	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Trafico de red
	Código:	PECRS113

CONTROL DE CAMBIOS

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

1. OBJETIVO

El objetivo de este procedimiento es almacenar el flujo de información generado por los sistemas de la red operacional de Comercializadora rápido S.A. de C.V.

2. ALCANCE

Aplica a todos los dispositivos y equipos que se encuentran conectados a red local y global.

Elaboró:	Vo. Bo.	Revisó:	Aprobó:
Zúrita Hegler Eusebio Lorenzo Administrador de Base Datos	Pitol Pimentel Carlos Adrián Gerente de Sistemas	Martínez Ponce Janelly 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 Internet:

Es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominados TCP/IP, que ofrece diversos servicios a sus usuarios como pueden ser el correo electrónico, chat o la web.

4.2 Router:

Es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes.

4.3 Sniffer:

Un Sniffer es un software que se encarga de capturar paquetes en tránsito (entrada y salida) en una cierta red y analizarlos.

4.4 Tráfico de red:

El tráfico de redes de área local se mide como la cantidad de información promedio que se transfiere a través del canal de comunicación, y a la velocidad que se transfiere por ello la importancia, del conocimiento de sus diferentes elementos para poder evaluar en formas más eficiente y eficaz el tráfico en la red.


5. RESPONSABILIDADES

5.1 Gerente de Sistemas IT

Es el responsable de asignar los permisos de usuario en el sistema que se encuentra instalado Wireshark y Microsoft Network Monitor.

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 1 de 3
--	-----------------------	--------------------------

"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:	Trafico de red
	Código:	PECRS113

5.2 Administrador de Infraestructura

El administrador de Infraestructura es el responsable secundario de configurar los sniffer y seleccionar la interfaz de red, así como actualizar e implementar nuevos dispositivos de red o equipos actuales.

5.3 Auxiliar de Sistemas

Es responsabilidad de auxiliar de sistemas de aplicar el procedimiento de tráfico de red en el sistema operativo de Comercializadora Rápido S.A. de C.V.

6. DESARROLLO

6.1 Generalidades

El flujo de datos de la red operativa de 7/24 comprende básicamente: Operaciones de venta a distancia, Contenidos de Información de clientes para operaciones de pago de tarjetas, Datos de Contabilidad, Inventarios, de Compras y de Cuentas por pagar y estas operaciones son comprimidas en Modo binario, de tal manera pueden almacenarse en un periodo de tiempo extenso.

En el **Lisado de equipos “tráfico de red” PECRS113_F01(1)** se enlista los equipos dentro de Comercializadora Rápido S.A. de C.V.

A partir de las pruebas se configuró soporte de Files Wireshark para almacenar la información durante plazos indefinidos debido a la carga del tráfico diario, siendo el límite de almacenamiento de 100 Mega Bytes, y para su posterior revisión, auditoría o investigación se direccionan al almacenamiento de servidor Núm. 11, en relación a las actividades en la captura y almacenamiento del flujo de datos se documenta el siguiente proceso:

6.2 Selección de la interfaz de red para capturar el tráfico de red

Desde la interfaz gráfica propia de Wireshark se realiza la selección de los dispositivos de red para comenzar el análisis y captura de los paquetes de datos. Esto depende del equipo donde se va a trabajar con Wireshark, porque los equipos disponen de diferentes tipos de dispositivos de interfaces de red.

6.3 Captura de paquetes de datos en una red


Para poder conocer la red se debe definir donde analizar el tráfico, además que la propia herramienta de Wireshark permite analizar y capturar el tráfico de los equipos a distancia de las sucursales y áreas administrativas se debe considerar alternativas del uso de técnicas para que el análisis sea de forma centralizada.

- Abrir el Sniffer de paquetes y ver el funcionamiento.
- Desde el menú principal se selecciona la opción de capturar y posteriormente interfaces y hacer comienzo dependiendo de la interfaz seleccionada.
- Detener para el caso que así se desee.
- Una vez que se complete estos pasos, el proceso de captura habrá terminado, mostrando la cantidad de datos capturados.

Los paquetes capturados contienen la información siguiente: Numero de paquete, tiempo, fuente, destino, protocolo utilizado, la longitud y alguna información general que se encuentre en el paquete.

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 2 de 3
--	-----------------------	--------------------------

“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:	Trafico de red	
	Código:	PECRSI13	

6.4 Guardar paquetes de datos

Wireshark puede guardar el paquete de datos en su formato. .pcapng para que otros analizadores puedan leer los datos de captura. Las etiquetas que se le asignan son las siguientes:

Nombre: red 724 [año] [mes] [día] y [hora].
Range cada 100 MB

La información se resguarda en un servidor centralizado, donde solo el personal de TI cuenta con acceso.

6.5 Monitoreo del tráfico de red

La captura de los datos se realiza de forma continua, éstos se almacenan de acuerdo a las condiciones que el administrador sujeta el programa. Por lo tanto, Wireshark permite que se almacenen para ser monitoreados en un tiempo posterior del análisis.

El análisis, se describe como el proceso de interpretación de datos en tiempo real. Y con la finalidad de encontrar anomalías en la actividad de la red, se realiza un monitoreo de la actividad del análisis por periodos de cada 7 días.

6.6 Solicitud de información para trazabilidad

En caso de requerirse revisiones por externos/internos con la finalidad de realizar una trazabilidad o consultar los históricos de datos, de un paquete de datos específicos, se debe solicitar por correo, indicando fecha y códigos específicos del paquete de datos y el motivo por el cual se requiere, esta solicitud tiene que ser autorizada vía correo por el jefe y gerente de IT y el gerente general, una vez realizada la trazabilidad se debe de informar el resultado de la trazabilidad y comunicar al personal que dio la autorización.

7. DIAGRAMA DE FLUJO

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

8. ANEXOS

TIPO	CODIGO	TITULO
Formato	PECRSI13_F01(1)	Lisado de equipos "tráfico de red"
Ayuda visual	NA	NA
Políticas	NA	NA
Otros (documento externo)	NA	NA

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

"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"