Departamento de Informática

DI-PO-07-2014

Política de disposición o eliminación de activos de tecnología

Fecha de envío:
Enero, 2014

1. Objetivo

La presente política tiene como objetivo proveer una guía básica sobre las medidas a tomar, para eliminar y/o volver a disponer de manera segura, los equipos informáticos de la Institución, a fin de resguardar a su vez, la información en ellos contenida.

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 Terceros ajenos al Ministerio:

Comprende todas aquellas personas físicas y/o jurídicas que no laboran directamente para El Ministerio de Cultura (incluyendo pero sin limitarse a personas o instituciones a las que se les brinda servicio, proveedores, contratistas, asesores, entre otros).

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

El Ministerio de Cultura y Juventud está en la obligación de proteger la información que le pertenece y/o que se encuentra en su custodia, de accesos no autorizados. Para ello, deberá asegurar su manejo adecuado durante todo el ciclo de la misma, pasando desde su creación, inserción a los sistemas, y transmisión, hasta su salida. Es precisamente el manejo seguro en la eliminación y re-disposición de equipos que contienen dicha información, a lo que se aspira con las presentes políticas.

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. Eliminación segura de activos físicos

9.1. De los procedimientos para la eliminación de los activos físicos

El Encargado de Seguridad creará los procedimientos necesarios para la eliminación segura de los activos físicos del Ministerio que contengan o puedan contener Información Confidencial o información sensitiva del Ministerio o en su custodia. Estos procedimientos deben ser aprobados por la Comisión de Seguridad.

El método o métodos elegidos por el Ministerio para la eliminación de sus activos físicos, debe elegirse con base en:

a) El análisis de riesgo llevado a cabo para tales efectos; y
b) El nivel de riesgo residual aceptado por la Administración Superior.

9.2. Eliminación de activos físicos

Ningún usuario podrá eliminar activos físicos, sin antes contar con autorización expresa válidamente emitida por el Ministerio, para ello. Toda eliminación de activos físicos corresponderá a personal autorizado debidamente capacitado.

Toda omisión o violación a esta política que derive en consecuencias dañosas para el Ministerio y/o los Administrados, será gravemente castigada y el infractor será hecho personalmente responsable por las mismas. El Ministerio tomará todas las medidas administrativas, laborales, civiles y/o penales que la ley le permite para sancionar a los responsables.

9.3. Reparación versus eliminación de medios de almacenamiento de información sensitiva

Debe hacerse un análisis de riesgo de previo a decidir si reparar o eliminar equipos de almacenamiento de Información Confidencial o sensitiva, que se hayan dañado.

9.4. Eliminación de medios de almacenamiento que contengan información sensitiva

Previo a ser descartados, los medios de almacenamiento que contienen material sensitivo deben ser físicamente destruidos o sobrescritos de forma segura en vez de utilizar funciones de borrado estándar. La eliminación de los activos físicos debe

hacerse conforme los procedimientos establecidos y aprobados por el Ministerio y debe obedecer a criterios de necesidad.

No deben eliminarse activos físicos, sin la debida autorización del Ministerio, para tales efectos.

10. Reutilización de activos físicos

10.1. De los procedimientos previos a la reubicación de activos dentro y fuera del Ministerio

El Encargado de Seguridad Informática debe crear procedimientos seguros para el borrado o eliminado (según lo determine el respectivo análisis de riesgo a ser llevado a cabo para tales efectos y según el nivel de riesgo residual aceptado por la Administración Superior) de la información contenida en los activos físicos que serán reubicados dentro del Ministerio mismo y/o colocados fuera de la Institución. Estos procedimientos deben ser aprobados por la Comisión de Seguridad.

10.2. Reubicación de los activos físicos dentro y fuera del Ministerio

Previa reubicación de activos físicos dentro y fuera del Ministerio, deben seguirse los procedimientos aprobados por el Ministerio para el respaldo, borrado y/o eliminación segura de la información contendida en dichos activos físicos.

11. Eliminación de medios informáticos

11.1. Eliminación de medios informáticos de almacenamiento

La eliminación de medios informáticos de almacenamiento que contengan Información Confidencial, crítica, sensitiva o de Uso Interno del Ministerio, debe ser llevada a cabo únicamente por personal autorizado, y en estricto cumplimiento con los procedimientos documentados y aprobados por la Institución para tales efectos. .

11.2. Procedimientos para la eliminación de medios informáticos de almacenamiento

El Encargado de Seguridad será el responsable de elaborar los procedimientos para la eliminación segura y controlada de los distintos medios informáticos de almacenamiento utilizados por el Ministerio. Los procedimientos deben ser consecuentes con la sensibilidad de la información contenida en los medios, y deben contemplar también los niveles de autorización necesarios, de previo a que la respectiva eliminación se lleve a cabo. El Encargado de Seguridad será el responsable de proponer tales procedimientos y la Comisión de Seguridad quien los valide.

11.3. Eliminación de medios informáticos de almacenamiento por parte de terceros

No se confiará a terceros la destrucción de sus medios informáticos de almacenamiento, sin antes asegurarse que la Información Confidencial, crítica o de Uso Interno ha sido debidamente eliminada de los mismos.

11.4. Registro de los medios eliminados

Tratándose de medios informáticos de almacenamiento que contengan información crítica o sensitiva, su destrucción así como el mecanismo elegido para ello, deben ser documentados en un registro formal que se llevará a los efectos, a fin de éste constituya una pista de auditoría.

11.5. Prohibición de acumular medios de almacenamiento para su eliminación

Una vez autorizada por el Ministerio, la eliminación de los medios de almacenamiento de información debe hacerse de manera gradual, aún cuando se trate de información no sometida a requerimientos de confidencialidad, esto porque la acumulación de información no sensitiva puede dar a conocer información clasificada como confidencial. Por ende, no se recomienda la acumulación de información a ser eliminada, sin antes prever y proveer protección para la misma.

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.