# LINEAMIENTOS CONTRASEÑAS UCM

## Introducción.

Las contraseñas ayudan a proteger toda nuestra información personal. Por lo tanto, saber cómo hacerlas fuertes e irrompibles es muy importante ya que el uso de contraseñas muy obvias o la exposición de contraseñas revelarán su información personal.

El robo de contraseñas suele producirse principalmente por la irresponsabilidad de los propios usuarios. Existen malas prácticas que comprometen su seguridad al crear una nueva contraseña. De las cuales algunas son:

* Compartir tu contraseña.
* Usar la misma contraseña para varias cuentas.
* Mostrar la contraseña públicamente.
* No cambiar la contraseña periódicamente.
* Escribir la contraseña en una nota cerca a la estación de trabajo.
* Almacenar la contraseña en los navegadores web.

Se propone entonces en este documento contenga los lineamientos de buenas prácticas que pretenden ayudar a la comunidad universitaria a tener un mejor manejo de sus contraseñas.

## Objetivo.

* Brindar mayor nivel de aseguramiento a la información concerniente a la UCM como a la información personal de cada una de las personas que tengan una asociación con la universidad.
* Dar mayor profundidad al tema de las contraseñas en la universidad en cuanto a su importancia.
* Crear las directrices necesarias que apoyen la generación de una contraseña segura y como debe de ser su uso correcto.

## Alcance.

Este documento tiene como propósito llegar a todos los estudiantes, docentes y colaboradores de la UCM, que hacen uso de equipos de cómputo, correo electrónico institucional y otros sistemas de información que requieran de un control de acceso dado por contraseña; esto con el fin de concientizar sobre las buenas prácticas y formalizar el correcto uso de las contraseñas seguras.

## Directrices Generales.

* 1. Hacer cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener los registros de auditoría.
  2. Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada.
  3. Exigir por que se escojan contraseñas de calidad, teniendo presente lo siguiente:
* Debe contener al menos doce caracteres.
* No se debe registrar el nombre de usuario, nombre real del usuario o nombre de la compañía.
* No debe contener una palabra completa.
* Debe ser significativamente diferente de las contraseñas anteriores.
* Debe incluir letras mayúsculas, minúsculas, números y símbolos.
* No debe ser una combinación de palabras o letras que se encuentren fácilmente en un diccionario o en el teclado.
  1. Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez.
  2. Exigir al usuario que se cambien las contraseñas en forma regular, según sea necesario.
  3. Llevar un registro de las contraseñas usadas previamente, e impedir su reúso.
  4. No visualizar contraseñas en la pantalla cuando se está ingresando.
  5. Almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones.
  6. Almacenar y transmitir las contraseñas en forma protegida y cifrada.
  7. En caso de tener equipo en las instalaciones de la universidad siendo colaborador o docente, se debe de tener un cifrado para acceder a los equipos de cómputo de la universidad. Manejando una contraseña única para acceder al equipo con conocimiento exclusivo del dueño o responsable del equipo de cómputo.
  8. Definir contraseñas diferentes a los nombres de usuarios o de documentos de identificación.
  9. Se recomienda el uso de gestores de contraseñas para el almacenamiento de estas, que salvaguarden de manera segura las claves de acceso (Psono, Dashlane, lastpass, entre otros). De igual manera se recomienda la creación de contraseñas de alto nivel con caracteres aleatorios.

## Directrices Especificas.

Estas directrices están dadas para usuarios que tengan un rol de administrador de los sistemas de información presentes en la UCM:

* 1. Las contraseñas definidas para acceder a información confidencial o sistemas como usuario de administrador deben de poseer:
* Debe de tener 12 caracteres como mínimo.
* Debe existir una mezcla entre mayúsculas, minúsculas, números y símbolos.
* Las contraseñas deben de ser exclusivas y complejas
* Las contraseñas deben de tener caracteres aleatorios y sin sentido lógico en su orden.
  1. Estas contraseñas se deben cambiar con periodicidad mínimo una vez al año.
  2. Queda estrictamente prohibido prestar las contraseñas de acceso a los sistemas de información de la universidad y a los servicios prestados por la misma.
  3. En la medida de lo posible salvaguardar las contraseñas en lugares seguros como los gestores de contraseña, evitando el uso del papel para tomar nota de estas.
  4. Se busca también que se cumplan las directrices generales por toda la comunidad universitaria, por lo tanto, para quienes tengan un rol de administrador en los sistemas de información deben cumplir todas y cada una de las directrices aquí plasmadas con rigurosidad.
  5. Cuando un colaborador tenga acceso a información confidencial o restringida, y este finalice ya sea su contrato o su necesidad de acceso a los recursos asignados, por parte de la unidad de sistemas se hará cambio de contraseña de equipos y de perfiles de acceso.

## Responsables.

Se define que cada persona es la mejor defensa para salvaguardar su información, por lo tanto, cada miembro involucrado en este proceso, se debe hacer cargo de su cumplimiento y del aseguramiento de la información.

Por otro lado, la unidad de sistemas se encargará de velar por el restablecimiento y las dudas generadas con respecto al manejo de las contraseñas; de igual manera la unidad de sistemas busca salvaguardar la información institucional y activos críticos de la universidad, por lo tanto, para cuando sea necesario se exigirán contraseñas seguras siguiendo las recomendaciones registradas en los presentes lineamientos.