Departamento de Informática

DI-PO-11-2014
Política para el Control de Contraseñas

Fecha de envío:
Enero, 2014

Política para el control de contraseñas

1. Objetivo

La presente norma tiene como objeto proveer una guía básica para la generación y control de contraseñas en los sistemas del Ministerio de Cultura y Juventud.

2. Alcance

Estas políticas son aplicables al Personal Usuario que utilice los Recursos Informáticos del Ministerio, en lo que a cada uno de ellos les corresponda.

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 las normas aquí incluidas, según corresponda.

5. Descripción

La utilización de contraseñas sólidas y robustas es un elemento fundamental en la protección de los Recursos Informáticos y de Información del Ministerio. Es por ello que en su elaboración, deben seguirse al menos, los parámetros mínimos de seguridad establecidos en las mejores prácticas relativas a la materia.

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. Responsabilidades con respecto al uso y tutela de contraseñas

9.1. Concientización de los usuarios con respecto al aseguramiento de sus contraseñas

Se debe instruir y concientizar a los usuarios con respecto a sus deberes y responsabilidades, en el manejo de las contraseñas que les han sido asignadas. Dicha instrucción y capacitación debe brindárseles de previo a la entrega de la contraseña, de manera que cuando éstos suscriban los documentos legales que amparan tales deberes y responsabilidades, entiendan a cabalidad los alcances de las mismas.

9.2. Procedimientos formales para la elaboración, elección y cambio de contraseñas

Se deben crear y aprobar procedimientos formales ajustados a las mejores prácticas, que guíen a los usuarios en la elaboración, selección y cambio de contraseñas, de manera que se propicie las mismas revistan en todo momento un alto grado de calidad, complejidad, confidencialidad y efectividad.

Además, estos procedimientos deben exigir de los usuarios al menos lo siguiente:

a) Mantener la confidencialidad de las contraseñas;
b) Evitar, en la medida de lo posible, escribir las contraseñas o en su defecto, almacenarlas únicamente en medios seguros y utilizando métodos de almacenamiento previamente aprobados por el Ministerio;
c) Cambiar las contraseñas cuando haya indicios de que éstas o los sistemas que las contienen, han sido comprometidos;
d) Cambiar las contraseñas a intervalos regulares y/o con base en cierto número predeterminado de accesos (las contraseñas para cuentas privilegiadas deben ser sometidas a cambios con mayor frecuencia);
e) No repetir contraseñas previamente utilizadas;
f) Cambiar las contraseñas temporales en el primer acceso;
g) No compartir contraseñas individuales; y
h) No guardar las contraseñas en sistemas automáticos de autenticación.

9.3. Responsabilidad del usuario por las contraseñas

A cada usuario al que se le haya asignado contraseñas de acceso para los diferentes sistemas e información del Ministerio, deberá advertírsele que con respecto a éstas, tiene las siguientes obligaciones:

a) Debe seguir todas las disposiciones y recomendaciones emitidas por el Ministerio, para la elaboración de contraseñas;
b) Debe utilizar sus contraseñas de acceso única y exclusivamente para los usos que le fueron asignadas;
c) En la medida de lo posible memorizará sus contraseñas a fin de evitar ponerlas en riesgo, sin embargo cuando esto no le sea posible, debe almacenarlas de

conformidad con los mecanismos seguros y controlados aprobados por el Ministerio;

d) No debe bajo ninguna circunstancia escribirlas en papel, ni almacenarlas sin protección;
e) No debe compartir, prestar, divulgar, trasferir, de cualesquier forma o medio, las contraseñas que le han sido asignadas para su uso personal;
f) Debe seguir todas las disposiciones emitidas por el Ministerio, para el cambio regular de contraseñas;
g) Debe cambiar las contraseñas cuando sospeche o tenga la certeza de que las mismas han sido comprometidas;
h) No debe utilizar las opciones de guardar o recordar contraseñas al inicio de sesión de los sistemas operativos;
i) De mantenerse una estrategia de autenticación centralizada para evitar el uso de múltiples contraseñas, y a la vez utilizar un método de autenticación de doble factor , bajo ninguna circunstancia el usuario debe prestar el medio por el cual se verificará sus credenciales;
j) Debe suscribir los documentos legales que el Ministerio estime convenientes, en los que estipule las obligaciones del usuario y sus responsabilidades específicas con respecto a las contraseñas;
k) No debe bajo ninguna circunstancia, utilizar contraseñas que no le han sido asignadas;
l) No debe, bajo ninguna circunstancia, intentar descifrar y/o violentar contraseñas de acceso que no le han sido asignadas; y
m) Las contraseñas de acceso son responsabilidad del usuario a quien le fueron asignadas, por lo que cualesquier consecuencia adversa que derive de su mal uso, generado por descuido, negligencia o dolo, deberá ser asumida personalmente por dicho usuario.

9.4. Elaboración, elección y cambio de contraseñas

Una vez que el Ministerio le haya asignado una contraseña de acceso provisional y/o cada vez que se requiera el cambio de éstas, el usuario debe proceder inmediatamente a elaborar nuevas contraseñas, que cumplan estrictamente con lo establecido por los procedimientos formalmente aprobados por la Institución, para tales efectos.

10. Administración de contraseñas de usuario

10.1. Administración formal de contraseñas

Se debe aprobar un procedimiento de administración formal de contraseñas que comprenda al menos:

a) Utilizar mecanismos seguros y controlados para el envío, transmisión o almacenamiento de contraseñas de acceso;
b) Requerir de los usuarios que suscriban un documento con valor legal en el que acusen recibo de su contraseña y estipulen sus obligaciones y responsabilidades en el manejo de las mismas;

c) Proveer a los usuarios de una contraseña provisoria segura que deben estos proceder a cambiar en el primer acto de identificación;
d) Imponer el uso de contraseñas individuales a fin de individualizar a cada usuario, rastrear su comportamiento y eventualmente poder exigir responsabilidades;
e) Obligar a los usuarios a cambiar sus contraseñas de acuerdo al tiempo establecido por la Comisión de Seguridad de la Información (plazo que nunca debe sobrepasar los noventa días) o cuando sea necesario en el caso de que las mismas se vean comprometidas;
f) Mantener un registro de contraseñas previas de cada usuario y verificar que las mismas no se repitan;
g) No mostrar contraseñas en pantalla cuando las mismas son ingresadas;
h) Almacenar en forma separada los archivos de contraseñas y los datos de los sistemas de aplicación;
i) Almacenar contraseñas de forma cifrada según los métodos de encripción aprobados por el Ministerio;
j) Modificar las contraseñas predeterminadas por los proveedores, en cuanto sea posible;
k) Verificar la identidad del usuario que ha perdido su contraseña, de previo a asignarle una nueva;
l) Utilizar al menos dos métodos distintos de autenticación de usuarios a fin de proveer una mayor protección;
m) Auditar periódicamente las constraseñas, de forma que se garantice las mismas cumplan con los requerimientos establecidos por el Ministerio; y
n) Establecer con claridad los pasos a seguir para la administración de contraseñas y cuentas de usuario que por su naturaleza y criticidad requieran un trato especial, como por ejemplo las cuentas de usuario con permisos avanzados, cuentas de usuario de servicios (que se utilizan para dotar de identidad), permisos a determinados procesos de un sistema en ejecución, y/o cuentas de usuario de administrador de dispositivos de comunicaciones, entre otras. Para estas cuentas de usuario especiales, deben establecerse controles que garanticen una robustez superior a la de las contraseñas de usuario común y un procedimiento de cambio que no ponga en riesgo la continuidad y/o disponibilidad de los sistemas del Ministerio.

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.