Política de Protección de Usuarios y Contraseñas del Sistema CMS

Julio 2020

1. Introducción

Las contraseñas son un aspecto muy importante de la Seguridad de la Información. Una contraseña débil puede dar lugar a accesos no autorizados y/o explotación de recursos federales. Todos los usuarios con acceso al Sistema CMS, son responsables de tomar las medidas adecuadas para seleccionar y proteger sus contraseñas, como se indica a continuación:

2. Objetivo

El propósito de esta política es establecer un estándar de uso de contraseñas seguras, la protección de esas contraseñas y su frecuencia de cambios.

3. Alcance

El alcance de esta política incluye a todo el personal que tiene o es responsable de una cuenta para ingresar y hacer uso del sistema CMS.

4. Altas de Usuarios para el CMS

4.1. Procedimiento

4.1.1. El alta de los usuarios debe solicitarse directamente en el sistema de acreditaciones en la URL: https://servicios.gob.mx/acreditaciones/,éste es el único medio autorizado para el alta de nuevos usuarios en el CMS.

4.1.2. Debe ingresar los siguientes datos.

4.1.2.1. El folio es de control interno de tu dependencia, ejemplo: CEDN/UGD/328/2020.

4.1.2.2. Cambio de contraseña.

4.1.2.3. Nombre completo del usuario

4.1.2.4. Correo electrónico institucional

4.1.2.5. Rol de usuario: Administrador, Editor o Redactor.

4.1.2.6. Cargo Institucional

4.1.2.7. Unidad, Dirección o Área

4.1.2.8. Institución

4.1.2.9. Se deberá firmar la carta con la FIEL (Certificado, Clave Privada y Contraseña)

5. Política

5.1. Cambio de Contraseña

5.1.1. Se recomienda que cuando le llegue su contraseña la cambie inmediatamente

5.1.2. Todas las contraseñas de nivel de usuario deben ajustarse a las especificaciones siguientes:

- La contraseña debe contener mínimo 12 caracteres, se recomienda el uso de mayúsculas, minúsculas, números.

5.1.3. Los usuarios no deben usar la misma contraseña de acceso al Sistema CMS para otro tipo de accesos no relacionados con el mismo o diferentes necesidades de acceso (por ejemplo, cuentas de correo personal, redes sociales, otros sistemas institucionales, etc.).

5.1.4. Todas las contraseñas de acceso al sistema deben ser cambiadas al menos cada mes.

5.1.5. Si una cuenta de usuario no ha sido utilizada en un periodo mayor a 6 meses, la contraseña de acceso será automática modificada.

5.1.6. Es responsabilidad de los administradores notificar al correo soporte.desarrollo@datos.gob.mx, cuando un usuario sea dado de baja de la institución para cancelar la cuenta, ya que los usuarios y contraseñas no son transferibles.

5.1.7. Se recomienda no hacer uso de contraseñas fáciles de adivinar como: Fechas, números consecutivos, nombres de seres queridos, nombres de la dependencia etc.

5.2. Protección de Contraseñas

5.2.1. La contraseña debe ser tratada como información confidencial.

5.2.2. La contraseña no se debe adjuntar en mensajes de correo electrónico u otras formas de comunicación electrónica.

5.2.3. La contraseña no debe ser revelada por teléfono a nadie.

5.2.4. No debe de revelar la contraseña en cuestionarios o formularios de seguridad de ningún tipo.

5.2.5. No deje pistas del formato de una contraseña (por ejemplo, "nombre de mi familia").

5.2.6. No comparta la contraseña con nadie, incluyendo asistentes, administrativos, secretarias, directivos, dueños, socios, compañeros de trabajo durante las vacaciones, amigos o miembros de la familia.

5.2.7. No escriba ni guarde la contraseña en post-its o papel en cualquier lugar de su oficina. No guarde la contraseña en archivos en su computadora o dispositivos móviles (teléfonos, tablets) sin cifrado.

5.2.8. No utilice la función "Recordar Contraseña" de aplicaciones (por ejemplo, navegadores web)

5.2.9. Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe reportar el incidente inmediatamente y cambiar la contraseña a la brevedad.

6. Excepciones

No hay excepción, cada persona es responsable de su propia contraseña, se recomienda que las instituciones cuenten con más de un usuario de acceso al sistema CMS, para asegurar que en todo momento habrá al menos una persona disponible para realizar las modificaciones necesarias.

7. Incumplimiento

En caso de que se identifique a un usuario violando esta política será reportado con la institución y con el administrador del sitio incluso puede estar sujeto a la baja de la cuenta del CMS.

En caso de tener dudas al respecto, favor de dirigirse a soporte.desarrollo@datos.gob.mx