Departamento de Informática

IGI- 6-7
Política de acceso a recursos de tecnología por parte de terceros

Preparado Para:
Ministerio de Cultura y Juventud
San José, Costa Rica

Realizado Por:
Ing. Catalina Cabezas Bolaños

Fecha de envío:
Enero, 2014

TE01 Objetivo

El objetivo primordial de esta sección es procurar la seguridad de las instalaciones de procesamiento de información y de los Recursos Informáticos a los que tienen acceso terceros ajenos a la Institución.

TE02 Alcance

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

TE03 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:

- **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).

- **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).

- **Visitante:**

  Se entenderá por visitante a las distintas áreas del Ministerio, toda aquella persona a quien aún cuando no labora directamente para el área a la que desea ingresar, le ha sido autorizado el acceso a ésta, en virtud de haberse comprobado que lo requiere para la realización de sus labores para con la Institución.

TE04 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.

TE05 Descripción

Los controles de acceso a los Recursos Informáticos deben implementarse tanto para los funcionarios, como para los terceros ajenos al Ministerio, quienes pueden también representar riesgos para la seguridad de la información de la Institución y/o en su custodia. Con el fin primordial de alertar sobre los riesgos que los accesos de terceros representan y proporcionar además, un guía base para administrar correctamente esos riesgos, es que se aprueban las presente políticas.

TE06 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.

TE07 Lista de distribución

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

TE08 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.

TE09 Seguridad frente al acceso por parte de terceros

TE0901-001 Acceso físico y lógico de terceros

Ningún tercero (incluyendo visitantes) debe acceder a las áreas restringidas, los Recursos Informáticos, los recursos de información, ni los sistemas del Ministerio, sin contar con autorización válidamente para ello.

No debe garantizarse acceso a ningún tercero a la información o Recursos Informáticos de la Institución, a menos que:

a) Se tenga autorización previa, de quien tenga potestad para hacerlo; y

b) Se hayan instaurado de conformidad, los controles necesarios para la protección de dichos Recursos.

TE0901-002 Control de accesos para terceras partes

Todos los accesos físicos y lógicos de terceros ajenos al Ministerio deben estar sometidos a controles y parámetros de autorización y autenticación que permitan salvaguardar la integridad, disponibilidad y cuando así correspondiere, la confidencialidad de los Recursos Informáticos y de Información de la Institución, y/o en su custodia.

El tipo de controles y parámetros autenticación y autorización para el acceso de terceros, no debe ser menos exigente, que los establecidos para los funcionarios del Ministerio. Lo anterior sin importar si los controles o parámetros internos de este tercero puedan incluso, aparentar ser más estrictos que los de la Institución misma.
A menos que previamente se haya demostrado la necesidad justificada de brindar acceso físico o lógico a un tercero a los sistemas, recursos de información y/o Recursos Informáticos de la Institución, para la realización de los intereses de ésta, dicho acceso no se concederá.

Este control de accesos debe aplicarse independientemente del tercero de que se trate, es decir, se aplicará a proveedores, contratistas, consultores, personas a las que la Institución brinda servicios, entre otros.

TE0901-003 Aspectos específicos a abordar de previo al acceso físico o lógico de personas a las que la Institución brinda servicio

Cuando así corresponda y de previo a conceder acceso físico o lógico a personas a las que la Institución brinda servicio, deben abordarse y evaluarse los siguientes aspectos:

a) La protección de los Recursos Informáticos involucrados, incluyendo:
    1. Los procedimientos a aplicar para la protección de los activos y para el manejo de vulnerabilidades conocidas;
    2. Los procedimientos para determinar cuándo se ha comprometido la seguridad de dichos activos;

3. Las previsiones a tomar para garantizar la integridad de los Recursos Informáticos;
4. Las restricciones en cuanto a la copia y transmisión de información.

b) La descripción del servicio a ser provisto;
c) Las diferentes razones, requerimientos y beneficios de brindar el acceso de que se trate;
d) La implementación de controles de acceso que incluyan:
    1. Métodos de acceso permitidos;
    2. Uso de identificadores únicos e individuales para cada autorizado;
    3. Procesos de autorización y autenticación;
    4. La prevención expresa de que todo lo que no está expresamente permitido, está por consiguiente prohibido;
    5. Procesos automáticos para revocar los derechos de acceso o interrumpir las comunicaciones entre sistemas, en caso de violación o abuso de privilegios; y
    6. Los requerimientos y disposiciones para mantener actualizada una lista de usuarios autorizados a utilizar los servicios que han de implementarse, y los derechos y privilegios de estos usuarios, con respecto a tales servicios.
e) Mecanismos formales para reporte, notificación, e investigación de inexactitudes en la información; incidentes de seguridad y violaciones o faltas en materia de seguridad.
f) La descripción de los servicios disponibles;
g) El nivel de servicio proporcionado y los niveles de servicio inaceptables;
h) La potestad de la Institución de monitorear y revocar cualquier actividad relacionada con sus Recursos Informáticos y la suscripción de documentos legales de apoyo a ese monitoreo dentro de los parámetros que permite la ley;
i) Las responsabilidades que asume el beneficiario con respecto a los derechos de acceso que se le concederán; y
j) Los derechos de propiedad intelectual, de autoría y demás derechos conexos a tutelarse y la forma adecuada de hacerlo.

TE0901-004 Valoración de riesgos a aplicar para la concesión de acceso a terceros

De previo a otorgar acceso físico o lógico a terceras partes, el Ministerio debe asegurarse de llevar cabo la correspondiente valoración de riesgos, que debe tomar en consideración:

a) El tipo de acceso requerido por el tercero;
b) El valor integral de los activos o de la información involucrada, y su importancia dentro del proceso de que se trate;
c) El impacto que dicho acceso pueda tener en la seguridad organizacional;
d) El nivel de riesgo residual aceptado por la Administración Superior;

e) Los controles a implementar, con el fin de que dicho tercero sólo pueda acceder a la información o Recursos Informáticos necesarios para desempeñar su función para con el Ministerio y/o para satisfacer razones de interés para la Institución;
f) Los controles y parámetros de autenticación y autorización a implementar para el acceso de terceros y los mecanismos de revisión de los mismos;
g) El costo real de la falta de disponibilidad de los recursos e información para su acceso por parte de dichos terceros;
h) Las medidas a tomar ante la ocurrencia de incidentes de seguridad y las responsabilidades atinentes en caso de ser éstos atribuibles al tercero; y
i) Los requerimientos normativos, regulatorios y contractuales involucrados directa o directamente.

TE10 Requerimientos de seguridad en contratos con terceros

TE1001-001 Selección de contratistas

De previo a la contratación de contratistas, se debe llevar a cabo un análisis que permita verificar si ese contratista es en efecto, el adecuado para realizar las labores que se le habrán de asignar para con la Institución. Para ello, debe no sólo requerirse recomendaciones previas en trabajos similares, sino también exigir que ante cualesquier cambio que haya de realizarse en el personal, se mantengan los mismos requerimientos estipulados desde un inicio.

Debe verificarse que los atestados presentados por los posibles contratistas sean verdaderos y en tratándose de recomendaciones, debe contactarse a quien las emitió, para corroborar su autenticidad y el grado de involucramiento de quien recomienda, con el proyecto o labor realizada.

TE1001-002 Disposiciones indispensables en la contratación con terceros

Siempre que se contrate con terceros que hayan de tener acceso a las instalaciones de procesamiento de la información del Ministerio, debe suscribirse con éstos, contratos formales que contengan todos los requerimientos y disposiciones en materia de seguridad que ellos habrán de resguardar; o al menos, hagan referencia a los mismos.

Toda contratación debe ser muy clara para las partes involucradas en cuanto a sus deberes, obligaciones y resultados esperados, a fin de evitar confusiones y delimitar responsabilidades.

No se debe otorgar acceso a terceros a la información, ni a las instalaciones de procesamiento de la misma, hasta tanto no se hayan implementado los controles de acceso apropiados y se hayan firmado los documentos legales que definan las condiciones de conexión y acceso.

La contratación con terceros, cuando así corresponda, debe al menos especificar:

a) Las Políticas, Estándares, Procedimientos y Lineamientos que en materia de seguridad, habrán de aplicárseles a los contratistas;
b) Los métodos y responsabilidades de ambas partes con respecto a la capacitación de los usuarios en materia de seguridad de la información;
c) Los procedimientos que en materia de seguridad de la información se deben implementar y la responsabilidad que por los mismos, asume el contratista;
d) Las obligaciones del contratista con respecto al reporte de los incidentes de seguridad de que tenga conocimiento y los métodos y canales seguros y controlados para hacerlo;
e) Los procedimientos para determinar si se ha cumplido a cabalidad con todo lo pactado y para auditar las responsabilidades contractuales asumidas;
f) Las disposiciones con respecto al monitoreo tanto del desarrollo de actividades del contratista referentes a los servicios o productos contratados, como de todo su actuar dentro de los sistemas de información del Ministerio y/o en el uso de los Recursos Informáticos del mismo;
g) La necesidad de presentación de informes de avance por parte del contratista, el formato esperado de éstos y la habitualidad de los mismos;
h) Las pruebas que se les van a realizar a los productos esperados;
i) El proceso claro y detallado de control de cambios que se utilizará a lo largo de la contratación;
j) El escalamiento en caso de que se presenten problemas o divergencias de criterios y los mecanismos para resolverlos;
k) Los servicios que habrán de estar disponibles para el contratista en la realización de su trabajo y los límites de utilización de dichos servicios;
l) Las especificidades y la garantía del trabajo que se ha contratado;
m) Los controles a implementar para garantizar la recuperación, devolución o destrucción de la información del Ministerio y/o los Administrados al finalizar la contratación o en el momento convenido durante la vigencia del mismo;
n) Las disposiciones en cuanto al resguardo, manejo, transmisión, tutela, protección, reproducción confidencialidad, disponibilidad e integridad de la información;
o) Las disposiciones en cuanto al resguardo, manejo, protección, mantenimiento, disponibilidad e integridad de todos los activos involucrados (incluyendo hardware y software);
p) Las disposiciones referentes a la transferencia o cooperación de personal cuando así corresponda;
q) Las responsabilidades establecidas por ley para ambas partes (e.g. responsabilidades en cuanto a protección de datos; protección de derechos de propiedad intelectual y autoría);
r) Las responsabilidades individuales e institucionales que asumen ambas partes;
s) Disposiciones con respecto a los derechos patrimoniales que surjan de los productos esperados y la protección de los mismos;

t) Determinación del personal a quién se le va a garantizar el acceso;
u) Disposiciones con respecto a la contratación de subcontratistas;
v) Disposiciones con respecto a la renegociación y terminación anticipada de acuerdos (incluyendo, medidas de contingencia en caso de terminación anticipada; renegociación en caso de cambios en los requerimientos de seguridad; posibilidad de contratar a un tercero que pueda asumir el compromiso, en caso de incapacidad sobrevenida del contratista); y
w) Los acuerdos de control de accesos que incluyan:

i. Los métodos de acceso permitidos,
ii. Uso de identificadores únicos e individuales para cada autorizado;
iii. Los procesos de autorización y autenticación;
iv. La prevención expresa de que todo lo que no está expresamente permitido, está por consiguiente prohibido;
v. Procesos automáticos para revocar los derechos de acceso o interrumpir las comunicaciones entre sistemas, en caso de violación o abuso de privilegios.
vi. Los requerimientos y disposiciones para mantener actualizada una lista de usuarios autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso; y
vii. Sanciones específicas por incumplimiento de las Políticas, Estándares, Procedimientos, Lineamientos y otros comunicados oficiales que en materia de seguridad, deban aplicar.

Todo documento contractual formal que haya de suscribirse con terceros, debe llevar el aval de la Asesoría Jurídica.

Toda medida, disposición y control que se tome y/o se implemente en virtud de la contratación de terceros, debe basarse en el análisis de riesgo llevado a cabo para tales efectos y debe ser consecuente con el nivel de riesgo residual aceptado por la Administración Superior.

TE1001-003 Monitoreo y revisión de los servicios contratados a terceros

Los servicios, registros y reportes provistos por los terceros contratados por la Institución para la realización de labores, deben ser monitoreados, revisados y auditados con regularidad, a fin de asegurar que se esté cumpliendo en tiempo, cantidad y calidad con todo lo pactado, y en especial con:

a. La normativa en materia de seguridad de la información;
b. Los procedimientos aprobados de control de cambios;
c. El nivel de servicio requerido;

d. El manejo y comunicación segura de incidentes, problemas y fallas de seguridad; y
e. La resolución de problemas.

La Institución debe exigir de los terceros con quienes contrate, el asignar el monitoreo de los servicios y del cumplimiento de las obligaciones contraídas a alguna persona de su propio equipo de trabajo, con conocimiento y autoridad suficiente para hacerlo. Ello, sin perjuicio del deber que mantiene la Institución, de hacer lo mismo por su parte.

Deben tomarse medidas apropiadas y en tiempo, cada vez que se detecten incumplimientos, a fin de que éstos puedan ser debidamente solventados.

TE11 Tercerización

TE1101-001 Exigencia de medidas calificadas de seguridad

Aplicarán a la contratación de terceros para la administración y control de sistemas de información, redes o cualesquier otro sistema de procesamiento de información propiedad del Ministerio y/o en su custodia, requisitos más estrictos en materia de seguridad informática, que los estipulados para cualesquier otro contratista, en virtud de la cantidad, importancia y sensibilidad de la información que estos manejen.

Así, además de las medidas y disposiciones contempladas en las otras normas, la contratación de este tipo de contratistas debe contemplar:

a) La forma en la cual se cumplirán los requisitos que establece la legislación nacional con respecto a derechos protegidos involucrados en la prestación de los servicios de administración (e.g. protección de los datos);
b) Los controles que se implementarán para que todas las partes incluidas en la tercerización (incluso los subcontratistas) estén al corriente de sus obligaciones en materia de seguridad de la información;
c) Los acuerdos y controles que deben utilizarse para el acceso seguro de los usuarios autorizados a la información de la Institución;
d) La forma en cómo se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres;
e) La posibilidad de ampliar los requerimientos de seguridad por medio de un plan de administración de seguridad a ser acordado entre ambas partes, cuando así se considere necesario; y
f) El derecho del Ministerio de realizar cuántas auditorías considere necesarias.

Toda medida, disposición y control que se tome y/o se implemente en virtud de la contratación de terceros para la administración de ambientes de procesamiento de información, debe basarse en el análisis de riesgo llevado a cabo para tales efectos y debe ser consecuente con el nivel de riesgo residual aceptado por la Administración Superior.

Debe tenerse presente que cuando la tercerización implica el procesamiento de información, el Ministerio sigue siendo, en última instancia, la principal responsable por el cuido y protección de dicha información.

TE12 Administración de instalaciones externas

TE1201-001 Decisión de contratar a terceros ajenos al Ministerio

La decisión de contratar a terceros ajenos al Ministerio para la administración de ambientes de procesamiento de información (incluyendo pero sin limitarse a redes, Recursos Informáticos y/o sistemas de información), debe ser una decisión tomada con base en los resultados de los análisis de riesgo llevados a cabo para tales efectos así como con base en el riesgo residual aceptado por la Administración Superior. La responsabilidad última con respecto a la contratación de terceros residirá en la Administración Superior, la cual tomará en cuenta el criterio experto del Encargado de Seguridad.

TE1202-002 Controles mínimos a implementar de previo a la contratación de terceros para la administración de ambientes de procesamiento de información

Previa contratación de terceros para la administración de ambientes de procesamiento de información, se deben tomar en cuenta los siguientes aspectos:

a) Deben identificarse claramente los sistemas que por su criticidad o sensibilidad, el Ministerio desarrollará e implementará por sí mismo;
b) Deben tomarse en cuenta las implicaciones que el sistema tiene para la continuidad de las operaciones; es decir, no sólo debe tomarse en cuenta el sistema en sí mismo, sino las repercusiones que tal sistema tiene en los diferentes procesos o sistemas del Ministerio con los que se interrelaciona;
c) Deben aclararse y definirse los estándares aplicables al proyecto en cuestión, así como los mecanismos para medir cumplimiento;
d) Deben definirse y asignarse las responsabilidades y procedimientos para asegurar y monitorear las actividades y controles de seguridad;
e) Deben establecerse procedimientos de reporte y manejo de incidentes de seguridad.

TE1202-003 Contratistas externos en la administración de ambientes de procesamiento de información

Previa contratación de un contratista externo para la administración de ambientes de procesamiento de información, deben acordarse controles basados en los análisis de riesgo llevados a cabo al efecto y en el nivel de riesgo residual aceptado por la Administración Superior. Estos controles deben estar orientados a proteger toda

información sometida a requerimientos de confidencialidad, en su integridad y disponibilidad.

Los controles aprobados por el Ministerio para el caso en concreto, que impliquen el desarrollo de obligaciones por parte del contratista o su deber de abstenerse de llevar a cabo ciertos comportamientos u acciones, deben quedar claramente plasmados en los contratos a suscribir con dicho contratista. Asimismo, debe documentarse todo estándar que habrá de aplicarse, así como los mecanismos para asegurar su cumplimiento. Estos contratos deben ser previamente revisados por la Asesoría Jurídica.

TE1202-004 Consideraciones en la contratación de personas físicas o jurídicas extranjeras que no cuentan con representación local

Debe tenerse especial cuidado en tomar en cuenta las implicaciones legales existentes en la contratación de personas físicas o jurídicas extranjeras, que no cuentan con representación local. Para ello debe solicitarse la asesoría experta de la Asesoría Jurídica del Ministerio, que examine aspectos de jurisdicción y competencia, así como de validez de las declaraciones de los contratantes y su aplicabilidad en el foro elegido.

TE1202-005 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 ítemes 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.

TE1202-006 Requerimientos de seguridad a terceros

A fin de realizar intercambios de información y software seguros, el Ministerio debe requerir que las personas u organizaciones con las que haya de ejecutar dichos intercambios, le garanticen un nivel aceptable de seguridad. El nivel de seguridad que se requiera de cada persona u organización con la que se lleven a cabo dichos intercambios, dependerá no sólo de la criticidad de la información que se comparta, sino de las obligaciones de resguardo del Ministerio con respecto a la información y/o software involucrados.

Deben requerirse de los terceros, controles al menos tan estrictos como los establecidos por el Ministerio mismo, para el resguardo de la información o software de que se trate.

TE1202-007 Sistemas de Información Compartidos

Debe tenerse especial cuidado, con la información a la que tendrán acceso los terceros con quienes la Institución comparte sistemas de información (e.g. SIGAF). A fin de proteger dicha información, y sin perjuicio de otros controles aplicables incluidos en el presente documento, deben implementarse controles que incluyan al menos:

a) La protección frente a vulnerabilidades conocidas y eventuales que podrían hacer peligrar la información que se comparte;
b) Los mecanismos y medios seguros y aprobados, por los cuales se habrá de compartir información sensitiva;
c) La prohibición de manejar información confidencial o sensitiva por medio del sistema compartido, si este no ofrece las medidas apropiadas para su resguardo;
d) Los procedimientos de autorización de accesos al sistema de que se trate;
e) Las restricciones de acceso a determinados niveles, según el perfil de usuario; y
f) Los derechos y obligaciones de retención y respaldo de la información contenida en el sistema.

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.