 SERTRACEN	PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE CALIDAD	CODIGO SPA-024
TÍTULO POLITICA DE CAMBIO DE CLAVES DE ACCESO		REV: 11

Objetivo:

Establecer estándares para cambios periódicos a las claves de acceso a programas de informática para todos los usuarios.

Controlar el acceso de los usuarios a los sistemas de Licencias de Conducir, Registro Público de Vehículos, Refrenda de Tarjetas de Circulación y Administración y Cobro de Infracciones de Transito según los privilegios definidos.

Alcance:

Usuarios del sistema informático Jefaturas, subjefturas y operadores del Registro Público de Vehículos, Licencias de conducir, Administración, Soporte Técnico, Operaciones, Desarrollo Humano, el VMT y todas sus unidades, y todas las instituciones externas que se conectan por aplicaciones cliente/servidor o aplicaciones WEB

DESCRIPCION:

El siguiente instructivo se utilizará como política de cambios de clave de acceso de los usuarios a las diferentes aplicaciones que tiene asignadas para prevenir la divulgación de éstas y que sea utilizada por un usuario diferente al asignado.


USUARIOS CON ACCESO AL SISTEMA DE BASE DE DATOS

Las cuentas de usuarios que se creen en el sistema generalmente estarán conformadas por la primera letra del primer nombre, seguida del primer apellido. Para los casos en los que, al aplicar la política, la cuenta de usuario resultante ya exista, se utilizará la primera letra del segundo nombre o el segundo apellido y como siguiente alternativa la primera letra de ambos nombres, seguida del primer apellido.

Los responsables de crear usuarios con accesos a las bases de datos serán [la Gerencia de I+D.](#)

La información asociada a cada cuenta será el nombre completo, la unidad laboral, el origen (SS, SA, SM, CS, LD o PM), el puesto, el indicador si esta autorizado a solicitar expedientes, si corresponde el uso de PIN y si es un usuario externo. Para los usuarios que operan aplicaciones en ambiente web se debe relacionar la cuenta de correo institucional con la cual podría autogestionar desbloques de cuentas, olvido de contraseñas o

EMITE REYNALDO CERÓN	REVISA VILMA MOLINA	APRUEBA BERNARDO LOPEZ	FECHA DE VIGENCIA 27/05/2021	Página 1 de 5
------------------------------------	-----------------------------------	--------------------------------------	---	---------------

 SERTRACEN	PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE CALIDAD	CODIGO SPA-024
TÍTULO POLITICA DE CAMBIO DE CLAVES DE ACCESO		REV: 11

finalización de vigencia de los passwords. Toda esta información debe venir incluida en el formulario en mesa de ayuda SFA-032 FORM.CREACION Y ADMON.DE USUARIOS


La contraseña asignada en la creación del usuario de base de datos, para el caso de la primera vez, estará compuesta por las dos primeras letras del usuario + un numero de 4 cifras asignado aleatoriamente + dos letras asignadas aleatoriamente.

Esta contraseña inicial solamente será utilizada para identificarse en el sistema la primera vez y desde ese instante será el mismo sistema que le obligará a cambiarla antes de acceder a cualquier otra opción y a partir de ese momento será el mismo usuario el responsable de administrar su password siguiendo las políticas establecidas en este procedimiento.

Habrá cuatro políticas para el uso del password o palabra clave:

- Tendrá validez de 30 días calendario, pasados los 30 días el sistema dará 5 días más para que sea cambiado. Durante estos 5 días de gracia, cada vez que el usuario se conecte a sus menús de trabajo, el sistema le alertará que debe cambiar su clave, de la siguiente manera: *SU PASSWORD EXPIRA EL<fecha_de_expiracion>, CAMBIELO DENTRO DE <numero_de_días> DÍAS*. Este mensaje solo es informativo, por lo que el sistema le permitirá ingresar y operar sin ningún tipo de restricción; cuando realice el cambio al nuevo password volverán a iniciar los 30 días de validez. Si la clave de acceso no fuese actualizada, durante los primeros 4 días de gracia, el quinto día el sistema modificará el mensaje de alerta, por el siguiente: *SU PASSWORD EXPIRA ESTE DIA, CAMBIELO EN ESTE MOMENTO O SE BLOQUERA SU USUARIO*, y nuevamente permitirá el ingreso; sin embargo, estará obligado a cambiarlo en esa misma sesión de trabajo, de lo contrario se bloqueará y no le permitirá ingresar nuevamente al sistema (ora-28000: the account is locked).
- Los passwords que cada usuario seleccione debe contener las siguientes características: la longitud debe tener entre 8 y 15 caracteres, tener al menos un numero; no debe ser el mismo user como parte de la clave, solamente debe contener letras y números no caracteres especiales, y no ser las siguientes palabras 'welcome1', 'password1', 'password12', 'password123', 'clave123', 'clave1234', 'sertracen1', 'sertracen123', 'abc12345', 'a1234567', 'a12345678', 'a123456789', 'a0123456', 'a01234567', 'a012345678', 'a0123456789', 'dios1234', 'amor1234', 'fe123456', 'jesus123', 'aaa12345', 'bebe1234'

EMITE REYNALDO CERÓN	REVISA VILMA MOLINA	APRUEBA BERNARDO LOPEZ	FECHA DE VIGENCIA 27/05/2021	Página 2 de 5
------------------------------------	-----------------------------------	--------------------------------------	---	---------------

 SERTRACEN	PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE CALIDAD	CODIGO SPA-024
TÍTULO POLITICA DE CAMBIO DE CLAVES DE ACCESO	REV: 11	

- La reutilización del password será permitida solamente después de haber transcurrido 1 día y de haber realizado dos cambios históricos con diferentes claves. El error que se mostrará en la parte inferior de la aplicación de cambio de password será ORA-28007
- Solamente se permitirán 3 intentos fallidos de ingreso al sistema. Después del tercer intento, el usuario se bloqueará (ora-28000: the account is locked).

Los usuarios que estén autorizados al uso de PIN se les seteará inicialmente el 1234 y podrán modificarlo en la misma opción de cambio de password en la sección definida para ello.

Habrán dos políticas para el uso de sesiones:

- Las sesiones simultáneas o concurrentes que un usuario podrá operar son de 3, y esto incluye la conexión por ejecución de reportes; la excepción de esta cantidad será autorizada por la GG. Esta política aplica para ambiente cliente/servidor y aplicaciones WEB.
- El tipo de conexión inactiva permitida será de 60 minutos, pasado este tiempo la sesión no podrá ser utilizada. Estas sesiones suspendidas por tiempo de inactividad serán eliminadas de la base de datos cada 15 minutos por un proceso automático programado a nivel de base de datos.


La configuración de las políticas de password y sesiones, así como sus excepciones, están determinadas por “profiles” asignado a cada usuario por su ubicación laboral según lo establecido en el procedimiento SPA-150 POLITICA DE BASE DE DATOS.

Si algún usuario interno o externo con acceso al sistema se le expira su clave de acceso o llega a bloquear el usuario, por el no cumplimiento de alguna de las políticas anteriores, deberá seguir el procedimiento SPA-080 Proceso de Desbloqueo de Usuarios.

CONTROL DE ACCESO Y PROGRAMAS


- Innovación y Desarrollo de Sistemas en coordinación con la Gerencia de Operaciones y las jefaturas de SERTRACEN define los perfiles de acceso que uno o más usuarios de dicha área podrán tener asignados en la Base de Datos. En el caso de usuarios Externos la coordinación es siempre con la Gerencia de Operaciones y la jefatura de Soporte Operativo.

EMITE REYNALDO CERÓN	REVISA VILMA MOLINA	APRUEBA BERNARDO LOPEZ	FECHA DE VIGENCIA 27/05/2021	Página 3 de 5
------------------------------------	-----------------------------------	--------------------------------------	---	---------------

 SERTRACEN	PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE CALIDAD	CODIGO SPA-024
TÍTULO POLITICA DE CAMBIO DE CLAVES DE ACCESO		REV: 11

- A cada uno de los perfiles se le asocia directamente uno a uno los programas a los que se requiere el acceso tanto en ambiente cliente/servidor como web.
- Cada programa tiene asociada una versión, la que se actualiza con cada cambio solicitado con los formularios de MODIFICACION A OBJETOS DEL SISTEMA SPA-009 y de CREACION DE OBJETOS AL SISTEMA SPA-008 en la mesa de ayuda respectivamente, para los programas versión cliente/servidor por la residencia local de estos se utiliza para asegurar que no hayan versiones desactualizadas; para las versiones Web por ser una publicación única para todos los autorizados la versión es para referencia de la operatividad con respecto a los cambios gestionados.
- Innovación y Desarrollo mantendrá una matriz, en el sistema, de accesos autorizados a los programas, con una relación USUARIO-PERFILES-PROGRAMAS
- Los usuarios solamente podrán ejecutar aquellos programas que están relacionados a alguno de los perfiles que tiene asignados.
- Los perfiles definidos para usuarios internos estarán basados en roles de base de datos.
- Los perfiles definidos para usuarios externos serán administrados por un mecanismo diseñado en tablas de base de datos y los roles Estándar que se asignarán serán rpv_consulta, rpv_general y password.
- Los usuarios internos o externos podrán ejecutar solamente los programas con la versión vigente y registrada en la base de datos si es ambiente cliente/servidor.
- Los usuarios internos o externos tendrán autorizado el ingreso simultaneo a tres sesiones como máximo, caso contrario será autorizado por la GG.
- Los usuarios externos autorizados exclusivamente a consultas solamente tendrán asignado el role de RPV_CONSULTAS o LIC_CONSULTAS
- Ningún usuario que se cree para base de datos tendrá asignado permisos de “alter user”; así que los programas de cambios de claves personales invocan procesos programados a nivel de base de datos que se ejecutan con el owner del esquema de base de dato en RPV o Licencias.
- El acceso a consultar información critica como direcciones, teléfonos, características básicas de los vehículos (chasis, VIN, motor), imágenes de fotos, huellas o firmas solamente será asignándosele un perfil específico que será solicitado por nota del VMT para el caso de usuarios externos y por la Gerencia General para usuarios internos.

EMITE REYNALDO CERÓN	REVISA VILMA MOLINA	APRUEBA BERNARDO LOPEZ	FECHA DE VIGENCIA 27/05/2021	Página 4 de 5
------------------------------------	-----------------------------------	--------------------------------------	---	---------------

 SERTRACEN	PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE CALIDAD	CODIGO SPA-024
TÍTULO POLITICA DE CAMBIO DE CLAVES DE ACCESO	REV: 11	

- Todos los usuarios internos o externos accesarán al sistema por aplicaciones cliente/servidor o ambiente web identificándose en el menú de trabajo asignado a su área ya que estos están “certificados” como desarrollo propio de SERTRACEN. Cada programa y/o reporte, después de validar el acceso autorizado a través de una función de SYS, marcará la sesión del usuario como “APP STC+[PROGRAMA]+[HORA DE CONEXIÓN]”.
- Innovación y Desarrollo considerará como intrusa una conexión que no ingrese por un aplicativo autorizado:
 - Identificación a las bases de datos por SQL Plus, SQLDeveloper o TOAD que no se realice con usuarios de I+D.
 - Desarrollo en Developer 2000 (forms) certificado como “APP STC+[PROGRAMA]+[HORA DE CONEXIÓN]”.
 - Desarrollos Web publicados en servidores internos propiedad de Sertracen SERVER6.SERTRACEN.COM.SV y OAS.SERTRACEN.COM.SV, JBOSS1.SERTRACEN.COM.SV
 - Programas de ejecución calendarizada a nivel base de datos y servidores invocados por usuarios automáticos, detallados en la sección usuarios de procesos automáticos del procedimiento SPA-154 REGISTRO DE PROCESOS AUTOMATICOS EN BASE DE DATOS.
- Innovación y Desarrollo de Sistemas monitorea las conexiones de base de datos y al identificar una conexión que sea considerada como intrusa, a través de un monitoreo programado, lo desconectara e ingresara a bitácora correspondiente la acción.

FIN DEL PROCEDIMIENTO

EMITE REYNALDO CERÓN	REVISA VILMA MOLINA	APRUEBA BERNARDO LOPEZ	FECHA DE VIGENCIA 27/05/2021	Página 5 de 5
------------------------------------	-----------------------------------	--------------------------------------	---	---------------