos y de Información

10.1. Del monitoreo legal a llevarse a cabo en los sistemas del Ministerio

Dado que el MCJ se encuentra en la obligación de velar por el uso correcto de sus Recursos Informáticos, éste llevará a cabo un monitoreo legal del acontecer en todos sus sistemas, según así se lo permita el ordenamiento jurídico vigente.

10.2. De los límites del monitoreo permitido y apoyado por el Ministerio

El monitoreo de los sistemas informáticos y de información deberá ser ejecutado, única y exclusivamente por personas formalmente autorizadas para tales efectos, siguiendo estrictamente las direcciones emitidas por la Institución a ese respecto.

Deberá registrarse toda actividad de monitoreo, ya que las mismas estarán sometidas a revisión por parte del Encargado de Seguridad.

El Ministerio no tolerará ningún desvío u omisión en la aplicación de los procedimientos aprobados para tales efectos, considerando de gravedad cualesquier desviación, en virtud de que las mismas podrían ocasionar que el monitoreo resulte ilegal. Por lo tanto, quien haciendo caso omiso a lo aquí estipulado se aparte de los procedimientos y directrices emitidas por el MCJ para tales efectos, asumirá personalmente toda consecuencia adversa que de ello derive, al punto de deber asumir incluso, los costos y gastos de la defensa de la Institución, cuando así correspondiere. Lo anterior sin perjuicio de que el Ministerio tome todas las medidas administrativas, laborales, civiles y/o penales que la ley le permita, para sancionar a los responsables.

10.3. Documento de aceptación de monitoreo

Previo a conceder el acceso a los sistemas a cualquier funcionario o tercero, se le solicitará suscribir un documento legal en el que éste reconozca y acepte expresamente que toda actividad dentro de los sistemas de la Institución va a ser monitoreada, y además los equipos y software involucrados, serán eventualmente sometidos a revisión.

Debe solicitarse la asesoría de la Asesoría Jurídica para la elaboración de dicho documento, así como para que ésta delimite las situaciones y los medios en que será requerida la firma del mismo.

11. Inventario y clasificación de Recursos Informáticos

11.1. De la importancia del inventario y la clasificación de Recursos Informáticos

A fin de poder determinar el tipo de controles a aplicar sobre sus Recursos de Información, el Ministerio deberá tener claridad sobre cuáles son esos recursos y la importancia de los mismos para el proceso institucional al que han sido asignados.

11.2. Valor estratégico de los activos

Con base en el nivel de criticidad establecido por la Administración Superior para los diferentes procesos del Ministerio, se instruirá a los dueños de proceso, para que definan el valor estratégico de los activos bajo su responsabilidad. Los dueños de cada proceso del Ministerio deberán identificar el valor relativo e importancia de los activos informáticos a su cargo, para su proceso en específico. Tomando en consideración esta información y con base en los análisis de riesgo llevados a cabo para tales efectos y en el nivel de riesgo residual aceptado por la Administración Superior, el Departamento de Informática valorará lo propuesto por los dueños de los procesos, lo validará o desechará y finalmente elevará lo que corresponda ante la Administración Superior para su aprobación final.

11.3. Inventario de Recursos Informáticos

El MCJ mantendrá un inventario actualizado de los Recursos Informáticos. En este inventario, se documentará e identificará:

a) Cada sistema de información;
b) Su responsable a cargo;
c) Su clasificación en cuanto a seguridad; y
d) La ubicación vigente del mismo.

El Responsable Asignado deberá informar a su superior jerárquico sobre cualquier cambio del estado o ubicación del activo.

12. Aseguramiento de Activos

12.1. Aseguramiento de activos informáticos

Cuando así lo haya determinado la Administración Superior, los activos informáticos que el Ministerio considere importantes (incluyendo pero sin limitarse a aquellos móviles, y/o a ser utilizados fuera de las instalaciones del Ministerio de Cultura y Juventud), serán objeto de aseguramiento.

El Responsable Asignado a estos activos velará porque se cumplan todas las condiciones impuestas por el ente asegurador, a fin de mantener los activos informáticos debidamente protegidos.

13. De los Incidentes de Seguridad

13.1. Responsabilidad del Usuario de reportar incidentes relacionados con la Seguridad de la Información

Cada usuario de los sistemas y Recursos Informáticos del Ministerio está en la obligación inexcusable de reportar cualesquier comportamiento anómalo que detecte, ya sea en los sistemas y/o en los Recursos Informáticos o de información de la Institución, y de conocer

los mecanismos y procedimientos aprobados por el Ministerio para hacer este tipo de reportes.

El reporte debe hacerse en el momento mismo en que el usuario note el comportamiento anómalo, a fin de que se pueda tomar acción inmediata y se controlen y/o minimicen posibles daños.

El reporte podrá hacerse ya sea: a) Ante el superior jerárquico inmediato y ante el Encargado de Seguridad; o b) Únicamente ante el Encargado de Seguridad.

El usuario no debe tratar de verificar por sí mismo la existencia efectiva del incidente, esto corresponderá a expertos designados por el Ministerio, sin embargo, el usuario sí debe hacer el respectivo reporte, aun cuando solamente suponga o tenga la sospecha de que el comportamiento anómalo se está dando.

Toda la información relacionada con los incidentes de seguridad debe ser considerada Información Confidencial y por ende, debe ser manejada exclusivamente por los canales formalmente estipulados por el Ministerio para tales efectos y únicamente tratada con las personas responsables del manejo de dichos incidentes (i.e. el superior jerárquico inmediato y Encargado de Seguridad).
Por la importancia del tema y las consecuencias que puede generar, la omisión o violación al cumplimiento de esta Norma será considerada de gravedad y el Ministerio procederá a tomar las medidas, administrativas, civiles, laborales y/o penales que la ley le permita.

13.2. De los procedimientos controlados de reporte de incidentes

Se deben establecer procedimientos de reporte de incidentes en materia de seguridad, que aseguren la subsanación de los mismos en forma eficiente, rápida y controlada, teniendo presente que los canales por donde viaje la información relativa al incidente sean canales seguros y adecuados.

Debe tenerse presente que la información relativa a incidentes en materia de seguridad debe tratarse como información altamente confidencial y no debe ser conocida más que por quienes tienen la necesidad de saberlo. La necesidad de saber de los incidentes en materia de seguridad la tienen básicamente quienes deben corregirlos, a fin de evitar que los mismos sean explotados y quienes por disposición normativa o contractual, deban ser informados.

Cuando haya necesidad de reportar la ocurrencia de incidentes de seguridad a terceros ajenos al Ministerio, es decir, cuando exista la obligación legal o contractual de la Institución de hacerlo, la forma en que ello se hará, será una determinación que tomará la Administración Superior, contando con la asesoría experta de la Asesoría Jurídica.

13.3. Conductas u omisiones que impidan el reporte de incidentes de seguridad

El Ministerio considera de extrema gravedad el que se intenten llevar a cabo o efectivamente se lleven a cabo, conductas u omisiones de cualesquier tipo que prevengan, interfieran, obstruyan o impidan los esfuerzos de reportar y/o documentar debilidades, anomalías, vulnerabilidades y/o incidentes de seguridad.

Quien incurra en este tipo de conductas u omisiones será sancionado y el Ministerio tomará las acciones administrativas, laborales, civiles y/o penales que la ley le permita a fin de exigir las responsabilidades correspondientes.

13.4. Prohibición expresa de causar incidentes

Está estrictamente prohibido al Usuario corromper, inutilizar, alterar, modificar o en forma alguna impedir el funcionamiento de los Recursos Informáticos del Ministerio, sin contar con permiso expreso válidamente emitido, para ello. También le está terminantemente prohibido al Usuario hacer pruebas de vulnerabilidad a los Recursos Informáticos del Ministerio, sin contar con autorización expresa válidamente emitida, para ello.

Cada usuario de los Recursos Informáticos del Ministerio de Cultura y Juventud tendrá la obligación de utilizarlos, únicamente para los efectos para los que le fueron asignados y éste no tolerará ningún otro tipo de usos, aun cuando los mismos se pretendan llevar a cabo ocasionalmente.

13.5. Prohibición de dar a conocer a terceros los canales de reporte de incidentes de seguridad

Ningún usuario debe, bajo ninguna circunstancia, revelar a terceros ni a personal no autorizado los mecanismos utilizados para el reporte, manejo o constatación de incidentes de seguridad.

13.6. Responsabilidad del Usuario de Actuar de Buena Fe ante un incidente de Seguridad de la Información

El manejo de los incidentes de seguridad corresponde principalmente al Encargado de Seguridad, sin embargo, ante la ocurrencia de un incidente de este tipo, el Ministerio podrá solicitar el apoyo y ayuda del Usuario para el restablecimiento de sus funciones normales, y será responsabilidad ineludible del Usuario brindar la cooperación solicitada.

La buena fe en las relaciones laborales es uno de los principios claramente estipulados en el Código de Trabajo Costarricense[2], y el coadyuvar en el restablecimiento de las actividades del Ministerio con ocasión de un incidente de seguridad de la información, está dentro de los aspectos contemplados por este principio, aun cuando esta ayuda se requiera excepcionalmente fuera del horario normal de trabajo.

[2] *Código de Trabajo de Costa Rica: "*El contrato de trabajo obliga tanto a lo que se expresa en él, como a las consecuencias que del mismo se deriven según la buena fe, la equidad, el uso, la costumbre o la ley", Artículo 19.

14. Protección del hardware

14.1. Responsabilidades básicas de los usuarios con respecto a los equipos informáticos provistos por el Ministerio

Sin perjuicio de cualesquier otra estipulación respecto a los equipos informáticos debidamente aprobada por el Ministerio, todo usuario debe al menos cumplir con las siguientes disposiciones:

a) Utilización del equipo informático: Todo equipo informático provisto por el Ministerio, se asigna única y exclusivamente para fines laborales. Estos equipos serán considerados en todo momento propiedad de la Institución y por lo tanto, el Ministerio podrá tomar las medidas que el ordenamiento jurídico costarricense les permita, con respecto a ellos.

b) Autorización para conectar equipos informáticos a la red del Ministerio: Previo a conectar cualquier equipo informático a la red del Ministerio, será indispensable contar con autorización expresa y por escrito válidamente emitida por la unidad institucional a la que el usuario reporta o pertenece y por el Departamento de Informática.

c) Requisitos mínimos de seguridad de los equipos informáticos: Todo equipo informático que se conecte a los sistemas del Ministerio, sea remota o directamente, debe cumplir con los requisitos de seguridad impuestos por la Institución y estar configurado y programado por el Departamento de Informática, de acuerdo a los parámetros de seguridad establecidos.

d) Explotación de vulnerabilidades en los equipos informáticos del Ministerio: Se prohíbe explotar las vulnerabilidades en los equipos informáticos del Ministerio, a menos que se cuente con permiso expreso y por escrito, válidamente emitido por el Departamento de Informática, para tales efectos.

e) Préstamo de equipos informáticos a terceros: Los equipos informáticos del Ministerio, son para el uso exclusivo del usuario a quien le son directamente asignados. No deben ser facilitados a personas no autorizadas.

f) Responsabilidad por cuido de los equipos informáticos del Ministerio: Todo equipo informático facilitado o provisto por el Ministerio es responsabilidad del usuario a quien se le asigna, éste por tanto, debe velar por el equipo y la información contenida en el mismo.

g) Retiro de equipo informático de las instalaciones del Ministerio: Para el retiro de equipos informáticos fuera de las instalaciones del MCJ, todo usuario debe contar con autorización expresa válidamente emitida por la Institución para tales efectos. Aún habiendo sido previamente autorizado el retiro de equipos, el usuario que lo efectúe será personalmente responsable por el cuido diligente de los mismos.

h) Devolución del equipo del Ministerio: Todo equipo del Ministerio debe ser inmediatamente devuelto, cuando:

i) La relación contractual o laboral del usuario para con la Institución termine o se suspenda; y/o

ii) El Ministerio así lo solicite.

15. Protección del software

15.1. Usos permitidos del software institucional

Solamente se autorizarán aquellos usos del software institucional que no violenten:

a) Las Políticas, Estándares, Procedimientos, Lineamientos y otros comunicados oficiales que en materia de seguridad de la información, ha aprobado formalmente la Institución;
b) La normativa aplicable con respecto al software;
c) Los derechos de propiedad intelectual, de autoría y demás derechos conexos existentes sobre el software de que se trate;
d) Los términos y restricciones de las licencias respectivas.

Asimismo, sólo se autorizará el uso del software institucional a quienes así lo requieran con base en una necesidad comprobada, en virtud de su relación para con el Ministerio.

15.2. Cuidados especiales con software a instalar en el equipo informático ajeno

La autorización para la instalación de software institucional en equipo informático ajeno, sólo debe darse una vez que se haya comprobado que dichos equipos, se encuentran en regla y que quien los aporta posee los permisos correspondientes.

La instalación del software institucional en equipo informático ajeno, sólo debe permitirse si la licencia del software involucrado así lo autorizara, o si se cuenta con el permiso expreso y por escrito del dueño de los derechos de propiedad intelectual y/o de autoría sobre el mismo, para tales efectos.

15.3. Mecanismos de administración de licenciamiento del software institucional

Todos los sistemas del Ministerio deben utilizar programas de administración de licenciamiento de software, aptos para detectar no sólo cambios o reproducciones no autorizadas en/del software institucional, sino también detectar la inclusión de software no autorizado en los sistemas de la Institución.

Para dar cumplimiento al decreto de derechos de autor y conexos se está trabajando temporalmente con el software de control de instalaciones suministrado por el Registro de Derechos de Autor, el mismo se ubica en la página web del ministerio http://www.mcj.go.cr/archivos/instalacion.aspx

Paralelamente debe confeccionarse un expediente que contenga información de respaldo de las licencias con la información que se defina de previo.

15.4. Obligación de garantizar la desinstalación del software

La jefatura inmediata o el responsable del proyecto de que se trate, debe solicitar al funcionario autorizado la desinstalación del software institucional de equipo ajeno, con ocasión de la terminación o suspensión del usuario en su relación laboral y/o contractual para con el Ministerio. Corresponderá a la jefatura inmediata o al responsable del proyecto, garantizar que la desinstalación se lleve a cabo.

15.5. Responsabilidades básicas de los usuarios con respecto al software institucional

Sin perjuicio de cualesquier otra estipulación respecto al software institucional debidamente aprobada por el Ministerio, todo usuario debe al menos cumplir con las siguientes disposiciones:

a) Previa autorización para instalación de software: El usuario no debe, bajo ninguna circunstancia, instalar software en los equipos utilizados o provistos en/por el Ministerio, sin contar con expresa autorización emitida por escrito por el Departamento de Informática. Esta prohibición contempla incluso, la instalación no autorizada de versiones actualizadas del software institucional.

b) Instalación de software institucional en equipo ajeno: El usuario no debe, bajo ninguna circunstancia, instalar software propiedad del Ministerio o licenciado a favor de éste, en equipo no propiedad de la Institución (aun cuando se trate de equipo ajeno autorizado para poder ser utilizado en los sistemas del MCJ), sin contar para ello con la aprobación expresa y por escrito del Departamento de Informática.

c) Software licenciado: Previo a instalar cualquier tipo de software en los equipos utilizados y/o provistos en/por el Ministerio, se debe contar con la licencia respectiva, que así lo autorice. El no contar con la licencia para la utilización de software puede constituir delito.

d) Software no autorizado: Es totalmente prohibido instalar en los equipos utilizados o provistos en/por el Ministerio, software no autorizado proveniente de Internet o software no autorizado enviado o facilitado por terceros ajenos a la Institución (incluyendo pero no limitado a shareware y freeware). De tenerse duda con respecto a qué software está autorizado, debe consultarse al Departamento de Informática.

e) Alteraciones del software institucional: Es totalmente prohibido modificar, alterar, inutilizar o destruir el software institucional, así como copiar el mismo, sin contar con autorización expresa y por escrito del Departamento de Informática.

f) Copias del software institucional: Salvo autorización expresa válidamente emitida por el Ministerio, está terminantemente prohibida la reproducción del software institucional.

g) Transferencia del software institucional: Es totalmente prohibido prestar, vender, alquilar y/o de cualesquier forma transferir el software institucional o su uso, sin el permiso expreso y por escrito del Departamento de Informática, para ello.

No debe facilitarse el software institucional a terceros ajenos al Ministerio, a menos que la licencia provista por el fabricante del software lo permita, se haya recibido autorización expresa y por escrito de la Institución para tales efectos y se hayan firmado los contratos necesarios que determinen la asignación de responsabilidades, las obligaciones y derechos de los contratantes, y se garantice a la vez, la protección de los derechos de autoría y de propiedad intelectual de quien corresponda.

h) Información con respecto al software institucional: Es totalmente prohibido divulgar cualesquier información relacionada con el software institucional, sin contar con permiso expreso y por escrito para ello, dado por el Departamento de Informática.

i) Uso del software institucional: El software institucional se provee para usos laborales únicamente. Están estrictamente prohibidos usos no autorizados y/o ilegales.

j) Software de detección de vulnerabilidades: El uso de software de detección de vulnerabilidades es totalmente prohibido para el usuario, con excepción de quienes por las labores que realizan para el Ministerio, hayan sido encargados para ello por el Encargado de Seguridad.

k) Devolución del software institucional: Con ocasión de la terminación o la suspensión de la relación laboral y/o contractual del usuario para con el Ministerio, todo software institucional, así como sus aditamentos en cualquier formato, debe ser retornado a la Institución de manera inmediata.

l) Desinstalación del software institucional: Todo software institucional que se encuentre en equipo ajeno (siempre que así lo permita la licencia del fabricante), debe ser inmediatamente desinstalado con ocasión de la terminación de la relación laboral y/o contractual del usuario para con el Ministerio. El usuario tendrá la responsabilidad personal y directa, de informar por escrito a la jefatura inmediata o al responsable del proyecto por parte del Ministerio, de la terminación de su relación con la Institución, para que se proceda a desinstalar el software institucional. Si por cualesquier motivo, aún después de la terminación de la relación del usuario con el Ministerio, hubiese software institucional instalado en equipo ajeno al mismo, el usuario debe desinstalar dicho software, haciéndose responsable por no utilizarlo, ni permitir que nadie más lo utilice indebidamente.

15.6. Copia de respaldo del software institucional

Sólo aquellos que han sido debidamente encargados a los efectos, deben realizar una copia de seguridad para todo software que el Ministerio adquiera, misma que se mantendrá bien resguardada y no será utilizada a menos que el software sufra daño y deba recurrirse a ésta. Es importante confirmar que la licencia del software de que se trate, permita la creación de esta copia de respaldo. Si la licencia no lo permite, es indispensable contactar al fabricante del software o a quien detente los derechos sobre éste, para que emita permiso expreso y por escrito, para hacer la copia de respaldo. El no contar con el permiso respectivo, ya sea en la licencia misma del producto o en su defecto por media carta de autorización para dicha copia, puede constituir delito.

15.7. Reproducción no autorizada de software

Reproducciones de software para efectos distintos a la copia de respaldo realizadas por quienes hayan sido debidamente autorizados para tales efectos (cuando la licencia así lo permite), son absolutamente prohibidas y podrían ser ilegales.

15.8. Licencia como requisito indispensable

Los encargados deben asegurarse que todo software que se instale en los sistemas del Ministerio, cuente con la debida licencia para su uso. Esta licencia deber ser legítimamente emitida por quien tenga los derechos para poder otorgarla así como ser adquirida de acuerdo con el procedimiento de compra definido por la Proveeduria Institucional.

Este documento debe estar archivado en el expediente de control de licencias.

15.9. Revisión básica de los términos de las licencias previa instalación

Los encargados, previo a instalar software en los sistemas del Ministerio, deben realizar el análisis de los términos de la licencia respectiva, a fin de determinar las restricciones en su utilización.

15.10. Alteración no autorizada de software institucional

Los encargados deben configurar, mantener y monitorear los mecanismos de administración de licenciamiento del software institucional, formalmente aprobados por la Institución. Ante la ocurrencia de cualquier intento de modificación, reproducción o instalación no autorizada informará de inmediato al Encargado de Seguridad, por los medios y canales provistos para tales efectos por la Institución.

15.11. Mantenimiento de pruebas y evidencias de uso autorizado del software

Deben resguardarse y protegerse en una ubicación segura, todas las pruebas y evidencias con que cuenta el Ministerio, a fin de poder demostrar en cualquier momento (en caso que sea necesario), que se está haciendo uso autorizado de todos los programas y aplicaciones utilizadas. Deben por tanto, mantenerse muy bien documentados, al menos:

a) Las licencias correspondientes;
b) Los permisos o autorizaciones especiales del dueño de los derechos de propiedad intelectual para llevar a cabo usos excepcionales;
c) Los documentos en los cuales el creador del software hecho a la medida, se hace responsable por cualesquier problema que pueda surgir con respecto a la propiedad intelectual y/o autoría del software.

Asimismo, deben guardarse los discos maestros y manuales originales de todo el software propiedad y/o licenciado a favor del Ministerio, así como cualesquier otra evidencia que compruebe el uso legal del software utilizado por la Institución.

15.12. Responsabilidad personal por la protección de los derechos de propiedad intelectual del software que le es provisto por el Ministerio

Cada usuario será personalmente responsable del software que le es provisto por el Ministerio, de manera que debe utilizarlo en estricto acato a la legislación aplicable en materia de propiedad intelectual.

Las consecuencias del uso no autorizado y/o ilegal del software deben ser asumidas directamente por su causante, al punto incluso de deber asumir por su propia cuenta y riesgo, la defensa de la Institución.

15.13. Archivos y/o software proveniente de fuentes desconocidas o no confiables

No deben ejecutarse archivos ni software que provengan de fuentes desconocidas o no confiables en los equipos o sistemas conectados a la red del Ministerio. Siempre que se tenga motivo suficiente y fundamentado para creer que un archivo o software de fuente desconocida o no confiable pueda contener información de importancia para el Ministerio, debe contactarse inmediatamente al Encargado de Seguridad, para que este último proceda a abrir el archivo o correr la aplicación en un ambiente controlado y seguro.

Disposiciones finales

- **Reserva de derechos del Ministerio**

El Ministerio se reserva el derecho de hacer cualquier tipo de modificación a estas políticas sin que ello implique responsabilidad de su parte, incluso sin previo aviso. Asimismo, la Institución se reserva el derecho de ampararse en una plataforma legal de apoyo a sus políticas, que habrán se suscribir los usuarios que pretendan tener acceso a los Recursos Informáticos.

- **Fiscalización de cumplimiento**

El Ministerio se abroga el derecho de controlar estrictamente el debido cumplimiento de estas políticas, así como de tomar cualquier acción, de cualesquier naturaleza, sea ésta civil, penal, laboral y/o administrativa que le sea permitida por el ordenamiento jurídico, con el fin de castigar la violación a las mismas, para lo cual deberá respetar el debido proceso.

- **Usos ilícitos y/o no permitidos**

El Ministerio facilita sus Recursos Informáticos únicamente para usos permitidos y legales. Por ende, quien haga uso de los mismos para fines ilegales y/o no permitidos, deberá asumir todas y cada una de las consecuencias que de su actuar u omisión deriven.

- **Políticas como una guía básica**

Las Políticas incluidas en el presente documento pretenden ser una guía básica, no una lista exhaustiva. Por ende, de tener el usuario alguna duda que las Políticas no puedan aclarar, deberá consultarla, según corresponda, ya sea con el Jefe del área a

que pertenece; con el supervisor del proyecto de que se trate; y/o con quien dirige el Departamento de Informática.

- **Tolerancia**

El que el Ministerio por cualesquier razón decida no tomar acciones en un determinado momento para exigir responsabilidades o sancionar algún comportamiento, no impide que pueda hacerlo en cualquier momento posterior. Deberá tenerse presente que el Ministerio estará siempre en potestad de actuar, según se lo permita el ordenamiento jurídico aplicable.

- **Política Integral de Seguridad de la Información**

Las presentes políticas son complemento de las Políticas Integrales de Seguridad de la Información aprobadas por el Ministerio y por ende, la rigen los mismos principios rectores.

Así, los conceptos básicos que se infieren de las Políticas Integrales de Seguridad de la Información, se mantienen inalterados (e.g. seguridad de la información como factor prioritario; confidencialidad de la información del Ministerio y/o los Administrados; intereses del Ministerio y/o los Administrados por sobre intereses Personales; legalidad de toda actuación y respeto irrestricto a la legislación aplicable; respeto irrestricto a los Derechos de Autor y de Propiedad Intelectual; balance seguridad-productividad; prevalencia del interés público, entre otros).

De haber contraposición entre las Políticas Integrales de Seguridad de la Información y las presentes políticas, prevalecerán las que sean más específicas para el usuario con respecto al desempeño de sus responsabilidades para con la Institución.