	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Control de accesos
	Código:	PECRSI05

CONTROL DE CAMBIOS

Cambio en Formato a partir del PGCRC02 Elaboración de información Documentada
Organización de la información

1. OBJETIVO

Asegurar que se cumplan los criterios de acceso para usuarios de los sistemas autorizados de Comercializadora Rápido S.A de C.V. a través de revisión de los privilegios y permisos de acuerdo a las funciones del personal.

2. ALCANCE

Aplica a la revisión y monitoreo de usuarios de los sistemas críticos y POS 724 de Comercializadora Rápido S.A de C.V.

Elaboró:	Vo. Bo.	Revisó:	Aprobó:
 Romero Girón Carmen Belem Auxiliar de Sistemas	 Pitol Pimentel Carlos Adrián Gerente de Sistemas	 Martínez Ponce Janely Gestión de Calidad	 Montes Barrera Elliioth Abdel Gerente General

3. REFERENCIAS

ISO 27001:2022 Sistemas de gestión de la seguridad de la información (SGSI)

4. DEFINICIONES Y ABREVIATURAS

4.1 Usuario:

Identificación y contraseña que se le asigna al trabajador y con el que le da autorización para realizar las transacciones

4.2 Usuario de Sistema Crítico:

Identificación y contraseña que se le asigna al trabajador para el monitoreo de transacciones, acceso a la base de datos, Web Service y Aplicaciones de 724.

4.3 Acceso:

Acceso es el resultado positivo de una autenticación, para que el acceso dure un tiempo predeterminado.

5. RESPONSABILIDADES

5.1 Gerente General


Aprobar la información documentada del SGC, asegurando que los recursos necesarios estén disponibles para lograr sin problema la implementación efectiva del documento.

5.2 Gerente Sistemas IT

Es el responsable de verificar el buen uso del sistema de la información de la empresa, gestionar los permisos en usuarios para el sistema crítico.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 1 de 4
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Control de accesos
	Código:	PECRSI05

5.3 Gestión de Calidad

Gestionar el cumplimiento documental según lo establecido en el SGC, asegura su adecuada implementación, manteniendo la eficacia, así como la mejora continua de estas, resguardando y emitiendo la documentación controlada.

5.4 Administrador de infraestructura

Es el responsable de crear el acceso de los usuarios al sistema Punto de Venta en tiendas y monitorear el acceso a la red de los distintos usuarios administrativos, modifica los privilegios a los usuarios de los sistemas de acuerdo a las funciones y peticiones por parte de Gerencia de Sistemas IT o Gerente General, responsable del monitoreo de los accesos y los eventos que se presenten antes y durante de la recolección de pruebas.

6. DESARROLLO

6.1 Perfil de usuario

El personal con perfil de usuario es todo aquel que usa los sistemas de la información de la empresa para realizar su actividad laboral de forma responsable.

Este personal tiene las siguientes normas y responsabilidades:

- Respetar **Política de Control de Accesos PECRSI05_PO01(1)**
- Mantener la confidencialidad de la información.
- Hacer un buen uso de los activos de la información.
- Notificar al responsable de seguridad de las anomalías o incidentes de seguridad, así como las situaciones sospechosas.

6.2 Usuarios de sistemas no críticos

Los usuarios de sistemas no críticos tienen su acceso controlado a partir del alta solicitada por el departamento de RH a través un procedimiento de solicitud por correo electrónico de acuerdo con la política de control de acceso.

6.3 Usuarios con privilegios y accesos


En Comercializadora Rápido S.A. de C.V. solo hay tres perfiles del área de Sistemas TI con acceso privilegiado a los sistemas de información críticos, estos perfiles tienen acceso de administrador a los sistemas de información, tanto equipos de usuario como sistemas del centro de datos, aplicativos y de web service y cuentan con acceso físico a las áreas restringidas relacionadas con los servidores, los cuales son los siguientes:

- Gerente de Sistemas IT
- Administrador de Infraestructura
- Administrador Base de Datos

Nota: ver **Manual Del Sistema De Gestión De Seguridad De La Información MNCRSI01** para la descripción de sus funciones

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 2 de 4
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Control de accesos
	Código:	PECRSIO5

6.3.1 Alta de usuario con privilegios

El Gerente de Sistemas será el responsable de dar la alta de usuario de sistemas críticos y solicitará a través de correo electrónico la designación de permisos al usuario nuevo.

6.4 Administración de privilegios

El Administrador de Infraestructura es el responsable de asignar los privilegios de acuerdo a las funciones que el usuario va a realizar, asegurándose de no cometer algún error en la asignación de los privilegios en el sistema, de requerirse nuevos ajustes el Gerente de Sistemas le realizara la solicitud vía correo electrónico.

6.4.1 Definir al usuario y las IP de los equipos que tendrá acceso autorizado al sistema

El Administrador de Infraestructura validará la información de los usuarios que le fueron solicitados en el correo electrónico con la base de datos contenida en el inventario de activos de la información.

Ejemplo: Accesos

724 Abiertos Fast (38 - 54)										
SERVIDORES 724 (79 - 100)										
724 Solo Correos (101 - 122)										
101	CRAUXAbastos	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
102	all	all	always	ALL	✓ ACEPTAR	Deshabilitar				
103	CRPRACTICANTE2	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
104	CRFASTFOOD	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
105	Diseñador Merca WIFI	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
106	CROPERACIONES CR OPERACIONES WIFI	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
107	CRAUXCONTA3	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
108	CRAUXCONTA3	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
109	CRPRACMERKA	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
110	CRAUXRH2	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
111	CRAUXLOGISTICA CRAUXABASTOS	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
112	CRCOMPRAS-PRAC1	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB OFICINAS 7/24	APP Oficinas 7/24	
113	CRAUXCOMP	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	
114	CR AUDITORIA CRAUDITORIA	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24		APP Oficinas 7/24	
115	CRAUXAuditoria	all	always	ALL	✓ ACEPTAR	Habilitar	AV Oficinas 7/24	WEB SoloCorreos	APP Oficinas 7/24	

6.5 Monitoreo de accesos

Para el monitoreo de los accesos se utiliza la herramienta de fortinet, el Administrador de Infraestructura podrá monitorear a los usuarios de cada sistema no crítico, así mismo el Administrador de infraestructura podrá hacer uso de la herramienta para monitorear los accesos a los usuarios en tiendas y oficinas.


6.6 Verificación de usuario para sistemas críticos

Los cambios, bajas y monitoreo de los usuarios para otorgar y revocar el acceso a los sistemas, base de datos y servicios de información (web service) deberá ser registrado en la bitácora de usuarios de sistemas críticos, esto con el objetivo de dar trazabilidad de las cuentas activas y cambios realizados durante periodos semestrales. **Revisión de usuarios de sistemas críticos PECSIO5_F01(3)**

El Gerente de Sistemas revisará el documento con la finalidad de validación, firmará el documento y almacenará en carpeta física denominada: "Revisión de usuarios de sistemas críticos".

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 3 de 4
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Control de accesos
	Código:	PECRSI05

El formato **Revisión de usuarios de sistemas críticos PECRSI05_F01(3)** deberá mantener un registro interno de todos los usuarios que cuentan con privilegios en los sistemas críticos con la finalidad siguiente:

- 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:
 - a) Cancelar identificadores y cuentas de usuario redundantes.
 - b) Inhabilitar o eliminar cuentas inactivas dentro de un periodo no mayor a 30 días.
- Garantizar que los identificadores de usuario no se asignen a otros usuarios.
- El Administrador de infraestructura será el responsable del registro de usuarios de Sistemas Críticos.

7. DIAGRAMA DE FLUJO

Puesto involucrado	Puesto involucrado	Puesto involucrado	Puesto involucrado
NA	NA	NA	NA

8. ANEXOS

TIPO	CODIGO	TITULO
Formato	PECRSI05_F01(3)	Revisión de usuarios de sistemas críticos
Ayuda visual	NA	NA
Políticas	PECRSI05_PO01(1)	Política de Control de Accesos
Otros (documento externo)	MNCRSI01	Manual Del Sistema De Gestión De Seguridad De La Información

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 4 de 4
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"