

|  |
| --- |
| Normativa de Alta, Baja y Modificaciones de Usuarios |

**Junio, 2024**

**Versión [5.0]**

**Contenido**

[Objetivo 3](#_Toc175824798)

[Alcance 3](#_Toc175824799)

[De las responsabilidades 3](#_Toc175824800)

[Gerencia de Tecnología e Innovación – Colmena Tech Support 3](#_Toc175824801)

[Gerencia de Personas 3](#_Toc175824802)

[Todas las gerencias de Colmena que sean responsables de un servicio externo 3](#_Toc175824803)

[Área de Seguridad de la información y Ciberseguridad 3](#_Toc175824804)

[De la gestión de ABM de usuarios internos 4](#_Toc175824805)

[Altas de usuarios internos 4](#_Toc175824806)

[Autorización para AGV con Licencia o Desvinculados 4](#_Toc175824807)

[Bajas de usuarios internos 5](#_Toc175824808)

[Control de Bajas de usuarios internos 6](#_Toc175824809)

[Modificaciones de usuarios internos 6](#_Toc175824810)

[Suspensión de cuentas 6](#_Toc175824811)

[De la gestión de ABM de usuarios externos 7](#_Toc175824812)

[Alta de usuarios externos 7](#_Toc175824813)

[Baja de usuarios externos 7](#_Toc175824814)

[Modificaciones de usuarios externos 8](#_Toc175824815)

[De las prohibiciones 8](#_Toc175824816)

[Evaluación y difusión 8](#_Toc175824817)

[Control de Versión 8](#_Toc175824818)

## Objetivo

Establecer directrices, roles y responsabilidades para la alta (creación), baja (bloqueo o eliminación) y modificaciones a las cuentas de los sistemas de Colmena, con objeto de resguardar el acceso a los activos de información de forma adecuada, así como su desvinculación oportuna para colaboradores que ya no pertenecen a la compañía.

## Alcance

Esta normativa aplica a todos las cuentas de acceso a los sistemas propios de Isapre Colmena y los que se encuentren bajo administración de terceros que contengan información y datos de Isapre Colmena; o cualquier otro que preste servicios utilizando suscripciones en modalidad Cloud (Nube).

## De las responsabilidades

### Gerencia de Tecnología e Innovación – Colmena Tech Support

El Equipo CTS es responsable de la **gestión de altas, bajas y modificaciones de usuarios** en los sistemas de Isapre Colmena, tanto para usuarios internos como externos. El equipo de operaciones SAP para las Altas y Modificaciones del sistema SAP.

Para cada Solicitud se debe **adjuntar en el ticket la evidencia de los privilegios otorgados o de las bajas realizadas**.

### Gerencia de Personas

Es responsabilidad de las áreas correspondientes **comunicar de forma oportuna al área de TI** todos los nuevos ingresos, renuncias o desvinculaciones que ocurran dentro de la compañía, independientemente del rol del colaborador.

Esta comunicación es fundamental para que TI realice la **gestión de accesos** en los sistemas de Isapre Colmena, según las funciones que el colaborador desempeñe dentro de la organización.

Además, se debe:

* + **Informar semanalmente al equipo CTS** el detalle de todas las bajas registradas durante la semana anterior, **con fecha de corte cada viernes (**considera bajas del sábado anterior al viernes actual).
  + **Reportar mensualmente a Seguridad de la Información** el detalle consolidado de las bajas del mes, **con fecha de corte el último día hábil del mes**.

### Todas las gerencias de Colmena que sean responsables de un servicio externo

La gerencia contraparte de cada proveedor es responsable de gestionar con el área de TI el alta, baja y modificaciones de los usuarios que requieren accesos a sistemas de Colmena por parte del proveedor para realizar sus funciones, dejando registro de la solicitud, y así minimizar el riesgo de mal uso de la información y velar por el cumplimiento de las políticas y normativas establecidas. Además deben realizar seguimiento de las recomendaciones generadas y publicadas por Isapre Colmena.

### Área de Seguridad de la información y Ciberseguridad

Es responsabilidad actualizar la normativa de ABM con el fin de asegurar su efectividad y mejora continua, y velar por el cumplimiento de las directrices presentes en esta normativa.

## De la gestión de ABM de usuarios internos

### Altas de usuarios internos

Para la creación de una cuenta a un nuevo colaborador, el Bussines Partner de la Gerencia de Personas (quien realiza esta gestión como apoyo al área de Ventas para los nuevos ingresos de jefes comerciales o agentes de venta) o el jefe directo es quien debe crear el ticket en la plataforma del área de Soporte Digital de Aplicaciones Colmena, indicando los datos del nuevo colaborador tales como: Rut, nombre, cargo que va a ocupar, área y gerencia a la que va a pertenecer.

En el caso de los agentes de venta o jefes comerciales, las aplicaciones transversales que les corresponden son:

* Correo, slack
* Código SIS
* Brío Comisiones
* Consulta integral
* Declaración Salud Electrónica
* Simulador y costeador de planes
* Sistema de funes.

El ticket deberá contener visto bueno VB de jefatura para que el área de Soporte Digital proceda a crear los accesos de acuerdo a la información indicada en el ticket. Independiente del rol del colaborador.

Para los gerentes que soliciten accesos vinculados a SAP, la aprobación deberá ser otorgada por el Gerente General o el Gerente de Finanzas.

Para la solicitud de accesos, se deberá indicar el RUT de un usuario con un rol equivalente, quien deberá pertenecer a la misma unidad organizacional (área o gerencia) que el solicitante.

Mientras las matrices de privilegios no se encuentren actualizadas, se mantendrá vigente este control complementario como medida de referencia para la asignación de accesos.

En los casos donde se soliciten accesos que no correspondan a roles equivalentes existentes, será obligatoria la validación previa del área de Seguridad de la Información antes de otorgar los privilegios.

Todo nuevo nombre de usuarios generado para ingresar a sistemas debe ser el correo corporativo como usuario ID o RUT, y en el caso que el sistema no permita esta nomenclatura, debe seguir el siguiente formato: La inicial del nombre principal y de los dos apellidos + numero correlativo (3 dígitos) de acuerdo a lo definido en la normativa de “usuarios y contraseñas”.

Ejemplo: Juan Antonio Pérez González. Usuario: jpg001

Ejemplo AGV: ZZZ0101

### Autorización para AGV con Licencia o Desvinculados

Si un agente de ventas se encuentra de licencia médica o se ha desvinculado, se podrá solicitar la habilitación de sus accesos solo cuando se requiere completar un proceso de venta. La cual debe solicitar el Jefe comercial a través de ticket JIRA al área de Soporte Digital y solo para terminar el proceso de venta. Una vez finalizado el proceso, se debe bloquear nuevamente la cuenta.

Para otorgar los accesos se debe obtener la aprobación del Jefe de Operaciones comerciales de la Gerencia de Ventas, quien definirá el plazo máximo de habilitación excepcional de la cuenta.

### Bajas de usuarios internos

Para la baja o bloqueo de un usuario interno, la Gerencia de Personas debe informar de forma oportuna al área de Soporte Digital de la Gerencia de Tecnología e innovación para que se proceda al bloqueo de cuentas usuarias. Esta información será proporcionada de forma automática a través de la aplicación Talana, la cual es gestionada y administrada por la Gerencia de Personas, en caso de falla de la aplicación Talana, la Gerencia de Personas deberá enviar una planilla Excel con los datos necesarios para la baja o bloqueo de la cuenta usuaria a través de ticket en sistema JIRA.

Para la baja de roles privados debe ser solicitada oportunamente mediante la creación de un ticket, por el área de Personas.

El área de Soporte Digital deberá realizar las siguientes acciones para completar la baja de la cuenta usuaria en todos los sistemas y aplicativos:

* Utilizar Sistema de Privilegios para bloquear la cuenta usuaria de todos los aplicativos desarrollados por Colmena
* Utilizar Active Directory para deshabilitar la cuenta de correo, con esta acción se bloquea acceso a VPN y repositorio de archivos Apolo2.
* Luego de deshabilitar lo anterior, se procede a reportar a través de Slack, para continuar con el resto de las aplicaciones No internos.
* Dentro del ticket se deja un listado con las aplicaciones las cuales fueron dadas de baja (check-list), esto también se utiliza para tickets generados automáticamente por Talana, verificando que se encuentre realizada la baja de accesos correctamente. Adicionalmente dentro del ticket se adjunta una captura de pantalla del Sistema de Privilegios, como evidencia de que la cuenta se encuentra deshabilitada.

Ejemplo de check list:

|  |  |
| --- | --- |
| **Aplicaciones** | **Respuesta** |
| AD y Exchange(\*) | Deshabilitado o No existe |
| Big-Data | Deshabilitado o No existe |
| BRIO | Eliminado o No existe |
| CRM | Deshabilitado o No existe |
| SAP/Portal | Deshabilitado o No existe |
| DevOps | Deshabilitado o No existe |
| Sybase (BBDD) | Deshabilitado o No existe |
| Jira, Slack, Zoom, G-drive y Miro | Deshabilitado o No existe |
| Sistema de Privilegios(\*\*) | Deshabilitado o No existe |

(\*): En caso de “No existe” se adjunta captura de pantalla dentro del ticket.

(\*\*): Siempre que se deshabilite una cuenta se adjunta captura de pantalla dentro del ticket.

Las cuentas deben ser bloqueadas dentro de 30 horas hábiles por el área de Soporte Digital.

### Control de Bajas de usuarios internos

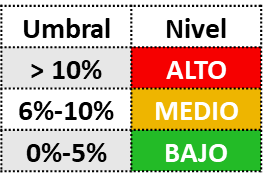
Semanalmente la Gerencia de Personas al área de Soporte Digital enviará una planilla con el resumen de los usuarios desvinculados en el período (cada viernes, considera bajas del sábado anterior al viernes actual), de modo que pueda validar el correcto bloqueo de estas cuentas.

Mensualmente la Gerencia de Personas enviará al área de Seguridad de la Información un reporte con el resumen de los usuarios desvinculados en el periodo. (Desde el primer al último día de cada mes).

El área de Seguridad de la Información realizará una validación mensual y trimestral respecto de la correcta baja de las cuentas de correo a través de reporte de Active Directory, SAP y Base de Datos suministrado por TI, para lo cual deberá recibir desde la Gerencia de Personas el resumen de los usuarios desvinculados al final de cada mes y al final de cada trimestre. Esto con el objetivo de verificar que se cumplió con las bajas de cuentas respecto a la totalidad de desvinculados. En caso de encontrar cuentas usuarias que debieron ser dadas de baja y aún se encuentran vigentes, el área de Seguridad de la información generará un ticket por cada usuario para regularizar la situación.

Dado que este proceso es eminentemente manual, se define el siguiente nivel de riesgo de tolerancia en cuanto al % total de cuentas vigentes que debieron ser dadas de bajas en el período analizado.

Indicador: Cuentas vigentes de usuarios desvinculados / Total desvinculados del mes= % de umbral



### Definición de Controles de Línea

Primera línea: Áreas solicitantes deben garantizar que los accesos solicitados son necesarios y proporcionales. (Personas y CTS).

Segunda línea: Seguridad de la Información validará (mensualmente y trimestralmente) que las solicitudes y accesos estén conforme a las políticas vigentes.

Tercera línea: Auditoría Interna revisará periódicamente (trimestral) el cumplimiento de este procedimiento.

### Modificaciones de usuarios internos

Para la modificación de privilegios de un usuario interno, la jefatura responsable debe autorizarlo mediante correo de justificación para tener los respaldos competentes.

Usuario o jefatura deberá generar una solicitud a través de ticket indicando los accesos y los sistemas requeridos adjuntando correo de autorización.

Para la modificación de accesos, se deberá indicar el RUT de un usuario con un rol equivalente, quien deberá pertenecer a la misma unidad organizacional (área o gerencia) que el solicitante.

Mientras las matrices de privilegios no se encuentren actualizadas, se mantendrá vigente este control complementario como medida de referencia para la asignación de accesos.

En los casos donde se soliciten accesos que no correspondan a roles equivalentes existentes, será obligatoria la validación previa del área de Seguridad de la Información antes de otorgar los privilegios.

El área de Soporte Digital realizará los ajustes de acuerdo a lo que indica el ticket.

### Suspensión de cuentas

La suspensión de cuentas será aplicada solo a los colaboradores con cargo de “Agente de venta” del área Comercial en cada situación en que se encuentren con Licencia Médica a partir del día 1.

El ticket se genera de forma automática desde Talana al área de Soporte Digital, con ello se procede a la suspensión temporal de la cuenta en todos los aplicativos de la compañía. Es decir, todas aquellas aplicaciones que son utilizadas para generar ventas (VEA, Portal Ejecutivo, FUN Web, Consulta Integral, entre otros).

Posteriormente, en el momento del retorno de la licencia es el jefe Comercial quien debe notificar la reactivación de las cuentas a los Agentes de Venta que han vuelto de licencia a través de ticket JIRA al área de Soporte Digital.

## De la gestión de ABM de usuarios externos

### Alta de usuarios externos

En todos los casos en que un proveedor o servicio externo requiera accesos a los sistemas de Isapre Colmena, es responsabilidad de la Gerencia contraparte realizar la solicitud a través de ticket en JIRA, mantener las comunicaciones y notificaciones oportunas con el proveedor y con el área de Soporte Digital para dar el o los accesos que correspondan. Además es su responsabilidad contar con un contrato debidamente firmado antes de iniciar sus funciones, dicho contrato deberá contener clausula explicita de las responsabilidades en el proceso de alta, baja y modificaciones de usuarios, alineado con lo que se menciona en esta normativa. Todo esto deberá ser pactado y firmado por las partes antes de otorgar los accesos.

Los accesos deben definirse con un ID único que será el RUT, asociado a su nombre completo nombres y apellidos. En caso de externos además, se deberá colocar la palabra “externo” en el dominio de su correo junto a colmena.cl ([usuario@externo.colmena.cl](mailto:usuario@externo.colmena.cl)). No se crearán cuentas genéricas para colaboradores externos y éstas siempre deben identificar al usuario responsable de su uso.

Los accesos deberán otorgarse de acuerdo a las funciones a realizar por el externo, como recomendación dar el acceso mínimo necesario o de “solo lectura” en todos los casos que sea posible.

### Baja de usuarios externos

En todos los casos en que un proveedor o servicio termine relación con Isapre Colmena, o bien termine su función determinada en los sistemas, se deberá bloquear los accesos a los sistemas de forma inmediata, es responsabilidad de la Gerencia contraparte mantener las comunicaciones y notificaciones oportunas con el proveedor y el área de Soporte Digital para dar de baja los accesos que correspondan.

### Modificaciones de usuarios externos

En todos los casos en que un proveedor o servicio requiera agregar, quitar o modificar un privilegio o perfil de los sistemas a los cuales tiene acceso, deberá solicitarlo a la gerencia contraparte con evidencia de un correo electrónico las razones que justifican dicha solicitud.

Es responsabilidad de la Gerencia contraparte realizar la solicitud, mantener las comunicaciones y notificaciones oportunas con el proveedor y el área de Soporte Digital para dar los accesos que correspondan.

La Gerencia contraparte o el área de Soporte digital podrán realizar las consultas que requieran al área de Seguridad de la información en caso de dudas con los accesos a otorgar.

## De las prohibiciones

Queda expresamente prohibido traspasar las credenciales de acceso de sistemas o aplicativos a otro usuario, sin ninguna excepción.

## Evaluación y difusión

La presente normativa será evaluada por el área de Seguridad de la Información en forma anual o cuando un cambio significativo la impacte, esto con el fin de asegurar que es idónea para la organización.

Una vez aprobada deberá ser difundida a los colaboradores internos y externos, mediante alguno de los medios de comunicación corporativa que se encuentren disponibles.

## Control de Versión

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Código de versión | Realizado por: | Revisada por: | Aprobado por: | Fecha |
| V1 | Analista de Seguridad de la Información – Davelys Carrillo | Jefe de Operaciones – Ingrid Vergara  Ing. Ciberseguridad – Felipe Oyarzo  Jefe Auditoría – Patricia Meza  Ing. Ciberseguridad - Felipe Borquez | Gerente de Personas - Oscar Galvez  Gerente de Contraloría – Rodolfo Gomez | Septiembre 2020 |
| V2 | Área Seguridad de la Información – Francisco Santin - Davelys Carrillo | Jefe de Operaciones – Ingrid Vergara  Ing. Ciberseguridad – Felipe Oyarzo  Ing. Ciberseguridad – Felipe Borquez  SubGte Auditoria – Patricia Meza | Gerente de Personas - Oscar Galvez  Gerente de Contraloría – Rodolfo Gomez | Julio 2021 |
| V3 | Área Seguridad de la Información – Francisco Santin - Davelys Carrillo | Jefe de Soporte– Pamela Neira  Líder Mea Soporte - Gloria Morales | Jefe de Personas – Cesar Navarro  Gerente de Contraloría –Rodolfo Gomez | Julio 2022 |
| V4 | Área Seguridad de la Información – Francisco Santin - Davelys Carrillo | Jefe de Soporte– Pamela Neira  Líder Mea Soporte - Gloria Morales | Gerente de Personas – Cesar Navarro | Julio 2023 |
| V5 | Área Seguridad de la Información – Francisco Santin - Davelys Carrillo | Jefe de Soporte– Pamela Neira  Líder Mea Soporte - Gloria Morales | Gerente de Personas – Cesar Navarro | Junio 2024 |
| V6 | Área de Soporte Digital, Seguridad de la Información y Auditoría Interna.   * Pamela Neira * Francisco Santin * Patricia Meza |  |  | Mayo 2025 |