MINAGRICULTURA	INSTRUCTIVO	Versión 1
	CREACIÓN DE CONTRASEÑAS SEGURAS	IN-GST-05
		FECHA EDICIÓN 22-09-2016

1. OBJETIVO

Facilitar al personal del Ministerio de Agricultura y Desarrollo Rural la elaboración de contraseñas seguras para el acceso a los servicios, sistemas de información y sistemas informáticos de la Entidad, con el fin de reducir la posibilidad de acceso no autorizado y divulgación de la información del Ministerio.

1 DEFINICIONES

Clave o Contraseña: Es una forma de verificar la identidad de un usuario. Por lo general está compuesta por una secuencia de caracteres (números, letras, signos de puntuación o caracteres especiales) que el usuario debe suministrar después de escribir su nombre para poder tener acceso a un servicio, sistema de información o equipo informático. Existen otras formas de verificar identidad de los usuarios como: huellas digitales, patrones de voz o dispositivos electrónicos que pueden almacenar la contraseña.

2 CONDICIONES GENERALES

Las contraseñas son creadas por los usuarios previa autorización de la creación de su cuenta de usuario por parte de los debidamente autorizados.

Las contraseñas están expuestas a múltiples riesgos como el olvido, lo que conduce a no poder tener acceso al servicio, sistema de información o equipo informático. Por lo anterior los usuarios deben seleccionar contraseñas que sean de fácil recordación.

La contraseña también está expuesta a la divulgación no autorizada, lo que conduce a la pérdida de la confidencialidad cuando un usuario no autorizado tiene acceso a la contraseña y hace uno no autorizado de un servicio, sistema de información o equipo informático.

Las contraseñas son personales e intransferibles y se deben mantener es estricta confidencialidad.

La contraseña asignada a un usuario es personal e intransferible. Los usuarios no deben divulgar, prestar, exhibir, comunicar en forma escrita o verbal su contraseña. Cuando por labores de soporte o mantenimiento se requiere la contraseña de usuario, el usuario es quién debe digitarla y al final de las actividades de soporte se debe cambiar por una contraseña nueva.

REVISO	APROBO
Angelica M Salinas Mayorga. Nombre: Angélica Maritza Salinas Mayorga Cargo: Profesional Especializado Fecha: Septiembre 22 - 2016	Nombre: Fidel Antonio Torres Moya Cargo: Jefe Oficina de Tecnologías de la Información y las Comunicaciones Fecha: Septiembre 22 - 2016

Los administradores de servicios, sistemas de información, equipos informáticos deben utilizar contraseñas diferentes para sus cuentas de usuario y para sus cuentas como administradores.

Los usuarios son responsables de todas las acciones que se realicen con sus contraseñas. En caso de que la contraseña haya sido conocida por terceros, el usuario debe informar inmediatamente a la mesa de servicios para bloquear cualquier acceso a servicio, sistema de información o equipo informático que utilizará la contraseña comprometida.

El uso de software para visualizar, descifrar o interceptar contraseñas de servicios, sistemas de información o equipos informáticos del Ministerio de Agricultura y desarrollo Rural está prohibido.

Los usuarios de servicios, sistemas de información o equipos informáticos de la Entidad no deben usar las contraseñas asignadas de la Entidad en servicios gratuitos de correo electrónico, mensajería instantánea o redes sociales, igualmente, las contraseñas personales de servicios externos no se deben usar como contraseñas de servicios, sistemas de información o equipos informáticos del Ministerio.

Si el administrador de un servicio, sistema de información o equipo informático le asigna una contraseña inicial, usted deberá cambiarla por una nueva contraseña, que solo sea de su conocimiento.

Las contraseñas no deben ser enviadas por correo electrónico, sistemas de mensajería instantánea, ni impresas.

Las contraseñas no deben estar almacenadas en archivos legibles o escritas en papel, no la deje al alcance de terceros (debajo del teclado, en un cajón del escritorio, etc.) y NUNCA pegadas en áreas visibles.

Cambie sus contraseñas si sospecha que alguien puede conocerlas.

3 DESARROLLO

Cuanto más segura sea la contraseña, más protegido estará el equipo contra personal no autorizado y amenazas como hackers y software malintencionado. Siempre se deben tener contraseñas seguras para el uso de servicios, sistemas de información o equipos informáticos.

3.1 ¿Qué es una contraseña segura?

Se considera que una contraseña es segura si cumple con los siguientes criterios

- Tiene (8) ocho caracteres como mínimo.
- No contiene el nombre de usuario, el nombre real o el nombre de la Entidad o partes del nombre de la Entidad.
- No contiene una palabra completa.
- Es significativamente diferente de otras contraseñas anteriores.

- Está compuesta por combinación de los siguientes caracteres:

Mínimo una letra Mayúscula, ejemplo: A, M, O, F, H, E, X, O
Mínimo una letra Minúscula, ejemplo: p, c, r, s, a, d, l
Mínimo un número (digito), ejemplo: 0, 1 ,2 3,4 5,6 7,8, 9,
Mínimo un signo o carácter, Símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números) y espacios, por ejemplo: ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? / ;

3.2 ¿Qué no debe contener una contraseña?

A continuación, vera algunos ejemplos de MALAS contraseñas

No utilice solamente palabras o números — Nunca debería utilizar únicamente letras o sólo números en una contraseña. Los siguientes son ejemplos de MALAS contraseñas:

- 8675309
- Juan
- Atrapame
- Qwerty
- 12345
- German1967
- Minagricultura

No utilice palabras reconocibles — Palabras tales como nombres propios, palabras del diccionario o hasta términos de shows de televisión o novelas deberían ser evitados, incluso si utiliza números al final de éstos. Ejemplo: Perro, Elefante, Orion, Zeus,

No utilice palabras en idiomas extranjeros — Los programas de descifrado de contraseñas a menudo verifican listas de palabras que abarcan diccionarios de muchos idiomas. No es seguro confiarse en un idioma extranjero para asegurar una contraseña. Ejemplo: harigato, domo, spasiva, obrigado, merci

No utilice información personal — Manténgase alejado de la información personal. Si un atacante conoce quién es usted, la tarea de deducir su contraseña será aún más fácil. La lista siguiente muestra los tipos de información que debería evitar cuando esté creando una contraseña:

- Su nombre
- El nombre de sus mascotas
- El nombre de los miembros de su familia
- Fechas de cumpleaños
- Su número telefónico
- La dirección de su casa

- Sus gustos o aficiones

3.3 Cómo crear una contraseña segura

Hay muchos métodos que la gente utiliza para crear contraseñas seguras. Un método que le ayudará a crear una contraseña segura y que además pueda recordar con facilidad es el uso de acrónimos. A continuación, se explica el método:

1) Piense en una frase memorable, tal como:

Todo colombiano, tiene derecho a su buen nombre y a su intimidad.

2) Luego, cambie la frase a un acrónimo (incluyendo la puntuación). En este ejemplo se usó la primera letra de cada palabra, pero usted puede seleccionar cualquier letra dentro de las palabras

Tc,tdasbnyasi.

3) Añada complejidad sustituyendo números y símbolos por letras en el acrónimo. Por ejemplo, sustituya la t por el número 7, la s por el signo $, la a por el símbolo @

7c,7d@$bny@$i.

4) Añada un poco más de complejidad colocando mayúscula al menos una letra,

7c,7d@$BnY@$i.

5) Por último, no utilice esta contraseña de ejemplo en ninguno de sus sistemas o computadores.

4 HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
22-09-2016	1	Versión inicial del documento