Lineamientos para el uso de Contraseñas del Instituto Electoral de Michoacán

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Los presentes Lineamientos son de observancia general y obligatoria para todas las personas servidoras públicas del Instituto.

Tienen por objeto establecer medidas útiles para mejorar la seguridad de la información digital del Instituto, con la finalidad que solo pueda tener acceso a ella el personal autorizado.

Artículo 2. Para efectos de estos Lineamientos se entenderá por:

Coordinación:	Coordinación de Informática del Instituto Electoral de Michoacán.
Instituto:	Instituto Electoral de Michoacán.
Intranet:	Red interna institucional para compartir información y servicios informáticos.
PIN:	Número de Identificación Personal
Usuario:	Palabra técnica que identifica una cuenta en determinada plataforma

CAPÍTULO II

DEL USO ADECUADO DE CONTRASEÑAS

Artículo 3. Las contraseñas constituyen la primera línea de defensa para garantizar que el acceso a la información del Instituto solo sea por parte del personal autorizado.

Artículo 4. Ninguna persona usuaria podrá hacer uso de las contraseñas para adjudicarse o apoderarse de manera exclusiva de ningún equipo o servicio tecnológico del Instituto.

Podrá tener la posesión del equipo o servicio tecnológico del Instituto desde que se le asigne hasta que concluya su servicio laboral o hasta que el cambio de funciones dentro del Instituto constituya razón debida para que se le sustituya, cambie o retire el servicio.

Artículo 5. Se entenderá por persona usuaria, aquella persona servidora pública del Instituto que utilice un sistema, aplicación, programa informático, computadora, teléfono inteligente o cualquier otro dispositivo electrónico, al que se tenga que acceder mediante una contraseña institucional.

Artículo 6. Las contraseñas de los servicios del Instituto son exclusivas, secretas e individuales para cada persona usuaria, estas no deben ser compartidas con otras personas.

Artículo 7. La Coordinación está facultada para evadir las contraseñas cuando a solicitud de la persona usuaria se requiera algún ajuste y recuperación de información.

En los casos en que se requiera evadir alguna contraseña por inspección o vigilancia del resguardo y protección de datos del Instituto o de su personal, se deberá dar aviso por escrito previamente a la persona usuaria, señalando los motivos que justifican dicha acción.

Artículo 8. El control de acceso a todos los Sistemas de Información del Instituto y en general cualquier servicio de tecnologías de información, debe realizarse por medio de Credenciales de Acceso (Usuario y Contraseña), las cuales son de uso exclusivo e intransferible.

CAPÍTULO III

ATRIBUCIONES DE LA COORDINACIÓN EN MATERIA DE CONTRASEÑAS

Artículo 9. La Coordinación tiene las siguientes funciones en materia de contraseñas:

I. Asignar usuario y contraseña a la persona usuaria para el acceso a un sistema, aplicación, programa informático, computadora, teléfono inteligente o cualquier otro dispositivo electrónico, al que se tenga que acceder mediante una contraseña institucional.

II. Configurar el servicio de contraseñas en el Instituto.

III. Definir, establecer, difundir y capacitar a todo el personal del Instituto sobre las características que deben contener las Contraseñas de los distintos servicios con el fin de aumentar la seguridad de acceso.

IV. Vigilar que los equipos tecnológicos del Instituto, en particular las computadoras asignadas fuera del Instituto cuenten con una clave que puede ser PIN o contraseña para tener acceso al usuario desde donde labora.

V. Llevar un registro confidencial de las claves de los equipos de cómputo del Instituto, con el fin de resguardarlas y utilizarlas en caso de ser requeridas en situaciones debidamente justificadas.

VI. Autorizar a personal externo al Instituto para que tenga acceso a contraseñas o a información asegurada con estas cuando sea necesario para algún caso particular del personal del Instituto y en el que la Coordinación haya trabajado previamente sin éxito, para lo cual dará previo aviso a la persona resguardante.

CAPÍTULO IV

DERECHOS Y OBLIGACIONES DE LA PERSONA USUARIA

Artículo 10. La persona usuaria tiene los siguientes derechos:

I. Poseer un nombre de usuario y contraseña para utilizar el equipo de cómputo que tiene asignado, para los servicios de red y telefonía IP, así como para el correo electrónico, archivos compartidos, Intranet, Internet, etc.

II. Solicitar el cambio de usuario y contraseña de acuerdo con las necesidades propias.

Artículo 11. La persona usuaria tiene las siguientes obligaciones:

I. Es responsable de todas las actividades llevadas a cabo con su identificación de usuario y contraseña, excepto cuando compruebe que fue víctima de hurto de su información.

II. Notificará inmediatamente a la Coordinación cualquier uso no autorizado de su cuenta, o cualquier intrusión de seguridad detectada.

III. Establecer un protector de pantalla con clave de desbloqueo en los equipos de cómputo institucional asignados, el cual será establecido a criterio personal sin que exceda más allá de 15 minutos.

IV. Procurar que las contraseñas utilizadas sean distintas para iniciar sesión en correo electrónico, la Intranet o Red Privada Virtual, o en alguna otra cuenta.

V. Evitar que los identificadores de usuario y contraseña se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo de la persona resguardante.

VI. Evitar almacenar las contraseñas en algún programa o sistema que proporcione esta facilidad como gestores de autoguardado de contraseñas o llaveros digitales.

VII. Cambiar las contraseñas inmediatamente después de que alguien ajeno al área resguardante de la información haya tenido acceso, aun cuando se trate de actividades institucionales.

CAPÍTULO V

DE LAS CARACTERÍSTICAS PARA CONTRASEÑAS SEGURAS

Artículo 12. Las contraseñas de los usuarios y equipos concernientes al Instituto deberán cumplir con las siguientes características para evitar que alguien no autorizado las vulnere:

I. Una longitud mínima de 8 caracteres donde además se incluyan:
   a) Mínimo de caracteres especiales: 1 (ejemplo *, %, $, #, @, [ ], <>, :, +, ^ etc.)
   b) Mínimo de caracteres en mayúsculas: 1 (letra en mayúsculas)
   c) Mínimo de caracteres en minúsculas: 1 (letra en minúsculas)
   d) Mínimo de caracteres numéricos: 1 (0,1,2,3,4,5,6,7,8,9)

II. No emplear contraseñas usadas previamente, ni usar las mismas para otras cuentas.

III. No utilizar patrones de teclado como: 12345678, 1q2w3e4r5t y qwertyu.

IV. No utilizar fechas de nacimiento o nombres de personas cercanas ya que pueden ser contraseñas vulneradas con facilidad.

CAPÍTULO VI

ACCIONES POTENCIALMENTE DAÑINAS RELATIVAS A LAS CONTRASEÑAS

Artículo 13. Los siguientes aspectos quedan estrictamente prohibidos:

I. Revelar su contraseña personal, así como autorizar o permitir su uso a terceros para actividades ajenas al Instituto. La prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario, cuando la conexión a la red del Instituto se realice vía remota.

II. Anotar la contraseña en cualquier otro medio físico y tenerla a la vista en su lugar de trabajo.

III. Hurtar, hackear usuarios, contraseñas, PIN, o información contenida en redes protegidas por claves de otras personas servidoras públicas del Instituto, desde el interior de éste hacia cualquier otra plataforma o equipo de información.

IV. Hacer mal uso de la información confidencial de alguien o usarla para fines distintos a los determinados entre las personas servidoras públicas. Cuando una de ellas comparta a otra tal información por motivos excepcionalmente urgentes que signifiquen una merma en el cumplimiento de los objetivos del Instituto. Esta responsabilidad se puede acreditar preferentemente cuando existe una solicitud autorizada de por medio para el intercambio de dicha información.

No se exime a los usuarios de la responsabilidad disciplinaria y legal correspondiente de toda aquella acción que no esté documentada y pueda afectar la Seguridad de la Información del Instituto o de alguna persona servidora pública de éste.

TRANSITORIOS

PRIMERO. Los presentes Lineamientos entrarán en vigor al día siguiente de su aprobación, quedando sin efecto cualquier disposición, ordenamiento, lineamiento, política o procedimiento internos que contravengan al mismo o a la normatividad vigente en la materia.

SEGUNDO. En un máximo de 45 días hábiles a partir de su aprobación, la Coordinación deberá elaborar los planes, programas y medidas operativas.