Referencia: DOC-SF-013

	CONTROLES ACTUALES	
Responsable: Administrador de la Seguridad	**Versión: 1**	**DOCUMENTO**
	Creado el: 06-05-2026	
Redactor: Líder de Proyecto	**Fecha de impresión:** 06-05-2026	
Autorizó:	CEO	

No	TIPO DE AMENAZA	VULNERABILIDAD	DESCRIPCIÓN DEL RIESGO	DESCRIPCIÓN DEL IMPACTO	CONTROLES ACTUALES	LOS CONTROLES ¿CUBREN EL RIESGO?		
						TOTAL	PARCIAL	NO CUBREN
1	Estado de la infraestructura tecnológica **(TECNOLOGÍA)**	Fallas internas por ausencia de mejores prácticas para administrar la infraestructura y sus componentes	Error en el proceso de **Monedero Electrónico.**	La imagen pública de **SENDERO FUEL** se ve dañada y la empresa no cumple con los Niveles de Servicio acordados con el Cliente.	Desarrollo e implementación de Mejores prácticas de ITIL. Se cuenta con procedimientos aplicados como: • Administración de La Capacidad • Cambio y Aumento de Infraestructura • Cotización Alterna Para Cambio y Aumento En Infraestructura • Solicitud de Cambios • Control de Cambios – Aplicativo • Control de Cambios - Actualización de Parches SO y BD • Control de Cambios - Base de Datos, Creación de Objeto Se Cuenta Con Diagramas Basados En Las Mejores Prácticas De Itil Para Administrar La Infraestructura Y Componentes: • Diagrama de Arquitectura (Corto, Mediano y Largo Plazo)			
2	Ataques lógicos.	Acceso interno o externo no autorizado por un diseño deficiente de los procesos de seguridad del **Software de Monedero Electrónico**	Ataque de virus. Acceso no autorizado a los sistemas. Daño en el sitio de internet. Espionaje industrial.	Mantener erróneamente la integridad de la información y de la infraestructura de procesamiento del **Software de Monedero Electrónico**	Se cuenta con los siguientes controles para mitigar los ataques lógicos: • Antivirus Sophos • Firewall • Programación de seguridad en la Base de datos, Aplicativo • Procedimiento Control de Cambios-Parches para Mitigar Vulnerabilidades			
3	Destrucción de infraestructura.	Mal uso o destrucción de la infraestructura tecnológica por actores internos o externos, ya sea de forma accidental o maliciosa	Destrucción de centro de cómputo. Destrucción accidental de equipo de cómputo.	No tener protegidos los activos de Tecnologías de Infomación de **SENDERO FUEL** y la información pertinente de su operación para minimizar el riesgo de interrupciones en el negocio.	• Se cuenta con servicios tercerizados de **NGX** certificados en la norma **ISO27001**, que además cuenta con políticas que marcan características como la barda perimetral que rodea a las instalaciones y equipos de seguridad que evitan la destrucción de infraestructura, bitácoras de acceso así como la contratación de su personal con el perfil adecuado, los valores y la ética profesional para el resguardo y cuidado de la infraestructura. • Se cuenta con la Matriz de Roles y Responsabilidades (muestran el perfil que debe tener el personal que trabaje en **SENDERO FUEL** y es de gran ayuda al momento de hacer una contratación ya que los valores y ética profesional cuidarán de la infraestructura y la información sensitiva)			
4	Robo de infraestructura.	Robos internos o externos de infraestructura.	Robo de equipo con información sensitiva relacionada con el **Software de Monedero Electrónico**	No tener protegidos los activos de Tecnologías de Infomación de **SENDERO FUEL** y la información pertinente de su operación para minimizar el riesgo de interrupciones en el negocio.	• Se cuenta con servicios tercerizados de **NGX** certificados en la norma **ISO27001**, que además cuenta con políticas que marcan características como la barda perimetral que rodea a las instalaciones y equipos de seguridad que evitan la destrucción de infraestructura, bitácoras de acceso así como la contratación de su personal con el perfil adecuado, los valores y la ética profesional para el resguardo y cuidado de la infraestructura. • Se cuenta con la Matriz de Roles y Responsabilidades (muestran el perfil que debe tener el personal que trabaje en **SENDERO FUEL** y es de gran ayuda al momento de hacer una contratación ya que los valores y ética profesional cuidarán de la infraestructura y la información sensitiva)			
5	Personal de TI.**(OPERATIVOS)**	Fallas internas por incumplimiento en el proceso de administración de recursos humanos; considerando tanto los procedimientos de la organización como la gente que participa en ellos	No contar con el personal clave para brindar el soporte al **Software de Monedero Electrónico**. Carencia de recursos para contratar a personal de Tecnologías de Información.	Personal incompetente y desmotivado para crear y entregar los servicios ofrecidos por **SENDERO FUEL.**	• Se cuenta con la Matriz de Roles y Responsabilidades (muestran el perfil competitivo que debe tener el personal que trabaje en **SENDERO FUEL** y es de gran ayuda al momento de hacer una contratación)			
6	Infraestructura (Hardware).	Modificaciones, destrucción o uso inapropiado de la infraestructura por figuras internas o externas a **SENDERO FUEL**	Configuración inadecuada de los componentes de hardware. Daño de servidores críticos. Alteraciones intencionales de hardware.	No contar con infraestructura de Tecnologías de Información integrada y estandarizada para proveer el **Software de Monedero Electrónico**	• Desarrollo e implementación de Mejores prácticas de ITIL. • Se cuenta con la Matriz de Roles y Responsabilidades (muestran el perfil que debe tener el personal que trabaje en **SENDERO FUEL** y es de gran ayuda al momento de hacer una contratación ya que los valores y ética profesional cuidarán de la infraestructura y la información sensitiva)			

7	Rendimiento del software.	Fallas internas por un diseño deficiente en **Software de Monedero Electrónico**	Funcionamiento no adecuado del software. Problemas con el sistema operativo del servidor que contiene el **Software de Monedero Electrónico**	No contar conel **Software de Monedero Electrónico**. de acuerdo con los requerimientos establecidos por la autoridad.	• Se cuenta con personal altamente calificado de acuerdo a la Matriz de Roles y Responsabilidades, el cual diseña, desarrolla y programa el software Aplicativo • Se cuenta con procedimientos implementados basados en las mejores prácticas de ITIL como: o SOLICITUD DE CAMBIOS o CONTROL DE CAMBIOS – APLICATIVO o CONTROL DE CAMBIOS - ACTUALIZACIÓN DE PARCHES SO Y BD o CONTROL DE CAMBIOS - BASE DE DATOS, CREACIÓN DE OBJETO • Se cuenta con el DIAGRAMA ENTIDAD-RELACIÓN			
8	Capacidad Tecnológica del Sistema.	Fallas internas por un diseño deficiente de los procesos de capacidad tecnológica	Los sistemas no pueden manejar el volumen de transacciones cuando éstas se incrementan.	Desempeño ineficiente de la infraestructura tecnológica para cubrir los requerimientos transaccionales de los clientes de **Monedero Electrónico.**	• Se cuenta con el procedimiento implantado de Administración de la Capacidad Tecnológica basado en las Mejores Prácticas de ITIL • Basado en las Mejores Prácticas de ITIL se tiene el DIAGRAMA DE ARQUITECTURA (CORTO, MEDIANO Y LARGO PLAZO)			
9	Capacidad Operativa del Sistema.	Fallas internas por un diseño deficiente de los procesos de capacidad operativa	El personal existente no puede manejar la carga de trabajo cuando ésta se incrementa	Desempeño ineficiente del personal para cubrir los requerimientos del proceso de **Monedero Electrónico.**	• Se cuenta con el procedimiento implantado de Administración de la Capacidad Operativa basado en las Mejores Prácticas de ITIL • Basado en las Mejores Prácticas de ITIL se tiene la Matriz de Roles y Responsabilidades			
10	Software malicioso.	Ataques internos o externos por un diseño deficiente del proceso de seguridad del **Software de Monedero Electrónico**. Los ataques pueden ser accidentales o maliciosos.	Intrusión de software malicioso en servidores críticos relacionados con el **Software de Monedero Electrónico**. Infección regular de equipo de cómputo.	Mantener erróneamente la integridad de la información y de la infraestructura de procesamiento del **Software Monedero Electrónico.**	Se cuenta con los siguientes controles para mitigar ataques de software malicioso: • Antivirus Sophos • Firewall • Programación de seguridad en la Base de datos, Aplicativo • Procedimiento basado en las Mejores Prácticas de ITIL e implementado Análisis de Vulnerabilidades • Procedimiento basado en las Mejores Prácticas de ITIL e implementado Pruebas de Penetración • Procedimiento Control de Cambios-Parches para Mitigar Vulnerabilidades			
11	Integridad de los datos.	Modificaciones de información debido a fallas internas o externas.	Modificaciones intencionales de datos, de la infraestructura o del **Software de Monedero Electrónico.** Falta de Integridad de la base de datos.	No cumplir con los Niveles de Servicio acordados con el Cliente	Se cuenta con los siguientes controles basados en las Mejores Prácticas de ITIL para mantener la integridad de datos: • Antivirus Sophos • Firewall • Programación de seguridad en la Base de datos, Aplicativo • Procedimiento basado en las Mejores Prácticas de ITIL e implementado Análisis de Vulnerabilidades • Procedimiento basado en las Mejores Prácticas de ITIL e implementado Pruebas de Penetración • Procedimiento Control de Cambios-Parches para Mitigar Vulnerabilidades • Matriz de Roles y Responsabilidades • Matriz de Roles y Responsabilidades-Criptografía • Documento de Autenticación de Identidades • Políticas de **Sendero Fuel** para asegurar el Control de Acceso, Contraseñas, Pistas de Auditoría, Criptografía, Aseguramiento y Resguardo • Cartas Responsivas y Cartas de Aceptación de Responsabilidades • Procedimiento Recuperación de la Información-Respaldos • Procedimiento Etiquetado de Respaldos			
12	Acceso lógico no autorizado.**(USUARIOS MALINTENCIONADOS)**	Ataques internos o externos por un diseño deficiente o uso inapropiado del proceso de seguridad de los sistemas procedimentales y de información	Usuarios eluden los derechos de acceso. Usuarios obtienen acceso no autorizado a la información. Robo de información sensitiva	Mantener erróneamente la integridad de la información y de la infraestructura de procesamiento del **Software de Monedro Electrónico.**	Se cuenta con los siguientes controles basados en las Mejores Prácticas de ITIL para mitigar accesos lógicos no autorizados: • Antivirus Sophos • Firewall • Programación de seguridad en la Base de datos, Aplicativo • Procedimiento implementado Análisis de Vulnerabilidades • Procedimiento implementado Pruebas de Penetración • Procedimiento Control de Cambios-Parches para Mitigar Vulnerabilidades • Matriz de Roles y Responsabilidades • Matriz de Roles y Responsabilidades-Criptografía • Documento de Autenticación de Identidades • Cartas Responsivas y Cartas de Aceptación de Responsabilidades			
13	Medio ambiente	Eventos que destruyan la infraestructura tecnológica de **SENDERO FUEL** debido a un diseño deficiente del proceso de seguridad física.	Pérdida de la disponibilidad y retraso en la recuperación de procesos críticos (Corriente de electricidad y ruido eléctrico, Incendios y humo, Temperaturas extremas).	No contar con infraestructura de tecnologías de información integrada y estandarizada. No tener protegidos los activos de tecnologías de información y la información de **Sendero Fuel** relacionada el **Software de Monedero Electrónico.**	• Se cuenta con servicios tercerizados de **NGX Y ASSETEL** certificados en la norma **ISO27001**, que además cuenta con políticas que marcan características como la ubicación y condiciones que rodean a las instalaciones y equipos de seguridad que evitan la destrucción de infraestructura y la aislan de elementos que causan incendios ruido eléctrico o polvo, y que ofrecen respaldos de información y equipos de respaldo emergente y permiten la disponibilidad permanente del servicio			

14	Actos de la naturaleza **(CLIMATOLÓGICOS)**	Eventos naturales externos que destruyan la infraestructura y afecten a la gente y los procesos del negocio en un período determinado.	Pérdida de la disponibilidad y retraso en la recuperación de procesos críticos (Terremotos, Huracanes, Tormentas)	No tener protegidos los activos de tecnologías de información y la información de **SENDERO FUEL** y el CLIENTE relacionada con el **Software de Monedero Electrónico.**	• Se cuenta con servicios tercerizados de **NGX Y SSETEL** certificados en la norma **ISO27001**, que además cuenta con políticas que marcan características como la ubicación y condiciones que rodean a las instalaciones y equipos de seguridad que evitan la destrucción de infraestructura y protegen al personal, y que ofrecen respaldos de información y equipos de respaldo emergente y permiten la disponibilidad permanente del servicio			
15	Normatividad y legislación	Modificación a las normas vigentes que regulan la operación como **Proveedor de Monedero Electrónico**	Modificaciones que conlleven cambios importantes en la arquitectura o el diseño del **Software de Monedero Electrónico.**	El no contar con los recursos o tiempo suficientes para realizar los cambios que solicita la autoridad, nos llvaría al incumplimiento de nuestra parte, lo cual podría poner en riesgo nuestra certificación como **Proveedor de Monedero Electrónico.**	* Se cuenta con un mecanismo de control de cambios * Se dispone de un área de monitoreo el cual esta asignada a validar cualquier nueva normatividad emitida por la autoridad, lo que nos asegura conocer los cambios requeridos de forma oportuna. * Contamos con personal de desarrollo, dedicado 100% dedicado al mantenimiento de la plataforma del **Software de Monedero Electrónico**			
16	Sociales	Bloqueos y disturbios generados por manifestaciones.	No poder ingresar a las instalaciones operativas de **SENDERO FUEL**	No poder ingresar a las instalaciones de **SENDERO FUEL**, provocaría un daño en la imagen de la empresa, debido a que habría un lapso, en el cual no se podría dar el soporte a los clientes, por lo menos en lo que se activa el protocolo de **BCP.**	* Se cuenta con un BCM * Se realizan dos simulacros anuales			