



Proyecto DCV Evolución

Guía RSA del Administrador de Seguridad

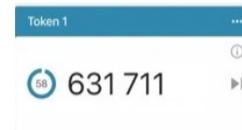
Acerca de esta Guía

 Esta guía describe las acciones que debe realizar un Administrador de Seguridad para gestionar los tokens de seguridad proporcionados por el DCV.

 RSA SecurID Software Token es un software de autenticación que transforma un teléfono inteligente en un dispositivo de autenticación, a través del registro digital de un Token proporcionado por DCV.



 Un token es un dispositivo lógico que genera una clave de 6 dígitos de forma aleatoria, actualizada cada 60 segundos. El código generado por el token será requerido para ingresar y para acceder a algunas funciones de la nueva plataforma DCVe .



 **Requisitos: Disponer de un teléfono inteligente con sistema operativo Android versión 6.0 o superior o Apple IOS 11.0 o superior. Se debe tener acceso a la tienda de aplicaciones Play Store o App Store según corresponda. (*)**



() Las tiendas de aplicaciones IOS y Android podrían modificar a futuro los requisitos de instalación de las aplicaciones.*

 Ayuda y soporte MAC - (562) 2393 90 01
Lunes a Viernes de 9:00hrs. a 18:30hrs.



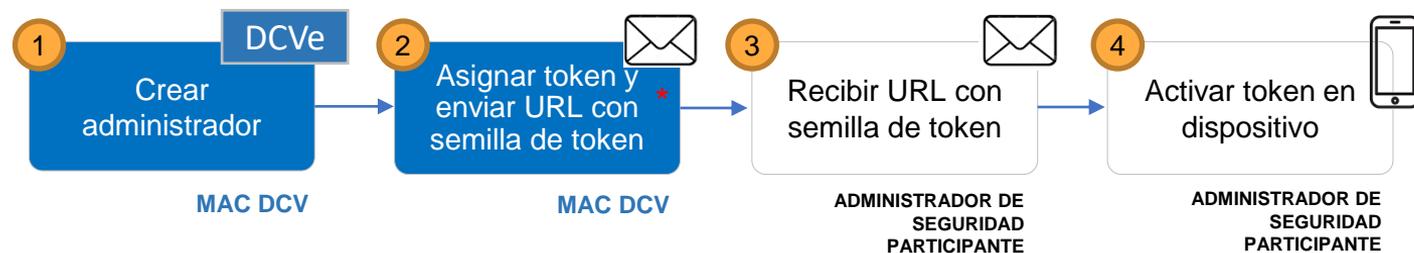
Índice

- 01** Activación del token del Administrador
- 02 Activación del token de Usuarios
- 03 Solicitud de cambio de token
- 04 Contingencia por no acceso a token
- 05 Activación RPA
- 06 Consultas y Soporte

Activación del token del Administrador

Para acceder a la nueva plataforma DCVe y poder realizar las funciones propias de un Administrador de Seguridad, la persona que tenga asignado el rol deberá disponer de un token RSA. El código generado por el token será requerido para ingresar “log in” y para realizar acciones que requieren la confirmación con el código de RSA.

Esquema habilitación RSA de un Administrador de Seguridad



(*) La información del sistema operativo del dispositivo del Administrador (Android/IOS) fue proporcionada en el nuevo Anexo 3 “Designación del Administrador de Seguridad”.

Activación del token del Administrador

Contenido

01

Instalación de aplicación RSA

Explica como instalar la aplicación RSA en el dispositivo del Administrador de Seguridad

02

Activación token lógico

Explica como activar el token lógico en la aplicación RSA, instalada previamente en el dispositivo

Activación del token del Administrador

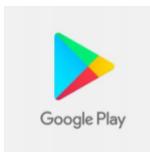
INSTALACIÓN DE APLICACIÓN RSA

- Para instalar la aplicación asegúrese que el dispositivo tenga conexión a Internet.
- En la lista de aplicaciones, toque en el icono de la App Store (IOS) o Play Store (Android).



Para celulares iphone (IOS), buscar “App Store”:

<https://apps.apple.com/cl/app/rsa-securid-softwaretoken/id318038618>



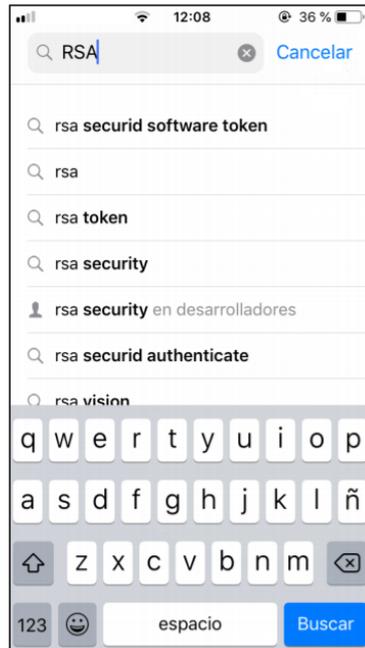
Para celulares Android, buscar “Google Play”:

https://play.google.com/store/apps/details?id=com.rsa.securidapp&hl=es_CL

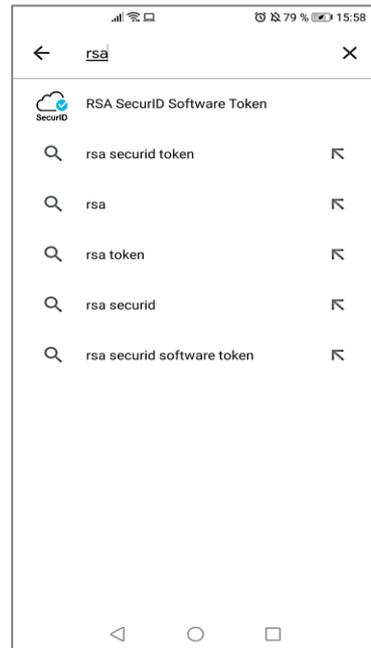
Activación del token del Administrador

INSTALACIÓN DE APLICACIÓN RSA (sólo si no está instalada previamente en el dispositivo)

1) En la tienda de aplicaciones de su dispositivo, busque la aplicación “RSA SecurID Software Token”.



IOS - Apple

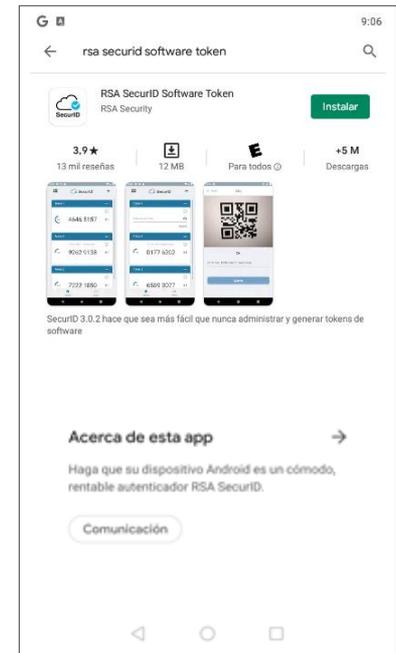


Android

2) Marque obtener/installar para descargar la aplicación “RSA SecurID Software Token”. La aplicación se instalará en su dispositivo.



IOS - Apple



Android

Activación del token del Administrador

ACTIVACIÓN DE TOKEN LÓGICO

La Mesa de Atención a Clientes DCV (MAC) le envió un correo con información para activar su token, abra el correo electrónico en su dispositivo y localice el mensaje que incluye un enlace del tipo URL. El enlace comienza con **com.rsa.securid://** para **IOS** o **http://127.0.0.1/securid** para **Android**.

Mantenga presionado el enlace y seleccione la opción **Copiar**.

En la lista de aplicaciones de su teléfono inteligente, busque el icono de la aplicación **RSA SecurID Software Token** y ejecútelo. Siga las siguientes instrucciones.

Estimada(o) *nombre_administrador_seguridad_solicitante*

En el presente correo se adjunta enlace para descargar token lógico para el siguiente usuario:

Nombre, Apellidos			
Correo electrónico corporativo			
Rut		Teléfono contacto	+56
Tipo de token solicitado	Token Android	Token IOS	

1) Enlace para para descargar y activar token lógico:

<http://127.0.0.1/securid/ctkip?scheme=https&url=amp.dcv.cl:443/ctkip/services/CtkipService&activationCode=009999999999>

Ejemplo correo de MAC con semilla de Token



Activación del token del Administrador

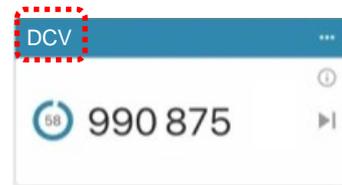
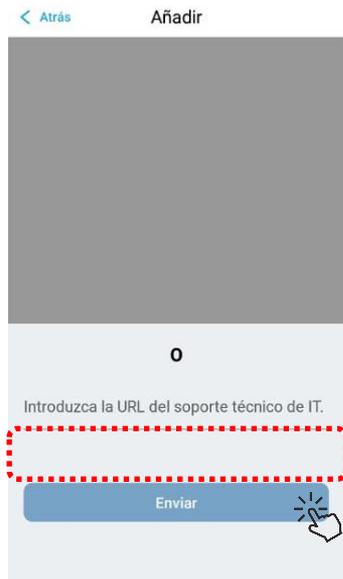
ACTIVACIÓN DE TOKEN LÓGICO

1) Abra la aplicación SecurID. Se desplegará el acuerdo de licencia.

2) Haga clic en “Comenzar”.

3) Introduzca el enlace enviado a su correo, que comienza con **com.rsa.securid://** para IOS o **http://127.0.0.1/securid** para Android. Haga clic en “Enviar”.

4) **Su token ha sido activado!**
El identificador asociado al token será DCV



Consideraciones:

- Si ya ha importado un token anteriormente, puede tocar el icono + para importar otro.

- La instalación del Token DCV se activa mediante un enlace URL y no mediante un código QR, por lo que no se requiere que la aplicación SecurID tenga acceso a hacer fotos y grabar videos en el dispositivo.

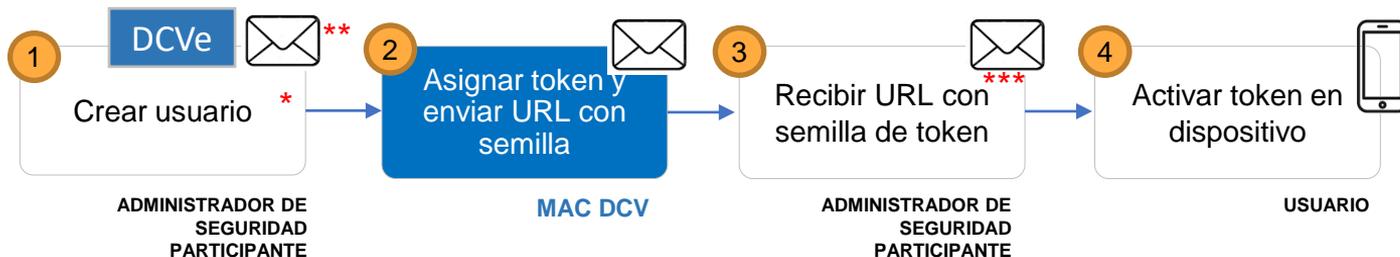
Índice

- 01 Activación del token del Administrador
- 02 Activación del token de Usuarios**
- 03 Solicitud de cambio de token
- 04 Contingencia por no acceso a token
- 05 Activación RPA
- 06 Consultas y Soporte

Activación del token a Usuarios

Todos los usuarios que accedan a **DCVe** requerirán un Token RSA.

Esquema habilitación RSA de un usuario



(*) El tipo de semilla (Android/IOS) se identifica en la pantalla de creación de usuario de PTW.

(**) El administrador de Seguridad, luego de el o los usuarios, debe formalizar la solicitud de asignación de tokens a la MAC a través un correo electrónico, indicando RUT y nombre del usuario(s).

(***) La semilla es enviada al Administrador de Seguridad con copia al Usuario del token.

Activación del token a Usuarios

Contenido

01

Solicitud de token para Usuarios

Explica como solicitar al DCV la asignación de un Token RSA.

02

Recepción de semillas de token

Explica como se recibe la semilla que permite la activación del Token RSA en un dispositivo.

03

Instalación de token en dispositivo Usuario

Explica como activar el Token RSA en un dispositivo del usuario.

Activación del token a Usuarios

SOLICITUD DE TOKEN PARA USUARIOS (1/2)

Los datos requeridos para habilitar el token a un usuario deben ser completados por el Administrador de Seguridad en la pantalla de creación de usuario de **DCVe**, identificando los datos del usuario y el tipo de sistema operativo del dispositivo donde se instalará el token lógico.

Datos de la persona para habilitar el token (*)

Tipo de dispositivo donde se instalará el token, Android / IOS

The screenshot shows the 'DCVe' user creation interface. At the top right is the DCVe logo with the tagline 'CUSTODIAMOS HOY EL VALOR DEL MAÑANA'. Below the logo is a navigation bar with tabs: 'Detalles', 'Perfiles de permisos', 'Perfil de permisos', 'Roles', 'Grupo de cuenta', and 'Cuentas'. The 'Detalles' tab is selected, showing the 'Detalles de la cuenta de usuario' form. The form includes fields for 'Participante', 'Identificador de Contribuyente', 'Nombre de usuario', 'Contraseña', 'Volver a ingresar la contraseña', 'ID de Usuario de RSA', 'Nombre', 'Apellido', 'Referencia interna', 'Corporate email', 'Phone Number', and 'RSA token type'. There are also radio buttons for 'Se permite el inicio de sesión' and 'La contraseña nunca expira', and a checkbox for 'Usar el RUT como Nombre de Usuario' and 'Cambiar contraseña'. A dropdown menu for 'Tipo de activación' is open, showing options: 'ANDROID', 'IOS', and 'OTRO'. At the bottom right are 'Guardar' and 'Cancelar' buttons.

Activación del token a Usuarios

SOLICITUD DE TOKEN PARA USUARIOS (2/2)

De forma complementaria a la creación en DCVe, el Administrador de Seguridad debe especificar a la(as) persona(s) a las cuales DCV debe asignar un token, mediante un formulario específico denominado *Formulario de Solicitudes Dispositivo Token*.

DCV:• FORMULARIO DE SOLICITUDES DISPOSITIVO TOKEN - *Solicitud de Token*

Razón social	Rut	Código DCV

Identificación del administrador de seguridad del Participante

Nombres	Apellidos	Rut	Nro telefono de contacto	Correo electrónico corporativo

Identificación del/los usuarios(s) y dispositivo(s) requerido(s):

N°	Nombres	Apellidos	Rut	Nro telefono de contacto	Correo electrónico corporativo	Tipo de dispositivo	Comentarios (opcional)
1						Android	
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							



Este formulario debe ser enviado a la MAC desde la cuenta corporativa de correo electrónico del Administrador de Seguridad.

Lista desplegable con tipo de dispositivo Android / IOS

Activación del token a Usuarios

RECEPCIÓN DE SEMILLAS DE TOKEN

La Mesa de Atención a Clientes MAC asignará los Tokens lógicos con cada usuario.

La MAC enviará un correo electrónico al Administrador de Seguridad del Participante que realizó la solicitud, copiando al Usuario, indicando:

- Enlace (link) para activación del Token en el teléfono inteligente. Enlace para descargar Guía de Instalación RSA.

Este enlace tiene vigencia de 07 días corridos, si en este plazo el usuario no activa el token en su dispositivo este enlace caducará, por lo que el Administrador de Seguridad debe solicitar el reenvío vía correo electrónico a mac@dcv.cl.



Es responsabilidad del Administrador de Seguridad asegurar que el token quedó instalado en cada dispositivo.

Estimada(o) nombre_administrador_seguridad_solicitante

En el presente correo se adjunta enlace para descargar token lógico para el siguiente usuario:

Nombre, Apellidos			
Correo electrónico corporativo			
Rut		Teléfono contacto	+56
Tipo de token solicitado	Token Android	Token IOS	

1) Enlace para para descargar y activar token lógico:

<http://127.0.0.1/segurid/ctkip?scheme=https&url=amp.dcv.cl:443/ctkip/services/CtkipService&activationCode=00999999999>

2) La guía de instalación del token lógico puede descargarse desde el siguiente enlace:

http://www.dcv.cl/documentos/formularios_token/

Este enlace tiene vigencia de 07 días, si en este plazo el usuario no activa el token en su dispositivo este enlace caducará, por lo que el administrador de seguridad debe solicitar el reenvío vía correo electrónico a mac@dcv.cl.

Saludos,



Nombre

Cargo

✉ nombre.apellido@dcv.cl

📍 Av. Apoquindo 4001 Piso 12, Las Condes, Santiago.

☎ (562) 23 939 001

🌐 www.dcv.cl

Ejemplo correo de MAC con semilla de Token

Activación del token a Usuarios

INSTALACION DE TOKEN EN DISPOSITIVO USUARIO

El correo generado por la MAC incluye un vínculo para descargar la **Guía de Instalación RSA en dispositivo**, que describe al usuario operador como instalar la aplicación **RSA SecurID Software Token** en el dispositivo y luego registrar el **Token** en la aplicación.

<http://127.0.0.1/securid/ctkip/scheme=https&uri=amp.dcv.cl:443/ctkip/services/Ctkipserver&activationCode=0099999999>

2) La guía de instalación del token lógico puede descargarse desde el siguiente enlace:

http://www.dcv.cl/documentos/formularios_token/

Este enlace tiene vigencia de 03 días, si en este plazo el usuario no activa el token en su dispositivo

El procedimiento de instalación de la aplicación RSA y el registro de Token para los usuarios es similar al descrito en la sección *Activación del token del Administrador* de esta Guía.

Índice

- 01 Activación del token del Administrador
- 02 Activación del token de Usuarios
- 03 Solicitud de cambio de token**
- 04 Contingencia por no acceso a token
- 05 Activación RPA
- 06 Consultas y Soporte

Solicitud de cambio de token

Por cambio de sistema operativo del dispositivo

Para cambios de dispositivo se debe utilizar un formulario **descrito en la página siguiente**.

En el caso de ser un cambio de dispositivo desde Android a IOS o de IOS a Android, el Administrador de Seguridad **debe realizar el cambio en la pantalla de modificación de datos de usuario de DCVe**, identificando el nuevo tipo de sistema operativo del dispositivo y guardando el cambio.

DCV: CUSTODIAMOS HOY EL VALOR DEL MAÑANA

Detalles | Perfiles de permisos | Perfil de permisos | Roles | Grupo de cuenta | Cuentas

Detalles de la cuenta de usuario

Participante: 2200

Identificador de Contribuyente: DCV

Identificador de Contribuyente: 10.000.000-1

Nombre de usuario: 10.000.000-1

Usar el RUT como Nombre de Usuario

Se permite el inicio de sesión: Sí No

La contraseña nunca expira: Sí No

Cambiar contraseña

Contraseña: []

Volver a ingresar la contraseña: []

ID de Usuario de RSA: 10.000.000-1

Nombre: Rafael

Apellido: Toro

Referencia interna: []

Corporate email: rtoro@rt.com

Phone Number: []

RSA token type: ANDROID

Información de revisión

Tipo de activación: ANDROID, IOS, OTRO

Guardar Cancelar

Tipo de dispositivo donde se instalará el token, Android / IOS

Solicitud de cambio de token

Solicitudes de cambios por pérdidas, cambios de sistema operativo del dispositivo o falla no solucionable.

La solicitud de cambio de token debe realizarla el Administrador de Seguridad, mediante un formulario específico llamado *Formulario de Solicitudes Dispositivo Token*, en la sección Cambio de Token.

DCV: FORMULARIO DE SOLICITUDES DISPOSITIVO TOKEN - Cambio de Token
Identificación del Solicitante

Razón social	Rut	Código DCV

Identificación del administrador de seguridad del Participante

Nombres	Apellidos	Rut	Teléfono contacto	Correo electrónico corporativo

Identificación del/los usuarios(s) y dispositivo(s) requerido(s):

N°	Motivo del Cambio	Nombres	Apellidos	Rut	Correo electrónico corporativo	Nro telefono de contacto	Dispositivo actual	Dispositivo nuevo	En caso de daño/falla indique el comportamiento detectado
1	Perdida/Robo								
2	Cambio dispositivo								
3	Daño/Falla								
4									
5									

Este formulario debe ser enviado a la MAC desde la cuenta corporativa de correo electrónico del Administrador de Seguridad.

Lista desplegable con motivos del cambio de token.

Formulario de Solicitudes Dispositivo Token, sección Cambio de Token

Lista desplegable con tipo de dispositivo Android / IOS

Índice

- 01 Activación del token del Administrador
- 02 Activación del token de Usuarios
- 03 Solicitud de cambio de token
- 04 Contingencia por no acceso a token**
- 05 Activación RPA
- 06 Consultas y Soporte

Contingencia por no acceso a token

Cuando un usuario no tenga acceso a su token y requiera ingresar a **DCVe** en forma urgente, para consultar información o para participar de alguna operación que requiera la doble autenticación, DCV puede asignar un **código fijo de emergencia** que reemplaza el código dinámico que entrega el token.

Condiciones

-  Debe ser solicitado vía correo electrónico por el Administrador de Seguridad a la MAC, identificando al usuario con su RUT, Nombre Completo y Correo Electrónico de contacto, el cual debe tener un token asignado al momento de la solicitud.
-  Tendrá 7 días corrido de vigencia, el token ya asignado al usuario no se inhabilitará en este periodo. Si es ingresado el código del token en lugar del código de emergencia durante este periodo, el código de emergencia se inhabilitará permanentemente.
-  El plazo de vigencia del código de emergencia no será prorrogado. En este periodo se debe resolver el acceso a un dispositivo para el usuario, en el que se registrará la semilla del token lógico.



Índice

- 01 Activación del token del Administrador
- 02 Activación del token de Usuarios
- 03 Solicitud de cambio de token
- 04 Contingencia por no acceso a token
- 05 Activación RPA**
- 06 Consultas y Soporte

Activación RPA



Con la finalidad de proceder con la Activación RPA (Robotic Process Automation), la cual permite obtener un código de acceso fijo de RSA, el Administrador de Seguridad debe realizar una solicitud al Depósito Central de Valores S.A. (MAC-DCV)

Condiciones

- Debe ser solicitado mediante un formulario denominado “SOLICITUD TOKEN RSA PARA ACTIVACION RPA”, proporcionado por DCV.
- Tendrá un periodo de vigencia limitado, para su renovación deberá existir una nueva solicitud.
- En caso de tener lugar el término de la relación contractual con DCV y/o la deshabilitación del usuario creado, al cual se le asignó el código de acceso fijo RSA, se inactivará este método de acceso.





Formulario asociado

FORMULARIO SOLICITUD TOKEN RSA PARA ACTIVACION RPA

Activación RPA (Robotic Process Automation)

Fecha: (dd/mm/aaaa)

PARTICIPANTE (RAZÓN SOCIAL):

RUT:

CODDEP:

Con la finalidad de proceder con la **Activación RPA (Robotic Process Automation)** solicito al Depósito Central de Valores S.A., Depósito de Valores (DCV) en mi rol de Administrador de Seguridad, la asignación de token RSA, esto es, un método de autenticación que generará claves aleatorias e irremplazables, para el acceso al sistema computacional y autorización por cuenta del Participante, de operaciones sensibles, con un valor autenticador que tendrá una vigencia de seis meses.

Estoy en conocimiento que:

1. El token RSA es un medio de autenticación que proveerá el DCV, para acceder al sistema computacional y participar en operaciones que requieran un segundo factor de autenticación de acuerdo con la reglamentación vigente del DCV.
2. El plazo de vigencia del token no será prorrogado automáticamente. Para su renovación deberá existir una nueva solicitud.
3. En caso de tener lugar el término de la relación contractual con DCV y/o la deshabilitación del respectivo usuario, implicará la inactivación del token solicitado.
4. El canal de comunicación con DCV para consultas o requerimientos será la Mesa de Atención a Clientes (MAC).

Responsabilidades:

1. Declaro conocer y aceptar que es mi responsabilidad como Administrador de Seguridad habilitar y asignar privilegios al usuario automatizado, fijar sus roles, las actividades que podrá realizar a través del Sistema Computacional de DCV y definir los Parámetros de Seguridad asociados.
2. El Participante de quien soy Administrador de Seguridad está en pleno conocimiento de esta solicitud y por consiguiente, asume y será el responsable por el buen uso de las claves de acceso y código autenticador, y de los roles que, como Administrador de Seguridad, haya habilitado al operador automatizado para actuar en el Sistema de DCV. En mérito de lo anterior, de las disposiciones del Contrato de Depósito y del Reglamento Interno vigente del DCV, este último queda liberado de toda responsabilidad por los perjuicios cuya causa directa o indirecta sea el uso erróneo, indebido o fraudulento de las credenciales otorgadas. Esta liberación comprende cualquier tipo de perjuicio que se haya producido, sea patrimonial o moral.

Documento Controlado, prohibida su reproducción parcial o total sin autorización. Clasificación: Uso Interno.

FORMULARIO SOLICITUD TOKEN RSA PARA ACTIVACION RPA

Identificación del usuario (RPA):

Nombre			
Correo electrónico corporativo			
Rut		Teléfono contacto	+56

Recomendaciones de DCV para el cuidado y buen uso del Token RSA:

1. Contar con una interfaz para alimentar con la clave de usuario y el token, y que sea provisto por personas diferentes.
2. Que el almacén donde se registre en la configuración, tanto la clave de acceso como el token, sean lugares seguros (encriptados y con permisos mínimos de acceso, auditados)

Identificación del Administrador de Seguridad solicitante:

Fecha	
Nombre	
Rut:	
Firma:	

Documento Controlado, prohibida su reproducción parcial o total sin autorización. Clasificación: Uso Interno.

Formulario *Solicitud Token RSA para activación RPA*, necesario para la formalización de la solicitud a DCV.

Índice

- 01 Activación del token del Administrador
- 02 Activación del token de Usuarios
- 03 Solicitud de cambio de token
- 04 Contingencia por no acceso a token
- 05 Activación RPA
- 06 Consultas y Soporte**



Si tienes dudas, contacta a:
Mesa de Atención a Clientes MAC
(562) 2 393 9001
mac@dcv.cl

Lunes a viernes de 9:00 a 18:30 horas.

Guía RSA del Administrador de Seguridad



Av. Apoquindo 4001, piso 12. Las Condes.
www.dcv.cl

