DIRECTORIO DE LA ADMINISTRACIÓN 2021-2025

UNIVERSIDAD AUTÓNOMA DE SINALOA | DIRECCIÓN DE INFORMÁTICA

Dr. Jesús Madueña Molina
Rector

Dr. Gerardo Alapizco Castro
Secretario General

MC. Salvador Pérez Martínez
Secretario de Administración y Finanzas

Lic. Porfirio Galindo Martínez
Director de Informática

MC. Héctor Ulises Salcedo Martínez
Coordinador de Sistemas

Lic. Paulina Soledad Ramos Parra
Responsable del Proceso SYSBD

INFORMES:
Dirección de Informática de la UAS
Tel:(667) 759 38 80
Correo: dirinfo@uas.edu.mx

POLÍTICAS PARA MANTENER SEGURAS LAS CONTRASEÑAS

El acceso a los datos a través de un sistema que controla los permisos específicos de los usuarios a la información, es la base de todo sistema de seguridad informático. La cooperación de los usuarios es esencial para la eficacia de esta, por lo tanto es necesario que sean consientes acerca de sus responsabilidades para el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas.

Para orientar en esta tarea, la dirección de informática ha elaborado el presente folleto con la finalidad de que nuestros usuarios conozcan sus obligaciones respecto al manejo de sus contraseñas.

Http://www.uas.edu.mx/

Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, ya que estas constituyen un medio de validación y autenticación de la identidad del usuario, y consecuentemente un medio para establecer derechos de acceso a los sistemas de información.

Políticas:

a) Mantener las contraseñas en secreto.

b) Realizar el cambio de la contraseña, siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a los siguientes criterios:

1. Que no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, CURP, etc.

2. Que no sean totalmente numéricos (*utilice combinaciones de números y letras*).

3. Que no sean palabras comunes o de diccionario.

4. La contraseña no puede ser igual a la clave de usuario.

5. Deberá de contener una longitud mínima de 8 caracteres.

d) Cambiar las contraseñas cada vez que el sistema lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión.

f) Evitar utilizar las opciones de “recordar contraseña” que ofrecen los diferentes navegadores y algunos sistemas operativos.

g) Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

h) Nunca comparta sus contraseñas con alguien más.

Las contraseñas representan la llave digital de tu identidad, protégela utilizando estas recomendaciones y recuerda que debes mantener su confidencialidad en todo momento.