Política de Contraseñas

Objeto:
Establecer reglas de configuración, gestión y control para la formación y uso de contraseñas robustas, ya sean de usuarios, sistemas y equipos, con el fin de evitar y/o reducir los incidentes de seguridad.
En aquellos servicios en los que el nivel de criticidad y riesgo exijan mayores niveles de seguridad en las contraseñas, podrán ser adoptadas medidas complementarias.

Alcance:
El ámbito de esta política abarca a todos los sistemas que administra el Ministerio. Se incluyen entonces, aplicaciones informáticas de cualquier naturaleza, servicios, sistemas operativos, sistemas de red y configuración de equipos.

Responsabilidades:
Todos los empleados del Ministerio y personal de terceros deben cumplir la presente política.

Desarrollo:
1 – Deben configurarse los sistemas con el objetivo de impedir el uso de contraseñas débiles. Para la formación de contraseñas robustas, se deberá configurar:

1.1. Caracteres utilizados. El uso combinado de caracteres alfabéticos en mayúsculas, minúsculas y números o símbolos especiales.
1.2. Longitud mínima. Contraseñas de 8 caracteres.
1.3. Número máximo de intentos fallidos. Limitar la cantidad de intentos de autenticación fallidos a un máximo de 5, en ese caso, se bloqueará la cuenta de usuario por un plazo mínimo de 30 minutos. Luego de 3 nuevos intentos de autenticación fallidos debe bloquearse la cuenta de usuario definitivamente siendo necesario recurrir al administrador del sistema.
1.4. Cambio de contraseña. Configurar la gestión de contraseñas para que obligue el cambio de las mismas al cabo de un período máximo de 180 días.
1.5. Histórico de contraseñas. Definir en 5, la cantidad de contraseñas que se almacenarán de forma de no permitir la reutilización de las mismas por parte del usuario.
1.6. Digitación de contraseñas. Los campos de ingreso de contraseñas deben tratar el ingreso de caracteres digitados de forma oculta.

2 – Las cuentas de usuario no utilizadas en un plazo máximo de 60 días deben ser bloqueadas.

3 – Al momento de pasaje a producción de un sistema, se deben cambiar las contraseñas utilizadas a las fases de desarrollo y prueba.

4 – La asignación de la primera contraseña a una cuenta de usuario, debe configurarse con obligatoriedad de cambio de la misma por parte del usuario al inicio de la sesión. Esta primera contraseña deberá ser válida por un plazo no superior a 24 horas y deberá ser seleccionada de forma aleatoria o diversa. La contraseña utilizada en la creación de las cuentas no debe ser siempre la misma combinación fija de caracteres.

5 – Los usuarios deben ser notificados formalmente de la creación de una cuenta de usuario bajo su responsabilidad. La asignación de una primera contraseña por defecto debe ser parte de dicha notificación.

6 – Debe estar al alcance de los usuarios una opción que habilite el cambio de su contraseña cuando este lo requiera, sin necesidad de solicitar apoyo.

7 – Queda prohibido al personal técnico solicitar las contraseñas a los usuarios de los sistemas para cualquier finalidad, incluyendo las de mantenimiento de las estaciones de trabajo.

8 – No pueden embeberse en código fuentes cuentas de usuario y contraseñas. Queda prohibido el uso de cuentas de usuario con contraseñas que no puedan ser modificadas o gestionadas por el administrador del sistema o usuarios.

9 – Luego de incidentes de seguridad se deben cambiar inmediatamente las contraseñas asociadas a los sistemas afectados.

10 – Las contraseñas de cuentas de usuario privilegiados deben ser distintas, independiente de que la cuenta de usuario se encuentre en sistemas distintos.

11 – La presente Política recoge la disposición establecida en el artículo 21 del Decreto 65/998, que reglamenta la implementación de medios electrónicos de transmisión, almacenamiento y manejo de documentos en la Administración Pública, el cual se transcribe a continuación:

> *"Art.21°- La divulgación de la clave o contraseña personal de cualquier funcionario autorizado a documentar su actuación mediante firmas o contraseñas informáticas, constituirá falta gravísima, aún cuando la clave o contraseña no llegase a ser utilizada."*

Elaborado por:	Gerencia Gobierno Electrónico
Fecha Elaboración:	27/05/2011
Autorizado por:	Dirección General de Secretaría
Fecha Autorización:	

Nº Versión:	1.0
Fecha Modificación:	
Autorizado por:	
Descripción:	

BICENTENARIO
URUGUAY
1811 - 2011

MIEM
MINISTERIO DE INDUSTRIA, ENERGÍA Y MINERÍA

Paysandú y Av. del Libertador Brig. Gral. Lavalleja
C.P. 11.100
Tel.: (598) 2900 0231 al 33
www.miem.gub.uy
Montevideo - Uruguay

SECRETARIA DE ESTADO
SIRVASE CITAR

MINISTERIO DE INDUSTRIA, ENERGÍA Y MINERÍA

Montevideo, 19 OCT 2011

VISTO: el Decreto Nº 452/009 de 8 de diciembre de 2009.----------

RESULTANDO: I) que el referido decreto dispone que las Unidades Ejecutoras de los Incisos 02 al 15 del Presupuesto Nacional, deberán adoptar en forma obligatoria una Política de Seguridad de la Información, tomando como base la "Política de Seguridad de la Información para Organismos de la Administración Pública", con el propósito de impulsar un Sistema de Gestión de Seguridad de la Información (SGSI).----------

II) que para tales fines las Unidades Ejecutoras del Inciso deberán brindar el apoyo necesario para alcanzar los objetivos de esta política general y de aquellas otras que se propongan implementar;----------

CONSIDERANDO: I) que en este marco normativo, se ha propuesto la aprobación y divulgación de la Política de Contraseñas a aplicarse en esta Secretaría de Estado----------

II) que todas las políticas deben ser conocidas y cumplidas por todo el personal del MIEM, independiente del cargo que desempeñe y de su situación contractual;----------

III) que procede aprobar el documento Política de Contraseñas y darlo a conocer mediante circular a todos los funcionarios del MIEM;----------

ATENTO: a lo expuesto.----------

----------**EL DIRECTOR GENERAL DE SECRETARÍA**----------

----------**R E S U E L V E** :----------

1º.- Apruébase el documento Política de Contraseñas en el Ministerio de Industria, Energía y Minería.----------

2º.- Dicho documento, que se anexa y forma parte de la presente resolución, se integrará a la normativa básica del MIEM.----------

3º.- Pase al Departamento de Recursos Humanos a efectos de dar a conocer el documento mediante circular, cumplido archívese.----------

MZ

Esc. H. Gustavo FERNÁNDEZ DI MAGGIO