

PR.TI.SI 02

PROCEDIMIENTO DE MANEJO DE USUARIO Y CONTRASEÑA

Gerencia TI - Seguridad de la Información

Elaborado por: GTI - Seguridad de la Información	Revisado por: GTI – Sistemas Corporativos	Aprobado por: Gerencia TI
Fecha: 1/07/2010	Fecha: 12/07/2010	Fecha: 03/01/2011

	PROCEDIMIENTO DE MANEJO DE USUARIO Y CONTRASEÑA	PR.TI.SI.02
		Versión 01
		Página 2 de 5

1. OBJETIVO

Este procedimiento define los requerimientos de control necesarios para acceder a los recursos vinculados al Sistema de Información de OSE.

2. ALCANCE

Este procedimiento se aplica para todos los empleados de OSE y terceros que acceden a dichos recursos o administren su acceso.

3. DESARROLLO

El acceso a los recursos vinculados al Sistema de Información de OSE debe ser otorgado de manera controlada en base a los requerimientos de negocio, dada la relevancia de los mismos. Se concederán permisos a los empleados que corresponda, en forma explícita A TRAVES DEL SISTEMA DE PERMISOS (SPI).

El proceso para administrar el acceso a la información debe incluir:

- Documentación adecuada respecto a la administración y responsabilidades de todos los empleados.
- Desarrollo e implementación de mecanismos de control de acceso técnicos y no técnicos para proteger de accesos no autorizados a los recursos de información en la red y los sistemas de aplicación.
- Realizar un seguimiento adecuado de los accesos y el uso de los recursos de información.

Administración de cuenta / contraseña de usuario

Todos los accesos especiales o privilegiados a los sistemas y datos se deben revisar cuando se considere necesario.

Los responsables de la información deben revisar los privilegios de acceso otorgados periódicamente, y deben revocar todos aquellos que ya no son requeridos por los usuarios. Los Administradores de los sistemas son responsables de brindar reportes actualizados a los responsables de la información para revisar los accesos de los usuarios actuales.

Los derechos de acceso se deben revisar regularmente para mantener un control del acceso efectivo. Se deben revisar los accesos de todos los sistemas cuando se considere necesario.

	PROCEDIMIENTO DE MANEJO DE USUARIO Y CONTRASEÑA	PR.TI.SI.02
		Versión 01
		Página 3 de 5

El responsable de la información debe notificar a la Gerencia de TI por el Sistema de permisos (SPI), la remoción de los accesos a la información en caso que los mismos ya no sean necesarios. Es obligación del responsable de la información ver si los privilegios de acceso están alineados con el negocio y están asignados basados en la “necesidad de saber”. Las listas de acceso se deben proporcionar en forma oportuna a la Gerencia de T.I.

Antes que los técnicos otorguen accesos privilegiados deben recibir la autorización de los responsables de la información a través del Sistema de Permisos (SPI), avalada por Seguridad de la Información. (PERMISOS ESPECIALES)

En situaciones donde ya no sean requeridos los accesos de los usuarios a información altamente sensible, el Superior debe dar las bajas en el Sistema de Permisos, el sistema comunica las bajas a Seguridad de la Información.

Cualquier privilegio especial concedido a los empleados en plataformas tecnológicas (como ser: cuentas de administración para sistemas operativos, bases de datos o aplicaciones o cuentas que pueden evitar los controles del sistema o aplicación), debe estar basado en las necesidades de trabajo. Estos privilegios sólo deben darse sobre la base de la “necesidad de saber” para los procesos de operaciones y soporte técnico.

Las cuentas de usuario que no se han accedido por noventa días se inhabilitarán automáticamente.

Todos los accesos a sistemas informáticos deben estar controlados por un método de autenticación que combine por lo menos usuario / contraseña. La combinación usuario / contraseña debe verificar la identidad del usuario

Dentro de lo posible, el sistema forzará a los nuevos usuarios que acceden al sistema a cambiar la contraseña inicial por una que cumpla los estándares de contraseñas.

Los usuarios deben ser forzados a cambiar las contraseñas cada cien días.

Los Administradores de Sistemas deben forzar esto por medios automáticos estableciendo la antigüedad de las contraseñas en el sistema.

Los usuarios deberían intentar utilizar diferentes esquemas de contraseñas.

Para los usuarios con tareas similares, se utilizarán controles de acceso basados en grupos o roles para asignar permisos y accesos a las cuentas individuales.

Se deben seguir los estándares de nombres de las cuentas de OSE para todos los sistemas. Cualquier desviación, incluyendo las cuentas de aplicaciones o de uso especial, debe estar aprobada por Seguridad de la Información conjuntamente con la Gerencia de TI.

 Obras Sanitarias del Estado	PROCEDIMIENTO DE MANEJO DE USUARIO Y CONTRASEÑA	PR.TI.SI.02
		Versión 01
		Página 4 de 5

Cuando sea factible técnicamente, los sistemas deben llevar históricos de contraseñas de los usuarios. El archivo histórico debe contener las últimas 3 contraseñas de los usuarios y almacenarlas encriptadas.

Todos los usuarios de los sistemas informáticos de OSE deben tener un ID de usuario único que sea válido para todo el trabajo del usuario. Los ID de los usuarios no deben reutilizarse para otras personas.

El sistema no debe permitir que los usuarios tengan múltiples sesiones en el mismo sistema a menos que el usuario esté autorizado.

REVISION	FECHA	MODIFICACIONES