

LINEAMIENTOS PARA CONTRASEÑAS ROBUSTAS

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
Gestión de Tecnologías de la Información

OBJETIVO

Establecer las condiciones especiales que deben tener todas las contraseñas usadas por cada usuario lasallista en las diferentes aplicaciones y/o sistemas de información a los que tiene acceso.

ALCANCE

Aplica para todos los usuarios de la Universidad de La Salle incluido terceros que cuenten con contraseñas de acceso a los sistemas de información, sistemas operativos o equipos propiedad de la Universidad.

TÉRMINOS Y DEFINICIONES

- **Contraseña:** cadena secreta de caracteres que se utiliza para verificar la identidad de un usuario y otorgarle acceso a un sistema, dispositivo, red o servicio.
- **Aplicaciones:** programas de software diseñados para realizar tareas específicas para el usuario, como procesadores de texto, navegadores web, juegos o redes sociales.
- **Sistema Operativo:** software principal que gestiona el hardware y los recursos de una computadora o dispositivo, permitiendo que otros programas funcionen. Ejemplos: Windows, macOS, Linux, Android.
- **Caracteres:** símbolos que representan letras, números, signos de puntuación u otros elementos usados en texto. Ejemplo: A, 9, %, @, etc.
- **Ataques de fuerza bruta:** métodos para descifrar contraseñas o claves probando todas las combinaciones posibles hasta encontrar la correcta.
- **Qwerty:** nombre del diseño más común de teclado, llamado así por las primeras seis letras de la fila superior izquierda del teclado alfabético.

1. CARACTERÍSTICAS

- Mínimo 10 caracteres, aconsejable que tenga entre 12 y 20 caracteres.
- Mezclar letras mayúsculas y minúsculas, números y caracteres especiales como @, \$, #, etc.
- No podrá tener espacios en blanco
- La contraseña no podrá contener nombre de usuarios

2. RECOMENDACIONES AL GENERAR UNA CONTRASEÑA

- Escoja una contraseña fácil de recordar, pero difícil de adivinar
- Cambie números por letras y viceversa, Ej. Seguridad / S3gur1d@d
- No utilice palabras que estén en diccionarios, ya que éstos se utilizan para realizar ataques de fuerza bruta por expertos para detectar las contraseñas.
- No incluya información personal como: nombres de familiares, mascotas, amigos, número de identificación, nombre de la institución, fechas de cumpleaños, patrones de letras o números tales como “123” o “qwerty”.

3. CAMBIAR CONTRASEÑA

- Puede realizar este proceso por medio de <http://www.outlook.com/lasalle.edu.co> (administrativos) y <https://www.outlook.com/lasalle.edu.co> (estudiantes y docentes)
- Ingrese a la plataforma y cambie la clave siguiendo las indicaciones de la plataforma
- Al final le mostrará un aviso informando que la contraseña ha sido cambiada con éxito.

4. RESTABLECER CONTRASEÑA

- Puede realizar este proceso por medio de <https://passwordreset.microsoftonline.com/> (Administrativos, docentes y estudiantes)
- Restablézcala con un código de seguridad al número celular o al correo alterno registrado allí.
- Al final le mostrará un aviso informando que la contraseña ha sido cambiada con éxito.
- Al correo institucional llegará un mensaje informando que ejecuto alguna acción en la plataforma.

5. PERIODO DE VALIDEZ DE LA CONTRASEÑA

- Las contraseñas tendrán una validez de 180 días. Una vez vencido este período, el sistema solicitará obligatoriamente el cambio de contraseña para continuar con el acceso, dicho cambio debe realizarse en <https://www.outlook.com/lasalle.edu.co> (administrativos) y <https://www.outlook.com/lasalle.edu.co> (estudiantes y docentes)
- Aquellos usuarios que no realicen el cambio de su contraseña a tiempo deberán enviar una solicitud desde su correo alterno a gestiondecuentas@lasalle.edu.co, incluyendo:
 - ✓ Carné de la Universidad escaneado
 - ✓ Nombres y apellidos completos
 - ✓ Número de documento
 - ✓ Correo institucional

6. RECOMENDACIONES DE SEGURIDAD

- El uso de contraseñas es personal e intransferible, por lo tanto, no comparta su usuario y contraseña y no permita que otras personas conozcan sus contraseñas

- Si tiene indicios que otra persona utiliza o conoce su contraseña, realice el cambio inmediatamente. En el caso que sus contraseñas se vean comprometidas de aviso inmediato a DTIC- Gestión de cuentas (gestiondecuentas@lasalle.edu.co) y Seguridad Informática (soportesequinfo@lasalle.edu.co)
- Recuerde que el uso inadecuado de cuentas de usuario y contraseñas es responsabilidad exclusiva del usuario y puede conllevar sanciones disciplinarias.
- Evite divulgar contraseñas a través de medios como Internet, correo electrónico o llamadas telefónicas, salvo que se encuentren en archivos cifrados con métodos seguros.
- Las contraseñas son personales y es responsabilidad del usuario a cargo, el uso que se haga de éstas.
- Trate a sus contraseñas con el mismo cuidado que trata a la información que está protegiendo.
- Mediante la integración de Microsoft Identity Manager (MIM), se realiza la creación automática de usuarios en el Directorio Activo a los cuales se les asigna contraseñas robustas provisionales.
- En el caso de aplicaciones o sistemas que no usan autenticación con el Directorio Activo, el administrador se encargará de crear la cuenta de usuario y asignar una contraseña provisional, que deberá cumplir con los requisitos establecidos en el procedimiento.
- Asegúrese de siempre que se ausente de su puesto de trabajo, quede bloqueada su sesión, para esto oprima (Windows + L)
- Si su equipo es compartido, deshabilite el recordatorio de contraseñas
- Utilice contraseñas diferentes para cada sistema o dispositivo.
- No guarde las contraseñas, memorícelas y nunca las comparta con ninguna persona.

CONTROL DOCUMENTAL

CONTROL DE CAMBIOS DEL DOCUMENTO		
VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	2025-11-13	Creación del documento

ELABORÓ	REVISÓ	APROBÓ
Coordinador Infraestructura de Cómputo y Seguridad Informática	DPE _ Equipo Coordinación de Calidad	Director de Tecnologías de la Información