I. DESCRIPCIÓN

OBJETIVO

Establecer las especificaciones de seguridad que permitan coordinar las acciones de creación, actualización y almacenamiento de contraseñas, así como el uso de mecanismos complementarios para acceder a los activos de Tecnologías de Información (TI) de la Universidad Veracruzana.

ALCANCE

Aplica a toda persona que haga uso y/o que sea responsable de administrar activos de TI de la Universidad Veracruzana.

DEFINICIONES.

Autenticación de doble factor	Es el proceso de seguridad por el cual el usuario confirma su identidad mediante al menos 2 métodos diferentes.
Cuenta institucional personal	Identificador único de usuario que le permite acceder a los servicios de red y sistemas de información institucional.
Cuenta institucional no personal	Cuenta creada para el uso de una dependencia, entidad académica, programa, evento, notificaciones y sistemas o aplicaciones, entre otros.
Contraseña	Clave confidencial conformada por la combinación de caracteres especiales y alfanuméricos utilizados para acceder a servicios y activos de TI, como equipos de cómputo, comunicaciones, correo electrónico, red institucional, entre otros.
Mecanismo de autenticación	Es el método que se utiliza para verificar que la cuenta y contraseña ingresada es válida e identifica al usuario.
Texto plano	Archivo informático que contiene texto formado por caracteres alfanuméricos legibles por personas.
Usuario	Para este lineamiento se entenderá como usuario, a todos aquellos que hagan uso de servicios o activos de TI de la Universidad Veracruzana.
Activo de TI	Componentes tecnológicos utilizados para procesar, almacenar y comunicar información.
CAPTCHA	CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) es un mecanismo de autenticación pregunta-respuesta, que permite diferenciar si el acceso a un activo de TI lo está realizando una

	persona o de manera automatizada una computadora o dispositivo móvil con internet o bot.
Bot	Programa informático que realiza tareas automáticas y repetitivas asignadas para un rol específico de usuario, con lo cual pretende imitar el comportamiento humano.

II. REGLAS Y CRITERIOS

Generales:

1. Todo activo de TI propiedad de la universidad debe contar con un mecanismo de control de acceso.

2. Todo usuario que requiera hacer uso de los activos de TI, propiedad de la Universidad, deberá hacerlo a través de los mecanismos de control de acceso y autorización vigentes.

3. Todos los usuarios son responsables de las actividades que se realicen con el uso de la información de autenticación bajo su custodia.

4. La longitud de toda contraseña debe ser de al menos 12 caracteres y como máximo 50 caracteres, cumpliendo con los siguientes requisitos:
   a. Al menos un caracter alfanumérico en mayúscula
   b. Al menos un caracter alfanumérico en minúscula
   c. Al menos un caracter numérico
   d. Alguno de los siguientes símbolos/caracteres especiales permitidos: ! # % * + - . = ? _ | ~

5. Para las contraseñas evitar palabras de diccionario o datos que sean de simple deducción, así como de información asociada al usuario como nombre completo, fecha de nacimiento, matrícula, nombre de mascota, entre otros. Ejemplos: "Abc123456789", "Qwerty", "Usuario", "Contraseña", etc.

6. Mantener de manera confidencial la información de autenticación.

7. No guardar las contraseñas en lugares de acceso público y formatos fácilmente identificables.

8. Cambiar la contraseña siempre que exista y/o identifique un indicio de riesgo y reportarlo al Equipo de Respuesta a Incidentes de Ciberseguridad de la Universidad Veracruzana en el correo contactocsirt@uv.mx.

9. No hacer uso de las funciones de "recordar contraseñas" existente en algunas aplicaciones y formularios.

Específicas:

10. Para uso de cuentas institucionales personales:
    a. Aplican las reglas y criterios generales.
    b. Una vez creada y entregada por el administrador del activo de TI, el titular de la cuenta debe cambiar la contraseña en su primer uso.
    c. La contraseña debe cambiarse, al menos, cada 6 meses.
    d. Al generar o actualizar la contraseña, no se podrá hacer uso de las últimas dos contraseñas que hayan sido utilizadas.
    e. No compartir contraseñas con otros usuarios.
    f. No utilizar cuentas institucionales personales en la implementación de aplicaciones o sistemas.
    g. No utilizar cuentas institucionales personales en servicios otorgados por terceros, ejemplos: redes sociales, comercio electrónico, etc.

11. Para uso de cuentas institucionales no personales:
    a. Aplican las reglas y criterios generales.
    b. Utilizar métodos de cifrado en el sistema o aplicación para controlar el uso de la cuenta de acceso al activo de TI.
    c. La periodicidad de cambio de contraseña debe ajustarse a los alcances y limitantes que el activo de TI permita, conforme a sus características y restricciones.

12. Para el establecimiento de controles de acceso al activo de TI, los responsables de administrar el activo deben incluir, si sus características lo permiten, lo siguiente:
    a. Control de número de intentos de acceso fallidos al acceder al activo de TI, bloquear la cuenta después de 3 intentos fallidos por un tiempo determinado.
    b. Incluir mecanismos automatizados de expiración y caducidad de contraseñas.
    c. Además de la contraseña, establecer la autenticación de doble factor como método complementario.
    d. Incluir un CAPTCHA como complemento de autenticación.
    e. Para la entrega de contraseñas a través de medios digitales, no enviarlas en texto plano.

Histórico de Revisiones

No. DE REVISION	FECHA REVISIÓN O MODIFICACIÓN	SECCIÓN O PÁGINA MODIFICADA	DESCRIPCIÓN DE LA REVISIÓN O MODIFICACIÓN
0			

Control de versiones

CÓDIGO	FECHA		VERSIÓN	NIVEL DE CONFIDENCIALIDAD
	VERSIÓN O AUTORIZACIÓN	ENTRADA EN VIGOR		
SGSI-CA-OT-012	04/04/2024	05/04/2024	V 1.0	Público

CREADO POR:

Lic. Rigo Daniel Salazar Falfán
Departamento de Seguridad y Monitoreo (UV-CSIRT)

VoBo:

Mtro. Héctor Bonola Virués
Director de Servicios de Red e Infraestructura Tecnológica

Mtro. José Alejandro Colunga Moreno
Director de Desarrollo Informático de Apoyo Académico

Mtro. Rafael Gomez Quezada
Director de Servicios Informáticos Administrativos

Mtra. Patsy Liliana Sánchez Flores
Director de Extensión de Servicios Tecnológicos

AUTORIZADO POR:

Mtra. María Dacia González Cruz
Director General de Tecnología de Información