Departamento de Informática

DI-PO-12-2014
Política sobre el uso del antivirus

Fecha de envío:
Enero, 2014

Política sobre el uso de antivirus

1. Objetivo

La presente política tiene como objetivo establecer los requerimientos que en materia de antivirus deben ser satisfechos, para todos los equipos computacionales conectados de manera lógica o física, a los sistemas informáticos o redes del Ministerio de Cultura y Juventud, a fin de prevenir y detectar de manera efectiva, instrucciones maliciosas.

2. Alcance

Estas políticas son aplicables a todos los usuarios de equipos computacionales que hayan de ser conectados a los sistemas informáticos del Ministerio de Cultura y Juventud, incluyendo tanto los ubicados en los edificios de la Institución, como en sitios externos.

3. Definiciones

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

- **Antivirus:** Programa informático cuyo propósito es el de detectar y eliminar virus y otros instrucciones maliciosas antes o después de que ingresen al sistema.
- **Equipos Computacionales:** Incluye computadores de escritorio, laptops, dispositivos móviles, y servidores.
- **Freeware:** Se refiere a un tipo de aplicaciones que se distribuyen sin costo por un tiempo determinado.
- **Shareware:** una modalidad de distribución de software, por medio de la cual el usuario evalúa de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales[1].

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 la pertenece y/o que se encuentra en su custodia, de instrucciones maliciosas. Así las cosas, con el fin de mantenerse alerta ante la presencia de virus, y de poder responder adecuadamente para prevenirlos o administrar sus consecuencias, es que se aprueban estas políticas de uso de antivirus.

[1] http://es.wikipedia.org/wiki/Shareware.

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. Protección contra instrucciones maliciosas

El objetivo de la presente sección es proteger la integridad, disponibilidad y confidencialidad del software y de la información, de instrucciones maliciosas que los puedan dañar, corromper, o comprometer de cualquier manera.

10. Uso del Antivirus y algunas mejores prácticas en la prevención de infestación

10.1. Responsabilidad del Personal Usuario con respecto a la aplicación del antivirus aprobada por el Ministerio

Todo el Personal Usuario debe tener instalada y efectivamente activa, en el equipo computacional que utiliza en el Ministerio, la aplicación antivirus formalmente aprobada, corriendo en su última versión, antes de proceder a conectarse a los sistemas de la Institución.

A menos que cuente con autorización expresa y por escrito válidamente emitida para tales efectos, ningún usuario debe por su propia cuenta y por ninguna razón, deshabilitar las aplicaciones de antivirus instaladas en los equipos de la Institución.

Toda instalación o desinstalación de las aplicaciones de antivirus, será llevada a cabo únicamente por personal del Departamento de Informática.

10.2. Prohibición del Personal Usuario de tratar de eliminar una instrucción maliciosa por sus propios medios

El Personal Usuario, no debe bajo ninguna circunstancia tratar de eliminar instrucciones maliciosas de los equipos y/o sistemas conectados a la red del Ministerio, por sus propios medios. Ante la mera sospecha de la existencia de una instrucción maliciosa en los sistemas del Ministerio, el usuario debe proceder inmediatamente a hacer uso de los

canales formalmente aprobados para hacer el respectivo reporte, ante el Encargado de Seguridad.

10.3. Instalación y actualización de software antivirus en equipo aprobado

Solamente quienes hayan sido debidamente encargados a los efectos, procederán a instalar el software antivirus que la Institución haya previamente aprobado y que cuente con su respectiva licencia. Este software se instalará únicamente en aquellos equipos computacionales que haya sido, a su vez, previamente autorizados.

10.4. Prohibición de utilizar cualesquier software no licenciado y/o no autorizado por el Ministerio

A menos que expresamente se estipule lo contrario, está absolutamente prohibida la instalación y/o utilización de cualesquier tipo de software no licenciado y/o no autorizado, en los equipos o sistemas conectados a la red de la Institución, incluyendo pero sin limitarse a “freeware” o “shareware”.

10.5. Archivos y/o software proveniente de fuentes desconocidas

No deben ejecutarse archivos ni software que provengan de fuentes desconocidas 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 pueda contener información de importancia para el Ministerio, debe contactarse inmediatamente al Encargado de Seguridad, para que este pueda accederla en un ambiente controlado.

11. Escogencia y administración de la plataforma Antivirus

11.1. Escogencia y aprobación de al menos una aplicación antivirus para el Ministerio

En pleno cumplimiento con las Políticas, Estándares, Lineamientos, y Procedimientos formalmente aprobados por el Ministerio, para el desarrollo, adquisición, modificación, y actualización de sus sistemas, se debe escoger y estandarizar el uso de al menos una aplicación de antivirus que provea la protección contra instrucciones malignas que la Institución necesita. Esta aplicación debe mantenerse permanentemente actualizada y licenciada corporativamente, para todas las redes, sistemas y estaciones de trabajo, tomando en cuenta las expectativas de crecimiento de la Institución. Asimismo, debe proporcionarse capacitación suficiente y constante a quienes administren la plataforma escogida.

11.2. Administración de la plataforma de antivirus

Corresponderá al Departamento de Informática la administración de la plataforma de antivirus, de modo que la misma se mantenga funcionando óptimamente y

permanentemente actualizada. El personal del Departamento de Informática tendrá la responsabilidad de mantenerse capacitado en la herramienta, de manera que pueda sacarle el mejor provecho en beneficio del Ministerio.

11.3. Revisión periódica de los equipos y sistemas conectados a la red del Ministerio a efectos de controlar instrucciones maliciosas

En la sana administración de los sistemas y a fin de evitar y controlar instrucciones maliciosas, el Departamento de Informática del Ministerio debe llevar a cabo revisiones periódicas a/en sus sistemas y equipos, dirigidas a garantizar que los mismos se encuentran libres de códigos malignos, así como asegurar que los usuarios posean instalado el software estándar y/o aprobado por la Institución. Las revisiones se realizarán únicamente dentro del ámbito permitido por ley.

Toda modificación no aprobada así como la presencia de archivos y/o software no autorizado, debe ser reportada al Encargado de Seguridad, por los medios provistos para el reporte de incidentes de seguridad.

11.4. Revisiones esporádicas de los equipos y sistemas conectados a la red

Cuando así se estime conveniente, y en pleno apego al ordenamiento jurídico costarricense, se debe proceder a la revisión de los equipos y sistemas del Ministerio que se considere pueden estar comprometiendo la seguridad de la Institución. Así, el Encargado de Seguridad procederá, en la sana administración de los sistemas informáticos, a hacer dichas revisiones.

Las revisiones se realizarán únicamente dentro del ámbito permitido por ley.

11.5. Plan de continuidad y recuperación frente a virus

Los planes de continuidad del Ministerio, deben contemplar entre otras cosas, provisiones para la recuperación rápida y eficiente ante ataques por virus, incluyendo protección de la información de la Institución y de los Administrados, el resguardo de los sistemas y las disposiciones para su recuperación.

11.6. Procedimientos para la verificación de toda información relativa a instrucciones maliciosas

El Encargado de Seguridad deberá proponer procedimientos para verificar que toda la información relativa a instrucciones maliciosas es cierta y válida y garantizar así, que los boletines de alerta son exactos e informativos. Las fuentes que se utilicen deben ser fuentes reconocidas y calificadas. Los procedimientos propuestos por el Encargado de Seguridad deben ser avalados por la Comisión de Seguridad.

Debe concientizarse al personal acerca del problema que ocasionan los falsos virus (hoax) y qué hacer al recibirlos.

11.7. De los controles contra puertas ocultas y códigos troyano

Se deben establecer controles dirigidos a procurar evitar la instalación de puertas ocultas y código troyano en los sistemas del Ministerio. Así, los controles mínimos que deben aplicarse serán:

a) Adquirir programas únicamente de proveedores acreditados;
b) Adquirir programas en código fuente de manera que el mismo pueda ser verificado, cuando ello aplique;
c) Utilizar productos previamente evaluados;
d) Examinar todo el código fuente antes de pasar un programa a producción, cuando ello aplique;
e) Controlar el acceso y las modificaciones al código una vez instalado el mismo; y
f) Emplear personal de probada confiabilidad para trabajar en los sistemas críticos.

11.8. Precauciones adicionales durante procedimientos de emergencia y de mantenimiento

Los controles convencionales contra instrucciones maliciosas pueden devenir insuficientes, ante la aplicación de procedimientos de emergencia y/o de mantenimiento. En razón de ello, deben establecerse controles específicos para esos casos, que permitan brindar una protección adecuada. Corresponderá al Encargado de Seguridad establecer dichos controles y a la Comisión de Seguridad, validarlos.

11.9. Revisión periódica de los equipos y sistemas conectados a la red del Ministerio a efectos de controlar instrucciones maliciosas

En la sana administración de los sistemas y a fin de evitar y controlar instrucciones maliciosas, el Departamento de Informática del Ministerio deberá llevar a cabo revisiones periódicas a/en sus sistemas y equipos, dirigidas a garantizar que los mismos se encuentran libres de códigos malignos, así como asegurar que los usuarios posean instalado el software antivirus estándar y/o aprobado por la Institución. Las revisiones se realizarán únicamente dentro del ámbito permitido por ley, para lo cual debe contarse de previo con la asesoría experta de la Asesoría Jurídica.

Toda modificación no aprobada así como la presencia de archivos y/o software no autorizado, debe ser reportada al Encargado de Seguridad, por los medios provistos para el reporte de incidentes de seguridad.

11.10. Implementación de los controles contra puertas ocultas y códigos troyano

Quienes hayan sido debidamente encargados a los efectos, deberán implementar estrictamente los controles contra puertas ocultas y código troyano, formalmente aprobado por la Institución.

11.11. Implementación de controles específicos en casos de procedimientos de emergencia y de mantenimiento

Los controles convencionales contra instrucciones maliciosas pueden devenir insuficientes, ante la aplicación de procedimientos de emergencia o de mantenimiento. En razón de ello, quienes hayan sido debidamente encargados a los efectos deben implementar los controles específicos para casos de emergencia o de mantenimiento, aprobados por la Institución.

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.

- **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; 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.