El objetivo es establecer los controles para los usuarios autorizados de Comercializadora Rápido S.A. de C.V., dichos controles permitirán el acceso a los servicios de información y que se harán a través de privilegios adecuados a su rol dentro de la organización.

1. Claves de Usuarios

Utilizar claves de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
Verificar que el usuario tiene autorización para el uso del sistema, base de datos o servicio de información.
Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la información de Comercializadora Rápido S.A. de C.V.
Mantener un registro interno de todas las personas registradas para utilizar el servicio.
Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, o sufrieron la pérdida/robo de sus credenciales de acceso.
Efectuar revisiones periódicas con el objeto de:

- Cancelar identificadores y cuentas de usuario redundantes.
- Inhabilitar cuentas inactivas por más de 30 días.
- Eliminar cuentas inactivas por más de 60 días. En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.
El Propietario de la Información será el responsable del registro de usuarios.

2. Administración de Privilegios

El Auxiliar de Sistemas IT es responsable de controlar la asignación y uso de privilegios.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones POS.

Asignar los privilegios a individuos sobre la base de la necesidad de su rol.

Mantener un proceso de autorización y un registro de todos los privilegios asignados.

Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de contratación.

Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Gerente de Sistemas de la Tecnología de la Información de Comercializadora Rápido S.A. de C.V. tiene la responsabilidad de aprobar la asignación de privilegios a usuarios y solicitar su implementación a Auxiliar de Sistemas.

3. Gestión de Contraseñas de Usuario.

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema.
- Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- Generar contraseñas nuevas por periodos bimestrales.

4. Administración de Contraseñas Críticas.

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

- El Gerente de Sistemas y Administradores de los Sistemas son responsables de la administración de dichas contraseñas críticas.
- Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
- Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.