1. PROPÓSITO

Establecer los lineamientos técnicos de creación y gestión de contraseñas robustas para el acceso seguro a sistemas y aplicativos institucionales, y que deberán ser de acatamiento obligatorio. Este lineamiento está dirigido a los Gestores de Tecnologías de Información, personal técnico y a la comunidad universitaria.

2. TÉRMINOS Y ABREVIATURAS

- **CSPN (Certification de Sécurité de Premier Niveau):** se utiliza para evaluar y certificar la seguridad de productos y sistemas de tecnología de la información.
- **CI:** Centro de Informática.
- **Código de usuario**: es un identificador único de cuenta institucional que se asigna a un usuario específico.
- **Contraseña segura**: es una combinación de letras, números y símbolos únicos que debe tener un mínimo de quince (15) caracteres de longitud y ser difícil de adivinar para cualquier persona que no sea el propietario de la cuenta.
- **Contraseña de un solo uso (OTP)**: es una contraseña que solo puede ser utilizada únicamente una vez.
- **Doble factor de autenticación (2FA)**: es un método de seguridad que requiere que los usuarios proporcionan dos formas diferentes de identificación para acceder a una cuenta o servicio.
- **FIDO2 (Fast Identity Online 2):** es un conjunto de estándares y protocolos de autenticación desarrollado por la Alianza FIDO (Fast Identity Online Alliance). FIDO2 permite la autenticación en línea segura y sin contraseñas utilizando métodos de autenticación más fuertes, como la autenticación basada en clave pública (PKI) y la autenticación biométrica.
- **FIDO2 UF (User-to-Factor):** se refiere a la autenticación basada en clave pública que se realiza directamente entre el usuario y el dispositivo de autenticación (como un lector de huellas dactilares o un escáner de iris).
- **FIPS (Federal Information Processing Standards) 140-2 Nivel 1 y 2**: establece los requisitos de seguridad para módulos criptográficos utilizados en productos de tecnología de la información. El nivel 1 se refiere a requisitos básicos de seguridad, mientras que el nivel 2 agrega requisitos adicionales, como protección física contra ataques físicos y una mayor capacidad de resistencia a los intentos de violación.
- **Generador de contraseñas**: es una herramienta que crea contraseñas seguras por métodos aleatorios de longitud variable usando combinaciones de letras, números y símbolos.

- **Gestión de contraseñas**: es el proceso de administrar, almacenar y proteger de manera segura todas las contraseñas que se utilizan para acceder a diferentes cuentas en línea.
- **Múltiple factor de autenticación (MFA)**: es un método de seguridad que requiere que los usuarios proporcionan dos formas diferentes de identificación para acceder a una cuenta o servicio, el cual puede ser un OTP generado por una aplicación de autenticación, entregado en un correo electrónico, un mensaje de texto SMS, o una llamada telefónica, controles biométricos como huella digital, reconocimiento facial o iris del ojo, token criptográfico físico, entre otros.
- **OATH-HOTP (HMAC-based One-Time Password):** es un algoritmo de generación de contraseñas de un solo uso basado en HMAC (Hash-based Message Authentication Code). Se utiliza para generar contraseñas desechables que se pueden utilizar como un factor adicional de autenticación en sistemas de autenticación de dos factores (2FA) o autenticación de múltiples factores (MFA).
- **PIV (Personal Identity Verification):** define los requisitos para la emisión de credenciales de identificación personal, como tarjetas inteligentes o tokens, utilizadas para la autenticación segura en entornos gubernamentales y empresariales.
- **Sistemas y aplicativos**: incluye sistemas operativos de servidores y estaciones de trabajo, plataformas, bases de datos, manejadores de contenido, servicios en nube, plataformas institucionales y afines.
- **UCR:** Universidad de Costa Rica.

3. LEYES, REGLAMENTOS O DOCUMENTOS DE REFERENCIA

3.1 El "*Reglamento General de las Oficinas Administrativas*", de la Universidad de Costa Rica, en su Capítulo III, Artículo 9 inciso *"f"* y en el Artículo 10, inciso o), que indica:

f) Emitir directrices, supervisar y establecer procedimientos de acatamiento obligatorio, propias de su área de competencia".

o) Establecer, en conjunto con el Consejo Técnico Asesor, las directrices propias del quehacer y prioridad de la oficina a su cargo".

3.2 El reglamento vigente del Centro de Informática establece en el Artículo 2:

c) Emitir lineamientos, directrices, estándares y normas, acorde con el área de competencia, según lo que establece el *Reglamento de Oficinas Administrativas*.

d) Definir, desarrollar y proponer a la Administración Superior y a la comunidad universitaria las directrices, lineamientos, planes, estándares y normas para la adquisición de productos y servicios de tecnologías de información y comunicación.

4. LINEAMIENTOS

4.1 La creación de contraseñas seguras contribuye con los mecanismos de autenticación mediante claves que deben ser robustas de difícil vulneración. Las siguientes pautas definen la creación y conformación de la contraseña:

a. Las contraseñas deben ser difíciles de descifrar ante una prueba exhaustiva de todas las posibilidades de descubrimiento mejor conocido como técnica de “fuerza bruta”.

b. Debe estar conformada por combinaciones aleatorias de letras mayúsculas, letras minúsculas, números y símbolos; se debe evitar el uso de caracteres como por ejemplo: 1 (uno), l (ele minúscula), I (i mayúscula), 0 (cero), o (o minúscula) y O (o mayúscula)

c. Evitar utilizar información personal o simple como fechas de nacimiento, nombres de mascotas, etc.

d. La contraseña no deberá ser reutilizada, ni estar formada por una concatenación de contraseñas ya utilizadas o de uso anterior.

e. La contraseña es un secreto personal intransferible a terceros, por lo cual no debe entregarse, compartirse, ni comunicarse a nadie.

f. Se recomienda el uso de generadores de contraseñas con los criterios de conformación y longitud indicados. Por ejemplo, https://passwordsgenerator.net/es/

g. Las contraseñas de sistemas institucionales deben cambiarse cada noventa (**90) días** naturales como máximo; este plazo es general, puede que según la relevancia de la plataforma este plazo sea menor, pero nunca superior. Además, el cambio de contraseña en el portal universitario se hace en la dirección: https://miperfil.ucr.ac.cr de acuerdo a las políticas definidas. Solo se aceptan los siguientes símbolos: $. , ! * + % ? @

4.2 Las buenas prácticas de gestión de contraseñas incluye:

a. Las contraseñas deben ser únicas para cada cuenta (no deben utilizarse en varios sistemas y plataformas), ya que esto aumenta el riesgo de que la contraseña sea comprometida.

b. No almacene la contraseña en los navegadores web, ya que, facilita el acceso a estas por terceros.

c. Las contraseñas no deben escribirse en papel, en archivos de texto, notas de dispositivos celulares, ni notas adhesivas en monitores o escritorios, ni bajo otro procedimiento no seguro.

4.3 En caso de que exista evidencia o presunción de compromiso de la contraseña, el cambio debe ser inmediato.

4.4 Utilice un administrador de contraseñas para simplificar y automatizar el proceso de generación y almacenamiento de contraseñas complejas y únicas asociadas a un código de usuario, así como, recordarlas automáticamente. Por ejemplo, aplicaciones como el *Microsoft Authenticator o Google Authenticator.*

4.5 La autenticación de múltiple factor (Multiple Factor Authentication), MFA por sus siglas en inglés, debe activarse cuando el sistema o plataforma lo permita; mediante servicios biométricos como la huella digital, geometría de rostro, o identificación de iris del ojo; tokens criptográficos físicos compatibles con FIDO2, FIDO 2UF, CSPN, PIV, FIPS 140-2 nivel 1 y 2, OATH-HOTP; sistemas contraseñas de un solo uso OTP; esto para fortalecer el acceso a la cuenta además de la contraseña.

4.6 Queda estrictamente prohibido incluir contraseñas en cualquier guion (script, playbook) o código fuente utilizado en sistemas y aplicativos. Las contraseñas son información sensible y su exposición indebida puede comprometer la seguridad y los datos almacenados en estos.

4.7 El encargado de una cuenta departamental debe cambiar periódicamente la contraseña con un máximo de noventa (90) días naturales.

4.8 Los usuarios en general son responsables cambiar todas sus contraseñas de forma periódica y cumplir con las políticas de seguridad establecidas.

4.9 El CI procederá por seguridad con la suspensión de las cuentas institucionales por inactividad mayor a 365 días naturales. El usuario deberá solicitar al CI la habilitación de la cuenta por los medios establecidos.

4.10 Todos los usuarios de los sistemas y servicios de la organización tienen la responsabilidad de crear y mantener contraseñas robustas como medida de protección contra posibles ataques cibernéticos. Una contraseña débil o fácilmente predecible puede comprometer la seguridad y la confidencialidad de la información almacenada.

5. APROBACIÓN

Actividad	Responsable

Elaboración	M.Sc. Abel Brenes Arce, Coordinador Unidad de Riesgos y Seguridad (URS)
Colaboración	Ing. Wilfredo Fonseca, Coordinador Área de Gestión de Servicios (AGS)
Registro y control	Ing. Jeffrey Dimarco Fernández, Coordinador Unidad de Calidad y Mejora Continua (UCM)
Aprobación	Máster Tatiana Bermúdez Páez, Subdirectora C.I. Bach. Cindy Arias Quiel, Coordinadora Área de Gestión de Adquisiciones (AGA) M.Sc. Abel Brenes Arce, Coordinador URS Lic. Jorge Carranza Chaves, Coordinador Área de Gestión de Infraestructura (AGI) Ing. Laura Castro Jiménez, Coordinadora Área de Desarrollo de Servicios (ADS) Ing. Jeffrey Dimarco Fernández, Coordinador UCM) M.Sc. Rebeca Esquivel Flores, Coordinadora Área de Gestión de Comunicaciones (AGC) Ing. Wilfredo Fonseca Vargas, Coordinador Área de Gestión de Servicios (AGS) Lic. Jairo Sosa Mesen, Coordinador Área de Gestión de Usuarios (AGU) Máster Ana Yanci Tosso, Coordinadora Unidad Administrativa y Recurso Humano (UAR) Dr. Henry Lizano, Director C.I.

UCR Firmado digitalmente