ESCUELA MILITAR DE INGENIERÍA
“MCAL. ANTONIO JOSÉ DE SUCRE”
BOLIVIA

TRABAJO PRÁCTICO

CARRERA : INFORMÁTICA

ESTUDIANTES : GARY N. HUANCA VICENTE

MATERIA : SOP. TEC. EN HARD. Y SOFT. II

SEMESTRE : 5TO. SEMESTRE

FECHA : 08 DE MAYO DEL 2025

COCHABAMBA - BOLIVIA

ESCUELA MILITAR DE INGENIERÍA
"MCAL. ANTONIO JOSÉ DE SUCRE"
BOLIVIA

Dinámica: "El Guardián Digital"

1. INTRODUCCIÓN.

En el presente subtitulo se presentará una lluvia de ideas con ejemplos sobre las buenas y malas practicas en cuanto al uso de contraseñas.

1.1. Buenas prácticas.

- Usar contraseñas con al menos 10 caracteres.
- Combinar letras mayúsculas, minúsculas, números y símbolos.
- Cambiar la contraseña periódicamente.
- No compartir contraseñas con otras personas.
- No almacenar las contraseñas en los navegadores.
- Usar autenticación en dos pasos

1.2. Malas prácticas.

- Usar contraseñas cortas y sencillas como 12345.
- Tener la contraseña en un papel en el escritorio.
- Usar la misma contraseña para varios sitios, redes sociales, cuentas, etc.
- Compartir contraseñas con otras personas.
- Mantener la misma contraseña durante largos periodos de tiempo.

2. JUEGO DE ROLES.

A continuación se presenta un juego de roles sobre el uso de contraseñas, desde el punto de vista técnico y desde el punto de vista del usuario.

2.1. Desde el punto de vista de TÉCNICO.

PROCEDIMIENTO DE USO SEGURO DE CONTRASEÑAS

A. Objetivo.

Establecer un procedimiento para la creación, uso y mantenimiento de contraseñas seguras, en cualquier institución pública o privada, a fin de garantizar la seguridad de la información.

B. Alcance.

El presente procedimiento es aplicable a todos los usuarios de la institución publica o privada en general.

C. Definiciones/abreviaturas.

Usuario.- Persona autorizada que accede a sistemas informáticos mediante credenciales como nombre de usuario y contraseña. Su identidad debe estar protegida mediante buenas prácticas de seguridad.

Seguridad de la información.- Conjunto de medidas y políticas destinadas a proteger la confidencialidad, integridad y disponibilidad de los datos frente a accesos no autorizados, pérdida o robo.

Caracteres.- Elementos que componen una contraseña, incluyendo letras (mayúsculas y minúsculas), números y símbolos. Una buena combinación de caracteres aumenta la seguridad de una contraseña.

Símbolos.- Son signos especiales como @, #, $, %, usados dentro de las contraseñas para hacerlas más fuertes y difíciles de adivinar por sistemas automáticos o personas malintencionadas.

Seguridad en 2F (doble factor).- Método que añade una capa extra de protección al requerir dos formas de verificación: por ejemplo, una contraseña más un código enviado al teléfono móvil del usuario.

D. Responsables.

Son responsables del cumplimiento de la implementación y control de este procedimiento, el área de Soporte Técnico con todos sus dependientes. Asimismo, los usuarios están en la obligación de cumplir mencionado procedimiento para las contraseñas seguras.

E. Descripción.

- Las contraseñas deben tener un mínimo de 10 caracteres, combinando letras mayúsculas, minúsculas, números y símbolos.
- No deben contener datos personales como nombres, números de celular, números de carnet, fechas importantes u otros que sean fáciles de identificar.
- Las contraseñas deben cambiarse cada al menos cada 90 días, evitando exceder ese límite de tiempo.

- Se debe utilizar el mecanismo de seguridad en dos factores 2F.
- Está prohibido compartir contraseñas con otros usuarios, este es de carácter personal y bajo responsabilidad.
- Esta prohibido entregar contraseñas escritas en papelitos, a fin de evitar infiltraciones o accesos no autorizados.
- El incumplimiento al presente procedimiento puede conllevar restricciones de acceso.
- 3 intentos fallidos en el ingreso de contraseña, bloqueara el acceso de forma inmediata.

2.2. Desde el punto de vista de USUARIO.

A. Requisitos de acceso.

- Nombre de usuario o correo electrónico y contraseña
- Limitar el acceso mediante roles definidos para administradores, Jefes de Área, personal administrativo y otros.
- Autenticación en dos pasos

B. Requisitos de equipamiento.

- Computadora, tablet o celular
- Acceso a una red.
- Software autorizado por el área de TI

C. Niveles de acceso.

- Usuario básico (solo correo y sistemas internos)
- Usuario intermedio (acceso a bases de datos)
- Administrador (configuraciones, usuarios, permisos)

2.3. Situación de ejemplo y solución

Un usuario que olvida su contraseña constantemente y la anota en un papel en su escritorio y después lo guarda en su billetera, perdió el papel lo cual ocasionando que la contraseña se filtre e ingresaron al sistema, provocando un acceso no autorizado. En consecuencia se expuso la seguridad de la información de la empresa, debido a la irresponsabilidad del usuario.

La solución es identificar el acceso no autorizado monitoreando la red y quitar el acceso indebido, recuperar la cuenta y cambiar la contraseña.

Finalmente dar una capacitación concientizando a todo el personal, sobre el riesgo del filtrado de contraseñas y el peligro que representa para la institución.

3. REFLEXIÓN

Una contraseña segura protege el acceso a nuestros datos personales y evita que terceros puedan usarlos sin autorización, reduciendo riesgos como el robo de identidad o la pérdida de información.

Aplicar buenas prácticas como las mencionadas anteriormente, en la creación y manejo de contraseñas es fundamental para mantener la seguridad digital tanto a nivel personal como en entornos institucionales.