Pontificia Universidad Católica de Chile

Política de Clave UC

Código documento	:	Política Clave UC
Versión	:	1.2.1
Preparado por	:	Dirección de Informática UC
Preparado para	:	UC
Autor	:	Marcelo Maraboli
Fecha creación	:	enero 2020
Última modificación	:	agosto 2022
Revisado por	:	Diego Biscar
Aprobado	:	agosto 2023

TABLA DE CONTENIDOS

1. INTRODUCCIÓN

1.1 Propósito

- Definir la Política de Clave de las Cuentas UC, Administradores de Sistemas, Cuentas de Infraestructura Backend y Cuentas Locales.
- Mejorar la seguridad del acceso a los recursos, sitios y sistemas UC.

1.2 Aplicabilidad

El documento aplica a cualquier persona o sistema que tenga acceso a algún recurso informático UC.

1.3 Glosario de términos y abreviaturas

AD	:	Repositorio central de cuentas de usuario, principalmente para sistemas basado en Windows
Backend	:	Sistemas que dan un servicio informático a otros sistemas y que no son accesibles directamente por los usuarios
CAS UC	:	Sistema Central de Autenticación para sitios y sistemas web UC
Clave UC	:	Clave de acceso para la Cuenta UC
Cuenta UC	:	Cuenta de usuario en ambiente LDAP y/o AD
DI	:	Dirección de Informática UC
LDAP	:	Repositorio central de cuentas de usuario
TI	:	Tecnología de Información
Red UC	:	Red de Datos UC
UC	:	Pontificia Universidad Católica de Chile

2. PRINCIPIOS

La Cuenta UC es una credencial que sirve para acceder a las aplicaciones y sitios principales de la universidad. Se compone de un login (usuario) y clave (contraseña).

Dicha clave informática en la UC se define como parte del mecanismo de autenticación de un usuario basado en un "secreto memorizado" que se utiliza para acceder a un sistema o servicio.

La fortaleza de dicha clave es un factor importante para evitar accesos no autorizados, es decir, accesos por parte de personas a las cuales no les fue otorgado el permiso de acceso al sistema o servicio y en consecuencia el acceso a información o acciones dentro del sistema.

Este documento estipula los requerimientos mínimos que una clave debe cumplir, así también como su gestión y ciclo de vida.

Se reconocen 4 tipos de cuentas de acceso

1. **Cuenta UC**: Cuenta de usuarios definidas en LDAP y/o AD. Aquí se encuentran las cuentas del dominio "@uc.cl", ucvirtual, "@iglesia.cl" entre otros.
2. **Sysadmin**: Cuenta de administradores de sistemas o aplicación para la gestión informática de sistemas, servidores y equipos de comunicación. Estas cuentas son generalmente destinadas a personal informático especializado con roles de administración y gestión.
3. **Cuenta de Infraestructura Backend**: Cuenta utilizada por un sistema para acceder a otro sistema o infraestructura (LDAP, BD, Web Service, etc.)
4. **Cuenta Local**: Cuenta definida en forma local dentro de un sistema específico y que no es almacenada en un repositorio central y solo sirve para acceder al sistema en cuestión.

Esta Política de Clave UC se basa en la Norma NIST SP 800-63 [1] de junio del 2017. La Universidad de Stanford [2] y el MIT [3] han adoptado esta misma norma.

En concordancia con la Norma NIST, la UC utiliza los siguientes niveles para las cuentas tipo (1), (2) y (4):

- **Nivel de aseguramiento de la Identidad del Usuario = nivel 3.**
  IAL Identity Assurance Level 3 (In-person identity proofed). La validación de identidad la realiza la Dirección de Personas, Dirección de Registros Académicos de alumnos y/o un Director Económico y de Gestión de facultad o unidad.

- **Nivel de aseguramiento del autenticador = nivel 1 o 2**
  AAL Authenticator Assurance Level 1 (Autenticación de un factor a través de Clave UC (un secreto memorizado o password)).
  AAL Authenticator Assurance Level 2 (Autenticación de dos factores).

Para las cuentas tipo (3), no aplican los IAL y AAL dado que son accesos automáticos de una aplicación a otra.

Para la gestión de las Cuentas UC y, en consecuencia, la gestión de la Clave UC, se definen 4 principios:

- **1)** ***Para crear una Cuenta UC es <u>requisito</u> exigir el correo personal e insertarlo en la BD***
    - Toda cuenta UC debe tener definido un email personal
    - El correo personal no puede ser @uc.cl o @puc.cl

- **2)** ***No se deben enviar claves a los usuarios***
    - Por ningún medio ni a través de terceros
    - El usuario debe utilizar los métodos de **Restablecer Clave** disponibles en micuenta.uc.cl

- **3)** ***Para fijar una CLAVE debe hacerse mediante un mecanismo vía webservice***
    - Un script sólo puede fijar claves aleatorias
    - Solo el usuario puede fijar una clave a elección que cumpla la política

- **4)** ***Los webservices son el único medio para gestión de Cuentas UC***
    - Crear/Modificar/Borrar/Bloquear Cuenta UC
    - Fijar clave Aleatoria (Wservice escoje y fija clave aleatoria)
    - Fijar clave por parte de un usuario
    - Consultar login de un RUT
    - Consultar login disponible dado (nombres, apellidos)
    - Otros de gesión de cuenta

3. RESPONSABILIDADES

3.1 Responsabilidad del usuario

La Cuenta UC es un acceso entregado a una persona individualizada miembro de la Comunidad UC. En consecuencia, la Cuenta UC es considerada PERSONAL, PRIVADA e INTRANSFERIBLE y la persona es considerada responsable de todas las acciones que se realicen con la Cuenta UC que le fue entregada.

Los deberes del usuario son:

- **Cuidar su Clave UC**, es decir, elegir una clave segura (difícil de adivinar o descubrir) y no almacenarla en forma insegura.
- **No compartir su Clave UC** (ni ninguna clave de un sistema UC) con otras personas o divulgarla por ningún medio.
- No debe utilizar su Cuenta UC para acceder a sistemas a los cuales no se le ha dado autorización para acceder.
- Si el usuario sospecha que su Cuenta UC ha sido vulnerada o posee actividad sospechosa, lo **debe reportar** de inmediato a la Dirección de Informática UC.

Recomendaciones:

- Utilizar un gestor de claves (Password Manager) para administrar sus múltiples claves y/o sus claves de gran largo.
- NO DEBE ocupar su clave UC como clave en otros sitios externos a la UC.
- No debe escribir su clave en un papel
- No almacenar claves en los programas (navegador, lector de email, etc).
- Si deja grabada la Clave UC en algún software (Outlook, navegador), el usuario no debe dejar el computador desatendido (sin clave de acceso) ni prestar temporalmente el computador a otro persona.
- No utilice la misma clave en diferentes sistemas o sitios web.

3.2 Responsabilidad del custodio de Claves UC

Las Claves UC son almacenadas en un repositorio LDAP y Active Directory. La unidad responsable de ese repositorio (DI) tiene las siguientes responsabilidades:

- Solo almacenar las Claves UC en forma cifrada con un estándar seguro e irreversible en su cifrado.
- Cautelar el acceso a las Claves UC cifradas para evitar copias no autorizadas
- Cautelar el acceso autorizado al repositorio LDAP/AD
- No permitir el transporte de datos sin cifrado de seguridad
- Habilitar notificaciones automáticas al usuario cuando la Clave UC ha sido cambiada.

- Monitorear el acceso al repositorio y alertar actividades irregulares al Área de Seguridad de la Dirección de Informática, con el propósito de conducir una auditoría.

3.3 Responsabilidad de los Jefes de Sistemas

Las Claves UC son ingresadas en los sistemas UC o en el sistema de autenticación central UC (CAS). A través de estos sistemas o sitios web transita la Clave UC y en consecuencia deben adoptarse ciertas medidas para su cuidado.

Los Jefes de Sistemas tienen la obligación de:

- No incluir claves de acceso de ningún tipo en el código fuente de sus programas.
- No incluir código que permita copiar o registrar las claves de acceso de los usuarios.
- No permitir el transporte de claves sin cifrado de seguridad
- Configurar o programar sus aplicaciones para autenticar a los usuarios mediante el sistema CAS o el repositorio central UC.

4. ESTRUCTURA DE CLAVE UC

4.1 Estructura de clave para Cuenta UC

Requisitos:

- **Longitud mínima**: 8 caracteres
- **Longitud máxima**: 128 caracteres
- **En base al largo de la clave escogida, debe cumplir**:
  - 8-11: mayúsculas, minúsculas, números, símbolos – al menos 1 de c/u
  - 12-15: mayúsculas, minúsculas, números – al menos 1 de c/u
  - 16-19: mayúsculas, minúsculas – al menos 1 de c/u
  - 20+: sin restricciones (al set de caracteres)
- **Caracteres permitidos**: **a-z, A-Z, 0-9, espacio**, signos de puntuación del teclado español: `.!"#%&()` `*+,-/:;<=>?_$@{}`
- NO DEBE exigirse expiración de la clave

- La clave NO DEBE COINCIDIR con:
  a) alguna las 5 últimas claves (se almacena el HASH de claves antiguas)
  b) una palabra del diccionario español o inglés (caso 16 char o mayor)
  c) una palabra del diccionario español o inglés (caso 16 char o mayor) con sustituciones conocidas de letras ($ = s, 4 = A, @ = a, etc.) [3]
  d) una palabra del diccionario español o inglés con capitalizaciones intermedias (i.e. cAsa, CAsa, CasA, casA) (caso 16 char o mayor)
  e) una clave del diccionario de claves conocidas [5]
  f) una clave de diccionario de claves divulgadas de sitios vulnerados (hackeados) [6]

- La clave NO DEBE CONTENER:
  a) el username
  b) alguno de los nombres o apellidos del usuario
  c) 4 caracteres consecutivos iguales

Recomendaciones al usuario:

- Utilizar una frase como clave.
- Ejemplos de claves válidas en Anexo A

4.2 Estructura de clave para Cuenta de Sysadmin

El enrolamiento de una cuenta de Administrador de un sistema DEBE verificar la identidad en forma presencial de la persona ([1] IAL2) asociada a una Cuenta UC. Cada sysadmin DEBE tener una cuenta nombrada personal y no utilizar la cuenta de administración general (sa, root, etc.).

Una cuenta de sysadmin DEBE poseer una estructura de clave igual a la Cuenta UC.

La posibilidad de exigir expiración de la clave será una definición del administrador del servicio en particular (BD, Sistema Operativo, LDAP, Cuenta Administración de una Aplicación, etc.). En consecuencia, un jefe del sistema/servicio en particular podrá exigir expiración de la clave de acceso y la frecuencia de ello, acorde al valor del activo institucional que se está protegiendo.

Se RECOMIENDA el uso de un segundo factor de autenticación para las cuentas de sysadmin. En este caso, no podrá exigirse la expiración.

4.3 Estructura de clave para Cuenta de Infraestructura Backend

- Se DEBE usar una clave difícil de recordar para seres humanos, es decir, de largo superior a 20 caracteres y complejidad alta (con mayúsculas, minúsculas, números, símbolos).

- Se RECOMIENDA utilizar claves aleatorias en formato SHA-256 (estándar SHA2 de 32 caracteres) o superior [7]

  Ejemplo 1:

  ```
  $ echo $RANDOM | shasum -a 256
  c899ead0dc3ecbd76965548ce251320b375f3334b48768e1da2aaf8c4cca32bb
  ```

  Ejemplo2:

  ```
  $ pwgen -vn -A 32 1
  ngr3zcnf5g9pnb5t9r3pk9qzzv243dx6
  ```

- Se RECOMIENDA el uso de API-Key entre aplicaciones.

4.4 Estructura de clave para Cuenta Local

Las cuentas locales en un sistema poseen formato de clave acorde con la política del sistema/software en particular y en muchas ocasiones no es posible fijar características o estructura de la clave.

Se identifican 3 posibilidades:

a) El sistema permite establecer una política de clave. Entonces, el administrador del sistema DEBE configurar el formato de clave lo más similar posible al formato de Cuenta UC (ítem 4.1). El usuario cambiará su clave acorde a esta estructura.

b) El sistema no permite política de clave. Entonces, el administrador del sistema DEBE instruir a los usuarios a fijar una clave de largo 15 o superior.

c) El sistema no permite a los usuarios cambiar su clave y la clave es fijada por el administrador del sistema. En este caso, el administrador DEBE fijar una clave acorde a la política de la Cuenta UC (ítem 4.1).

Se RECOMIENDA no utilizar Cuentas Locales y adoptar el servicio de autenticación central CAS como primera opción o directo al servicio de directorio LDAP/AD cuando sea posible.

5. CICLO DE VIDA DE LA CLAVE UC (BACKOFFICE)

5.1 Enrolamiento del usuario y generación de la Cuenta UC

El enrolamiento DEBE verificar la identidad de la persona única asociada a la Cuenta UC en proceso de creación, sea en forma remota o presencial ([1] IAL2)

El sistema/proceso

- DEBE registrar la fecha y hora de la creación de la Cuenta UC.
- DEBE exigir una dirección de "correo personal" para que quede registrado como mecanismo de Restablecer la Clave UC
- DEBE crear la Clave UC mediante la API "Gestión Cuenta UC" y suministrar el "correo personal" en el mismo proceso.
- El usuario luego debe ocupar el proceso de Restablecer Clave UC para generar por primera vez su Clave UC.

5.2 Uso de clave en sistemas como mecanismo de autenticación

Los sistemas y sitios web DEBEN permitir ciertas funcionalidades que faciliten y resguarden la Clave UC.

DEBEN cumplir con:

- Permitir funcionalidad de "paste" para "pegar" en el campo clave con el fin de permitir el uso de gestores de claves.
- No almacenar la clave del usuario durante el proceso de autenticación
- Utilizar CAS como mecanismo de autenticación o directo a LDAP/AD

5.3 Repositorio de Cuentas UC LDAP/AD: Almacén de la clave

Los sistemas que almacenen alguna clave de usuario DEBEN cumplir con los siguientes requisitos:

- Almacenar la clave en forma de HASH con SALT y nunca en forma de "texto plano".
    - Estándares permitidos son:
        - HMAC
        - SHA-2 (FIPS 180-4 - SHA-224, SHA-256, SHA-384 SHA-512, SHA-512/224 and SHA-512/256)
        - SHA-3 (FIPS 202 - SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 and SHAKE256)
    - El Salt debe ser al menos de 128 bits (16 bytes) de largo y de elección aleatoria por el sistema.

5.4 Proceso de cambio de clave por parte del usuario

El usuario DEBE tener la posibilidad de cambiar su clave de acceso cuando y cuantas veces lo desee en forma autónoma (sin contraparte humana).

- El sistema DEBE
    - Permitir funcionalidad de "paste" para "pegar" en el campo clave con el fin de permitir el uso de gestores de claves.
    - Cifrar el canal de comunicación entre el usuario y el sistema. Para sistemas WEB se DEBE usar Certificados SSL con SHA2 (SHA-256 o superior).
    - Permitir que el usuario opcionalmente pueda ver la clave en los campos de "nueva clave" y "clave actual"
    - Cumplir con nota A en el test de Qualys SSL [9]
- El sistema DEBE incluir un "Password strength meter" que asista al usuario en la elección de clave

5.5 Proceso de Restablecer ("*reset*") la Clave UC

La clave de un usuario puede ser restablecida por 2 motivos: la pérdida y la vulneración.

5.5.1 Por pérdida

En caso de pérdida, el usuario podrá restablecer la clave en forma autónoma en el sitio oficial para este caso mediante los mecanismos del sitio micuenta.uc.cl; Correo Personal y Clave Única del Registro Civil.

El usuario DEBE haber ingresado su Correo Personal previamente en este sitio para poder utilizar el mecanismo mediante Correo Personal y así restablecer su Clave UC.

En caso de no poder utilizar ninguno de los mecanismos establecidos, el usuario DEBE utilizar el mecanismo de asistencia de acuerdo con su ROL primordial:

a) **Profesor, Funcionario, Honorario, Postdoctorado y Alumno (vigente):** Concurrir a una Sala Crisol e identificarse (mediante carné de identidad o pasaporte vigente) con el encargado Crisol, quien le podrá ingresar un Correo Personal al sistema.

b) **ExAlumnos**: Comunicarse con la Dirección de Alumni UC, email: alumni@uc.cl Mayor información en Web Alumni UC

5.5.2 Por vulneración (seguridad)

- Si hay evidencia de compromiso de la cuenta (la clave está en posesión de alguien distinto del usuario de la cuenta o hay actividad maliciosa), el administrador del repositorio de las claves (Administrador LDAP/AD) DEBE cambiar la clave de la cuenta vulnerada y avisar al usuario.
- Este cambio de clave DEBE quedar registrado. Este registro no debe expirar.
- El registro DEBE enviarse mensual y automática al Área de Seguridad DI en formato CSV.
- La nueva clave DEBE cumplir ser una clave aleatoria de 20 caracteres.
- La nueva clave NO DEBE ser entregada al usuario.
- El usuario DEBE utilizar el mecanismo de Restablecer Clave UC para recuperar acceso a su Cuenta UC.

5.6 Proceso de cierre de la cuenta

- El bloqueo/cierre definitivo o temporal de una cuenta DEBE incluir el cambio de clave de la cuenta.
- Se DEBE eliminar de la base de datos del sistema Cambio de Clave los datos de "claves anteriores" cifradas y el "Correo Personal".
- La clave fijada DEBE cumplir los mismos requisitos que el ítem 4.1 "Generación de clave" o ser una clave aleatoria de 20 caracteres.
- La clave NO DEBE informarse al usuario.

5.7 Proceso de revisión de claves

- La Subdirección de Redes y Seguridad de la Dirección de Informática UC DEBE conducir al menos 2 pruebas exhaustivas al año para revisar la seguridad de todas las claves de Cuentas UC. La prueba DEBE incluir métodos heurísticos y uno o varios diccionarios de claves.
- Si alguna clave es descubierta por el proceso de revisión, se DEBE informar al usuario para que la cambie en un plazo breve (5 días hábiles). En caso de que el usuario no la cambie, DEBE ser cambiada por el administrador del repositorio LDAP/AD.
- La clave fijada DEBE cumplir los mismos requisitos que el ítem 4.1 "Generación de clave" o ser una clave aleatoria de 20 caracteres.
- La clave NO DEBE informarse al usuario.
- El usuario DEBE utilizar el mecanismo de Restablecer Clave UC para recuperar acceso a su Cuenta UC.

6. REFERENCIAS

[1] NIST SP 800-63 *Digital Identity Guidelines*
https://pages.nist.gov/800-63-3/

[2] Standford University Passwords
https://uit.stanford.edu/service/accounts/passwords

[3] MIT Strong Password
https://kb.mit.edu/confluence/display/istcontrib/Strong+Passwords

[4] Munged Passwords
https://en.wikipedia.org/wiki/Munged_password

[5] Diccionario de Claves será entregado periódicamente por la SRS.
Ejemplo: 10 million Passwords
https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495

[6] Listado de claves vulneradas y puestas al público será entregado periódicamente por la SRS
Ejemplo: Pwned Passwords
https://haveibeenpwned.com/Passwords

[7] Clave aleatoria en formato SHA2-256 :
Método 1: UNIX CLI → "echo $RANDOM | shasum -a 256"
Método 2: UNIX CLI → "pwgen -vn -A 32 1"

[8] NIST SP 800-63B *Digital Identity Guidelines*
5.1.1.2 Memorized Secret Verifiers
https://pages.nist.gov/800-63-3/

[9] Qualys SSL TEST
https://www.ssllabs.com/ssltest/

ANEXO A

Ejemplos de claves válidas de usar:

- Hpkm.123
- MiTelefono97
- MiPerrograndanes
- un dalmata me comio el celular

ANEXO B

Funcionamiento – Restablecer Clave UC usando el Correo Personal:

a) Usuario ingresa datos (Cuenta UC y Correo Personal) en el sitio web micuenta.uc.cl

b) Si ambos son correctos (coincide que están asociados previamente), se enviará un correo como el de más abajo al Correo Personal del usuario, con un link web para fijar una nueva Clave UC.

Estimado Usuario:
Hemos recibido una solicitud de recuperación de Clave UC, para completar dicha acción es necesario que acceda a la siguiente dirección web y digite una nueva clave:

https://cambiaclave.uc.cl/admclaveuc//ProcesaToken?token=DFF7B3754FF13EC1D28321708E57F4228BEFB0213317664A9EEAC247AAC9&uid=nn&mail=nn@gmail.com

Si usted no realizó esta solicitud, le solicitamos por favor no tomar en consideración el presente correo.

Atentamente,

Dirección de Informática

Fono:955045555

HISTORIA DE REVISIONES

REVISIÓN	VERSIÓN	FECHA	FICHA DE CONTROL DE CAMBIOS
1	1.0	16 enero 2020	Generación del documento
2	1.1	9 marzo 2020	Se agrega capitulo de responsabilidades
3	1.2	2 dic 2020	Se corrige a IAL = 3
4	1.2.1	18 ago 2023	Se elimina referencia al 5555@uc.cl en Anexo B