Departamento de Informática

DI-PO-10-2014
Política de acceso remoto

Fecha de envío:
Enero, 2014

1. Objetivo

La presente política tiene como objetivo mostrar los requerimientos básicos que han de cumplirse, así como las restricciones a imponerse, a las conexiones remotas que pretendan establecerse con/en los sistemas de información del Ministerio de Cultura y Juventud.

2. Alcance

Estas políticas son aplicables a todos los usuarios que utilicen el acceso remoto a los sistemas y Recursos Informáticos y de información de la Institución.

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. Acceso remoto:

Es cualquier conexión a las redes y sistemas informáticos y de información del Ministerio, establecida desde sitios externos (e.g. estaciones de teletrabajo, equipos móviles, dispositivos inalámbricos, entre otros).

3.2. Equipo informático ajeno autorizado:

Todo aquel equipo (e.g. computadores personales, computadores portátiles, agendas electrónicas, organizadores personales, teléfonos inteligentes, de nueva generación; dispositivos de almacenamiento masivo, tablets, palmtops, entre otros) que no siendo propiedad del Ministerio de Cultura, es utilizado bajo previa autorización, en actividades de su interés.

3.3. Personal Usuario o usuarios:

Los funcionarios, contratistas, vendedores, consultores, ciudadanos, Administrados, proveedores y/o aliados del MCJ a los que se les ha asignado el uso de Recursos Informáticos o se les ha proporcionado acceso a los sistemas de información.

3.4. Recursos Informáticos

Son todos aquellos recursos, sistemas, servicios, aplicaciones y/o medios de comunicación, que son propiedad del Ministerio de Cultura y Juventud y/o que son de su interés directo por ser utilizados para las labores propias de éste o en la ejecución de sus objetivos. Estos comprenden entre otros:

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 (energía eléctrica, iluminación, aire acondicionado).

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 no sólo las conexiones internas, sino también las externas, lo que implica establecer controles para el acceso remoto, procurando que el mismo se dé únicamente dentro de los parámetros autorizados. Con dicho fin, es que se aprueban las presentes Políticas de Acceso Remoto.

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. De la concesión de acceso remoto a los sistemas informáticos del Ministerio de Cultura

9.1. Acceso a los servicios de red de manera remota

La posibilidad de utilizar los servicios de la red de manera remota para los empleados de la Institución, debe ser una opción administrativa y no un derecho de todos los funcionarios. Asimismo, cuando se trate de brindarle acceso remoto a terceros, la decisión debe ser previamente analizada, fundamentada y tener su base en una necesidad comprobada de interés para la Institución.

El que un funcionario y/o tercero tenga este tipo de derecho es una decisión que debe ser tomada por la Administración Superior, previa comprobación de la necesidad laboral/contractual al respecto y previo análisis de riesgo llevado a cabo para tales efectos.

9.2. Acceso remoto a los servicios de red

Todo acceso remoto a los servicios de red, debe estar sometido a un sistema seguro de control de privilegios de acceso. El Encargado de Seguridad será quien deba definir los sistemas de control de privilegios de acceso, 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 Superior, mismos que deben ser aprobados por la Comisión de Seguridad.

10. Autenticación de usuarios para conexiones remotas

10.1. Autenticación y autorización para el acceso de usuarios remotos

Todo acceso de usuarios remotos a la red interna y a los sistemas informáticos del Ministerio debe estar sujeto a controles y mecanismos de autenticación y autorización. Estos controles y mecanismos 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 Superior.

Corresponderá al Encargado de Seguridad determinar los controles y mecanismos seguros de autenticación y autorización para el acceso de usuarios remotos a la red interna del Ministerio y a la Comisión de Seguridad, aprobar dichos mecanismos y controles.

11. Protección de los puertos de diagnóstico remoto

11.1. Controles para el acceso a los puertos de diagnóstico remoto

Para aquellos equipos que cuenten con capacidad de ser diagnosticados remotamente, el Ministerio debe establecer controles lógicos y físicos de acceso. Estos 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 Superior.

Corresponderá al Encargado de Seguridad determinar los controles seguros para el acceso a los puertos de diagnóstico remoto y a la Comisión de Seguridad, aprobar dichos mecanismos y controles.

12. Computación móvil y Teletrabajo

12.1. Seguridad del Teletrabajo

Se debe implementar la protección adecuada del sitio de Teletrabajo y de los Recursos Informáticos y de información utilizada con ocasión de éste, de manera que el grado de seguridad procurado sea equivalente al grado de seguridad deseado a lo interno del Ministerio.

Se debe asegurar que todas las disposiciones en materia de seguridad, así como los controles aprobados por la Institución aplicables al Teletrabajo o trabajo desde el hogar, sean estrictamente implementados. Para ello, se asignarán responsabilidades en la revisión periódica de los sitios de Teletrabajo y de los Recursos Informáticos involucrados.

Dichas revisiones serán conforme a Derecho y deben incluir al menos:

a) La valoración de los riesgos existentes;
b) La seguridad física existente en el sitio de Teletrabajo, tomando en cuenta la seguridad del edificio, así como la seguridad del ambiente local;
c) El ambiente propio de Teletrabajo propuesto;
d) Los requerimientos de seguridad de las comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas de la Institución; la sensibilidad de la información a la que se accederá y la vulnerabilidad de los sistemas de comunicaciones;
e) Las amenazas de acceso no autorizados a información o recursos por parte de terceros (e.g. vecinos, amigos, familiares, personal de limpieza);
f) El uso de redes caseras y los requerimientos o restricciones en la configuración de servicios inalámbricos; y
g) El uso de protección antivirus y de equipos firewall, aprobados por la Institución.

12.2. Disposiciones y controles en materia de seguridad del Teletrabajo

Se deben establecer e implementar controles y disposiciones en materia de seguridad del Teletrabajo que comprendan al menos:

a) La provisión por parte del Ministerio de mobiliario para el almacenamiento de los Recursos Informáticos involucrados;

b) La provisión por parte de la Institución, de equipo informático adecuado a los requerimientos de seguridad aprobados, cuando el equipo ajeno no cumpla dichos requerimientos;
c) La provisión por parte de la Institución, de capacitación y sensibilización adecuada en cuanto a los riesgos específicos que representa el Teletrabajo;
d) Establecimiento de los límites del trabajo permitido, con indicación del horario de trabajo; el manejo de la información según su clasificación; los sistemas internos del Ministerio, así como los servicios a los cuales el trabajador remoto puede acceder;
e) La provisión por parte de la Institución de un equipo de comunicación seguro, con inclusión de métodos para asegurar el acceso remoto;
f) La provisión por parte de la Institución, de aseguramiento para los equipos y sistemas utilizados;
g) Requerimientos mínimos a cumplir en materia de seguridad física;
h) Prohibiciones en cuanto a la utilización de los Recursos Informáticos por parte de terceros;
i) Procedimientos de respaldo;
j) Procedimientos para la continuidad de las operaciones;
k) Disposiciones en materia de auditoría y monitoreo de la seguridad;
l) Disposiciones en materia de anulación de derechos de acceso y devolución de los Recursos Informáticos al finalizar las actividades remotas;
m) Disposiciones con respecto a la utilización de software institucional en Equipo Informático ajeno autorizado;
n) Las políticas y procedimientos dirigidos a prevenir conflictos relacionados con derechos de autoría, propiedad intelectual y demás derechos conexos, que pudiesen surgir sobre trabajos realizados en equipo que no sea propiedad del Ministerio; y
o) Disposiciones en materia de anulación de derechos de acceso y devolución de los Recursos Informáticos, al finalizar las actividades remotas.

12.3. Uso permitido de equipos informáticos móviles

La Jefatura correspondiente asignará equipos informáticos móviles (e.g. agendas electrónicas; organizadores personales; computadores de mano; teléfonos celulares; computadores portátiles; llaves maya) a funcionarios que así lo necesiten en el desarrollo de sus labores para con la Institución. Estos equipos se asignarán excepcionalmente, con base en criterios de necesidad justificada y no crearán más derechos en los usuarios a los que les fueron asignados, que aquel de utilizarlos única y exclusivamente para efectos laborales. Usos ilegales y/o no autorizados serán debidamente sancionados.

Cuando así lo estime pertinente y sin necesidad de justificación alguna, el Ministerio podrá disponer de los mismos, retirarlos, cambiarlos y/o reasignarlos sin asumir por ello ninguna responsabilidad.

Estos equipos informáticos móviles deben utilizarse en estricto apego a la normativa en materia de Seguridad de la Información aprobada por el Ministerio y estarán sometidos a controles y revisiones según así lo disponga la Institución.

Los usuarios a quienes se les haya asignado equipos informáticos móviles, serán personalmente responsables de todo lo que ocurra con éstos, así como de lo que ocurra con la información que transita, se almacena y/o se resguarda en ellos, por lo tanto, deben tomar todas las medidas establecidas por el Ministerio, así como todas las demás medidas razonables a su alcance, para su protección.

12.4. Actualización de controles de seguridad en equipos informáticos móviles

Los equipos informáticos móviles deben tener debidamente implementados todos los controles y mecanismos de seguridad que el Ministerio haya aprobado aplicables a los mismos, por ende los usuarios a los que se les haya asignado éstos, estarán en la obligación irrefutable de poner a disposición de la Institución dichos recursos, en el momento en que así se les solicite.

Quien obvie o violente lo aquí estipulado, debe acarrear personalmente con todas las consecuencias adversas que de su actuar u omisión deriven, incluso al punto de deber sufragar por su propia cuenta y riesgo, todo costo y gasto de defensa del Ministerio, cuando así corresponda.

12.5. Conexión de equipos informáticos móviles a redes ajenas al Ministerio

Nunca deben conectarse equipos informáticos móviles a redes ajenas al Ministerio, a menos que:

a) Se cuente con autorización válidamente emitida por el Ministerio para tales efectos;
b) Se hayan utilizado los procedimientos de seguridad establecidos por el Encargado de Seguridad para proteger la información del Ministerio y/o los Administrados; y
c) Sea absolutamente necesario por razones de interés para la Institución.

12.6. Utilización de equipos informáticos móviles en lugares no protegidos y resguardo de la información

Se debe ser en extremo cuidadoso con la información que se maneja mediante equipos informáticos móviles en lugares públicos; salas de reuniones o áreas no protegidas. El manejo de la información propiedad del Ministerio y/o en su custodia, debe ser conforme en todo momento, con la normativa aplicable en materia de tutela de la información y con la normativa interna aprobada por la Institución, para tales efectos.

12.7. Posibilidad de utilizar la modalidad del Teletrabajo o trabajo desde el hogar

La Jefatura correspondiente de forma potestativa y discrecional podrá en casos de excepción tomar la decisión de permitir y facilitar la modalidad de Teletrabajo o trabajo desde el hogar, a ciertos funcionarios, cuando así lo estime necesario.

Al ser una decisión discrecional del Ministerio, la misma podrá ser revocada por la Institución cuando así lo considere conveniente a sus intereses, sin por ello asumir ninguna responsabilidad.

Esta posibilidad de Teletrabajo no hará nacer en su beneficiario, ningún derecho adicional al derecho de utilizarla únicamente para efectos meramente laborales y sólo durante el tiempo en que la misma sea concedida por el Ministerio.

12.8. Seguridad de la modalidad de Teletrabajo o trabajo desde el hogar

El usuario a quien se le conceda la modalidad de Teletrabajo o trabajo desde el hogar, debe cumplir estrictamente y le serán aplicadas con la mayor rigurosidad todas las disposiciones en materia de seguridad de la información aprobadas por el Ministerio.

Será deber y responsabilidad ineludible de los usuarios a quienes se les conceda el uso de esta modalidad, poner a disposición del Ministerio todos los recursos que le faciliten el Teletrabajo, a fin de que:

a) Se pueda verificar que todos los mecanismos, controles y medidas de seguridad aprobadas por la Institución estén siendo debidamente implementadas;
b) Se lleven a cabo las actualizaciones o modificaciones necesarias para resguardar la información y/o los Recursos Informáticos del Ministerio; y
c) Se puedan llevar a cabo las revisiones periódicas de seguridad que el Ministerio considere necesarias.

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 s 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.