MIEM
MINISTERIO DE INDUSTRIA, ENERGÍA Y MINERÍA

BICENTENARIO.UY
INSTRUCCIONES DEL AÑOXIII

Paysandú 1101 4º Piso - C.P. 11.000
Tel.: (598 2) 900 0231 al 33
Correo: info@miem.gub.uy
Montevideo - Uruguay

SECRETARIA DE ESTADO
SIRVASE CITAR
1289/13

MINISTERIO DE INDUSTRIA, ENERGÍA Y MINERÍA

Montevideo, 12 ABR 2013

VISTO: los documentos Política de Custodia de Cuentas y Procedimiento de Custodia de Cuentas.----------

RESULTANDO: que los referidos documentos fueron elaborados por la Gerencia de Gobierno Electrónico de esta Secretaría de Estado.----------

CONSIDERANDO: I) que la Política de Custodia de Cuentas tiene el objeto de establecer los lineamientos indispensables que permitan definir procedimientos, con el fin de asegurar la permanente disponibilidad de uso de las cuentas de acceso privilegiado nativas, para el manejo de activos críticos de tecnologías de la información (TI) del Ministerio de Industria, Energía y Minería;----------

II) que el Procedimiento de Custodia de Cuentas tiene el objeto de describir las actividades que se realizan orientadas a custodiar las cuentas de usuario de acceso privilegiado nativas, para el manejo de activos críticos de tecnologías de la información (TI) del Ministerio de Industria, Energía y Minería;----------

III) que procede aprobar los documentos referidos precedentemente.----------

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

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

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

1º.- Aprobar los documentos Política de Custodia de Cuentas y Procedimiento de Custodia de Cuentas, elaborados por la Gerencia de Gobierno Electrónico de esta Secretaría de Estado, que se adjuntan y forman parte de la presente resolución.----------

2º.- Comuníquese, etc..----------

MZ

Esc. H. Gustavo FERNANDEZ DI MAGGIO
Director General de Secretaría
Ministerio de Industria, Energía y Minería

Objeto:
Establecer los lineamientos indispensables que permitan definir procedimientos, con el fin de asegurar la permanente disponibilidad de uso de las cuentas de acceso privilegiado nativas, para el manejo de activos críticos de tecnologías de la información (TI) del Ministerio de Industria, Energía y Minería (MIEM).

Alcance:
Se aplica a todos aquellos activos críticos de TI.

Definiciones:
Se entiende por cuentas de usuario de acceso privilegiado nativas:
Todas aquellas cuentas de productos de TI que son utilizadas para la instalación y administración de los mismos y que cuentan con acceso irrestricto a las funcionalidades del producto (Ejemplos: administrador, administrator, admin, root, etc.).

Se entiende por activos críticos de TI:

1. Activos de información: archivos y bases de datos en las que residan datos de sistemas en producción alojados en servidores o equipos del tipo computadoras personales que funcionen en un rol similar a servidores, así como también pistas de auditoría de sistemas en producción.
2. Programas de software: software de aplicación, software de sistemas, herramientas de desarrollo y utilitarios.
3. Activos físicos: servidores o equipos del tipo computadoras personales que funcionen en un rol similar y equipos de comunicación de datos.
4. Servicios de control de acceso que requieran usuario y contraseña.

Responsabilidades:
El Responsable de Seguridad deberá controlar el cumplimiento de esta política. Los distintos funcionarios del MIEM que manejan estas cuentas de usuario de acceso privilegiado deberán asegurarse de cumplir con dicha política y los procedimientos que de aquí se deriven.

Descripción:
El uso de cuentas de usuario de acceso privilegiado nativas será únicamente para la instalación inicial del producto y para su posterior configuración. El mismo terminará en el momento de la puesta en producción del producto. A partir de este momento, la cuenta de usuario de acceso privilegiado sólo podrá ser utilizada de acuerdo a lo estipulado en la presente política.

Para la administración diaria de los productos se deberá asignar a uno o más usuarios nominados (de acuerdo a las necesidades) roles con los privilegios que sean requeridos para la adecuada gestión diaria de los mismos.

Objeto:
Describir las actividades que se realizan orientadas a custodiar las cuentas de usuario de acceso privilegiado nativas, para el manejo de activos críticos de tecnologías de la información (TI) del Ministerio de Industria, Energía y Minería (MIEM).

Alcance:
Se aplica a todos aquellos activos críticos de TI.

Responsabilidades:
El Responsable de Seguridad deberá controlar el cumplimiento de este procedimiento. La implantación de este Procedimiento corresponde a los Responsables de Seguridad de TI (Procedimiento sobre responsabilidades: SI_PRO001). Los distintos funcionarios del MIEM que manejan estas cuentas de acceso privilegiado deberán asegurarse de cumplir con dicho procedimiento.

Descripción:

1- Salvaguarda
Las contraseñas de las cuentas de usuario de acceso privilegiado nativas para el manejo de activos críticos de TI (archivos y bases de datos en las que residan datos de sistemas en producción alojados en servidores o equipos del tipo computadoras personales que funcionen en un rol similar, pistas de auditoría de sistemas en producción, software de aplicaciones, software de sistemas, herramientas de desarrollo, utilitarios, servidores o equipos del tipo computadoras personales que funcionen en un rol similar, equipos de comunicación de datos y servicios de control de acceso) deberán ser guardadas en dos sobres cerrados, los cuales quedarán en custodia de la Gerencia de Gobierno Electrónico junto a la denominación de la respectiva cuenta.
Las mencionadas contraseñas no serán de conocimiento del Gerente de Gobierno Electrónico ni del Responsable de Seguridad de la Información del MIEM, previéndose únicamente el acceso a las mismas de acuerdo a lo previsto en el punto 3 del presente documento.
Las contraseñas no deberán ser modificadas sin justificada razón, previo a lo cual se deberá requerir **indefectiblemente** la autorización previa del Responsable de Seguridad de TI correspondiente.
En este caso inmediatamente se deberá repetir el procedimiento de salvaguarda para proceder a la sustitución de los respectivos sobres.

2- Uso
Las cuentas de usuario de acceso privilegiado nativas no deberán ser utilizadas para la gestión diaria de los activos críticos de TI, debiéndose utilizar para este fin usuarios nominados con los privilegios necesarios.
En caso de necesidad urgente, y en forma eventual, el uso de aquellas deberá ser puesto en conocimiento, inmediatamente a posteriori, del Responsable de Seguridad de TI correspondiente, documentándose la situación de emergencia.
Si por limitaciones en la definición de nuevos roles el producto no permite una adecuada administración con otro usuario privilegiado diferente al nativo, este extremo deberá ser informado al Responsable de Seguridad de la Información del MIEM, debiéndose indicar un plan de solución de la situación a mediano plazo.

3- Control de vigencia de contraseñas de cuentas privilegiadas nativas

Como procedimiento de control interno el Responsable de Seguridad de la Información del MIEM deberá proceder a controlar la vigencia y correctitud de las contraseñas guardadas en los sobres al menos una vez al año.

La apertura de sobres se realizará según los procedimientos notariales de acuerdo a la normativa vigente.

Una vez corroborada la validez y vigencia se deberá proceder a modificar la clave y repetir el procedimiento de salvaguarda.

Si se constatara que las claves de acceso respaldadas en los sobres no se encuentran vigentes los funcionarios involucrados serán pasibles de sanciones disciplinarias de acuerdo a la gravedad de la omisión.

Elaborado por:	Gerencia Gobierno Electrónico
Fecha Elaboración:	06/02/2013
Autorizado por:	
Fecha Autorización:	

Nº Versión:	1.0
Fecha Modificación:	
Autorizado por:	