	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Tipo de documento
	Título:	Gestión de LOGS
	Código:	PECRSI24

CONTROL DE CAMBIOS

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

1. OBJETIVO

Establecer el proceso de revisión y monitoreo de logs que se generan en el servidor Bancomer para detectar y reaccionar ante posibles intrusiones que vulneren la seguridad de la información de Comercializadora Rápido S.A. de C.V.

2. ALCANCE

Aplica a las revisiones y acciones para la gestión de logs en SVR-BBVA realizadas por el personal de Sistemas TI.

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

4. DEFINICIONES Y ABREVIATURAS

4.1 Administración de Log:

Proceso mediante el cual se realiza la generación, transmisión, almacenamiento, análisis, monitoreo y reporte de los Logs.

4.2 Análisis de Log:

Estudio de los Logs para identificar eventos de interés o suprimir entradas de eventos insignificantes.

4.3 Incidente:

Es un evento o serie de eventos de seguridad de la información no deseado o no planeado, que afecte la prestación del servicio o reduzca la calidad de la prestación del servicio o que tenga una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

4.4 Log:


Es el registro secuencial de todos los acontecimientos que suceden dentro de la red y pueden afectar a los procesos de la Organización. Estos ayudan a evidenciar el comportamiento del sistema y de los usuarios de este, siendo una herramienta de registro del sistema para futuras referencias y análisis que permitan revisarse periódicamente y encontrar posibles fallas en la seguridad de la información.

4.5 Monitoreo de Logs:

Supervisan la actividad de la red, inspeccionan los eventos del sistema y almacenan diferentes acciones (por ejemplo, cambiar el nombre de un archivo o abrir una aplicación) que ocurren dentro de los sistemas

Vigente a partir de: 30-ABR-2024	Revisión: 4	Página: 1 de 6
--	-----------------------	--------------------------

"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:	Tipo de documento
	Título:	Gestión de LOGS
	Código:	PECRSI24

vigilados, contando con la capacidad de consolidar aquellos datos que podrían alertarte sobre una violación de políticas de seguridad.

4.6 Retención de Log:

archivar los Logs de eventos como parte de las actividades de administración de la infraestructura de acuerdo a las políticas de respaldo y recuperación de los mismos.

4.7 Rotación de Log:

proceso que consiste en la eliminación de un registro de logs con el objetivo de permitir la apertura de uno nuevo de acuerdo con la frecuencia de almacenamiento que se tenga establecida y con las políticas de seguridad de almacenamiento.

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 el responsable de la gestión de los procesos de seguridad de la información, así como el responsable de garantizar que los archivos de registro que se encuentren bajo su control se guarden y analicen para la detección de actividades inusuales.

5.3 Administrador de infraestructura

Es el responsable del monitoreo y análisis de la base de datos generada por el registro de logs e; identificar eventos o incidentes que se consideren sospechosos para la seguridad de la información.

5.4 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 Revisión de Logs a Servidor Bancomer.


De forma preventiva, se establece que de forma mensual el administrador de infraestructura debe revisar los logs de la Base de Datos que se generan durante el flujo de la información entre Bancomer y Comercializadora Rápido S.A. de C.V. En caso de detección de actividades inusuales se deberá dar aviso al Gerente de Sistemas IT.

6.1.1 Proceso

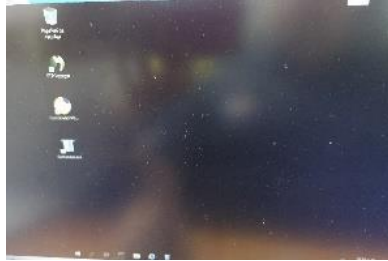
Se deberá ingresar al servidor de Santander y dirigirse a herramientas administrativas.

Vigente a partir de: 30-ABR-2024	Revisión: 4	Página: 2 de 6
--	-----------------------	--------------------------

"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"

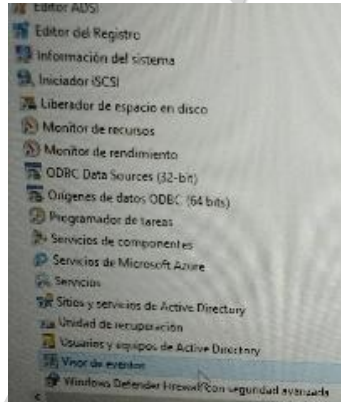
	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Tipo de documento
	Título:	Gestión de LOGS
	Código:	PECRSI24

Ejemplo: Servidor de Santander



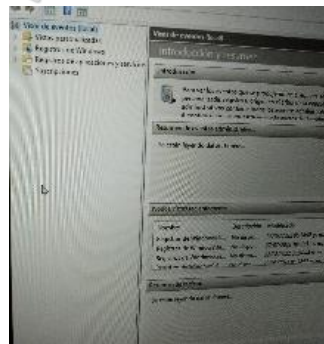
Seleccionar barra de selección emergente la opción de Visor de eventos y dar doble Click.

Ejemplo: Visor de evento



Dirigirse a la opción de registro de Windows y dar doble Click.

Ejemplo: Registro de Windows




Además, se podrá revisar de acuerdo al filtro requerido:

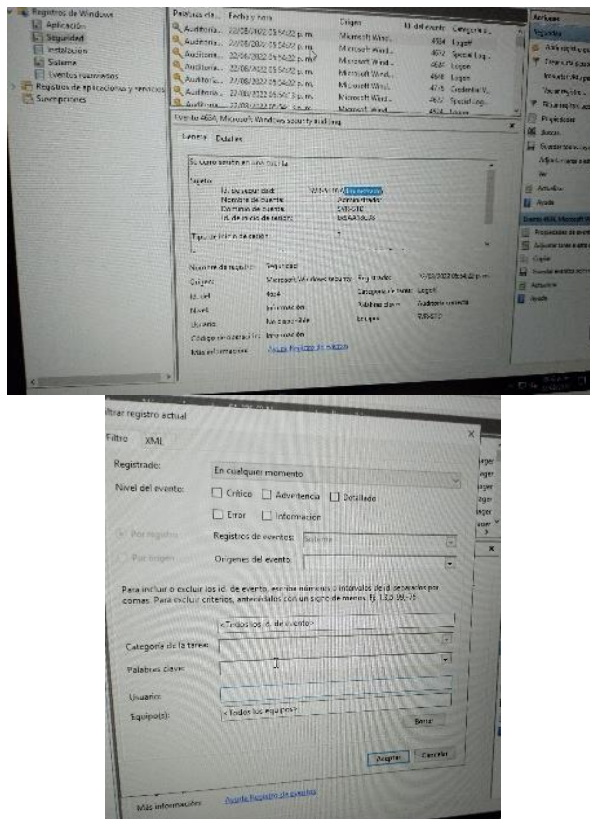
- Crítico
- Advertencia
- Detallado
- Error
- Información

Vigente a partir de: 30-ABR-2024	Revisión: 4	Página: 3 de 6
--	-----------------------	--------------------------

"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:	Tipo de documento
	Título:	Gestión de LOGS
	Código:	PECRSI24

Ejemplo: Seguimiento



6.2 Periodo de revisión de Logs

El administrador de infraestructura deberá registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información, además de la sincronización de tiempo precisa en todos los sistemas, el periodo de revisión es al menos 1 vez cada 6 meses o; en caso de que ocurra un cambio/baja de usuario con acceso a Servidor Bancomer (administradores).

6.3 Respuesta ante la detección de actividades inusuales


el administrador de infraestructura al detectar alguna falla o la identificación de log inusual se deberá revisar la causa raíz del problema a través de las herramientas que se disponen dentro de la red: firewall, antivirus y logs de Windows.

6.4 Registro de logs inusuales.

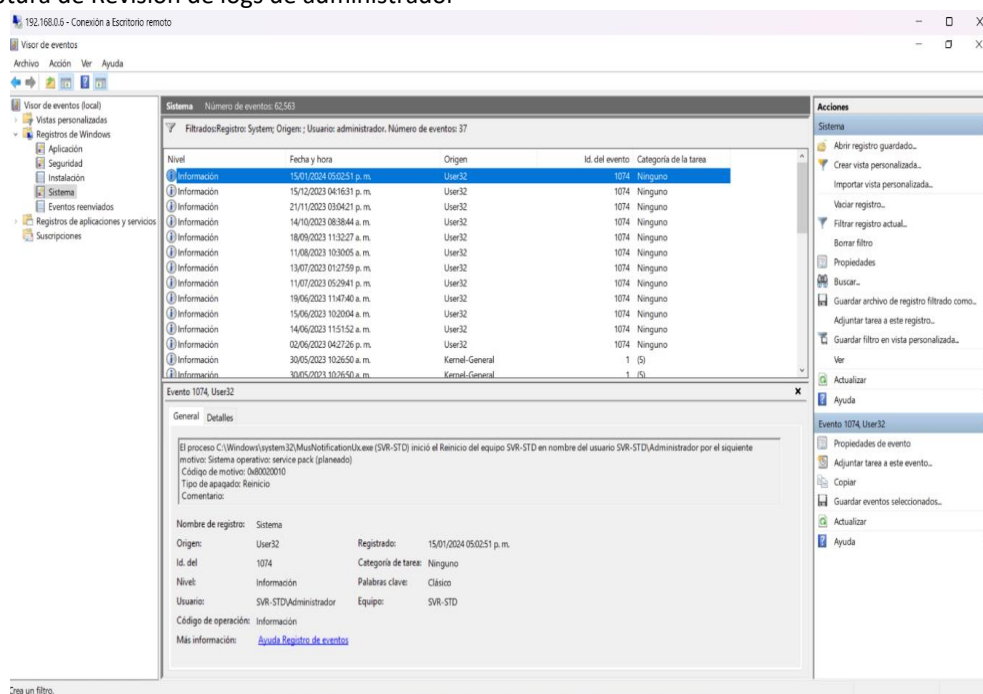
En el caso que se presente un registro de log inusual, el Gerente de Sistemas junto con el Comité de Riesgos deberán detectar el origen y solucionarlo de forma inmediata, dicho incidente se deberá registrar en el formato **Matriz de vulnerabilidades PECSI20_F01(2)** y almacenar la evidencia en captura de pantalla.

Vigente a partir de: 30-ABR-2024	Revisión: 4	Página: 4 de 6
--	-----------------------	--------------------------

"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:	Tipo de documento
	Título:	Gestión de LOGS
	Código:	PECRSI24

Ejemplo: Captura de Revisión de logs de administrador



Todo registro deberá anexarse información relevante:

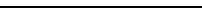
- Id de Usuario quien realiza la revisión.
- Fecha y hora de la ocurrencia.
- Tipología del evento.

6.5 Almacenamiento de logs para auditoría.

El equipo de seguridad de la información conformado por el Gerente de Sistemas, Administrador de la Infraestructura y auxiliares de Sistemas (Soporte técnico) establecerán un programa de respaldo de logs para constituir un sistema de evidencia para la identificación de incidentes de seguridad la cual deberá comprender 1 revisión y mantenerse durante un periodo de 6 meses.

Vigente a partir de: 30-ABR-2024	Revisión: 4	Página: 5 de 6
--	-----------------------	--------------------------

"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:	Tipo de documento
	Título:	Gestión de LOGS
	Código:	PECRSI24

Ejemplo: Histórico de logs para evidencia

6.6 Autorización de acceso.

6.7 Difusión.

7. DIAGRAMA DE FLUJO

8. ANEXOS

Vigente a partir de: 30-ABR-2024	Revisión: 4	Página: 6 de 6
--	-----------------------	--------------------------