POLÍTICA PARA CREACIÓN Y MANEJO DE CUENTAS Y CONTRASEÑAS PARA USUARIOS UNAB

Contenido

1. Propósito de la política 2
2. Alcance 2
3. Principios 2
   3.1 Confidencialidad de las contraseñas 2
   3.2 Independencia de la autenticación y la autorización 2
4. Creación del usuario 2
5. Reglas de construcción de las contraseñas 2
6. Cambio de contraseñas 3
7. Entrada de contraseñas 3
8. Asignación de contraseñas 3
9. Almacenamiento de la contraseña 3
10. Responsabilidades de los usuarios finales 4
11. Usuarios con cuenta de administrador en los equipos de cómputo de la UNAB 4
12. Remoción de cuentas y permisos de usuario 4

1. Propósito de la política

Las cuentas de usuario y sus contraseñas asociadas son una parte importante en el esfuerzo de la UNAB para asegurar que únicamente las personas autorizadas tengan acceso a los sistemas de información.

En esta política se establecen las directivas para la creación y el manejo de las contraseñas asociadas a las cuentas de usuario en las aplicaciones y en los sistemas operacionales de los equipos de cómputo de la UNAB, esto con el objetivo de establecer los permisos mínimos necesarios para que los funcionarios y estudiantes puedan realizar sus tareas administrativas y académicas.

2. Alcance

Todos los empleados, estudiantes, contratistas, asociados de negocios y proveedores de la UNAB a quienes se les concede el acceso a los sistemas de información.

3. Principios

3.1 Confidencialidad de las contraseñas. Para suministrar autenticación en forma efectiva las contraseñas solo deben ser conocidas por el usuario responsable de la cuenta. Los usuarios finales deben asegurar la confidencialidad de sus contraseñas en todo momento.

3.2 Independencia de la autenticación y la autorización. Para realizar la autenticación de los usuarios se utilizará un repositorio o base de datos de autenticación, de tal modo que los sistemas de información puedan determinar la identidad de un usuario. En cada sistema de información se manejará en forma independiente la autorización y los permisos de acuerdo al rol que desempeña cada usuario en el mismo.

4. Creación del usuario

Los usuarios en los sistemas de información se crearán de acuerdo a la política “Control de acceso a la información en las aplicaciones”.

5. Reglas de construcción de las contraseñas

a) Una contraseña debe estar compuesta por:

- Mínimo Ocho (8) caracteres.
- Al menos una letra en mayúscula.
- Al menos una letra en minúscula.
- Al menos un digito (0 a 9) o símbolo especial ($, #, @, etc.)

b) Una contraseña no debe incluir:

- El nombre o login del usuario.
- El nombre del grupo al que pertenece la cuenta.
- Nada que pertenezca al entorno privado o actividades del usuario, tal como: nombre, fechas significativas (cumpleaños, aniversarios), nombres de los hijos, números telefónicos etc.
- No debe ser el número de identificación de la persona.
- No debe ser una simple variación de una clave o frase contraseña utilizada previamente.

6. Cambio de contraseñas

a) Los sistemas de información deben obligar al usuario a cambiar su contraseña mínimo cada 90 días.

b) Una clave de usuario debe ser diferente de sus tres (3) claves anteriores.

c) En caso de olvido de la contraseña, la misma no podrá ser recuperada, se asignará una nueva contraseña.

d) Los usuarios serán libres de cambiar su contraseña en cualquier momento.

7. Entrada de contraseñas

Los sistemas solo permitirán tres intentos de login. Si la contraseña no es correcta en el último intento permitido, la cuenta del usuario será bloqueada y el usuario deberá utilizar el procedimiento de recuperación de clave.

8. Asignación de contraseñas

Siempre que se asigne por parte del sistema una contraseña a un usuario, la misma debe entregarse vencida, de tal modo que se obligue al usuario a colocar una nueva contraseña.

9. Almacenamiento de la contraseña

Los sistemas de información deben almacenar las contraseñas de forma cifrada e irreversible. Se prohíbe el almacenamiento de la contraseña de los usuarios en texto claro o el descifrado de las mismas.

10. Responsabilidades de los usuarios finales

Un usuario final de los sistemas de información de la UNAB tiene las siguientes responsabilidades:

a) Debe conservar sus contraseñas en secreto.
b) No debe guardar las contraseñas de forma legible en medios impresos expuestos a otros usuarios o terceros a la universidad.
c) No debe entregar su contraseña a nadie, incluso a los administradores o personal de soporte técnico de la UNAB en caso de que ellos lo soliciten como condición para realizar un servicio.
d) No se debe utilizar en sistemas externo incluyendo bancos y redes sociales una clave que se esté usando en los sistemas de la UNAB.
e) No se debe utilizar la función "Remember password" o "Recordar contraseña" en los navegadores.
f) No se deben prestar las contraseñas y no se deben utilizar las credenciales de acceso de usuarios retirados o en periodo de vacaciones.

11. Usuarios con cuenta de administrador en los equipos de cómputo de la UNAB

Para la asignación de un usuario con privilegios de administración, la persona responsable del mismo debe firmar el documento denominado "compromiso de buen uso de las cuentas de administrador" que la UNAB tenga establecido.

12. Remoción de cuentas y permisos de usuario

En el momento en que un usuario termina su vinculación laboral, contractual o convenio con la Universidad se deben remover todos sus permisos en los sistemas de información y se debe desactivar el acceso del usuario a los mismos.

Declaración Final

Esta política fue creada por la Oficina de Seguridad de la Información y revisada por el Comité de Tecnología UNAB. Cada año o en el momento en que se requiera, se verificará la legislación y normas que apliquen en el entorno en el que se desenvuelve la organización para mantener actualizada esta política.