Procedimiento de Resolución de Problemas de Altas, Bajas, Modificación de permisos y Acceso a Transacciones SAP	arauco
Código: **P-GEN-019** Revisión: 4	Preparado por: Seguridad SAP
Fecha Revisión: Octubre 2025	Revisado por: Normas y Procedimientos (GAJyR)
Fecha de Vigencia: Enero 2012	Aprobado por: Subgerencia de Informática

I - OBJETO

- Aportar el conocimiento que necesita el usuario, el Key User y las Áreas de Seguridad, a fin de que sepan cómo proceder ante aquellas situaciones en las que un usuario tiene un problema de acceso a transacciones de SAP o durante el uso de estas.
- Aportar el conocimiento que necesitan las áreas de Seguridad y cada funcional SAP al momento de que sea necesario dar de alta un nuevo rol o modificar uno existente.

II – SECTORES INTERVINIENTES

- Subgerencia de Informática
- Analista de Seguridad SAP
- Soporte Funcional SAP
- Gerencia de Personas
- Usuarios SAP
- Usuarios Clave SAP (Key Users)

III - DESCRIPCIÓN

Se describirán a continuación consideraciones generales sobre las problemáticas de accesos de usuarios a SAP, uso de transacciones, valores fijos, altas y modificaciones de roles. Para ver la acción a tomar referirse a los documentos mencionados en cada problemática.

Problemas de acceso (PRD)

Si el usuario encuentra alguna dificultad de accesos en SAP, correspondientes a sus tareas, ya sean habituales o esporádicas, deberá informar al Key User de su área vía e-mail, adjuntando, de ser necesario, la pantalla con la transacción SU53 correspondiente, quien si detecta que se trata de un problema de falta de autorización podra:

1- Generar un TKT GRC solicitando los permisos para que el área de Seguridad SAP evalúe su asignación o rechazo ó
2- Generar una solicitud en la APP “Aranda” dirigida al área de Seguridad, quienes evaluarán y determinarán si es necesario que el incidente deba ser analizado por el Soporte Funcional o no.

Todas las modificaciones de usuarios deben ser gestionadas mediante la herramienta GRC Access Control excepto los mencionados en el párrafo “*Asignaciones por fuera de GRC”.*

Para cada tipo de solicitud, GRC AC cuenta con un workflow de autorización preestablecido.

El análisis del problema de acceso a SAP o a transacciones SAP se efectuará de acuerdo con las siguientes premisas:

a) Altas de Usuarios
Un empleado de ARAUCO (interno o externo) necesita acceso al sistema SAP PRD y no cuenta con nombre de usuario ni contraseña.
Ver *"I-INF-001 Instructivo de resolución de problemas para KU".*

b) Falta de autorización
El usuario carece de autorización a una transacción que debería tener asignada para el cumplimiento de sus tareas.
Ver *"I-INF-001 Instructivo de resolución de problemas para KU".*

c) Las transacciones no coinciden con su puesto
El usuario no puede operar en el sistema porque las transacciones que trata de ejecutar no coinciden con las tareas declaradas en su oportunidad para dicho puesto.
Ver *"I-INF-001 Instructivo de resolución de problemas para KU".*

d) Ingreso erróneo de datos
El usuario debería poder ejecutar la transacción, pero el inconveniente surge porque se están ingresando los datos en forma errónea o no se emplea en forma correcta la transacción.
Ver *"I-INF-001 Instructivo de resolución de problemas para KU".*

e) Asignaciones temporales
En las asignaciones temporales de roles ante la ausencia de un usuario, el Analista de Seguridad procederá a la asignación temporal siempre y cuando la delegación no genere incompatibilidad de funciones y sea delegada en un usuario del mismo nivel jerárquico o superior al usuario ausente.
Ver *"I-INF-001 Instructivo de resolución de problemas para KU".*

f) Asignar/Modificar impresoras o parámetros
El usuario debería tener acceso a determinados valores fijos o parámetros y, al querer utilizarlos, no tienen acceso.
Ver *"I-INF-001 Instructivo de resolución de problemas para KU".*

Baja de Usuarios:

Un empleado de ARAUCO (interno o externo) deja de pertenecer a la compañía
La baja de usuarios en SAP PRD puede estar dada por dos motivos:

- Desvinculación de la compañía: un empleado es desvinculado de la compañía cuando renuncia o cuando la compañía decide que ya no necesita de sus servicios. En cualquiera de los dos casos, el área de Personas generará la baja correspondiente en SSFF, el cual mediante un job programado se enviará un mail al área de Seguridad SAP para bloquear al usuario en cuestión.

- Inactividad por un periodo de 45 días: Todos los días domingo corre un job que extrae un reporte de usuarios que no hayan tenido actividad en el sistema durante los últimos 45 días, los bloquea, los cambia de grupo a "inactivos" y les pone fecha de vencimiento inmediata. Están exceptuados de este proceso todos aquellos usuarios que no sean de diálogo, Gerentes y Subgerentes internos y corporativos.

Alta y Modificación de roles transportables a PRD

Cualquier creación y modificación de roles que será transportable a PRD deberá ser solicitada por el Funcional SAP a cargo del módulo.
El análisis de ABM roles se efectuará de acuerdo con las siguientes premisas:

a) Un usuario necesita acceso a una transacción que no se encuentra dentro de los roles activos de la compañía.
b) El usuario tiene acceso a la transacción, pero no puede ejecutar su tarea por algún impedimento en la funcionalidad de esta.
c) El funcional implementa una mejora.
d) Se necesita la creación o modificación de roles debido a nuevos procesos vinculados a proyectos de la compañía.
Ver *"I-INF-002 Instructivo para ABM de roles y GRC".*

Asignaciones por fuera de GRC

Se podrán asignar permisos por fuera de GRC cuando sean:

a) Asignaciones URGENTES (son aquellas asignaciones que pongan en riesgo la continuidad del negocio y estén correctamente justificadas por la Subgerencia de Informática).
b) Asignaciones no programadas por proyectos.
c) Asignaciones manuales por corte en la funcionalidad del sistema GRC. (Se solicitará previamente autorización al área correspondiente)
d) Problemas de acceso DEV-QAS: todos los problemas de accesos relacionados con los ambientes de DEV100, 120 y QAS serán tratados de forma manual, exceptuando aquellos casos en donde la modificación también sea necesaria en PRD300, tanto en ABM usuarios como en ABM roles, en dicho caso la asignación o modificación será por GRC AC.