Departamento de Informática

DI-PO-05-2014

Política de uso y resguardo de la información

Fecha de envío:
Enero, 2014

1. Objetivo 4
2. Alcance 4
3. Definiciones 4
   3.1. Cadena de Custodia de la Evidencia: 4
   3.2. Responsable Asignado: 4
4. Responsabilidades de las áreas o puestos involucrados 4
5. Descripción 4
6. Fecha de creación, y entrada en vigencia de las políticas 4
7. Lista de distribución 4
8. Referencia a otros documentos y Anexos 4
9. Propiedad de la información 5
   9.1. Propiedad de la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada y/o creada en los sistemas del Ministerio 5
   9.2. Propiedad de la información producida por funcionarios del Ministerio 5
   9.3. Propiedad de la información producida por contratistas y consultores 5
   9.4. Devolución de la Información del Ministerio 6
10. De la confidencialidad, integridad, disponibilidad y expectativas de privacidad de la información 6
   10.1. Confidencialidad de la información del Ministerio y/o los Administrados 6
   10.2. De los controles para garantizar la confidencialidad, integridad y accesibilidad de la información propiedad del Ministerio y/o en su custodia 6
   10.3. Conflictos de interés 7
   10.4. Aseguramiento de la información previa ausencia (por vacaciones, permisos, incapacidades y/o rotación) 7
   10.5. Información de los Administrados en lugares de acceso no restringido 7
   10.6. Información sometida a requerimientos de confidencialidad y lugares de acceso público 7
   10.7. Privacidad de la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada, creada y/o eliminada en los sistemas del Ministerio 7
   10.8. Integridad de la información 8
11. De los respaldos y recuperación de la información 8
   11.1. Respaldos de la información del Ministerio 8
   11.2. Respaldos de la información del Ministerio 9
   11.3. Asignación de responsabilidades en la realización de respaldos de información 10
   11.4. Alcance de los respaldos 10
   11.5. Estandarización de los medios de respaldo 10
12. De los procedimientos de manejo de la información 10
   12.1. De los procedimientos necesarios para evitar el uso inadecuado o divulgación no autorizada de la información 10

12.2. De la obligación de acatar los procedimientos aprobados para el manejo y almacenamiento seguro de la Información 11
12.3. Registro formal de los receptores autorizados de datos 11
12.4. Resguardo protegido de medios de almacenamiento de información 11
13. Restricción del acceso a la información 11
13.1. Controles para la restricción del acceso a las aplicaciones 11
14. Áreas aisladas 12
14.1. Información sometida a requerimientos de confidencialidad y áreas aisladas 12
15. Medios de almacenamiento 12
15.1. Medios de almacenamiento y manejo de los mismos para el resguardo efectivo de los registros importantes del Ministerio 12
16. Aspectos Legales referentes al intercambio de información y software 13
16.1. Intercambio de información y/o software 13
16.2. Aspectos legales a tomar en consideración para el intercambio de información y/o software 13
16.3. Acuerdos con terceros para el intercambio de información y software 13
17. Recolección y protección de la evidencia 14
17.1. Prohibición de violentar la evidencia que le pueda servir al Ministerio para establecer acciones contra personas físicas o jurídicas 14
17.2. La importancia de la evidencia en la toma de acciones en contra de personas físicas y/o jurídicas y de la proporcionalidad de la sanción 14
17.3. Reglas para la recolección de evidencia 15
Disposiciones finales 15

1. Objetivo

El objetivo de esta sección es dotar de protección a la información que es propiedad del Ministerio y/o está bajo su custodia, en todas las formas en las que la misma se puede presentar, desde su creación hasta su eliminación.

2. Alcance

Estas políticas son aplicables a todos el Personal Usuario, en los que a sus responsabilidades particulares corresponda.

3. Definiciones

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

3.1. Cadena de Custodia de la Evidencia:

Es el proceso que garantiza la integridad de la evidencia, desde el momento en que se recopila, hasta el momento en que se hace valer ante las autoridades.

3.2. Responsable Asignado:

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

4. Responsabilidades de las áreas o puestos involucrados

Las responsabilidades de las áreas o puestos involucrados se definen en el cuerpo mismo de las normas aquí incluidas, según corresponda.

5. Descripción

La información como activo más valioso del Ministerio, debe ser tutelada, independientemente del formato en que se encuentre, del medio de transmisión que se use, del lugar donde esté y durante todo su ciclo de la misma, desde su creación hasta su eliminación. Estas políticas pretenden proporcionar una guía básica para que el lector pueda brindar a la información que maneja, un grado adecuado de protección.

6. Fecha de creación, y entrada en vigencia de las políticas

El presente documento fue creado en enero de 2014, y se encuentra en plena vigencia desde febrero 2014.

7. Lista de distribución

Las presentes políticas se distribuirán al Personal 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.

9. Propiedad de la información

9.1. Propiedad de la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada y/o creada en los sistemas del Ministerio

Toda la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada y/o creada en los sistemas del Ministerio, será considerada información propiedad del Ministerio de Cultura y Juventud, salvo que el ordenamiento jurídico y/o acuerdos específicos establezcan lo contrario. Por ende, no podrán los usuarios bajo ninguna circunstancia, transmitirla en manera alguna a terceros, modificarla ni eliminarla, sin contar con autorización previa.

Aún y cuando la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada y/o creada en los sistemas del Ministerio de Cultura y Juventud no sea propiamente información suya, la misma puede estar protegida por derechos preferentes de terceros (e.g. derechos de propiedad intelectual, de autoría o conexos), por lo tanto, no debe disponerse de ésta sin contar con la autorización expresa y por escrito del dueño de la información o en su defecto del Responsable Asignado al resguardo de la misma.

9.2. Propiedad de la información producida por funcionarios del Ministerio

Toda información producida, generada o creada por los funcionarios del Ministerio en sus quehaceres para con éste, es información que pertenece a la Institución. El Ministerio de Cultura y Juventud será el propietario de todos los derechos de disposición y patrimoniales sobre la misma y podrá utilizarla, como así lo requiera. En consecuencia, los funcionarios no podrán disponer de dicha información para efectos no relacionados con sus labores, a menos que cuenten con autorización válidamente emitida y por escrito, para ello.

9.3. Propiedad de la información producida por contratistas y consultores

La propiedad de la información que se produzca, cree o genere por contratistas y/o consultores, para y/o por solicitud del Ministerio debe negociarse caso por caso y por acuerdo de Partes. Especificaciones referentes a la propiedad de la información producida, deben estipularse en los respectivos contratos con dichos contratistas y/o consultores.

9.4. Devolución de la Información del Ministerio

Al momento de terminación de la relación laboral y/o contractual del usuario para con El Ministerio de Cultura y Juventud, toda información perteneciente al Ministerio y/o en su custodia (incluyendo pero sin limitarse a la información de los Administrados) le debe ser devuelta inmediatamente.

10. De la confidencialidad, integridad, disponibilidad y expectativas de privacidad de la información

10.1. Confidencialidad de la información del Ministerio y/o los Administrados

La información propiedad del Ministerio y/o en su custodia debe necesariamente ser tratada con extrema cautela y debe ser conocida únicamente por quienes estén expresamente autorizados para tales efectos. Por ende, cuando se tenga duda sobre la clasificación de la información de que se trate, la misma debe ser considerada como información sometida a requerimientos de confidencialidad.

El usuario debe entender que la confidencialidad de la información que en virtud de su relación laboral y/o contractual para con el Ministerio maneja, es un deber impuesto por la legislación vigente, y su incumplimiento es sancionado incluso con pena de prisión[1]. Sin perjuicio alguno de lo anterior, a fin de reafirmar esta noción y clarificar qué se espera de los usuarios en ese sentido, el Ministerio se reserva el derecho de solicitar la suscripción de los documentos legales correspondientes, que garanticen que la información propiedad de la Institución o en su custodia, será manejada con base en los requerimientos de confidencialidad de la misma. Estos contratos deben ser suscritos por todos los usuarios.

Sin embargo, se sebe tener presente que aún y cuando el Ministerio no solicitara la suscripción de dichos contratos o acuerdos de confidencialidad, la obligación impuesta por ley subsiste, incluso una vez terminada la relación del usuario para con la Institución.

10.2. De los controles para garantizar la confidencialidad, integridad y accesibilidad de la información propiedad del Ministerio y/o en su custodia

Se deben establecer e implementar los controles necesarios para garantizar la confidencialidad, integridad y accesibilidad de la información propiedad del Ministerio y/o en su custodia, de manera que la misma sólo pueda ser accedida por quienes hayan sido debidamente autorizados para conocerla; se resguarde su exactitud, fidelidad, veracidad y se asegure que la misma sea completa y esté disponible para los autorizados, cuando así la necesiten.

[1] Al respecto ver *Ley 7975 "Ley de Información no Divulgada"*; art. 7; *Código Penal*, artículos 203 y 339 y *Código de Comercio*, art. 615.

Dichos controles deben ser consecuentes con el análisis de riesgo llevado a cabo para tales efectos y con el nivel de riesgo residual aceptado por la Administración Superior.

Corresponderá al Encargado de Seguridad establecer los controles mencionados y a la Comisión de Seguridad aprobarlos.

10.3. Conflictos de interés

Todos los funcionarios deben evitar conflictos de interés reales o aparentes, en su proceder comercial con la Institución. De haber alguna duda sobre la existencia de conflictos potenciales de interés o de efectivamente surgir los mismos, el funcionario involucrado deberá avisar inmediatamente a su superior jerárquico, a fin de que se pueda encontrar una solución viable que no dañe a ninguna de las partes, ni mucho menos a los Administrados del Ministerio.

10.4. Aseguramiento de la información previa ausencia (por vacaciones, permisos, incapacidades y/o rotación)

Antes de proceder a ausentarse de sus labores para con el Ministerio, todo usuario de los sistemas informáticos y de los recursos de la Institución, deberá asegurarse de implementar los controles adecuados para proteger la seguridad de la información a su cargo.

10.5. Información de los Administrados en lugares de acceso no restringido

No debe nunca discutirse la información de los Administrados del Ministerio, ni la clase de servicio que se les brinda, en lugares de acceso no restringido ni fuera de las instalaciones de la Institución, a menos que se cuente con autorización expresa y por escrito del cliente para hacerlo. Esta Norma debe aplicar, aún cuando no se dé a conocer la identidad del cliente, pero la misma pueda inferirse fácilmente.

10.6. Información sometida a requerimientos de confidencialidad y lugares de acceso público

No debe examinarse, ni discutirse información sometida a requerimientos de confidencialidad en lugares de acceso público.

10.7. Privacidad de la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada, creada y/o eliminada en los sistemas del Ministerio

La información que se almacena, transita, es recopilada, distribuida, reproducida, procesada, creada y/o eliminada en los sistemas que el Ministerio facilita con ocasión de la realización de labores a sus funcionarios, será considerada propiedad del Ministerio y por lo tanto es de su interés directo. No podrá el usuario pretender reclamar derecho personal alguno de privacidad sobre la misma, frente a los derechos e intereses legítimos de la Institución.

El Ministerio a su vez, se reserva el derecho de acceso a tal información, cuando así lo estime conveniente, a fin de cumplir con el deber que le impone la ley de proteger adecuadamente los bienes y la información propiedad de éste y/o bajo su custodia, y

ejercer además, el derecho de administrar eficazmente y protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los usuarios. Todo de conformidad con lo que establezca el ordenamiento jurídico.

No obstante, como una consideración excepcional y estrictamente potestativa del Ministerio, éste podría, eventualmente y a su propia conveniencia, decidir poner a disposición de sus funcionarios, equipos informáticos para usos no laborales. En caso de que el Ministerio dispusiera proveer estos equipos para usos no laborales, los mismos serán claramente y previamente determinados como tales, funcionarán de forma aislada independiente completamente de la red de la Organización, y serán utilizados conforme al reglamento de uso que se establezca a los efectos. Dado que la información contenida, transmitida, transportada, almacenada, borrada, eliminada o en tránsito que se encuentre en esos equipos no podrá ser accedida en su contenido por el Ministerio, salvo situaciones de excepción permitidas por el ordenamiento jurídico costarricense, cada usuario será responsable único y absoluto por el uso de tales equipos durante el tiempo en que los utilice. Así, a fin de individualizar a cada usuario en particular, se le asignará una clave de identificación única, de manera tal que si llevara a cabo comportamientos anómalos o ilegales, debe responder por los mismos hasta las últimas consecuencias, al punto de tener que indemnizar al Ministerio, debiendo incluso cubrir la defensa legal del mismo, si éste se viere directa o indirectamente involucrado, esto sin perjuicio alguno del deber que tendrá también el usuario de indemnizar por sí mismo a cualquier tercero que resultare agraviado o perjudicado. El usuario de estos equipos destinados a usos no laborales debe tener presente que pese a que el Ministerio no conocerá ilegítimamente los contenidos de los archivos que allí se encuentren, sí llevará registro de quién utiliza los utiliza y en qué momento.

La utilización de éstos equipos aislados debe ser racional y legal en todo momento, y dado que tendrá el carácter de mera consideración del Ministerio hacia sus funcionarios, en caso de que en algún momento llegase a ser abusiva o inconveniente para la Institución, ésta, dentro de los límites permitidos por el ordenamiento, podrá limitarla y/o eliminarla sin asumir por ello responsabilidad alguna, dado que la ley no le obliga a tolerar abusos.

10.8. Integridad de la información

Será obligación de todo usuario reportar por los medios y canales provistos por la El Ministerio de Cultura y Juventud, cualesquier situación que pudiese comprometer la integridad (i.e. exactitud, fidelidad y veracidad) de la información del Ministerio y/o en su custodia.

11. De los respaldos y recuperación de la información

11.1. Respaldos de la información del Ministerio

La información crítica del Ministerio y/o en su custodia debe ser debidamente respaldada, de conformidad con los procedimientos y esquemas de respaldo expresamente aprobados por la Institución.

Si bien los respaldos habrán de ser realizados únicamente por Responsables Asignados por el Ministerio a tales efectos, cada usuario tendrá la responsabilidad de velar porque la información bajo su cuido, sea debidamente respaldada según el esquema de respaldos oficial, de manera que de no haberse realizado ésta en el tiempo debido, el usuario deberá informarlo a la brevedad.

11.2. Respaldos de la información del Ministerio

La información esencial del Ministerio debe ser respaldada y resguardada en instalaciones seguras y controladas, a fin de que pueda recuperarse una vez ocurrido un desastre, emergencia o falla en/de los dispositivos y/o sistemas de información.

Todos los procedimientos y controles que se establezcan en materia de respaldo de la información, deben ser periódicamente evaluados, de conformidad con las disposiciones del plan de continuidad del negocio, aprobado por el Ministerio.

Deben como mínimo, crearse los siguientes controles:

a) Los respaldos deben responder y ser consistentes con los niveles de clasificación que se haya hecho de la información de que se trate;
b) Se deben mantener registros de las copias de respaldo, así como de los procedimientos aprobados de restauración de la información;
c) La extensión (i.e. totales o parciales) y frecuencia de los respaldos debe responder a la criticidad de la información que se maneja; a los requerimientos propios del MCJ; a los riesgos propios de los equipos (equipos portátiles son más propensos a riesgos) y a la normativa en materia de seguridad;
d) Se debe almacenar, en una ubicación alterna, la información de respaldo, junto con sus registros exactos, actualizados y completos, así como con los procedimientos documentados de restauración. La ubicación alterna debe estar lo suficientemente lejos del sitio principal, para así evitar que el desastre en éste, pueda provocar daños a la información respaldada;
e) Se debe proporcionar a la información de respaldo un nivel de protección física y ambiental, consecuente con los niveles de protección física y ambiental implementados en el sitio principal. Los controles aplicados a los Recursos Informáticos en el sitio principal, deben ser replicados en la ubicación alterna;
f) Se debe asegurar que la información respaldada se resguarde, al menos, por todo el plazo requerido por el Ministerio y/o por el ordenamiento jurídico aplicable;
g) Se deber evaluar y verificar los procedimientos de restauración, de forma periódica, a fin de verificar su efectividad, dentro de los plazos establecidos;
h) Se debe asegurar que previa restauración de la información de que se trate, se lleve a cabo una copia de los mismos, a fin de evitar su pérdida o corrupción;
i) Para información sometida a requerimientos de confidencialidad, los respaldos deben hacerse utilizando los mecanismos criptográficos aprobados por la Institución; y

j) Tratándose de sistemas y/o procesos críticos, deben respaldarse todos los sistemas de información, las aplicaciones y los datos necesarios para ponerlo en completa operación, en caso de desastre.

Todos los procedimientos y controles que se aprueben en este sentido, deben ser conformes con el análisis de riesgos llevado a cabo para tales efectos; el nivel de riesgo residual aceptado por la Administración Superior, la normativa aprobada por el Ministerio, en materia de seguridad de la información y los requerimientos legales aplicables.

Corresponderá al Encargado de Seguridad elaborar los controles que deban aplicarse para efectuar respaldos, así como al Responsable Asignado del sistema o en su caso, al dueño de proceso correspondiente, definir los procedimientos necesarios. Tanto los procedimientos como los controles, deben ser aprobados por la Comisión de Seguridad.

11.3. Asignación de responsabilidades en la realización de respaldos de información

Los procedimientos y controles en materia de respaldos de información deben definir y establecer claramente las responsabilidades en la realización de los mismos. Los responsables deben ser capaces no sólo de generar los respaldos necesarios, sino de recuperar la información en caso de ser necesario.

11.4. Alcance de los respaldos

Todo respaldo debe considerar tanto los datos de la aplicación (e.g. archivos y bases de datos, entre otros), como los demás elementos necesarios para asegurar la prestación del servicio, tales como el software de la aplicación, las configuraciones y parámetros de operación, documentación complementaria a los procesos, software ambiental, entre otros.

11.5. Estandarización de los medios de respaldo

Los medios de respaldo del Ministerio responderán a un estándar institucional, debidamente aprobado por la Comisión de Seguridad.

12. De los procedimientos de manejo de la información

12.1. De los procedimientos necesarios para evitar el uso inadecuado o divulgación no autorizada de la información

Dependiendo de la clasificación de la información adoptada por el Ministerio, se deben elaborar, aprobar y documentar procedimientos formales para el manejo y almacenamiento de la información propiedad del Ministerio y/o en su custodia, a fin de protegerla contra su uso o divulgación no autorizada y a la vez, garantizar su disponibilidad, confidencialidad e integridad en todo momento. Estos procedimientos deben incluir niveles de autorización y deben contemplar el manejo de la información

contenida, almacenada y/o en tránsito en cualesquier tipo de medios, incluyendo pero sin limitarse a medios atómicos (i.e. papel), digitales, analógicos, e informáticos.

Corresponderá al Encargado de Seguridad, definir dichos procedimientos y a la Comisión de Seguridad, aprobarlos.

12.2. De la obligación de acatar los procedimientos aprobados para el manejo y almacenamiento seguro de la Información

Los procedimientos aprobados por la Institución para el manejo, procesamiento, almacenamiento y comunicación segura de la información del Ministerio, de los Administrados y/o en su custodia, según la clasificación adoptada, deben ser estrictamente acatados e implementados por todos los usuarios.

El MCJ deberá adoptar procedimientos adecuados tendientes a garantizar al menos:

a) El ingreso seguro y controlado de datos a los sistemas del Ministerio;
b) La protección de los datos en espera;
c) El procesamiento correcto de los mismos; y
d) La validación de las salidas.

12.3. Registro formal de los receptores autorizados de datos

Todo Responsable Asignado de los recursos de información debe mantener un registro formal de los receptores autorizados de la información bajo su tutela. Estos receptores autorizados serán aquellos quienes el creador de la información designe como tales y/o el Ministerio autorice expresamente.

La información crítica o sensible del MCJ, de los Administrados y/o en su custodia, así como aquella sometida a criterios de confidencialidad nunca debe ser develada a personas o entes no autorizados.

Con regularidad deberá revisarse los registros formales de los receptores autorizados de información. Estos registros deberán ponerse a disposición de la Auditoría Interna del Ministerio.

12.4. Resguardo protegido de medios de almacenamiento de información

Deben idearse, documentarse e implementarse estrictamente:

a) Controles lógicos y físicos para el adecuado resguardo de los medios de almacenamiento de información, según los criterios de clasificación de la información contenida en ellos;
a) Las condiciones óptimas de resguardo físico de los medios de almacenamiento, según las recomendaciones del fabricante, tendientes a garantizar la integridad y disponibilidad de la información contenida en éstos.

13. Restricción del acceso a la información

13.1. Controles para la restricción del acceso a las aplicaciones

Se deben establecer al menos los siguientes controles para la restricción de acceso a las aplicaciones:

a) Proveer menús para controlar el acceso a las funciones de los sistemas de aplicación;
b) Restringir el conocimiento de los usuarios únicamente a las aplicaciones a las que ellos han de acceder en virtud de sus actividades para con la Institución;
c) Limitar los derechos de los usuarios dentro de los sistemas, a los estrictamente requeridos para la realización de sus labores para con el Ministerio (e.g. escritura; lectura, eliminar y ejecutar);
d) Procurar que las salidas de los sistemas de aplicación que administran información sensible, contengan solo la información que resulte necesaria para el uso de la misma y que ésta se envíe solamente a las estaciones de trabajo y ubicaciones autorizadas; y
e) Revisar periódicamente las salidas a fin de garantizar la remoción de la información redundante.

Los controles deben establecerse con base en el análisis de riesgo llevado a cabo para tales efectos y con base en el nivel de riesgo residual aceptado por la Administración.

14. Áreas aisladas

14.1. Información sometida a requerimientos de confidencialidad y áreas aisladas

Toda la información, propiedad del Ministerio y/o en su custodia, sometida a requerimientos de confidencialidad debe ser almacenada en áreas aisladas, seguras y controladas. Para ello, debe haberse predefinido la criticidad y clasificación de la información y de los sistemas que se desean proteger, a fin de instaurar sólo aquellos controles que sean necesarios.

15. Medios de almacenamiento

15.1. Medios de almacenamiento y manejo de los mismos para el resguardo efectivo de los registros importantes del Ministerio

Los medios de almacenamiento autorizados por el Ministerio para el resguardo de sus registros importantes, deben utilizarse de conformidad con las recomendaciones y estipulaciones del fabricante, a fin de garantizar su conservación y por consiguiente, la integridad de los registros almacenados. Deben tomarse en consideración las necesidades de retención y de acceso a la información por todo el plazo requerido, para lo cual, debe considerarse la capacidad y durabilidad de los medios autorizados. Los medios de almacenamiento deben rotularse según los procedimientos de rotulación aprobados por el Ministerio.

16. Aspectos Legales referentes al intercambio de información y software

16.1. Intercambio de información y/o software

El Ministerio establecerá las Políticas, Estándares, Procedimientos, Lineamientos, y niveles de autorización necesarios para el intercambio legal y seguro de información, así como de software con terceras personas y organizaciones.

Dichas Políticas, Estándares, Procedimientos y Lineamientos, así como niveles de autorización deben ser estrictamente observados por cada usuario, de manera que se garantice que los intercambios solamente se llevarán a cabo, cuando éstos:

a) Hayan sido expresamente autorizados por quien válidamente pueda brindar dicha autorización;
b) Se ejecuten con destinatarios debidamente autorizados para recibir dicha información y/o software;
c) Sean legales conforme la legislación de los países involucrados en el intercambio;
d) Respeten los acuerdos y obligaciones suscritos por el Ministerio; y
e) Se lleven a cabo por medios seguros debidamente aprobados por el Ministerio.

16.2. Aspectos legales a tomar en consideración para el intercambio de información y/o software

Los intercambios de información y software, sólo deben autorizarse en las condiciones de legalidad permitidas por las legislaciones de los países involucrados en estos intercambios y en absoluto respeto de los acuerdos y obligaciones suscritos por el Ministerio.

Debe requerirse la asesoría de la Asesoría Jurídica, cuando se tenga duda sobre las condiciones de legalidad de cualesquier tipo de intercambio de información y/o software.

Los procedimientos para el intercambio de información y/o software, así como los niveles de autorización requeridos, deben ser claramente documentados por el Ministerio.

16.3. Acuerdos con terceros para el intercambio de información y software

Todas las estipulaciones, incluyendo obligaciones y responsabilidades, tanto del Ministerio como de terceros para el intercambio seguro y legal de información y software, deben quedar debidamente plasmadas en los acuerdos suscritos con esos terceros, para tales efectos. De esta forma, deben quedar plasmadas las estipulaciones con respecto a:

a) La confidencialidad de la información compartida;
b) Los canales por los cuales se va a manejar dicha información y/o software y la seguridad de los mismos;
c) La obligación de establecer Políticas, Estándares, Procedimientos y Lineamientos para la adecuada tutela, manejo, clasificación, rotulado, envío (digital o físico, incluyendo controles para contratación de empresas de

mensajería), recepción, copia, resguardo, distribución, transmisión, utilización, almacenamiento y eliminación de la información y/ software de que se trate;

d) Los procedimientos a utilizar para identificar la clasificación de la información o software involucrado en el intercambio, así como para interpretar el rotulado llevado a cabo por otras instituciones;
e) Los procedimientos aprobados de detección y protección contra instrucciones maliciosas;
f) Los procedimientos aprobados para asegurar pistas de auditoría y el no repudio;
g) La obligación y los alcances de la custodia de dicha información y/o software, incluyendo responsabilidades de carácter gerencial;
h) Los requerimientos técnicos mínimos para el envío y transmisión de paquetes de información;
i) Los estándares técnicos acordados para registro y lectura de la información o software;
j) Los acuerdos específicos para la tutela de información o el software dado en custodia;
k) Las responsabilidades y obligaciones en caso de pérdida de datos;
l) La propiedad de la información y/o el software y demás aspectos de Propiedad Intelectual y Autoría; y
m) La definición de controles especiales a aplicar, a fin de proteger ítems en extremo sensibles (incluyendo controles criptográficos).

Debe solicitarse la asesoría de la Asesoría Jurídica, a la hora de suscribir dichos acuerdos, a fin de asegurar que los mismos no violentan la legislación aplicable, ningún otro tipo de obligaciones asumidas por el Ministerio, y/o derechos preferentes de terceros.

17. Recolección y protección de la evidencia

17.1. Prohibición de violentar la evidencia que le pueda servir al Ministerio para establecer acciones contra personas físicas o jurídicas

Está absolutamente prohibido siquiera intentar violentar (e.g. alterar, modificar, eliminar) cualesquier tipo de evidencia que le pueda servir al Ministerio para establecer acciones en contra de personas físicas o jurídicas.

17.2. La importancia de la evidencia en la toma de acciones en contra de personas físicas y/o jurídicas y de la proporcionalidad de la sanción

A fin de respaldar cualesquier acción en contra de una persona física o jurídica, se debe contar con evidencia legalmente válida, que demuestre fehacientemente la comisión del hecho punible. Cualquier acción que se haya de tomar, debe sustentarse en evidencia completa, exacta, fidedigna, veraz y concluyente.

Toda acción que se tome en contra de una persona física o jurídica debe ser proporcional a la gravedad del hecho punible y debe ser conforme a Derecho.

De previo a la toma de cualesquier acción de cualquier naturaleza en contra de una persona física o jurídica, debe solicitarse la asesoría de la Asesoría Jurídica, a fin de garantizar el debido proceso y el derecho de defensa del presunto implicado.

17.3. Reglas para la recolección de evidencia

A fin de asegurar que la evidencia recolectada sea legalmente válida, ésta debe cumplir estrictamente con los requerimientos que la ley aplicable exige. Corresponderá a la Asesoría Jurídica identificar cuáles son esos requerimientos normativos y documentarlos adecuadamente.

En la documentación de los requerimientos normativos que garanticen la eficacia de la prueba recolectada, debe al menos tomarse en cuenta:

a) La recolección legal de la evidencia: Requisitos para asegurar que la evidencia se recopile conforme a lo estipulado por la legislación aplicable y que todo el proceso de recolección sea legítimo (e.g. que se establezca un registro detallado de quién hizo el hallazgo, cuándo se halló, quien lo presenció, así como la hora y fecha del mismo y su descripción);
b) La validez de la evidencia: Requisitos para asegurar que la evidencia a recolectar sea válida ante las autoridades correspondientes (incluyendo el poder garantizar que los equipos y sistemas de información del Ministerio cumplen con los estándares y mejores prácticas en materia de producción de evidencia válida);
c) El peso de la evidencia: Requisitos para asegurar que la evidencia sea completa, exacta, fidedigna, veraz y concluyente;
d) Prueba de manejo íntegro de la evidencia: Requisitos para demostrar que en todo el proceso de almacenamiento y procesamiento de la evidencia, ésta mantuvo su integridad y no fue en manera alguna alterada.

Toda la evidencia que se recopile debe protegerse contra toda alteración que la pueda desvirtuar.

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.