Departamento de Informática

DI-PO-06-2014

Política sobre el control de acceso a los recursos de tecnología

Fecha de envío:
Enero, 2014

1. Objetivo

La presente política tiene como objeto proveer una guía para establecer el control de accesos a los Recursos Informáticos del Ministerio de Cultura y Juventud, sobre la base de los requerimientos de seguridad y operacionales del Ministerio.

2. Alcance

Estas políticas son aplicables al personal encargado de conceder derechos de acceso, así como a aquel encargado de aplicar, implementar, monitorear y/o fiscalizar los respectivos controles de acceso a los Recursos Informáticos y/o de Información al Ministerio.

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.

4. Responsabilidades de los puestos involucrados

Las responsabilidades de los puestos involucrados se definen en el cuerpo mismo de cada una de las normas aquí incluidas, según corresponda.

5. Descripción

El Ministerio de Cultura y Juventud se encuentra en la obligación de administrar adecuadamente los accesos a sus sistemas y/o Recursos Informáticos. Para ello, debe dotarse de una normativa que le permita no sólo regular, controlar y monitorear la concesión y utilización de dichos accesos, sino también prevenir, detectar y registrar posibles violaciones y tomar las acciones correspondientes.

6. Fecha de creación, y entrada en vigencia de la Política.

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 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. Acceso Físico

9.1. Relación entre Seguridad Física y Seguridad Informática

La Administración Superior del Ministerio, al implementar el sistema de gestión integral de Seguridad de la Información, debe proporcionarle protección a todos sus elementos, como parte que son de un sistema. Así, deberán tomarse en cuenta aspectos de Seguridad Informática en la creación, constitución e implementación de Seguridad Física y viceversa.

9.2. Acceso a las áreas del Ministerio

Se regulará el acceso a las diferentes áreas del Ministerio, por lo que se instaurarán los debidos controles a fin de que sólo personal autorizado pueda ingresar en las distintas áreas.

9.3. Creación de Áreas Seguras

Se deberán tomar las acciones correspondientes para impedir accesos no autorizados, daños y/o intrusiones a/en las sedes de procesamiento de datos del Ministerio. Las instalaciones de procesamiento de la información crítica o sensible deben estar en áreas resguardadas por un perímetro de seguridad definido, debidamente provisto de controles apropiados.

9.4. Creación de perímetros de seguridad

Se crearán perímetros de seguridad para proteger las instalaciones de procesamiento de información y demás áreas restringidas del Ministerio. El nivel de protección de las áreas resguardadas será definido con base en:

a) Los riesgos identificados en el análisis de riesgo llevado a cabo para tales efectos;
b) Las necesidades de seguridad de cada área en específico; y
c) El nivel de riesgo residual aceptado por la Administración Superior.

Estos perímetros de seguridad estarán claramente definidos, deben ser físicamente sólidos, y cubrirán el llamado concepto de seguridad de “cielo a suelo” (desde el piso hasta el cielorraso), lo que implica que se tomará en cuenta la seguridad de puertas, ventanas, paredes, techos, ingresos, alarmas, sistemas de detección de intrusos, sistemas de ventilación, suelos, entre otros, impidiendo accesos físicos no autorizados.

La información con respecto a las especificidades de los perímetros de seguridad definidos, y aprobados por el Ministerio debe considerarse y tratarse como Información Confidencial, a fin de no incurrir en infidencias que puedan vulnerar la seguridad física.

9.5. Acceso físico controlado en áreas restringidas

Debe restringirse el acceso físico a las oficinas y áreas del Ministerio que utilicen equipo de cómputo y de comunicaciones en general, manipulen información sensitiva y/o manejen numerario, a fin de que en ellas ingrese solamente personal autorizado.

9.6. De los controles de acceso físico

Deben instaurarse controles de acceso físico acorde con:

a) Las necesidades específicas de seguridad de cada área en particular;
b) Los niveles de riesgo de cada área de trabajo, según el análisis de riesgo llevado a cabo para tales efectos; y
c) El nivel de riesgo residual aceptado por la Administración Superior.

Los controles deben incluir sistemas automatizados de identificación, que estipulen procedimientos dirigidos a añadir y eliminar personas de las listas de control de acceso, a las facilidades del Ministerio. Dichos procedimientos deberán ser auditables.

9.7. De los procedimientos para la autorización de accesos e instauración de controles de acceso

El Encargado de Seguridad junto con el Departamento de Informática serán los responsables de definir procedimientos específicos para autorización de accesos físicos y para la instauración de controles de acceso.

Estos procedimientos deben ser aprobados por la Comisión de Seguridad de la Información.

9.8. Registros históricos de acceso y de autorización en áreas restringidas

Debe mantenerse registro histórico de las personas que han accedido a áreas restringidas y de quiénes están debidamente autorizados para ingresar en dichas áreas. Estos registros deben ser mantenidos por un plazo no menor de cinco años y almacenados en medios controlados que permitan su resguardo efectivo.

9.9. Autorizaciones de acceso

Cada Coordinador de Seguridad junto con el jefe de departamento respectivo, serán quienes determinen las áreas a las cuáles podrán ingresar los distintos personeros de dicho departamento, así como terceros ajenos al Ministerio. Las respectivas autorizaciones serán suscritas por ambos funcionarios.

El Coordinador de Seguridad será el encargado de velar porque en el proceso se apliquen los procedimientos aprobados por el Ministerio para la autorización de accesos.

Las autorizaciones de acceso deben emitirse con base en la necesidad que tenga la Institución para que esa persona ingrese en las distintas áreas, a fin de poder realizar sus labores para con éste.

Los derechos de acceso deben revisarse y actualizarse periódicamente.

9.10. Visitantes y terceros ajenos al Ministerio en áreas restringidas

Solamente se le concederá acceso a visitantes y terceros ajenos al Ministerio, con propósitos específicos y autorizados. Debe supervisarse de cerca, todo el accionar del visitante o tercero dentro de las áreas restringidas. En virtud de lo anterior, ningún visitante o tercero podrá ingresar a dichas áreas a menos que cuente con autorización expresa válidamente emitida para tales efectos y se haga acompañar de un funcionario debidamente autorizado.

9.11. Instrucción sobre los requisitos de seguridad de las diferentes áreas

A cada funcionario, visitante o tercero ajeno al Ministerio autorizado a ingresar en sus distintas áreas, se le debe informar sobre los requerimientos de seguridad de cada área en específico. Sin embargo, debe tenerse mucha precaución en no divulgar y/o exponer Información Propietaria y/o Información Confidencial del Ministerio y/o los Administrados, así como cualquier otra información que permita o facilite vulnerar la seguridad del Ministerio. El Encargado de Seguridad se encargará de establecer los requisitos de seguridad de cada área y de brindar la instrucción necesaria.

Los requerimientos de seguridad de cada área deben ser determinados mediante una valoración de riesgos llevada a cabo para tales efectos y con base en el riesgo residual aprobado por la Administración Superior.

9.12. Consideraciones básicas para la selección de áreas restringidas

Para la selección de áreas restringidas debe tenerse en cuenta los alrededores y su localización, de manera que se reduzca la posibilidad de daños producidos por incendios, inundaciones, filtraciones de agua, explosiones, huelgas y conmoción civil, así como otras formas de desastres naturales y/o provocados por el hombre. Deben tomarse en cuenta disposiciones y normas en materia de salubridad, sanidad y seguridad. Asimismo, deben considerarse las amenazas a la seguridad que representan los edificios y zonas aledañas.

Las áreas restringidas deben encontrarse dentro de los perímetros de seguridad definidos y establecidos por el Ministerio.

9.13. Análisis de riesgo para instalaciones sensitivas o de cómputo

Para toda construcción o remodelación de áreas destinadas al proceso, manejo o custodia de información sensitiva o crítica, así como áreas donde se ubique equipo de cómputo y de comunicaciones, se debe realizar de previo un análisis de riesgo y se debe tener en cuenta el nivel de riesgo residual aceptado por la Administración Superior.

9.14. Rotulación de las áreas de cómputo, comunicaciones y procesamiento de información

Para efectos de seguridad, no se deben rotular los sitios donde se ubican los servidores, el equipo de comunicaciones y cómputo, ni las instalaciones de procesamiento de información.

9.15. Equipo de apoyo en áreas restringidas

A fin de evitar comprometer la Información Confidencial, cada área restringida debe estar debidamente provista de todo el equipo de soporte necesario para la realización de las tareas que ahí se llevarán a cabo (e.g. máquinas de fax; fotocopiadoras, entre otras). Esto evitará que la información deba ser enviada a sitios de acceso no controlado, en donde pueda caer en manos de personas no autorizadas.

Lo anterior no implica almacenar en las áreas restringidas ni equipo ni suministros innecesarios, sino únicamente los requeridos.

9.16. Protección de áreas abiertas

Deben crearse y aprobarse los controles físicos y lógicos necesarios para asegurar los equipos e información que se maneja en áreas abiertas. Corresponderá al Encargado de Seguridad el crear dichos controles y a la Comisión de Seguridad validarlos, con base en el análisis de riesgo llevado a cabo a los efectos y en el nivel de riesgo residual aceptado por la Administración Superior.

Será responsabilidad del Encargado de Seguridad, el asegurar que efectivamente se implementen los controles físicos aprobados.

9.17. Información sobre áreas protegidas

La información sobre áreas protegidas y el trabajo u operaciones que se llevan a cabo en ellas, sólo debe ser conocida por quienes tienen necesidad expresa de conocer de las mismas en función de sus labores para con el Ministerio.

Los directorios internos de las áreas restringidas, sólo deben estar disponibles para quien así lo necesiten, en virtud de las actividades que desarrollan para con la organización, no así para el público en general.

9.18. Personal de servicio de soporte externo y áreas restringidas

El personal de servicio de soporte externo debe tener acceso limitado a las áreas restringidas y/o las instalaciones de procesamiento de Información Confidencial o sensible. Este acceso debe ser autorizado y monitoreado.

9.19. Horario de acceso a áreas restringidas

El acceso a áreas restringidas que manejan información sensible, crítica o valiosa, se brindará sólo en horario normal de trabajo del Ministerio, a menos que en casos de excepción, se compruebe la necesidad de establecer horarios extraordinarios o ampliados.

9.20. Controles y barreras adicionales para áreas restringidas colindantes

Dependiendo de los requerimientos específicos de seguridad de las diferentes áreas restringidas, podrán requerirse barreras y perímetros adicionales de seguridad para controlar el acceso físico entre áreas colindantes.

9.21. Instalaciones de procesamiento de información

Las instalaciones de procesamiento de información administradas por la Institución, deben estar físicamente separadas de las administradas por terceros.

9.22. Separación entre las instalaciones de procesamiento de información y las áreas de entrega, carga y acceso irrestricto

Las áreas de entrega y carga deben ser controladas y deben estar aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados. Los requerimientos de seguridad de cada área deben ser determinados mediante una evaluación de riesgos llevada a cabo para tales efectos y con base en el riesgo residual aprobado por la Administración Superior.

9.23. Procedimientos seguros de carga y descarga

El Departamento de Informática junto con Encargado de Seguridad serán los responsables de definir procedimientos seguros y controlados de carga y descarga. Estos procedimientos deben al menos incluir los siguientes controles:

a) El acceso a áreas de carga y descarga desde fuera del edificio debe estar restringido a personal autorizado y plenamente identificado;
b) La áreas de carga y descarga deben estar definidas y controladas, de forma que se evite puedan ser utilizadas por personal no autorizado, para ingresar a otras áreas del edificio;
c) Las puertas exteriores del área de carga y descarga deben quedar debidamente cerradas y aseguradas, debiendo previamente desalojarse a todo personal no autorizado, cuando las puertas internas de la Institución se abran para el ingreso de materiales, insumos y mercadería a otras áreas del Ministerio;
d) Todo material, insumos y/o mercadería entrante debe ser objeto de inspección, de previo a su envío al área en que va a ser utilizada, a fin de descartar posibles amenazas;
e) Todo material, insumos y/o mercadería entrante debe registrarse en el inventario de activos correspondiente; y
f) Cuando ello sea posible, la carga entrante y la saliente deben ser debidamente separadas, para facilitar su manejo controlado.

Estos procedimientos deben ser validados por la Comisión de Seguridad de la Información.

9.24. Revisión y análisis periódico de los derechos de acceso físico

Los derechos de acceso físico deben ser periódicamente revisados, analizados y actualizados, a fin de mantener sólo aquellos que son estrictamente necesarios para

que la persona objeto de los mismos, pueda llevar a cabo sus obligaciones para con el Ministerio. La revisión de los derechos de acceso debe ser realizada al menos una vez cada tres (3) meses.

9.25. Inhabilitación permanente de códigos de acceso físico

Cuando un funcionario termine su relación laboral con el Ministerio o sea trasladado, debe ser reportado por su superior jerárquico a fin de ser desactivado todo código de acceso físico por él conocido y/o utilizado. Dichos códigos no deben ser asignados a ninguna otra persona.

9.26. Inhabilitación temporal de códigos de acceso físico

Deben inhabilitarse temporalmente los derechos de acceso físico para aquellos funcionarios que se ausenten de sus puestos por un período mayor a cinco días hábiles.

9.27. Retención de registros de acceso a áreas restringidas

Para un mayor control, es necesario mantener respaldados y debidamente archivados los registros de los últimos diez años sobre las personas que ingresaron en las áreas restringidas, así como la información sobre ingresos frecuentes. Además, debe mantenerse un control sobre las personas que diariamente ingresan y salen a fin de facilitar acciones en caso de tener que evacuar áreas restringidas.

10. Seguridad de los activos físicos

10.1. Protección de los activos físicos

Los activos físicos deben ser ubicados o protegidos de tal manera que se reduzcan las amenazas y peligros ambientales, y oportunidades de acceso no autorizado.

10.2. Implementación de controles

Se deben implementar controles para minimizar el riesgo de amenazas potenciales, incluyendo pero sin limitarse a robo; incendio; explosivos; humo; agua; falla en la provisión de agua; inundaciones, polvo; vibraciones; temblores; interferencia en las comunicaciones, efectos químicos; y vandalismo, entre otros.

10.3. Activos físicos que requieran protección especialmente calificada

Para aquellos activos críticos que requieran protección especialmente calificada, (ya sea en función de la información que se maneja a través de éstos o por su valor para un proceso esencial del Ministerio), la Institución podrá decidir aislarlos, si ello resultare más efectivo y el costo fuera más eficiente, que implementar otro tipo de controles.

Al momento de decidir aislar equipos que requieran protección especialmente calificada, debe tomarse en cuenta la posibilidad de que la información que estos contienen, sea objeto de fuga no intencional de información por medio de campos electromagnéticos.

Si ese fuera el caso, deben establecerse controles que permitan camuflar o en su defecto, filtrar los contenidos sensibles o confidenciales.

La decisión de aislar equipos críticos debe ser consecuente con el análisis de riesgo llevado a cabo a los efectos, y con el nivel de riesgo residual aceptado por la Administración Superior.

10.4. Ubicación de activos físicos que contienen información sensitiva

Los activos físicos que almacenan, transmiten, transportan, guardan o de cualesquier forma manejan información sensitiva, deben ubicarse en lugares con ámbito visual restringido, de manera que se reduzca al máximo posible la probabilidad de que dicha información sea vista por personas no autorizadas.

10.5. Bloqueo de equipos informáticos que no están en uso

Deben aprobarse y documentarse mecanismos seguros y controlados para el bloqueo de equipos informáticos que no están en uso, a fin de evitar que los mismos sean objeto de accesos no autorizados.

11. Seguridad de los activos físicos fuera de la organización

11.1. Seguridad de los Recursos Informáticos fuera del Ministerio

Deben tomarse todas las medidas e implementarse los controles necesarios, a fin de garantizar que la seguridad de los Recursos Informáticos fuera del Ministerio, sea equivalente a la implementada dentro de la Institución.

Entre los controles a aplicar para estos efectos, deben contemplarse los siguientes:

i. Los usuarios autorizados para remover equipo de las instalaciones de la Institución, deben ser claramente identificados;
ii. Si ello aplicare, deben establecerse plazos determinados durante los cuales el equipo puede mantenerse fuera de la Institución y deben implantarse revisiones periódicas, a fin de determinar que el mismo haya sido efectivamente devuelto. De dichas revisiones se mantendrá registro;

Los equipos críticos que se utilicen fuera de la Institución deben contar con sus respectivas pólizas de seguro.

12. Requerimientos institucionales de control de accesos

12.1. Controles, Políticas, Estándares, Procedimientos y Lineamientos en materia de control de accesos

Deben establecerse e implementarse los Controles, Políticas, Estándares, Procedimientos y Lineamientos de control de accesos a la información y procesos institucionales del Ministerio, con base en:

a) Los requerimientos específicos de seguridad de cada proceso de negocio crítico del Ministerio y de la información que se maneja en el proceso;
b) El análisis de riesgo llevado a cabo para tales efectos; y
c) El nivel de riesgo residual aceptado por la Administración Superior.

Dichos Controles, Políticas, Estándares, Procedimientos y Lineamientos de control de accesos, serán evaluados por el Encargado de Seguridad y aprobados por la Comisión de Seguridad.

12.2. Aspectos básicos a tomar en cuenta en la creación de controles, Políticas, Estándares, Procedimientos y Lineamientos de control de accesos

Deben tomarse en cuenta al menos los siguientes aspectos básicos de cada proceso crítico del Ministerio, para la creación de los Controles, Políticas, Estándares, Procedimientos y Lineamientos necesarios para cada uno de ellos:

a) Requerimientos de seguridad específicos de cada proceso y aquellos en paralelo, necesarios para la concreción de los primeros;
b) Riesgos atinentes a cada proceso crítico;
c) Identificación, valoración y clasificación de todos los Recursos Informáticos críticos para los procesos examinados;
d) Controles aprobados con respecto al manejo, tutela, clasificación y resguardo de la información propia de cada proceso;
e) Legislación aplicable y las obligaciones contractuales del Ministerio, con respecto al resguardo y tutela de la información de que se trate;
f) Requerimientos de manejo de controles de acceso en ambientes distribuidos y de red, que reconozcan todos los tipos de conexiones involucradas;
g) Perfiles y necesidades de acceso de los usuarios, a los diferentes procesos; y/o a la información que se maneja en éstos; y
h) Requerimientos de autorización de accesos específicos o la necesidad de remoción de éstos.

12.3. Procedimientos formales de asignación de derechos de acceso

Se deben crear e implementar procedimientos formales para controlar la asignación de derechos de acceso a los Recursos Informáticos del Ministerio. Dichos procedimientos

comprenderán todas las etapas del ciclo de vida de los accesos de los diferentes grupos de usuarios, iniciando con el registro de nuevos usuarios y culminando con la eliminación de los derechos de acceso. Especial atención debe prestarse a los accesos privilegiados, a fin de evitar que éstos impliquen la posibilidad de violentar controles establecidos.

12.4. Del procedimiento formal de registro y eliminación de usuarios

Debe crearse un procedimiento formal de registro y eliminación de usuarios de las listas de acceso a todos los sistemas y servicios de información multi-usuario del Ministerio.

Este procedimiento debe contemplar al menos los siguientes controles:

a) Asignar una contraseña de usuario única que permita individualizar a cada usuario sin excepción;
b) Verificar que todo usuario tenga autorización del Responsable Asignado (ya sea del sistema o de la información) y de la Administración Superior, para tener acceso a los mismos;
c) Verificar que el nivel de acceso otorgado es el estrictamente necesario para la realización de las labores del usuario en virtud de su relación con el Ministerio y que es coherente además con las Políticas de Seguridad aprobadas por el Ministerio;
d) Asegurarse que los usuarios reciban documentación específica sobre sus derechos de acceso;
e) Instruir a los usuarios sobre los derechos de acceso y requerir de ellos que suscriban un documento legal en que se estipule se les ha instruido adecuadamente y ellos por su parte han entendido las condiciones de acceso;
f) En caso de tercerización del servicio, asegurar que los proveedores no brindan acceso hasta tanto no se hayan completado los procedimientos de autorización aprobados por el Ministerio;
g) Mantener un registro formal y actualizado de las personas registradas para utilizar el servicio. Este registro sólo debe ser conocido por quienes tienen necesidad expresa y comprobada para ello;
h) Eliminar los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la organización;
i) Verificar y cancelar claves de identificación y cuentas de usuario redundantes; e
j) Incluir cláusulas en los contratos con funcionarios y contratistas, que especifiquen responsabilidades (civiles, administrativas y/o penales), en caso que éstos intenten llevar a cabo accesos no autorizados, ya sea por ellos mismos o por medio de terceras personas.

12.5. Restricción en el uso y asignación de privilegios

No se deben asignar privilegios de acceso que le permitan a usuario evadir controles impuestos por el Ministerio. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada

mediante un proceso de autorización formal que tome en cuenta al menos los siguientes pasos:

a) Deben identificarse los privilegios asociados a cada producto del sistema (e.g. sistemas operativos, aplicaciones, bases de datos, entre otros), así como al usuario al que se le han concedido;
b) Los privilegios deben otorgarse caso por caso, con base en criterios de necesidad comprobada y asignarse a una clave de usuario diferente a la que habitualmente utiliza la persona referida;
c) Se debe mantener un registro actualizado y documentado de todos los privilegios asignados;
d) Se deben otorgar los privilegios únicamente cuando ya se haya completado el proceso de autorización;
e) Se debe mantener y promover el uso de programas utilitarios que evitan el otorgamiento de privilegios; y
f) Se debe mantener y promover el desarrollo y uso de rutinas en los sistemas para evitar otorgar privilegios no autorizados a los usuarios.

Toda asignación de privilegios de acceso a sistemas multiusuario, debe ser aprobada por la Administración Superior, con base en la necesidad del funcionario de que se trate, en la realización de sus labores para con la Institución. Esta asignación de privilegios debe ser validada por el usuario principal de cada sistema.

12.6. Del procedimiento formal de revisión de derechos de acceso

Debe crearse e implementarse un procedimiento formal de revisión de derechos de acceso que incluya:

a) Revisión de derechos de acceso a intervalos regulares (como mínimo cada seis meses);
b) Revisión de derechos de acceso cada vez que haya cambios importantes en los sistemas de información;
c) Revisión de derechos de acceso cada vez que haya cambios de personal, de contratistas o proveedores o cambios de funciones de éstos; y
d) Revisión de derechos de acceso privilegiados y de asignación de éstos (como mínimo cada tres meses).

13. Control de Acceso a la Red

13.1. De la documentación de los servicios de red autorizados a cada usuario y los procedimientos de autorización

Cada usuario debe tener muy claro cuáles son los servicios de red a los cuales se le autoriza tener acceso. Asimismo, los encargados de brindar los accesos deben conocer con exactitud los procedimientos de autorización aprobados por el Ministerio.

Se debe documentar:

a) Para cada usuario sus derechos de acceso; y
b) Para los responsables de asignar los derechos de acceso, los procedimientos de autorización.

13.2. Mecanismos de seguridad a nivel de sistema operativo

En la medida de lo posible y en lo pertinente para el Ministerio, deben utilizarse los mecanismos de seguridad propios de los sistemas operativos, a fin de restringir el acceso a los recursos de información de los computadores.

Deben preferirse sistemas operativos, y habilitar los recursos de éstos, que permitan:

a) Identificar y verificar la identidad, terminal o ubicación de cada usuario autorizado;
b) Registrar todo acceso exitoso y/o fallido al sistema;
c) Registrar el uso de privilegios especiales dentro del sistema;
d) Activar alarmas en caso de violación a las PSI establecidas;
e) Introducir mecanismos de autenticación y autorización suficientes a las necesidades del Ministerio; y
f) Restringir tiempos de conexión de los usuarios, cuando así se estime apropiado.

La evaluación de los recursos de seguridad a habilitar en los diferentes sistemas operativos y la determinación de la utilidad y conveniencia de su uso, corresponderán al Encargado de Seguridad y deben ser aprobados por la Comisión de Seguridad.

13.3. Identificación automática de estaciones de trabajo

Si se requiere que una determinada sesión sólo pueda iniciarse desde una estación de trabajo o una ubicación predefinidas, deben implementarse mecanismos que permitan la identificación automática de estaciones de trabajo. Lo anterior sin perjuicio de la aplicación de cualesquier otra técnica de autenticación que se estime conveniente.

13.4. De los procedimientos de conexión de estaciones de trabajo

Toda conexión a los servicios de información del Ministerio, debe ser segura. Por ello, deben establecerse procedimientos de conexión de estaciones de trabajo diseñados para minimizar la oportunidad de accesos no autorizados.

Estos procedimientos deben divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de información innecesaria a usuarios no autorizados.

Estos procedimientos deben al menos:

a) Evitar desplegar identificadores de sistemas o aplicaciones, hasta tanto no se haya completado exitosamente la conexión;
b) Desplegar avisos de la Administración Superior advirtiendo que sólo usuarios autorizados deben utilizar la computadora;

c) Evitar brindar mensajes que faciliten el procedimiento de conexión de usuarios no autorizados;
d) Evitar que se despliegue en pantalla la clave que está siendo ingresada al sistema;
e) Impedir que se envíen claves de acceso, por medios inseguros;
f) Validar la información de la conexión cuando se haya incluido la totalidad de los datos de entrada;
g) Limitar el número de intentos de conexión fallidos al máximo formalmente establecido por el Ministerio y enviar un mensaje de alarma a la consola si este número de intentos es excedido;
h) Registrar los intentos de acceso no exitosos;
i) Implementar demoras obligatorias antes de permitir nuevos intentos de identificación o rechazar nuevos intentos sin autorización específica;
j) Limitar el tiempo máximo y mínimo permitido para el proceso de conexión, finalizando la conexión en caso de que el mismo sea excedido; y
k) Desplegar la siguiente información al completarse una conexión exitosa:

    i. Fecha y hora de la última conexión anterior a la que se realiza; y
    ii. Detalle de los intentos de conexión fallidos desde la última conexión exitosa.

Corresponderá al Encargado de Seguridad evaluar los procedimientos para la conexión de estaciones de trabajo y a la Comisión de Seguridad aprobarlos.

13.5. Métodos de identificación y autenticación de usuarios

A fin de proveer un mayor grado de seguridad en los accesos, se deben elegir métodos de identificación y autenticación, que permitan no sólo individualizar a los diferentes usuarios dentro de la red, sino también evitar accesos no autorizados. Estos métodos deben comprender una combinación de tecnologías, controles y normas, acordes a las necesidades de la Institución.

13.6. Desconexión de estaciones de trabajo inactivas

Después de cierto lapso de inactividad, las conexiones de las estaciones de trabajo que se encuentren en ubicaciones de alto riesgo, que sirvan a sistemas de alto riesgo, o que manejen información sensitiva o confidencial, deben terminarse automáticamente.

La herramienta de desconexión que se utilice para estos efectos, debe ser capaz de limpiar la pantalla de la estación de trabajo y de cerrar tanto la sesión de la aplicación, como de la red.

El lapso de inactividad pasado el cual debe operarse la desconexión, debe definirse en relación con los riesgos intrínsecos al área, sistema o información que se desea asegurar y toma también en cuenta, los riesgos que representan los usuarios de la estación de trabajo de que se trate. Este control es particularmente importante en áreas

de acceso público e irrestricto, así como en áreas fuera del perímetro de seguridad definido por la Institución.

Corresponderá al Encargado de Seguridad, proponer los controles para el proceso de desconexión, así como el lapso de inactividad después del cual este proceso operará.

13.7. Controles para la limitación de horarios de conexión a estaciones de trabajo

Todas las aplicaciones informáticas sensibles del Ministerio, especialmente aquellas estaciones de trabajo instaladas en áreas de alto riesgo, (e.g. áreas abiertas al público), deben estar sometidas a restricciones en cuanto al horario de conexión en el que las mismas se pueden acceder.

Las restricciones a aplicar en el Ministerio, dependerán de:

a) Los riesgos de seguridad a los que están expuestas las estaciones de trabajo de que se trate;
b) La criticidad y sensibilidad de las aplicaciones informáticas, almacenadas en dichas estaciones de trabajo; y
c) Las necesidades de acceder dichas estaciones de trabajo y/o aplicaciones en diferentes horarios, según los requerimientos específicos del Ministerio.

Los controles para la limitación de horarios de conexión a las estaciones de trabajo, deben ser propuestos por el Encargado de Seguridad y aprobados por la Comisión de Seguridad.

14. Acceso Avanzado

14.1. Controles de acceso a los equipos y sistemas críticos del Ministerio

Se deben establecer controles estrictos para el acceso a los equipos y sistemas críticos del Ministerio (e.g. servidores de control de acceso, routers y firewalls, entre otros), a fin de evitar que los mismos sean accedidos por entes o personas no autorizadas. Estos controles deben establecerse con base en:

a) La criticidad de la información que se almacena, transita y/o se resguarda en los mismos;
b) Las vulnerabilidades propias de estos equipos o sistemas críticos;
c) El análisis de riesgo llevado a cabo para tales efectos; y
d) El nivel de riesgo residual aceptado por la Administración Superior.

Corresponderá al Encargado de Seguridad establecer los controles requeridos y la Comisión de Seguridad, aprobarlos.

15. Monitoreo del uso y acceso a los sistemas

15.1. Bitácoras de Auditoría

Deben mantenerse registros completos, actualizados y debidamente documentados de auditoría que comprendan todos los eventos de seguridad que se presenten en los sistemas y en la red del Ministerio. Estos deben mantenerse por el período establecido por la Comisión de Seguridad de la Información, el cual no debe ser menor al período exigido por ley.

Entre los registros de auditoría que habrán de mantenerse están al menos:

a) La identificación del usuario implicado;
b) La información sobre el evento y sobre las acciones correctivas tomadas;
c) La fecha y hora de inicio y terminación de la sesión;
d) La identidad o ubicación de estación de trabajo, si ello es posible;
e) Los intentos fallidos y exitosos de acceso a los sistemas los resultados de su análisis y las acciones tomadas en consecuencia; y
f) Los intentos fallidos y exitosos de acceso a datos y recursos, los resultados de su análisis y las acciones tomadas en consecuencia;
g) Los cambios en las configuraciones de los sistemas;
h) El uso de privilegios;
i) El uso de sistemas utilitarios y aplicaciones;
j) Los archivos accedidos y las clases de accesos efectuados;
k) Las direcciones de red y protocolos ingresados;
l) Las alarmas activadas por los controles de acceso a los diferentes sistemas; y
m) La activación y desactivación de la protección instaurada a los sistemas (e.g protección antivirus y detección de intrusos).

Estos registros deben almacenarse en lugares seguros, controlados y protegidos, máxime cuando contengan información confidencial o sensitiva.

Deben establecerse controles que les impidan a los administradores de sistemas borrar o desactivar los registros de sus propias actividades.

15.2. De los procedimientos de monitoreo

Se deben establecer procedimientos para monitorear el acontecer en los sistemas del Ministerio, así como el uso de sus Recursos Informáticos, información y datos, e instalaciones de procesamiento de la información, a fin de garantizar que los usuarios desempeñen solamente actividades que les hayan sido autorizadas; que el Ministerio no esté siendo objeto de ataque, hurto de tiempo o de información y datos; desvío de datos; acciones ilegales, entre otros. El nivel de monitoreo requerido en cada una de

las instalaciones de procesamiento de información, sistemas y/o Recursos Informáticos, debe establecerse mediante evaluaciones de riesgo llevadas a cabo para tales efectos.

El monitoreo que se lleve a cabo debe versar únicamente sobre los aspectos que son de interés directo del Ministerio y sobre los cuales las Institución pueda asumir algún tipo de responsabilidad y/o le puedan causar algún daño o pérdida. Intromisiones infundadas que no sean de interés para el Ministerio y/o los Administrados, las cuales no obedezcan a la sana administración de los sistemas informáticos, no deben ser llevadas a cabo, ya que pueden resultar ilegales.

De previo a autorizar cualquier tipo de monitoreo, debe consultarse con la Asesoría Jurídica, a fin de que éste determine el ámbito y las circunstancias dentro de las cuales el monitoreo es legal y determine y apruebe a su vez, los documentos de respaldo y apoyo a dicho monitoreo, a ser suscritos por los usuarios.

15.3. Áreas objeto de monitoreo

Se debe al menos monitorear lo siguiente:

a) Los accesos no autorizados incluyendo detalles tales como: identificación del usuario involucrado; fecha y hora de eventos clave; tipos de eventos; archivos que son accedidos; utilitarios y programas utilizados.
b) Las operaciones con privilegios de acceso, incluyendo: la utilización de cuentas de administrador; inicio y cierre de sesión de los sistemas; conexión y desconexión de dispositivos en los sistemas; identificación de cuenta y usuario; y procesos involucrados. Estas actividades deben monitorearse regularmente, mediante mecanismos fuera del control de los administradores y operadores de los sistemas involucrados;
c) Los intentos de acceso no autorizado incluyendo: intentos fallidos; quebrantos a la normativa interna en materia de accesos aprobada por el Ministerio; alertas emitidas por los firewall y demás dispositivos de seguridad.
d) Las alertas emitidas por los sistemas propietarios de detección de intrusos del Ministerio;
e) Los daños o usos no autorizados a/de los Recursos Informáticos del Ministerio;
f) Los cambios no autorizados a las configuraciones y controles de los sistemas de seguridad;
g) Los envíos de información no autorizados;
h) Los usos no autorizados de los sistemas de procesamiento de información; y
i) Las alertas o fallas de/en los sistemas, incluyendo: alertas o mensajes de consola; excepciones a los sistemas de registro y alarmas de los sistemas de administración de redes.

Sucesos que puedan implicar la ocurrencia de incidentes de seguridad deben ser comunicados de inmediato al Equipo de Respuesta a Incidentes de Seguridad, por los medios seguros y controlados provistos por el Ministerio para tales efectos.

15.4. Revisión periódica del resultado de las actividades de monitoreo

Se debe llevar a cabo periódicamente, la revisión de las actividades de monitoreo del Ministerio, así como de las medidas utilizadas para solventar las fallas encontradas. La periodicidad de dichas revisiones dependerá de:

a) La criticidad de los procesos de aplicaciones involucrados;
b) El valor, la sensibilidad y/o la criticidad de la información involucrada;
c) La importancia de los procesos elegidos;
d) La vulnerabilidad de los sistemas involucrados y la facilidad con que se llevan a cabo intromisiones por parte de entes no autorizados; y
e) La experiencia acumulada del Ministerio en materia de detección de intrusos, infiltración y detección de usos no autorizados.

La revisión de las actividades de monitoreo, deben ser llevadas a cabo por funcionarios o contratistas diferentes a aquellos objeto del monitoreo

15.5. Protección de las herramientas de monitoreo y de sus registros

A fin de procurar que los registros generados por las herramientas de monitoreo utilizadas por el Ministerio, sean fidedignos, se deben establecer controles que permitan proteger estas herramientas y registros contra acciones no autorizadas tales como:

a) Desactivar la herramienta de registro;
b) Causar alteraciones a los tipos de mensajes registrados;
c) Editar o suprimir archivos de registro;
d) Saturar los medios de transporte o almacenamiento de archivos;
e) Dañar los registros de eventos, rescribir sobre los mismos o provocar que las herramientas mismas dañen los registros de eventos o rescriban sobre los mismos.

Estos controles se establecerán tomando en cuenta el análisis de riesgo llevado a cabo para tales efectos, así como el nivel de riesgo residual aceptado por la Administración Superior.

Los registros producto del monitoreo realizado, deben archivarse de manera segura y controlada, según lo establecido por el Encargado de Seguridad y validado por la Comisión de Seguridad de la Información, por todo el plazo que la ley o la normativa impongan para la información de que se trate. Ello a efecto de contar con evidencia, en caso de resultar necesario.

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; 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.