	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Reglas firewall</b>
	Código:	<b>PECRS112</b>

#### CONTROL DE CAMBIOS

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

### 1. OBJETIVO

El objetivo de este procedimiento es definir las reglas esenciales relativas a la gestión y mantenimiento del Firewall (fortigate) empleado en todos los equipos de Comercializadora rápido S.A. de C.V.

### 2. ALCANCE

Aplica a todos los dispositivos y equipos empleados en las operaciones de Comercializadora rápido S.A. de C.V.

Elaboró:	Vo. Bo.	Revisó:	Aprobó:
 Cid Palacios Jesús David Administrador de infraestructura	 Pitol Pimentel Carlos Adrián Gerente de Sistemas	 Martínez Ponce Janely Gestión de Calidad	 Montes Barrera Elliioth Abdel Gerente General

### 3. REFERENCIAS

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

### 4. DEFINICIONES Y ABREVIATURAS

#### 4.1 Firewall.

Es un sistema cuya función es prevenir y proteger a una o varias redes, de intrusiones o ataques de otras redes, bloqueándole el acceso

#### 4.2 Host:

Un host o anfitrión es un ordenador que contiene datos o programas que otras computadoras pueden acceder de a través de una red o modem.

#### 4.3 Dirección IP

Una dirección IP (protocolo de internet, por sus siglas en inglés) es una representación numérica que identifica una interfaz concreta de manera única en la red.

#### 4.4 Reglas Firewall.

Las reglas podrán crearse para el tráfico entrante y saliente, una regla se puede configurar para especificar en los equipos, los usuarios, o el protocolo. También especifica el tipo de adaptador de red al que se aplicará la regla; red de área local LAN inalámbrica, acceso remoto, como una conexión de red privada virtual (VPN).

### 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 de Sistemas IT

Es responsable de garantizar el cumplimiento de las reglas de Firewall.

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>5</b>	Página: <b>1 de 5</b>
--	-----------------------	--------------------------

"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"

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Reglas firewall</b>
	Código:	<b>PECRS112</b>

### 5.3 Administrador de Infraestructura.

Es el responsable de la ejecución de las tareas y permisos del firewall para los equipos, la revisión y verificación de las políticas es actividad esencial y periódica del administrador de infraestructura.

### 5.1 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.

## 6. DESARROLLO

### 6.1 Firewall perimetrales

El objetivo del Firewall perimetral es impedir que se realicen conexiones entre la red de la Organización e Internet, permite el tráfico de red a los Hosts fuera de la sucursal y otorga los privilegios necesarios a los usuarios para las operaciones de Comercializadora rápido S.A. de C.V.

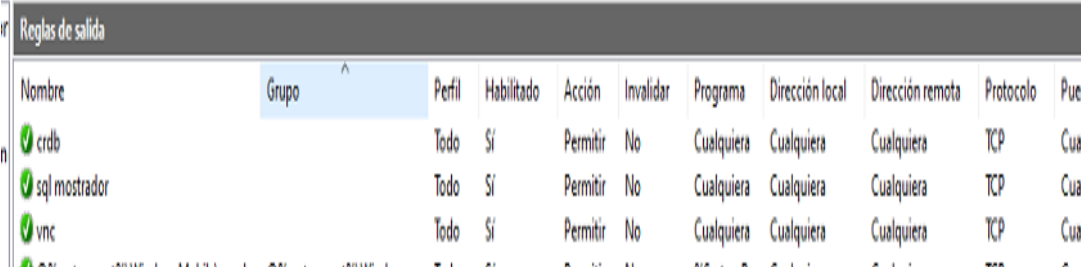
Para establecer las reglas de firewall que tiene como default en herramientas desde el equipo del administrador de Infraestructura realiza la siguiente metodología

#### 6.1.1 Reglas de Salida

Se deselecciona lo siguiente:

Se dirige a panel de control → Opción de Firewall de Windows Defender → Configuración avanzada → Reglas de Salida → Nueva regla → Puerto se considera el número de puerto **SQL1433** → Puerto Ultra VNC Servidor **220005** → Para conexión VNC al **mostrador.20006** → Puerto de SQL de oficinas remoto **10948** → Marcar la casilla Permitir la conexión → Privado → **Nombre de 724** para identificar el nombre de la regla → **FIN**

Ejemplo: Reglas de salida



Nombre	Grupo	Perfil	Habilitado	Acción	Invaldar	Programa	Dirección local	Dirección remota	Protocolo	Pue
crdb		Todo	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	TCP	Cua
sql mostrador		Todo	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	TCP	Cua
vnc		Todo	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	TCP	Cua

#### 6.1.2 Reglas de entrada:


Esta regla permitirá que los programas utilizados para las actividades esenciales de comercializadora rápido S.A. de C.V. puedan tener acceso de comunicación remota, de igual modo se restringen protocolos TCP y UDP.

Se deselecciona lo siguiente:

Se dirige a panel de control → Opción de Firewall de Windows Defender → Configuración avanzada → Reglas de Entrada → Nueva regla → Puerto se considera el núm. de puerto **SQL1433** → Puerto Ultra VNC Servidor

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>5</b>	Página: <b>2 de 5</b>
--	-----------------------	--------------------------

"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"

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Reglas firewall</b>
	Código:	<b>PECRSI12</b>

**2"20005** → Para conexión VNC al **mostrador.20006** → Puerto de SQL de oficinas remoto.**10948** → Marcar la casilla Permitir la conexión → Privado → **Nombre de 724** para identificar el nombre de la regla → **FIN**

#### Ejemplo: Reglas de entrada

Reglas de entrada										
Nombre	Grupo	Perfil	Habilitado	Acción	Invalidar	Programa	Dirección local	Dirección remota	Protocolo	Puerto
✓ crdb		Todo	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	TCP	1135
✗ Java(TM) Platform SE binary		Privado	Sí	Bloquear	No	C:\progra...	Cualquiera	Cualquiera	UDP	Cua
✗ Java(TM) Platform SE binary		Privado	Sí	Bloquear	No	C:\progra...	Cualquiera	Cualquiera	TCP	Cua
✗ Java(TM) Platform SE binary		Público	Sí	Bloquear	No	C:\progra...	Cualquiera	Cualquiera	UDP	Cua
✗ Java(TM) Platform SE binary		Público	Sí	Bloquear	No	C:\progra...	Cualquiera	Cualquiera	TCP	Cua
✓ Skype		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP	Cua
✓ Skype		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP	Cua
✓ sql mostrador		Todo	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	TCP	1435
✓ Teamviewer Remote Control Application		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP	Cua
✓ Teamviewer Remote Control Application		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP	Cua
✓ Teamviewer Remote Control Application		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP	Cua
✓ Teamviewer Remote Control Application		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP	Cua
✓ Teamviewer Remote Control Service		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP	Cua
✓ Teamviewer Remote Control Service		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP	Cua
✓ Teamviewer Remote Control Service		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP	Cua
✓ Teamviewer Remote Control Service		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP	Cua
✓ vnc		Todo	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	TCP	2000
✓ vnc5800		Privado	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	TCP	5800
✓ vnc5900		Privado	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	TCP	5900
✓ vncviewer.exe		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP	Cua
✓ vncviewer.exe		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP	Cua
✓ winvnc.exe		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP	Cua
✓ winvnc.exe		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP	Cua

#### 6.1.3 Firewalls basados en host Santander.

Para dispositivos Microsoft Windows, las configuraciones de firewall para host debe estar en ejecución y configurado desde Firewall Windows Defender para bloquear o permitir todo el tráfico saliente mediante el registro de la sucursal, el registro de la identificación alfanumérica de la terminal, seguidos de la IP/MAC contenidos en un archivo tipo .txt llamado sucursal y almacenado en C://Windows, de esta forma se reconoce que los datos son los mismos que tiene en el archivo y permite las operaciones; para caso contrario al no coincidir estos criterios, el host no reconoce las operaciones y rechaza por automático los datos de la información. Los datos deben coincidir de esta forma:

IP 192.168.SUB RED (2 A 251). RED (0 A 254):

PUERTO

Puerto 9430 Para Santander

Puerto 4385 Para BBVA

MAC cuenta con 6 bloques de 2 dígitos Hexadecimal.

#### 6.1.4 Firewall para CCTV

Para el Circuito Cerrado de las instalaciones y sucursales de Comercializadora Rápido S.A. de C.V., se cuentan con reglas de firewall las cuales cuentan con los siguientes puertos:


445, 2200, 8100, 8200, 8201, 8016, 8116, 1019, dichas reglas son configuradas de Mikrotik.

#### 6.2 Conexiones externas.

Todas las conexiones externas en tiempo real en comunicación a las redes internas de centros de datos de Comercializadora rápido S.A. de C.V. deben pasar a través de un Mikrotik.

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>5</b>	Página: <b>3 de 5</b>
--	-----------------------	--------------------------

"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"

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Reglas firewall</b>
	Código:	<b>PECRSI12</b>

### 6.3 Cambio de firewall

Las reglas de configuración del firewall y las reglas de servicios permisibles no deben cambiarse a menos que el gerente de Sistemas IT dé la autorización, el registro se llevará a cabo en **Solicitud de Cambio TI PECRSI03\_F01(3)**

### 6.4 Auditoría periódica

Debido a que los firewall proporcionan una barrera tan importante; el acceso no autorizado debe ser auditado regularmente.

Como mínimo un periodo de 6 meses; este proceso de auditoría debe incluir la consideración de parámetros de configuración definidos y habilitados, servicios, conectividad permitida, prácticas administrativas actuales y adecuación de las medidas de seguridad implementadas.

### 6.5 Registros.

Todos los cambios en los parámetros de configuración del firewall, los servicios habilitados y los permitidos para la conectividad deberán estar registrados en **Validación Firewall PECRSI12\_F01(3)**. Además, toda actividad sospechosa que pueda ser un indicador de vulnerabilidad como el uso no autorizado o algún intento de poner en peligro las medidas de seguridad también deberá registrarse en observaciones del mismo formato.

Estos registros deben revisarse periódicamente para asegurarse de que los firewalls están operando de manera segura.

### 6.6 Seguridad física del firewall

Todos los dispositivos que operan bajo la protección del firewall de Comercializadora rápido S.A. de C.V. deben estar ubicados en las sucursales y áreas administrativas permitidas bajo operación de personal autorizado para realizar las tareas asignadas por la Organización.

### 6.7 Flujo de aprobación:

El gerente de Sistemas recibe el formato en físico **Validación Firewall PECRSI12\_F01(3)** por parte del administrador de infraestructura para cambio y revisión de reglas de acuerdo al periodo establecido (cada 6 meses) y altas de los equipos.

El Gerente de sistemas valida el contenido del documento y autoriza firmando al calce del mismo.


Si la solicitud de configuración de reglas firewall es aceptada, el Administrador de infraestructura analiza su urgencia (cambio cuya solución no puede esperar por su alto impacto en la prestación del servicio).

Si la solicitud indica que se trata de un cambio urgente, se realiza el procedimiento de reglas firewall, Una vez realizada las actividades de modificación, se registran las IP involucradas.

Si la Solicitud NO es aceptada, ésta debe volver al administrador de infraestructura para reestructurar la petición y documentar en el formato **Validación Firewall PECRSI12\_F01(3)** "X" en columna de NO y posteriormente en observaciones hacer las anotaciones del porque se rechazó la solicitud.

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>5</b>	Página: <b>4 de 5</b>
--	-----------------------	--------------------------

*"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"*

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Reglas firewall</b>
	Código:	<b>PECRSI12</b>

Si el Gerente de Sistemas NO aprueba la configuración luego de evaluar sus repercusiones en la operación de Comercializadora, deberá responder la solicitud correspondiente no se acepta y vuelve a quien lo envió, aclarando que por el momento no se puede ejecutar el cambio.

## 7. DIAGRAMA DE FLUJO

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

## 8. ANEXOS

TIPO	CODIGO	TITULO
Formato	PECRSI12_F01(3)	Validación Firewall
Ayuda visual	NA	NA
Políticas	NA	NA
Otros (documento externo)	PECRSI03_F01(3)	Solicitud de Cambio TI

DOCUMENTO CONTROLADO  
Prohibida su reproducción

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>5</b>	Página: <b>5 de 5</b>
--	-----------------------	--------------------------

*"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"*