Plataforma de Ciudadanía Digital 2.0

Especificaciones de Caso de Uso

Versión Documento 1.0.2

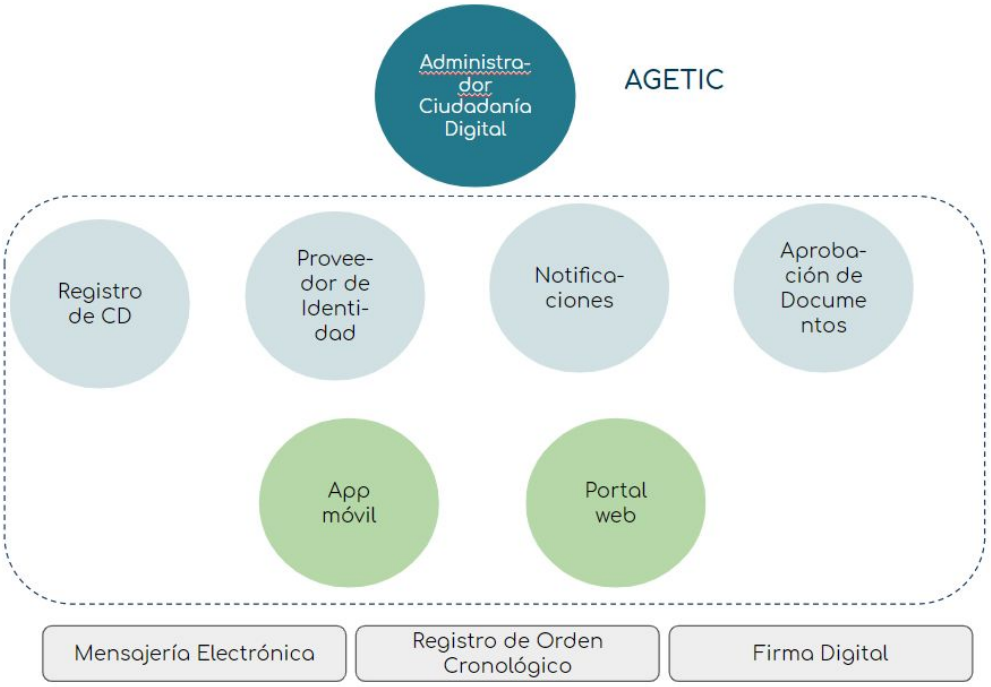
Índice General

Introducción

Ciudadanía Digital se encuentra operando en nuestro país desde la promulgación de la Ley N°1080 y la publicación de los Lineamientos y Estándares Técnicos de Implementación de Ciudadanía Digital y Notificaciones Electrónicas.

La Plataforma de Ciudadanía Digital actualmente está compuesta por los siguientes sistemas:

Figura 1: Componentes de Ciudadanía Digital



Fuente: Elaboración propia.

En relación a la retroalimentación obtenida de la primera versión de ciudadanía digital tanto por los canales de soporte, como de las entidades clientes, se ve la necesidad de realizar una segunda versión de Ciudadanía Digital que considere mejoras técnicas de usabilidad, seguridad y simplificación de pasos que permita realizar acciones fáciles, seguras y ágiles con la cuenta de ciudadanía digital.

Estas mejoras técnicas pueden implicar un ajuste a los Lineamientos y Estándares Técnicos de Implementación de Ciudadanía Digital y Notificaciones Electrónicas.

Descripción del Proyecto

La Plataforma de Ciudadanía Digital, permite realizar todas las tareas que un ciudadano puede realizar desde la creación hasta la baja de su cuenta de Ciudadanía Digital, en el marco de lo establecido en la Ley 1080, de Ciudadanía Digital y Lineamientos de Estándares Técnicos de implementación de Ciudadanía Digital y Notificaciones Electrónicas.

Todas sus interfaces gestionarán la información dentro del entorno web, y también se tiene funcionalidades realizadas desde la aplicación móvil.

La versión 2.0 de la Plataforma de Ciudadanía Digital, debe considerar mejoras de usabilidad, seguridad, simplificación de procesos y digitalización de procesos que en la primera versión no fueron considerados.

Objetivo General

Mejorar los sistemas que componen la Plataforma de Ciudadanía Digital considerando simplificación de pasos, usabilidad y seguridad que permita la gestión de credenciales desde la solicitud hasta la baja o suspensión y las acciones de aprobación de documentos y notificaciones electrónicas en el marco de la Ley 1080 y lineamientos y estándares técnicos de implementación de ciudadanía digital y notificaciones electrónicas.

Alcance General

Soportará las actividades relacionadas con mejoras en simplificación de pasos, usabilidad, seguridad y actualización línea gráfica en:

- Registro
- Autenticación y Cierre de Sesión
- Gestión de Cuenta
- Suspensión, baja de credenciales
- Aprobación de documentos
- Notificaciones y comunicaciones electrónicas
- Aplicación Móvil de Ciudadanía Digital y Portal Web de Ciudadanía Digital

Esta versión no incluirá la digitalización de los procesos de solicitud de uso de los mecanismos de ciudadanía digital por parte de las entidades públicas.

En el presente documento inicialmente se hace referencia al registro y autenticación.

Capítulo I: Registro y Autenticación con Ciudadanía Digital

Objetivos Específicos

Optimizar el proceso de registro y autenticación con ciudadanía digital simplificando pasos y mejorando la experiencia del ciudadano, la usabilidad y seguridad.

Alcance

Soportará las actividades relacionadas con mejoras en simplificación de pasos, usabilidad, seguridad y actualización línea gráfica en:

- Registro de Ciudadanos Digitales
- Autenticación - Restablecer Contraseña
- Actualización de correo, teléfono desde el portal web de ciudadanía digital y aplicación móvil.

Actualización de Línea Gráfica[1]:

- Portal Web y Aplicación Móvil Ciudadanía Digital
- Aprobación de documentos

No se considera dentro el alcance:

- Mejoras técnicas en el proceso de Habilitación, Inhabilitación de Entidad Registradora, Administrador de Registro de Ciudadanía Digital y Operadores de Registro de Ciudadanía Digital.
- Registro de Ciudadanía Digital con Firma Digital, establecido en el Lineamiento y estándares técnicos de implementación de ciudadanía digital y notificaciones electrónicas.
- Registro de ciudadanos bolivianos que se encuentren en el exterior.

Análisis

Registro de Ciudadanía Digital

Actualmente el Registro de Ciudadanía Digital está compuesto por procesos internos administrativos y procesos realizados por el ciudadano, acciones que son realizadas en los distintos sistemas de Ciudadanía Digital, detallados a continuación:

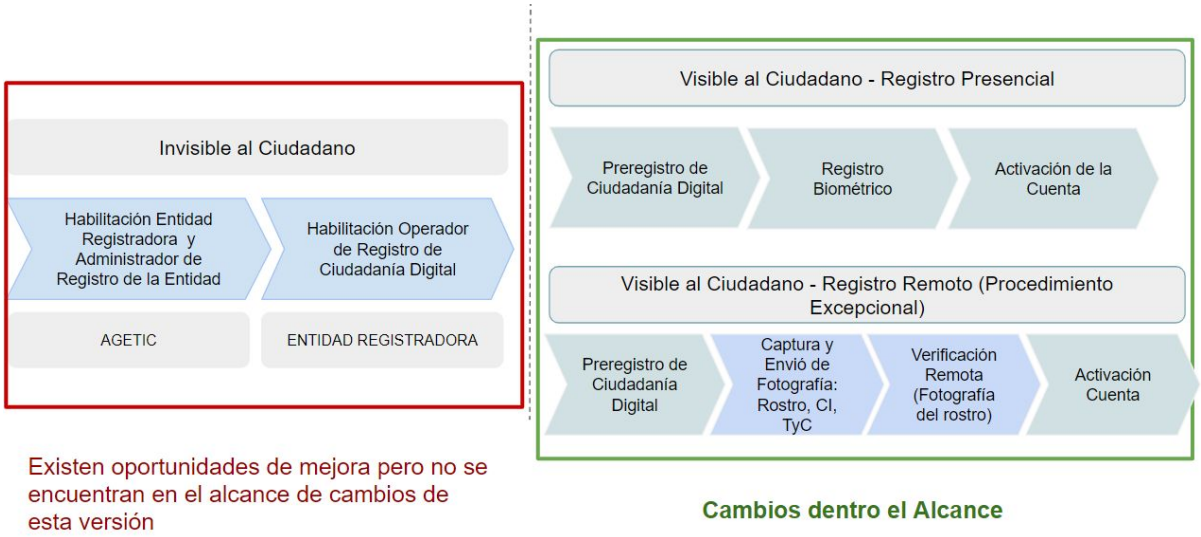
[1] Si la actualización gráfica requiere también algún ajuste técnico o mejora técnica debe ser indicado por el equipo de Desarrollo.

Procesos no visibles al ciudadano:

- *Habilitación/Inhabilitación/Actualización Entidad Registradora y Administrador de Registro de Ciudadanía Digital de la Entidad:* Plataforma de Administración de Ciudadanía Digital (backend y frontend).
- *Habilitación/Inhabilitación/Actualización Operadores de Registro de Ciudadanía Digital:* Plataforma de Registro de Ciudadanía Digital (backend y frontend) y Plataforma de Administración de Ciudadanía Digital (backend y frontend)

Procesos visibles al ciudadano:
Preregistro de Ciudadanía Digital: Portal web de Ciudadanía Digital y aplicación móvil de ciudadanía digital (frontend), plataforma de Registro de Ciudadanía Digital (backend).
Registro Biométrico/Verificación Remota: Plataforma de Registro de Ciudadanía Digital (Backend y Frontend)
Activación de la Cuenta: Plataforma de Registro de Ciudadanía Digital (Backend y Frontend), Proveedor de Identidad (backend).
Para el envío de correos y sms se utiliza la Plataforma de Mensajería Electrónica.

Figura 2: Procesos Actuales - Registro de Ciudadanía Digital



Fuente: Elaboración propia.

A continuación se detallan los problemas identificados en los procesos dentro el alcance de esta sección:

- Proceso de registro no intuitivo y con gran cantidad de pasos:
    - Verificación presencial (biométrico): Aproximadamente 13

    - Verificación remota: Aproximadamente 16
- Etapa de Activación no realizada por los ciudadanos: Aprox 15000 registros pendientes de activación.
- Problemas en la verificación contra SEGIP por los datos ingresados por los ciudadanos: Complemento, tildes, espacios
- Error en el ingreso de códigos de verificación (vigencia o errores en el registro manual)

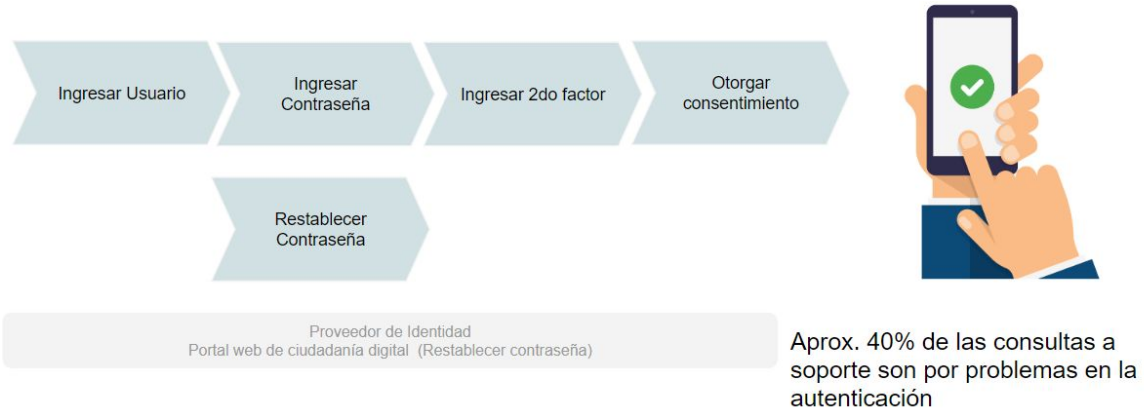
Autenticación con Ciudadanía Digital

Actualmente la Autenticación con Ciudadanía Digital, es realizada una vez que se ha realizado la verificación presencial o remota de la cuenta y su respectiva activación, los sistemas que intervienen en la autenticación de Ciudadanía Digital son:

- Proveedor de Identidad (frontend y backend): Ingreso de usuario, contraseña, 2do factor, y otorgación de consentimiento por parte del ciudadano digital.
- Portal web de Ciudadanía Digital (frontend) y proveedor de identidad (backend): Restablecer contraseña.
- Aplicación móvil de Ciudadanía Digital: Generación del código de 2do factor

Para el envío de correos y sms se utiliza la Plataforma de Mensajería Electrónica.

Figura 3: Procesos Actuales - Autenticación con Ciudadanía Digital



Fuente: Elaboración propia.

A continuación se detallan los problemas identificados:

- Desconocimiento de cuál es el Usuario de la cuenta de ciudadanía digital
- Proceso de restablecer contraseña tedioso: el proceso actual no es intuitivo y provoca bloqueos y solo se puede realizar a través de correo electrónico (Aprox de tiempo de dar soporte en restablecer contraseña a un usuario: 30 - 60 min)

- Ingreso del 2do factor: No permite cambiar el método de verificación, lo cual perjudica a los usuarios si no tienen al alcance su correo electrónico o aplicación móvil.
- No reconoce cuando el usuario elige: No volver a preguntar en este ordenador

Asimismo, se detallan las siguientes mejoras para ser consideradas en esta versión:

- Habilitar el mecanismo de autenticación para aplicaciones móviles. Considerar que este mecanismo debe estar integrado a la aplicación móvil de Ciudadanía Digital.
- En relación al nivel de seguridad que requiera el servicio digital la entidad puede configurar si se da la opción de elegir Ordenador Conocido
- Mejorar las alertas de seguridad.
- Mejorar las verificaciones de seguridad de la cuenta.

ECU 1.01 - Registro de Ciudadanos Digitales

Registro de Ciudadanos Digitales

Para registrarse en ciudadanía digital el ciudadano interesado realizará su autoregistro y verificación. Este proceso le permitirá obtener credenciales para acceso a sistemas que empleen ciudadanía digital, de acuerdo el nivel de registro del ciudadano.

Deben distinguirse los estados:

1. Ciudadano autoregistrado, aquel que completó con éxito el flujo básico de solicitud de registro de ciudadanía digital (habiendo efectivizado su autoregistro/preregistro), sin completar ningún tipo de verificación.
2. Ciudadano verificado, aquel que completó con éxito el flujo alternativo 1, siendo verificado presencialmente o que completó con éxito el flujo alternativo 2, siendo verificado de manera remota.

Figura 4: Especificación de datos para Registro de Ciudadanos Digitales

Etiqueta	Descripción
Número telefónico de celular	Número telefónico de 8 dígitos otorgado por un proveedor de telefonía móvil.
Código de verificación	Código numérico recibido por SMS
Correo electrónico	Dirección de correo electrónico
Nombres	Nombres de la persona natural registrados en SEGIP.
Primer Apellido	Primer apellido de la persona natural registrados en SEGIP.
Segundo Apellido	Segundo apellido de la persona natural registrados en SEGIP

Número de documento de identidad + Complemento	Número de identificación otorgado por SEGIP mediante la cédula de identidad nacional o de extranjería. En ese campo se considera, en caso de corresponder, el número y letra que complementan la cédula de identidad, solo en los casos en que exista duplicidad en el Número de documento de identidad.
Fecha de nacimiento	Fecha de nacimiento dd/mm/aaaa registrada en el SEGIP.
Contraseña	Contraseña registrada por el ciudadano para su cuenta de ciudadanía digital.
Retrato	Fotografía de busto del ciudadano.
Fotografía del CI	Fotografía capturada por el ciudadano de su cédula de identidad.
Huella digital	Imagen escaneada mediante dispositivo biométrico de una huella digital del ciudadano.
Observaciones	Párrafo abierto en el que el operador de registro ingresa observaciones.

El formulario de registro puede ser desplegado desde la aplicación móvil, o mediante un navegador web.

Los datos a registrar en el sistema se debe parsear siempre a mayúsculas.

Actores

- Ciudadano
- Operador de registro habilitado con el Rol Ventanilla.

Precondiciones

- Bolivianas y los bolivianos, extranjeros residentes en Bolivia, mayores de dieciocho (18) años de edad, y aquellos menores de edad conforme a la capacidad que les reconozca el ordenamiento jurídico, registrados en el SEGIP, con toda su información actualizada al día y sin observaciones.
- Entidad de Registro y operadores de registro con rol ventanilla habilitados en la Plataforma de Registro de Ciudadanía Digital.

Flujo de eventos

Flujo Normal

1. El ciudadano ingresa al sistema desde un navegador web, o mediante la aplicación móvil de ciudadanía digital.

2. El sistema presenta un formulario donde el ciudadano ingresa su número telefónico móvil personal.
3. El ciudadano ingresa su número telefónico.
4. El sistema, comprueba que el número telefónico no se encuentre asociado a una cuenta de ciudadanía digital (autoregistrada, verificada).
    - En caso de que el teléfono se encuentre vinculado a un usuario de ciudadanía digital, anuncia esta condición al ciudadano, sin identificar a qué cuenta está asociado. Solicita otro número de celular al ciudadano o que se comunique con soporte.
5. El sistema verifica el número de celular del ciudadano mediante un código de verificación por SMS.
    - Si está empleando la aplicación móvil para efectuar el registro, detecta el código de forma automática.
    - Caso contrario pide al solicitante que ingrese el código enviado manualmente y lo verifica.
    - Si el ciudadano no recibe o introduce a tiempo el código de verificación puede volver a solicitarlo en un periodo de tiempo determinado.
    - El código enviado debe tener un tiempo de vigencia (configurable).
6. El sistema presenta un formulario donde el ciudadano ingresa su correo electrónico personal.
7. El ciudadano ingresa su correo electrónico.
8. El sistema, comprueba que el correo electrónico no se encuentre asociado a una cuenta de ciudadanía digital (autoregistrada, verificada).
    - En caso de que el correo electrónico se encuentre vinculado a un usuario de ciudadanía digital, anuncia esta condición al ciudadano, sin identificar a qué cuenta se encuentra asociado. Solicita otro correo electrónico al ciudadano o que se comunique con soporte.
9. El sistema valida el formato del correo electrónico y verifica el mismo mediante un enlace enviado al correo electrónico, al cual el ciudadano deberá ingresar y hacer clic en la opción de verificación.
    - Formato del correo electrónico:
        - El sistema verifica si el dominio es gob.bo, edu.bo y mil.bo y otros sugeridos por la ADSIB, en caso de que si, el sistema muestra un mensaje de advertencia indicando que el correo debe ser personal y si desea continuar.
        - El sistema verifica que el correo no sea un formato de correo temporal (ej. yopmail, mailinator), en caso de que si, el sistema muestra un mensaje indicando que debe registrar un correo válido.
    - Si el ciudadano no recibe o atiende a tiempo al correo de verificación puede volver a solicitarlo en un periodo de tiempo determinado, configurable (inicialmente se determina 15 minutos).
    - El enlace enviado debe tener un tiempo de vigencia configurable (inicialmente se determina 15 minutos).
10. La verificación del correo es mostrada al ciudadano.

11. El sistema presenta un formulario donde solicita al ciudadano ingresar sus datos personales: Nombres, Primer Apellido, Segundo Apellido, Número de documento de identidad +Complemento del documento de identidad (si corresponde), Fecha de nacimiento, contraseña, confirmación de contraseña y aceptación de Términos y Condiciones de Uso de Credenciales de Ciudadanía Digital.
    - La robustez de la contraseña será verificada con https://github.com/dropbox/zxcvbn
12. El ciudadano ingresa sus datos personales.
13. El sistema realiza la siguientes validaciones:
    - Contrastación de Nombres, Apellidos y Número de Documento de Identidad con el servicio web de SEGIP.
        i. Para la contratación el sistema no debe considerar tildes, ni espacios.
        ii. Si los datos son verificados con éxito y el usuario no se encuentra autoregistrado, verificadosuspendido, el flujo continúa hacia el paso 14.
    - Si los datos no coinciden con los existentes en SEGIP, el sistema mostrará un mensaje al ciudadano que sus datos no coinciden con el registro en SEGIP.
    - Si el servicio del SEGIP no se encuentra disponible mostrará un mensaje indicando la situación y que vuelva a intentar.
    - Si el registro del ciudadano se encuentra observado en SEGIP, el sistema mostrará el mensaje indicando la situación.
    - Si los datos ya corresponden a un usuario autoregistrado, verificado o suspendido, el sistema mostrará un mensaje esta condición al ciudadano y sugerirá al ciudadano entrar en contacto con soporte.
    - La contraseña cumpla con los parámetros establecidos y que ambos valores introducidos por el usuario coincidan.
14. El ciudadano acepta los términos y condiciones de uso de ciudadanía digital. Caso contrario abandona el sistema en cualquier paso anterior, anulando todas las acciones realizadas.
15. El sistema explica al ciudadano que para activar sus credenciales debe realizar la verificación de su registro hasta una fecha determinada y que en caso de no realizarlo, deberá volver hacer el proceso de solicitud de registro (autoregistro/preregistro) nuevamente y le ofrece seleccionar un medio para esta verificación. Explica además los requerimientos y características de cada uno de estos medios de verificación.
    - El sistema debe calcular la fecha con días hábiles, y debe ser configurable en el sistema, inicialmente se estaría considerando 3 días (es decir no contabilizar feriados nacionales ni fines de semana). Por otra parte tomar 3 días enteros para el vencimiento del plazo y no 72 horas exactas a partir de la solicitud, de tal manera que una solicitud caduque la última hora del tercer día después de la solicitud.
    - Si el ciudadano no realiza la verificación de su cuenta hasta el día establecido, el sistema envía un correo electrónico al ciudadano

comunicando que el plazo venció y que debe realizar nuevamente la solicitud de su registro, dando de ese modo baja la solicitud de registro.

16. El ciudadano efectúa una de las siguientes acciones de manera obligatoria:
    a. Elige verificar su cuenta presencialmente en oficinas de una entidad pública, el sistema le muestra los puntos de registro disponibles y los requisitos que debe presentar en el punto de registro. Continuará por el Flujo alternativo 1.
    b. Elige verificar su cuenta de manera remota. Por lo que continuará por el flujo alternativo 2.
17. Fin de la especificación de caso de uso.

Flujo alternativo 1(Verificación Presencial)

1. El sistema envía un correo electrónico al ciudadano indicando que se ha realizado con éxito su solicitud de registro de ciudadanía digital y que realice la verificación hasta el día establecido.
    a. En caso que el ciudadano no haya realizado su verificación hasta un día antes de la fecha límite (valor parametrizable), el sistema le envía un mensaje de alerta por correo electrónico y sms indicando el vencimiento para realizar su verificación.
2. El ciudadano autoregistrado, acude a oficinas de cualquier entidad que cuente con ventanillas para el registro de ciudadanos digitales, portando su documento de identidad vigente, que será recepcionado por un operador de registro de ciudadanía digital con rol ventanilla.
3. El operador de registro de ciudadanía digital con rol ventanilla, se autentica al sistema de registro de ciudadanía digital, como se muestra en el ECU - Autenticarse con las credenciales de Ciudadanía Digital.
4. El operador de registro de ciudadanía digital con rol ventanilla, mediante un buscador en el sistema de registro, localiza al ciudadano autoregistrado (independientemente si este ha solicitado verificación remota o presencial) buscándolo por su número de documento de identidad.
5. En caso de encontrarlo, el sistema despliega los datos principales del ciudadano autoregistrado, mostrando entre las acciones posibles la de validar el registro del ciudadano.
    - En caso de no encontrarlo, el sistema mostrará un mensaje indicando la situación.
6. El sistema obliga al operador de registro a autoasignarse el caso .).
    a. Si el operador abandona el registro éste deberá ser desasignado.
    b. Una vez autoasignado, si otro operador
    c. Si otro operador busca al ciudadano seleccionado, el sistema muestra un mensaje indicando que ya se encuentra siendo atendido por otro operador.
7. El operador de registro de ciudadanía digital con rol ventanilla, selecciona la opción para validar el registro del ciudadano autoregistrado.
    a. Caso contrario, si el operador de registro decidiera rechazar la solicitud, selecciona la opción para eliminar el registro.
    b. El sistema solicita al operador de registro que redacte el motivo del rechazo.
    c. El operador de registro redactará este motivo y confirmará la acción.
    d. El sistema validará que el operador de registro haya ingresado un motivo de rechazo y despliega una ventana modal para la firma digital.

e. El operador de registro de ciudadanía digital con rol ventanilla, firma digitalmente la solicitud introduciendo su contraseña.
f. El sistema envía un mensaje al correo electrónico empleado para esta solicitud de registro conteniendo el motivo por el cual el registro fue rechazado. Ejemplo:
   Su solicitud de registro a ciudadanía digital fue rechazada debido al siguiente motivo especificado por el operador:
   ….
   Por favor vuelva a realizar su solicitud tomando en cuenta esta observación.
g. Fin del caso de uso.

8. El sistema despliega la información de registro proporcionada por el ciudadano autoregistrado, junto con un formulario para que el operador de registro capture un retrato, la huella digital del ciudadano autoregistrado, y un campo para que emita observaciones.
9. El operador de registro de ciudadanía digital con rol ventanilla, tomará una fotografía (retrato), la lectura de su huella digital del ciudadano autoregistrado.
    a. En caso de no poder obtener la huella digital, esto explicará el motivo en observaciones.
10. Luego hará clic en la opción para verificar el registro del ciudadano.
11. El sistema validará que se haya tomado una fotografía, que se haya tomado una huella digital (o, caso contrario, se haya escrito texto en el campo de observaciones). Desplegará la ventana para que el operador de registro confirme esta acción, con un resumen de los datos.
12. El operador de registro de ciudadanía digital con rol ventanilla confirma la acción.
13. El sistema despliega una ventana modal para la firma digital.
14. El operador de registro de ciudadanía digital con rol ventanilla, firma digitalmente la solicitud introduciendo su contraseña.
15. El sistema concluye la verificación del registro del ciudadano digital, enviando un mensaje por correo electrónico de confirmación al ciudadano digital indicando que la verificación fue realizada exitosamente y que su cuenta fue activada.
16. Fin de la especificación de caso de uso.

Flujo alternativo 2 (Verificación remota)

1. El ciudadano autoregistrado elige verificarse de manera remota.
2. El sistema despliega un formulario par que el ciudadano autoregistrado elija con qué entidad pública pretende realizar su verificación remota y el horario preferente para contactarse con él. Explica al ciudadano autoregistrado que deberá elegir esta opción en concordancia con alguna solicitud, proceso o trámite que esté siguiendo con esta entidad de manera preferente y que en el momento de la verificación remota debe portar su cédula de identidad.
3. Para completar este formulario el ciudadano autoregistrado toma las siguientes fotografías:
    a. Rostro y CI (con silueta para el rostro y carnet)
    b. CI anverso y reverso (con silueta)
4. El ciudadano autoregistrado acepta el envío de la solicitud de verificación remota.
5. El sistema envía la solicitud para su atención por parte de la entidad de registro elegida. Muestra información al ciudadano respecto a los pasos siguientes.

6. El sistema envía un correo electrónico al ciudadano indicando que se ha realizado con éxito su solicitud de registro de ciudadanía digital y que un operador de registro de ciudadanía digital se contactará para la verificación remota.
    a. En caso que el ciudadano no haya realizado su verificación hasta un día antes de la fecha límite (valor parametrizable), el sistema le envía un mensaje de alerta por correo electrónico y sms indicando el vencimiento para realizar su verificación.
7. El operador de registro de ciudadanía digital con rol ventanilla, se autentica al sistema de registro de ciudadanía digital, como se muestra en el ECU - Autenticarse con las credenciales de Ciudadanía Digital.
8. El operador de registro de ciudadanía digital con rol ventanilla, encuentra al ciudadano autoregistrado solicitante por una de las dos vías posibles:
    a. Buscándolo por su número de identidad.
    b. Localizandolo en la lista de pendientes de la entidad a la que pertenece.
9. El sistema despliega los datos principales del ciudadano autoregistrado, mostrando entre las acciones posibles la de validar el registro del ciudadano. El sistema muestra de manera llamativa, (empleando iconos y/o un código de color) cual es el horario preferente elegido por el solicitante para que lo contacten (mañana o tarde)
10. El operador de registro de ciudadanía digital con rol ventanilla selecciona la opción para validar el registro del ciudadano.
    a. Caso contrario, si el operador de registro decidiera rechazar la solicitud, selecciona la opción para eliminar el registro.
    b. El sistema solicita al operador de registro que redacte el motivo del rechazo.
    c. El operador de registro redactará este motivo y confirmará la acción.
    d. El sistema validará que el operador de registro haya ingresado un motivo de rechazo y despliega una ventana modal para la firma digital.
    e. El operador de registro de ciudadanía digital con rol ventanilla, firma digitalmente la solicitud introduciendo su contraseña.
    f. El sistema envía un mensaje al correo electrónico empleado para esta solicitud de registro conteniendo el motivo por el cual el registro fue rechazado. Ejemplo:
    Su solicitud de registro a ciudadanía digital fue rechazada debido al siguiente motivo especificado por el operador:
    ….
    Por favor vuelva a realizar su solicitud tomando en cuenta esta observación.
    g. Fin del caso de uso.
11. El sistema despliega la información de registro proporcionada por el ciudadano autoregistrado solicitante junto con la fotografía de retrato y fotografías del carnet de identidad. El sistema despliega también un campo para que el operador de registro emita observaciones, en caso de corresponder. (No se solicitará la toma de huella digital, ni siquiera en el caso de que el ciudadano que solicitó un registro remoto se apersone a la ventanilla).
12. El operador de registro de ciudadanía digital con rol ventanilla se comunica con el ciudadano mediante sus datos de contacto registrados, con el fin de comprobar su identidad e intención de validación (podrá también haber recibido presencialmente al solicitante). (Ver en la sección de conformidad punto 2)
13. El operador de registro de ciudadanía digital con rol ventanilla redactará cualquier observación necesaria, podrá también agregar una fotografía de retrato a las 3 imágenes ya tomadas, si corresponde. Luego hará clic en la opción para verificar el

registro del ciudadano.

14. El sistema desplegará la ventana para que el operador de registro de ciudadanía digital con rol ventanilla confirme esta acción, con un resumen de los datos.
15. El operador de registro confirma la acción.
16. El sistema despliega una ventana modal para la firma digital.
17. El operador de registro de ciudadanía digital con rol ventanilla firma digitalmente la solicitud introduciendo su contraseña.
18. El sistema concluye el registro del ciudadano digital, enviando un mensaje de confirmación al ciudadano digital por correo electrónico indicando que la verificación fue realizada exitosamente y que su cuenta fue activada.
19. Fin de la especificación de caso de uso.

Postcondiciones

- El ciudadano con credenciales de ciudadanía digital para acceso a sistemas que emplean ciudadanía digital como mecanismos de autenticación en web y móvil.

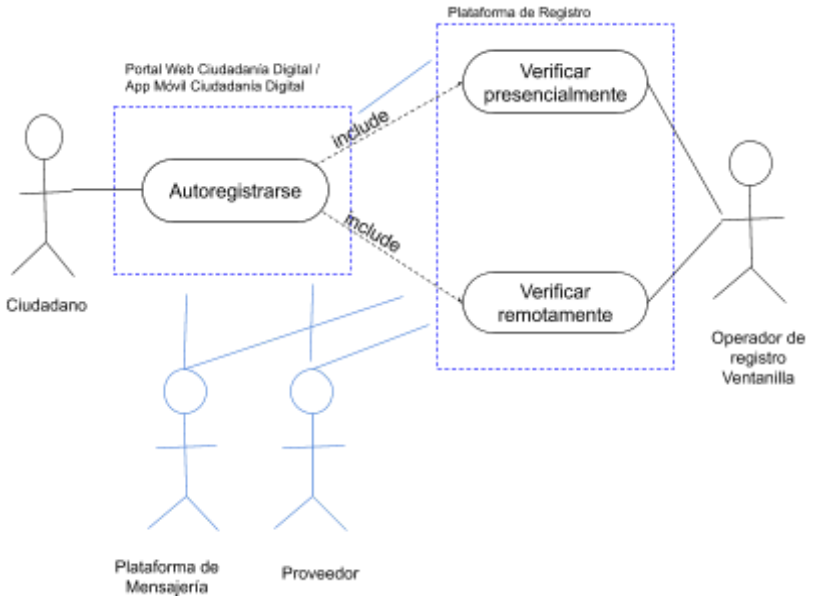
Frecuencia

El ciudadano efectuará su registro una sola vez.

Temas abiertos

- Definir si el autoregistro (pre registro) de ciudadanos digitales será realizado de forma nativa en la aplicación móvil de Ciudadanía Digital cómo es realizado actualmente.
- Revisar los efectos en los servicios web de registro: Contrastación y el de registro utilizado anteriormente por el SEGIP.
- Revisar la posibilidad que desde el sistema de registro de ciudadanía digital el operador de registro pueda realizar la videollamada y el ciudadano recibirla desde la aplicación móvil.
- Definir la factibilidad técnica de salir en esta versión que con un autorregistro ya puedes autenticarte así como lo hacen las identidades digitales de Uruguay, Argentina, USA, entre otros o solo si pasaste por la etapa de verificación con el operador de registro de ciudadanía digital.

Diagrama de caso de uso



Conformidad

Nombre, firma y fecha	Revisión, observaciones y comentarios
	Reunión 14/07/2020 (UIID, UGE, UX) Se definió que no se trabajará en esta versión que con el autorregistro ya se pueda autenticar el ciudadano a servicios digitales. **Revisión 24/07/2020 (UGE, UX, CGII, UIID)** 1) CGII: Considerar que los números de las líneas son reutilizados por los ISP, por tanto debe existir un estado inhabilitado del número, verificar que el dueño es el registrado con la línea. Para el punto detallado anteriormente, se elaborará un nuevo ECU que después de 3 meses en el login se añade la funcionalidad para que el usuario confirme sus datos (correo y teléfono). 2) Se verá la integración con jitsi en la plataforma de registro y app móvil o, en los mejores de los casos con operadora que nos permita realizar la videollamada. 3) Consideramos que debería ser en línea el registro con un operador en una línea de teléfono para soporte con libretos predefinidos (ejemplo call center del Banco). Realizar preguntas para identificar la persona con los datos que se consignaron.

ECU 1.02- Autenticarse con las credenciales de Ciudadanía Digital

Autenticarse con las credenciales de Ciudadanía Digital

Permite realizar la autenticación con las credenciales de Ciudadanía Digital a aplicaciones de terceros que han integrado el mecanismo de autenticación de ciudadanía digital.
La autenticación puede ser realizada cuando se ha realizado la verificación de la solicitud de registro, ya sea de manera presencial o remota.

El sistema en sus formularios debe mostrar siempre los siguientes enlaces:

- Contacto: Dirige al formulario de contacto para soporte y los número de atención (calidad y transparencia).
- Términos y Condiciones de Uso: Los que son aceptados al crear la cuenta de ciudadanía digital.
- Política de Privacidad: Los que son aceptados al crear la cuenta de ciudadanía digital.
- Preguntas frecuentes: Preguntas frecuentes respecto a la cuenta de ciudadanía digital.
- Logo AGETIC, incorporar también la versión del sistema.

Figura 5: Especificación de datos para Autenticarse con Ciudadanía Digital

Etiqueta	Descripción
Cédula de Identidad	Número de Cédula de Identidad del Ciudadano Digital.
Contraseña	Contraseña registrada por el ciudadano para su cuenta de ciudadanía digital.
Código de Seguridad (doble factor de autenticación)	Código numérico de 6 dígitos, que es enviado para verificar la identidad del ciudadano.

La autenticación está integrada a aplicaciones web y móviles. El diseño debe ser responsivo para distintos tipos de dispositivos.

Actores

Ciudadano Digital

Precondiciones

- Aplicación tercera (sistema cliente) integrada con el mecanismo de autenticación de Ciudadanía Digital.

- El ciudadano requiere ingresar a un servicio digital del Estado.

Flujo de eventos

Flujo Básico

1. El sistema presenta un formulario donde solicita ingresar la cédula de identidad y contraseña de la cuenta de Ciudadanía Digital.
    - Si la entidad propietaria de la aplicación tercera (sistema cliente) ha proporcionado su logo, el nombre de su sistema, se muestran también en esta pantalla.
    - En esta pantalla también se muestra la política de privacidad y términos y condiciones de uso de la aplicación tercera (si la entidad realizó la integración)
    - En esta pantalla se muestra los datos públicos los cuales el ciudadano está dando acceso (nombres, apellidos y número de documento de identidad).
    - Si el ciudadano se encuentra autenticado en un sistema cliente A, y el token de sesión sigue vigente (configurable), al ingresar a un sistema cliente B, que ya autorizó el acceso, el usuario ingresa directamente al sistema cliente B, sin solicitar su autenticación, siempre y cuando el sistema cliente no haya solicitado que el usuario debe autenticarse explícitamente.
    - Si el ciudadano se encuentra autenticado en un sistema cliente A, y el token de sesión sigue vigente (configurable), al ingresar a un sistema cliente B por primera vez, el sistema muestra una pantalla con el usuario en modo lectura y los datos públicos que está autorizando y si corresponde, los términos y condiciones de uso y política de privacidad del sistema cliente, para que el usuario continúe. (Siempre y cuando el sistema cliente no haya solicitado que el usuario debe autenticarse explícitamente).
        - De ser que son solamente datos públicos y el ciudadano acepta continuar, continúa con el paso 14.
        - De ser también datos no públicos, y el ciudadano acepta continuar, continúa con el paso 12.
2. El ciudadano registra su número de cédula de identidad (el número de la Cédula de Identidad sin lugar de extensión).
    - Si el número del documento de identidad tiene complemento, éste debe estar separado mediante un guión. Ej. 12346-1K

    Al registrar el usuario, el sistema debe parsearlo siempre a mayúsculas.*2.a. Ver Flujo Alternativo: El ciudadano no es ciudadano digital.*
3. El ciudadano registra su contraseña y continua.
    3.a. Ver Flujo Alternativo: El ciudadano digital no recuerda su contraseña.
4. El sistema verifica que se haya registrado la cédula de identidad y contraseña.
    4.a. En caso que no se haya registrado ambos campos, el sistema muestra un mensaje de campo obligatorio, debajo el campo que falta completar.
5. El sistema busca si el número de documento de identidad existe en las cuentas de ciudadanía digital y si la cuenta se encuentra activa.
    - El sistema verifica que el usuario no haya introducido extensiones (ej.LP), en caso de que si, el sistema muestra un mensaje indicando que solo debe introducir el número de CI y sin la extensión.

5.a. Ver Flujo Alternativo: El número de documento de identidad no se encuentra en las Cuentas de Ciudadanía Digital o la cuenta no se encuentra activa.

6. Si el número de documento de identidad se encuentra en las cuentas de Ciudadanía Digital y la cuenta se encuentra activa, el sistema verifica la contraseña.
7. Si la contraseña también es correcta:
    - El sistema verifica si la aplicación a la cual desea acceder el ciudadano solicita de manera obligatoria introducir el 2do factor.
        - Si la aplicación solicita de manera obligatoria introducir el 2do factor, continúa con el paso 8.
    - Si no solicita de manera obligatoria, el sistema verifica si la aplicación a la cual desea acceder tiene la autorización de acceso a la cuenta del ciudadano digital.
        - Si la tercera aplicación no tiene acceso a la cuenta del ciudadano digital, se continúa con el paso 8.
    - Si la aplicación tiene acceso a la cuenta del ciudadano digital, el sistema verifica si el ciudadano digital marcó como ordenador conocido.
        - Si no marcó “No volver a preguntar en este ordenador”, se continúa con el paso 8.
    - Si marcó como ordenador conocido, el sistema verifica si el ordenador desde donde intenta ingresar el ciudadano es el que marcó como conocido.
        - Si no es el mismo ordenador, continúa con el paso 8.
        - Si es el mismo ordenador, se continúa con el paso 15.

7.a. Ver Flujo Alternativo: La contraseña introducida es incorrecta.

8. El sistema presenta un formulario donde solicita ingresar el 2do factor enviado de manera predeterminada al correo electrónico o al último configurado desde la administración de cuenta o login, para validar su identidad.
    - El 2do factor es un código numérico de 6 dígitos
        - Puede ser enviado al correo electrónico del ciudadano digital
        - Puede ser enviado por SMS al número de celular del ciudadano digital.
        - Generado desde la aplicación móvil
        - El código tiene una vigencia parametrizable. (Inicialmente se configurará SMS 2 min, correo electrónico 3 min, código aplicación 30 segundos).
        - Una vez utilizado el código, éste debe dejar de estar vigente.
        - Este formulario también tiene la opción de marcar: No volver a solicitar en este ordenador. (Excepto cuando el sistema cliente haya requerido en su integración la obligatoriedad del ingreso del 2do factor)
        - Este formulario también tiene la opción de volver a solicitar el código en caso de no haber llegado, pasado un tiempo X (configurable). Este tiempo debe considerar la vigencia del código.
9. Si el ciudadano digital tiene acceso al medio por el cual le llegó el 2do factor, introduce el código.

    9.a. *Ver Flujo Alternativo: El ciudadano digital no tiene acceso al medio donde se envió su 2do factor.*
10. El sistema verifica que el código introducido es el correcto.
11. Si el código es correcto, el sistema verifica si la aplicación a la cual desea acceder tiene la autorización de acceso a la cuenta del ciudadano digital.

11.a. *Ver Flujo Alternativo: El código introducido no es el correcto*

12. De no tener acceso (primera vez que ingresa al sistema cliente), el sistema muestra un formulario con los datos no públicos que se estaría compartiendo con la aplicación tercera (depende si el sistema cliente solicitó en la integración también estos datos, caso contrario continúa con el paso 14).
    - Datos no públicos del Ciudadano Digital: correo electrónico, número de teléfono móvil, fecha de nacimiento (en relación a la configuración en la integración del mecanismo en la aplicación tercera)
    - De igual manera, si el sistema cliente ha optado por solicitar permiso para realizar operaciones sin la presencia del ciudadano digital, este permiso será consultado al usuario final para su consentimiento desde la pantalla de autorización o consentimiento.

    12.a. De haber ya dado acceso a la tercera aplicación, continúa con el paso 14.
13. El ciudadano digital permite el acceso a sus datos para acceder a la tercera aplicación.
    13.a. De no dar permitir el acceso, se cancela la solicitud y el ciudadano no ingresa a la tercera aplicación.
14. El sistema envía un correo electrónico al correo registrado del ciudadano digital.
    - En caso de ser la primera vez que accede a la aplicación tercera, envía un mensaje como el siguiente ejemplo:

    ¡Hola Eliana!
    NOMBRE DE LA APLICACIÓN TERCERA se vinculó correctamente a tu Cuenta de Ciudadanía Digital
    Recibiste este correo porque permitiste que este servicio accediera a la información que se encuentra en tu cuenta de Ciudadanía Digital Si no hiciste eso o estás experimentando un problema por favor comunícate con nosotros.
    Para administrar tu cuenta de Ciudadanía Digital, ingresá aquí
    - En caso de ser de un nuevo ordenador, un mensaje indicando que accedido al Nombre de la tercera aplicación, desde el ordenador X, en fecha y hora.
15. El ciudadano digital ingresa a la tercera aplicación (sistema cliente).
    - Cada vez que un ciudadano digital accede a una aplicación tercera (sistema cliente), el sistema cliente puede, según su configuración, actualizar los datos (correo electrónico y teléfono móvil) que ha autorizado el ciudadano digital la primera vez que accedió al sistema.
16. Fin de la especificación de caso de uso.

Flujo Alternativo

2.a. Flujo Alternativo: El ciudadano no es ciudadano digital.

1. En el formulario que presenta el sistema para ingresar el número de documento de identidad y la contraseña, tiene las siguientes opciones:
    - ¿Aún no eres Ciudadano Digital? Regístrate aquí
    - Volver
2. Si el ciudadano ingresa a la opción ¿Aún no eres Ciudadano Digital? Regístrate aquí, se procede según el ECU 1.01 Registro de Ciudadano Digital.
3. Si el ciudadano ingresa a la opción Volver, el sistema regresa a la página principal de la tercera aplicación (sistema cliente).

3.a. Flujo Alternativo: El ciudadano digital no recuerda su contraseña.

1. El sistema en el formulario donde solicita ingresar la contraseña, tiene la opción ¿Olvidaste tu Contraseña?
2. El ciudadano digital, ingresa a la opción ¿Olvidaste tu Contraseña?
3. El sistema muestra un formulario que solicita ingresar el número de documento de identidad del ciudadano digital.
   Ej.
   ¿Olvidaste tu Contraseña?
   Para continuar ingresa el número de tu Cédula de Identidad.

   Cédula de Identidad
   _____

4. El ciudadano digital ingresa el número de cédula de identidad
   a. Si el número de la cédula de identidad es mal introducido el sistema muestra un mensaje en el mismo formulario: Ej. Documento inválido, asegúrate de introducirlo correctamente.
5. El sistema verifica no sea un ´robot´ quien realiza la acción (captcha).
6. El sistema recupera los datos de contacto del ciudadano digital (correo electrónico y teléfono móvil) y muestra el siguiente formulario:
   Ej.
   ¿Cómo deseas restablecer tu contraseña?
   - Enviar un código por mensaje de texto a mi teléfono terminado en 75
   - Enviar un enlace por correo electrónico a ep*******@a*****.bo

   No tengo acceso a ninguno de los datos mostrados

7. El ciudadano digital elige la opción a la cual tenga acceso.

   I. Mensaje de texto al teléfono

   a) El sistema envía un mensaje de texto con un código numérico al número del ciudadano digital y muestra un formulario para que ingrese el código enviado.
      - El código debe tener una vigencia parametrizable. (Mantener los anteriores plazos establecidos)

      Ej. Formulario
      Enviamos un código al teléfono terminado en 75
      Ingresa el código enviado por mensaje de texto
      _____
      ¿No lo recibiste? Solicita uno nuevo

   b) Si el ciudadano digital no recibe el código, solicita uno nuevo y regresa al paso 7, del presente flujo alternativo (*3.a. Flujo Alternativo: El ciudadano digital no recuerda su contraseña)*
   c) El ciudadano digital ingresa el código que le llegó al celular

- En caso de realizar esta acción desde un móvil, el código enviado lo reconoce automáticamente.

d) El sistema verifica que el código sea el correcto y que se encuentre vigente.
e) Si el código introducido no es el correcto o ya no se encuentra vigente, el sistema muestra en el formulario donde solicita introducir el código:

   Mensaje: Código incorrecto o no vigente.
   Cantidad de Intentos
   Vuelve a solicitar uno nuevo
   - Si vuelve a solicitar uno nuevo, vuelve al paso 7, del presente flujo alternativo (*3.a. Flujo Alternativo: El ciudadano digital no recuerda su contraseña)*

f) Si el código es introducido incorrectamente N veces (cantidad configurable), el sistema bloquea por un tiempo de X (configurable), la funcionalidad de restablecer contraseña para esa cuenta de ciudadanía digital y muestra un formulario indicando lo siguiente:
   Ej.
   Por favor, inténtalo de nuevo más tarde.
   Has superado el número de intentos. Por favor, inténtalo en X minutos.

   Contacta con Nosotros

   *Al hacer clic en contacto con Nosotros, el sistema se dirige al formulario de Soporte (Contacto).
   *Si el ciudadano digital, solicita nuevamente restablecer su contraseña, al introducir su número de documento de identidad, el sistema mostrará en el formulario un mensaje de que por los intentos fallidos debe intentarlo nuevamente en X tiempo.

g) Si el código es correcto, el sistema muestra un formulario para que el usuario introduzca su nueva contraseña, con las validaciones correspondientes
   - El campo donde introduce la contraseña le permite visualizar la contraseña que introduce (ojito)
   - Mientras introduce la nueva contraseña (manteniendo los mismo parámetros establecidos en el registro), el sistema le indica qué característica le falta para tener un nivel de seguridad intermedia para ser aceptada
   - El formulario tiene la opción de ¿Cómo es una contraseña segura?, que al hacer clic, se despliega en el mismo formulario las características de una contraseña segura.
   - El formulario tiene el campo ‘’Repetir contraseña’’. Este campo no permite que se pegue texto (para evitar que copien y peguen la nueva contraseña introducida)
   - Una vez introducido el código y validado por el sistema, el código deja de estar vigente.
h) El ciudadano digital introduce su nueva contraseña y repite la misma.
   - Si el usuario no realiza esta acción en un tiempo X (configurable), el sistema le muestra un mensaje que por el tiempo transcurrido debe volver a solicitar restablecer su contraseña.

i) El sistema restablece la contraseña del ciudadano digital y muestra un formulario con un mensaje de cambio de contraseña exitosa y envía un mensaje al correo electrónico del ciudadano digital, indicando el cambio realizado, fecha y hora y desde donde se hizo el cambio.
j) El ciudadano digital, puede regresar a la página principal de la aplicación tercera desde donde intentó autenticarse y solicitó restablecer contraseña.
k) Regresa al paso 1 del Flujo Básico.

II. Enlace correo electrónico

a) El sistema envía un enlace al correo electrónico del ciudadano digital y muestra un formulario que se ha enviado un enlace al correo electrónico:
Ej.

Enviamos un correo electrónico a ep*******@a*****.bo

Haz click en el enlace enviado a tu correo para restablecer tu contraseña.

Si no ves el correo por favor revisa tu carpeta de correo no deseado o spam.
¿No lo recibiste?
Solicita uno nuevo

- Si el ciudadano, solicita uno nuevo, regresa al paso paso 7, del presente flujo alternativo (*3.a. Flujo Alternativo: El ciudadano digital no recuerda su contraseña).*

b) El ciudadano digital ingresa a su correo electrónico que se ha enviado y hace clic en el botón RESTABLECER CONTRASEÑA.

- El correo electrónico tiene la opción también de copiar y pegar el enlace, por si no sirve el botón.
- El enlace tiene una vigencia de X de tiempo, pasado ese tiempo si el ciudadano digital hace clic en el botón, el sistema debe mostrarle un mensaje indicando que el enlace ya no se encuentra vigente y que debe solicitar uno nuevamente. El formulario debe tener un enlace al portal web de ciudadanía digital.
- Una vez que haga clic en el botón de restablecer contraseña, el enlace deja de estar vigente.

c) El sistema muestra un formulario para restablecer su contraseña, y se prosigue según lo detallado en los incisos h) i) j) k) del punto I. Mensaje de texto al teléfono.

III. No tengo acceso a ninguno de los datos mostrados

a) Si el ciudadano digital, no tiene acceso ni a su correo electrónico, el sistema le muestra un formulario con los requisitos para realizar la actualización de sus datos y los puntos de registro disponibles para realizar la actualización.
b) El ciudadano procede según lo descrito en el ECU Actualización de Datos a través de un Operador de Registro de Ciudadanía Digital (ECU a ser desarrollado en Gestión de la Cuenta).
c) El ciudadano digital regresa al paso 1 del Flujo Básico.

5.a. Ver Flujo Alternativo: El número de documento de identidad no se encuentra en las Cuentas de Ciudadanía Digital o la cuenta no se encuentra activa.

1. El sistema muestra en el campo donde solicita ingresar el número de documento de identidad, un mensaje de error: Ej. Usuario no registrado o inactivo.
    - El sistema no bloquea por introducir un usuario inexistente o inactivo.

2. Regresa al paso 2 del Flujo Básico.

7.a. Flujo Alternativo: La contraseña introducida es incorrecta.

1. El sistema registra el intento fallido hasta N veces (5 veces, debe ser configurable) y muestra en el formulario los intentos restantes que tiene.
    - El intento fallido cuenta contra el mismo usuario.
2. Si el ciudadano digital falla en tres oportunidades, el sistema bloquea la cuenta del ciudadano digital por un tiempo X, parametrizable.
    - Siempre que se loguee o cancele se vuelve a contar los intentos de inicio de sesión.
    - Si ingresa a otro sistema y se encuentra bloqueado, al introducir su CI y contraseña, le aparecerá que el usuario se encuentra bloqueado y puede desbloquearse con el link enviado a su correo electrónico.
3. El sistema muestra un mensaje que informa al ciudadano el tiempo el cual se encuentra bloqueado y la posibilidad de desbloquear su cuenta desde el mail enviado a su correo electrónico o comunicándose con soporte. Asimismo, tiene la opción de restablecer su contraseña.
    - Si se desbloquea por el link enviado al correo o por soporte, los intentos de inicio de sesión se vuelven a reiniciar.
    - El link de desbloqueo enviado al correo electrónico tiene la vigencia hasta la misma hora que se encuentra bloqueado el usuario. Si el link es utilizado antes de ese tiempo, deja de estar vigente.
    - Si el usuario usa un link vigente enviado a su correo para el desbloqueo, el sistema muestra usuario desbloqueado correctamente, si el usuario usa un link que ya no es vigente (realmente ya está desbloqueado), el sistema muestra un mensaje que el usuario ya se encuentra desbloqueado
    - Si se encontraba bloqueado el usuario y restablecer su contraseña, el sistema desbloquea al usuario y vuelve a reiniciar el contador de bloqueos (todo de cero).
4. Si aún no es el tercer error, continúa en el paso 3 del flujo básico

9.a. Flujo Alternativo: El ciudadano digital no tiene acceso al medio donde le llegó su 2do factor.

1. En el formulario que solicita ingresar el 2do factor, se tiene la opción de solicitar de otra manera el código.
2. El ciudadano digital solicita el 2do factor por otro medio

3. El sistema muestra un formulario con las otras opciones disponibles y la opción para que el ciudadano marque si de ahí en adelante es por ese medio por donde quiere le llegue el 2do factor.
4. El ciudadano elige la opción.
5. El sistema envía el código por el método seleccionado por el ciudadano digital.
    a. Si el ciudadano marcó la opción de que el código le llegue de en adelante por ese medio, la siguiente vez que inicie sesión, el código le llegará por la opción marcada.
6. Regresa al paso 8, del flujo básico.

11.a. *Flujo Alternativo: El código introducido no es el correcto*

1. El sistema registra el intento fallido hasta N veces cuando el código es incorrecto o caducado (5 veces, debe ser configurable) y muestra en el formulario el mensaje que el código es incorrecto o caducado, según corresponda, y los intentos restantes que tiene.
2. Si el ciudadano digital falla en tres oportunidades, el sistema bloquea la cuenta del ciudadano digital por un tiempo X, parametrizable.
    - Siempre que se loguee o cancele se vuelve a contar los intentos de inicio de sesión.
    - Si ingresa a otro sistema y se encuentra bloqueado, al introducir su CI, le aparecerá que el usuario se encuentra bloqueado y puede desbloquearse con el link enviado a su correo electrónico o comunicándose con soporte.
3. El sistema muestra un mensaje que informa al ciudadano el tiempo el cual se encuentra bloqueado y la posibilidad de desbloquear su cuenta desde el mail enviado a su correo electrónico o comunicándose con soporte.
    - Si se desbloquea por el link enviado al correo o por soporte, los intentos de inicio de sesión se vuelven a reiniciar.
    - El link de desbloqueo enviado al correo electrónico tiene la vigencia hasta la misma hora que se encuentra bloqueado el usuario. Si el link es utilizado antes de ese tiempo, deja de estar vigente.
    - Si el usuario usa un link vigente enviado a su correo para el desbloqueo, el sistema muestra usuario desbloqueado correctamente, si el usuario usa un link que ya no es vigente (realmente ya está desbloqueado), el sistema muestra un mensaje que el usuario ya se encuentra desbloqueado
4. Si aún no es el tercer error, continúa en el paso 10 del flujo básico.

Postcondiciones

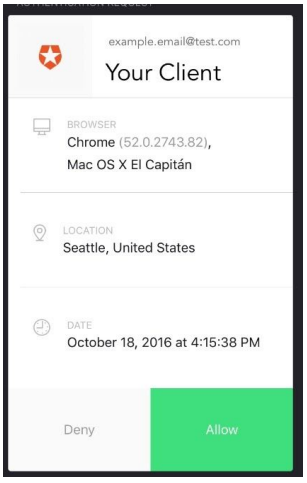
Ciudadano Digital autenticado en la tercera aplicación (sistema cliente).

Frecuencia

Cada que un ciudadano digital accede a un servicio digital del Estado.

Temas abiertos

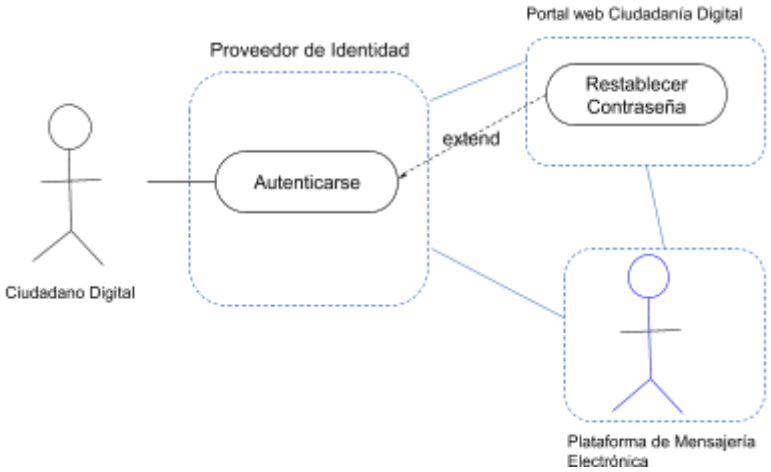
a) Revisar métodos de verificación de identidad a través de la aplicación móvil. Actualmente es una código generado continuamente en la aplicación móvil, esta opción puede ser cambiada a una más simple como la utilizada en google u otras aplicaciones donde se envía un mensaje push, misma que también podría ser utilizada como una manera adicional para restablecer contraseña.



b) Revisar mecanismos de seguridad al autenticarse, de ser necesario armar un equipo de investigación junto con el área de investigación, desarrollo y seguridad que permita de manera paralela mejorar la seguridad en la autenticación, ejemplo:

c) Identificar si el ciudadano se está autenticando de lugares no usuales, habituales (Ej. fuera del país, de otro departamento del cuál no es habitual) y pedir a parte de 2do factor (por más que haya marcado que es un ordenador conocido), un mecanismo adicional que valide su identidad, como ser preguntas de seguridad o validación con algún registro público.

Diagrama de Caso de Uso



Conformidad

Nombre, firma y fecha	Revisión, observaciones y comentarios
24/07/2020	1. En el mecanismo de autenticación se aumentará una sección de recomendación para que las entidades tengan una línea para definir si el servicio digital requiere de forma obligatoria introducir el 2do factor. 2. Opción de cerrar sesión en otros dispositivos, será incorporado en el ECU de gestión de cuenta. 3. Considerar que el token de ciudadanía digital sea utilizado para todos los posteriores servicios y/o trámites del usuario ya autenticado. 4. Al cerrar sesión en un sistema cliente, también debería cerrar sesión en la cuenta de ciudadanía digital. (Se recomienda aclarar este punto en el protocolo de autenticación y de ser posible implementar un proceso de certificación de los servicios que integran autenticación con ciudadanía digital)

ECU 2.01 - Actualizar datos desde la gestión de cuenta de Ciudadanía Digital

Actualizar de datos al iniciar sesión

Un ciudadano tiene la posibilidad de realizar la actualización de: Contraseña, Número telefónico de celular y Correo electrónico. Este proceso le permitirá tener actualizado sus datos para hacer un uso adecuado del sistema. La actualización puede ser realizada desde la aplicación móvil de ciudadanía digital y el portal web de ciudadanía digital.

Para efectuar las actualizaciones correspondientes, el ciudadano debe contar con una cuenta activa de Ciudadanía Digital.

Se pueden distinguir los siguientes momentos donde se realizan estas actualizaciones:

- Contraseña: En cualquier momento que el ciudadano desee realizar la actualización de su contraseña. Después que ha pasado un tiempo determinado desde la última vez que se ha establecido la contraseña (por motivos de seguridad).
- Número telefónico: En cualquier momento que el ciudadano desee realizar la actualización de su número de teléfono celular.

- Correo electrónico: En cualquier momento que el ciudadano desee realizar la actualización de su correo electrónico.

Figura 1: Especificación de datos para Actualización de datos al iniciar sesión

Etiqueta	Descripción
Número telefónico de celular	Número telefónico de 8 dígitos otorgado por un proveedor de telefonía móvil.
Código de verificación	Código numérico recibido por SMS
Correo electrónico	Dirección de correo electrónico
Contraseña	Contraseña registrada por el ciudadano para su cuenta de ciudadanía digital.

El formulario para actualizar correo, teléfono, contraseña puede ser desplegado desde la aplicación móvil, o mediante el portal web de ciudadanía digital.

Actores

- Ciudadano Digital

Precondiciones

- El ciudadano tiene una cuenta activa de Ciudadanía Digital.

Flujo de eventos

Flujo Normal

1. El ciudadano ingresa al sistema desde un navegador web, o mediante la aplicación móvil de ciudadanía digital en relación al ECU 1.02- Autenticarse con las credenciales de Ciudadanía Digital.
2. El sistema presenta en su menú la opción de información personal.
3. El ciudadano selecciona la opción Información Personal.
4. El sistema despliega una pantalla donde se visualiza:
   Sección Perfil:
   a. Nombres
   b. Apellidos
   c. Fecha de nacimiento
   d. Contraseña (escondida: *********), actualizable
   Sección Información de contacto:
   e. Teléfono, actualizable
   f. Correo electrónico, actualizable

- Los datos Nombres, Apellidos y Fecha de nacimiento no pueden ser actualizados.

5. El ciudadano elige la opción que requiera actualizar (contraseña, teléfono, correo electrónico).
   - Si el ciudadano selecciona la opción Actualizar número telefónico celular, continuará en el Flujo alternativo 1.
     5.a. Ver Flujo Alternativo: Actualizar número telefónico celular.
   - Si el ciudadano selecciona la opción Actualizar correo electrónico, continuará en el Flujo alternativo 2.
     5.b. Ver Flujo Alternativo: Actualizar correo electrónico.
   - Si el ciudadano selecciona la opción Actualizar contraseña, continuará con el paso 6.
6. El sistema presenta un formulario donde ingresa su contraseña actual, este formulario tiene la opción también de: Olvidaste tu contraseña?
7. El ciudadano ingresa su contraseña actual.
   7.a. Si el ciudadano hace clic en olvidaste contraseña, el sistema direcciona a la funcionalidad de restablecer contraseña.
8. El sistema verifica que la contraseña sea la correcta, caso contrario muestra un mensaje indicando la situación.
   8.a. Si el ciudadano introduce una contraseña incorrecta una cantidad configurada de veces, la sesión del ciudadano es cerrada y es devuelto al inicio del portal.
9. El ciudadano ingresa su nueva contraseña.
10. El ciudadano ingresa una confirmación de su nueva contraseña.
11. El sistema comprueba que la contraseña cumpla con las recomendaciones de contraseña, también que la contraseña y sus confirmación sean las mismas.
    - En caso de que la nueva contraseña tenga alguna observación, se anuncia esta condición al ciudadano. Solicita se vuelva a ingresar la nueva contraseña y su confirmación.
12. El sistema desplegará una ventana para que el ciudadano confirme el cambio de contraseña.
13. El sistema muestra un mensaje al ciudadano avisando que se cerrará sesión en todos los dispositivos y sistemas que usen ciudadanía digital.
14. Fin de la especificación de caso de uso.

Flujo alternativo

5.a. Ver Flujo Alternativo: Actualizar número telefónico celular

1. El sistema presenta un formulario donde ingresa su contraseña actual, este formulario tiene la opción también de: Olvidaste tu contraseña?
2. El ciudadano ingresa su contraseña actual.
   2.a. Si el ciudadano hace clic en olvidaste contraseña, el sistema direcciona a la funcionalidad de restablecer contraseña.
3. El sistema verifica que la contraseña sea la correcta, caso contrario muestra un mensaje indicando la situación.

3.a. Si el ciudadano introduce una contraseña incorrecta una cantidad configurada de veces, la sesión del ciudadano es cerrada y es devuelto al inicio del portal.

4. El sistema presenta un formulario donde el ciudadano ingresa su nuevo número telefónico celular personal.
5. El ciudadano ingresa su nuevo número telefónico.
6. El sistema, comprueba que el número telefónico no se encuentre asociado a una cuenta de ciudadanía digital (autoregistrada, verificada).
    - En caso de que el teléfono se encuentre vinculado a un usuario de ciudadanía digital, anuncia esta condición al ciudadano, sin identificar a qué cuenta está asociado. Solicita otro número de celular al ciudadano o que se comunique con soporte.
7. El sistema verifica el número de celular del ciudadano mediante un código de verificación por SMS.
    - Si está empleando la aplicación móvil para efectuar el registro, detecta el código de forma automática.
    - Caso contrario pide al solicitante que ingrese el código enviado manualmente y lo verifica.
    - Si el ciudadano no recibe o introduce a tiempo el código de verificación puede volver a solicitarlo en un periodo de tiempo determinado.
    - El código enviado debe tener un tiempo de vigencia (configurable).
8. La verificación y actualización del número telefónico es confirmada al ciudadano.
9. Continúa con el paso 14 del flujo normal.

5.b. Ver Flujo Alternativo: Actualizar correo electrónico

1. El sistema presenta un formulario donde ingresa su contraseña actual, este formulario tiene la opción también de: Olvidaste tu contraseña?
2. El ciudadano ingresa su contraseña actual.
   2.a. Si el ciudadano hace clic en olvidaste contraseña, el sistema direcciona a la funcionalidad de restablecer contraseña.
3. El sistema verifica que la contraseña sea la correcta, caso contrario muestra un mensaje indicando la situación.
   3.a. Si el ciudadano introduce una contraseña incorrecta una cantidad configurada de veces, la cuenta es bloqueada y esta condición es anunciada por el sistema.
4. El sistema presenta un formulario donde el ciudadano ingresa su correo electrónico personal.
5. El ciudadano ingresa su correo electrónico.
6. El sistema, comprueba que el correo electrónico no se encuentre asociado a una cuenta de ciudadanía digital (autoregistrada, verificada). Y valida el formato del correo electrónico.
    - En caso de que el correo electrónico se encuentre vinculado a un usuario de ciudadanía digital, anuncia esta condición al ciudadano, sin identificar a qué cuenta se encuentra asociado. Solicita otro correo electrónico al ciudadano o que se comunique con soporte.

- El sistema verifica si el dominio es gob.bo, edu.bo y mil.bo y otros sugeridos por la ADSIB, en caso de que si, el sistema muestra un mensaje de advertencia indicando que el correo debe ser personal y si desea continuar.
- El sistema verifica que el correo no sea un formato de correo temporal (ej. yopmail, mailinator), en caso de que si, el sistema muestra un mensaje indicando que debe registrar un correo válido.

7. El sistema verifica el mismo mediante un código enviado al correo electrónico.
    - Si el ciudadano no recibe o introduce a tiempo al correo de verificación puede volver a solicitarlo en un periodo de tiempo determinado.
    - El código enviado debe tener un tiempo de vigencia configurable (inicialmente se determina 15 minutos).
8. La verificación y actualización del correo es confirmada al ciudadano.
9. Continúa con el paso 14 del flujo normal.

Postcondiciones

- El ciudadano con datos, relacionados a la contraseña, número telefónico celular y correo electrónico, actualizados.
- El número y correo liberado en la actualización, puede ser usado por otro ciudadano en su pre registro.

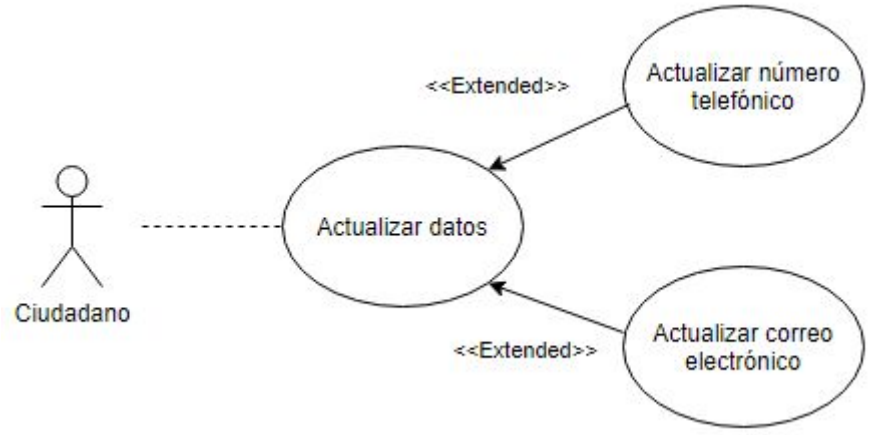
Frecuencia

- Cada vez que un ciudadano digital desee actualizar sus datos relacionados a la contraseña, número telefónico celular y correo electrónico, actualizados.
- En el caso de la contraseña, después que ha pasado un tiempo determinado desde la última vez que se ha establecido la contraseña, el sistema solicita de manera automática que se actualice la contraseña.

Temas abiertos

- Definir el tiempo de vigencia del código SMS enviado para la verificación del número de teléfono celular.
- Definir el tiempo de vigencia del enlace enviado para la verificación del correo electrónico.

Diagrama de caso de uso



Conformidad

Nombre, firma y fecha	Revisión, observaciones y comentarios
	Reunión 8/09/2020 (UIID, UGE) Se efectuaron los ajustes sugeridos por la unidad de Desarrollo.