Monedero Electrónico XIGA, S.A. de C.V.	Tipo / No. De Documento:	XIGA-A28-POL-09	Número de Revisión:	10	Req. SAT	15	Fecha de Efectividad:	03-04-2025
	Título del documento:	Política de uso aceptable						

RESUMEN DE HISTORIA DE CAMBIOS

Revisión	Fecha	Razón del Cambio
00	01-03-2018	- Documento de nueva creación bajo el Sistema de Administración.
01	10-12-2018	- Se realizó adecuación de acuerdo con el Anexo 28 del SAT.
02	06-03-2019	- Se agregó punto 5 Periodicidad de revisión de la política.
03	14-05-2019	- Se realizó modificación al pie de página.
04	13-05-2020	- Se realizó la revisión anual del documento.
05	12-05-2021	- Se modificaron numerales para que coincidan con los del anexo 28.
06	22-04-2022	- Se realizó la actualización anual del documento. - Se actualizó el número de control y se estructuró bajo el nuevo formato organizacional.
07	21-04-2023	- Se realizó la revisión anual del documento.
08	19-04-2024	- Se realizó la revisión anual del documento.
09	19-03-2025	- Se realizó la revisión anual del documento.
10	03-04-2025	- Se actualizó la tabla de participantes y aprobaciones. - Se actualizó "Antivirus Cylance" por "Agente de protección contra software malicioso".

	Elaboró	Revisó	Aprobó
Nombre	Merced Ortiz	Miguel Ricario	Elodia Robles
Puesto	Coordinador de XIGA	Gerente de XIGA	Representante Legal
Firma			

1. Objetivo

1.1. Definir las reglas para el uso de los sistemas y de otros activos de información en el Monedero Electrónico XIGA.

2. Alcance

2.1. Este documento aplica para todos los sistemas y demás activos de información utilizados dentro del alcance del SGSI.

2.2. Los usuarios de este documento son los colaboradores de Monedero Electrónico XIGA.

3. Políticas

3.1. **Definiciones.**

3.1.1. **Uso aceptable:** Se considera como uso aceptable de los activos de la información, al hecho de conocer datos de operación, clientes y proveedores, contando con previa autorización explícita y limitada de la Gerencia para un empleado debidamente contratado y solo para los fines que requieran las responsabilidades de su puesto.

3.1.2. **Activos de información:** En el contexto de esta política, el término activos de información se aplica a los datos contenidos en los sistemas de información, equipos de cómputo, documentos impresos en papel, teléfonos móviles, soportes de almacenamiento de datos, correos electrónicos o información tratada verbalmente en reuniones. Que tenga que ver con la actividad de la Organización, sus clientes, proveedores, ventas, estados financieros u obligaciones contractuales.

3.1.3. **Sistema de información:** Incluye todos los servidores y clientes, infraestructura de red, software del sistema, aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por la Organización o que se encuentran bajo responsabilidad de la Organización. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a internet, correo electrónico, etc.

3.2. **Lineamientos para el uso aceptable de activos.**

3.2.1. Cada activo de información tiene designado un propietario en el inventario de activos.

3.2.2. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.

3.3. **Actividades prohibidas.**

3.3.1. Está prohibido utilizar los activos de información de manera tal que ocupen innecesariamente capacidad, que disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad.

3.3.2. También está prohibido:

- Descargar archivos de imágenes o vídeos que no tienen objetivos de negocios, enviar cadenas de correos electrónicos, jugar juegos, etc.
- Instalar software en un equipo local sin el permiso explícito del área de sistemas.
- Utilizar herramientas criptográficas (encriptado) sobre ordenadores locales, excepto en los casos especificados en la Política **XIGA-A28-POL-10 Política de clasificación y etiquetado de la información**.
- Descargar códigos de programa de soportes externos.

3.4. **Uso de activos fuera de las instalaciones.**

3.4.1. Mientras los activos en cuestión permanecen fuera de la Organización, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

3.5. **Devolución de activos a la finalización de un contrato.**

3.5.1. Al finalizar un contrato de empleo o de otro tipo, a raíz del cual se utilizan diversos equipos, software o información en formato electrónico o papel, el usuario debe devolver todos esos activos de información al área de Compras para el borrado seguro de la información.

3.6. **Procedimiento para copias de seguridad.**

3.6.1. El mecanismo oficial para realizar copias de seguridad es el agente de sincronización de OneDrive, el cual se configurará para respaldar solo los archivos contenidos en la carpeta de mis documentos, por lo cual es responsabilidad del usuario almacenar ahí los documentos para evitar posibles pérdidas.

3.7. **Protección antivirus.**

3.7.1. En cada equipo debe estar instalado un agente de protección contra software malicioso, con una suscripción de actualizaciones activada, de no tenerlo es responsabilidad del usuario solicitarlos al área de Sistemas.

3.8. **Facultades para el uso de sistemas de información.**

3.8.1. Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.

3.8.2. Los usuarios pueden utilizar los sistemas de información únicamente para las actividades para las cuales han sido autorizados; es decir, para las cuales les han sido otorgados derechos de acceso.

3.8.3. Los usuarios no deben participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información o filtrado web de internet.

3.9. **Responsabilidades sobre la cuenta de usuario.**

3.9.1. El usuario no deberá directa ni indirectamente, permitir que otra persona utilice sus derechos de acceso; es decir, su nombre de usuario; y no debe utilizar el nombre de usuario y/o clave de otra persona. El uso de nombres de usuario grupales está prohibido.

3.9.2. El propietario de la cuenta es responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.

3.10. **Protección de instalaciones y equipos compartidos.**

3.10.1. Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras, equipos de fax y fotocopiadoras.

3.10.2. Para hacer uso de las copiadoras, escáner y demás equipamiento compartido para copiado será necesario solicitar un calve de acceso a través de la cual se contabilizará su uso.

3.11. **Uso de Internet.**

3.11.1. Sólo se puede acceder a internet a través de la red local de la Organización, con la infraestructura y protección de cortafuegos adecuadas. El acceso directo a internet mediante módems, internet móvil, red inalámbrica u otros dispositivos de acceso directo a internet, está prohibido.

3.11.2. El área de Infraestructura puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los empleados de la Organización. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar una petición escrita al área de Sistemas solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.

3.11.3. El usuario debe considerar como no confiable la información recibida a través de sitios web no verificados. Ese tipo de información puede ser utilizado con fines comerciales solamente después de haber verificado su autenticidad y veracidad.

3.11.4. El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de internet.

3.12. **Correo electrónico y otros métodos de intercambio de mensajes.**

3.12.1. Entre los métodos de intercambio de mensajes, aparte del correo electrónico, se puede incluir la descarga de archivos desde internet, la transferencia de datos por medio de OneDrive, teléfonos, el envío de mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

3.12.2. Si se envía un mensaje con una etiqueta de confidencialidad, el usuario debe protegerlo de acuerdo con lo establecido en la **XIGA-A28-POL-10 Política de clasificación y etiquetado de la información**.

3.12.3. El usuario debe guardar todos los mensajes que contienen datos importantes para los negocios de la Organización en la carpeta de Mis Documentos, la cual está protegida por el control de versiones de OneDrive.

3.12.4. Cada correo electrónico debe incluir una exención de responsabilidad. Si un usuario envía un mensaje a través de un sistema de intercambio de mensajes (redes sociales, foros, etc.), debe declarar sin ambigüedades que no representa el punto de vista de la Organización.

3.13. **Derechos de autor.**

3.13.1. Los usuarios no deben realizar copias no autorizadas del software que pertenece a la Organización, excepto en los casos permitidos por la ley.

3.13.2. Los usuarios no deben copiar software ni otros materiales originales de otras fuentes y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.

3.14. **Computación móvil.**

3.14.1. Introducción.

3.14.1.1. Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

3.14.2. Reglas básicas.

3.14.2.1. Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos u otros medios de transporte, espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la Organización.

3.14.2.2. La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y en lo posible, debe quedar resguardado bajo llave o se deben utilizar medidas especiales para asegurarlo.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Los equipos deberán estar actualizados a las últimas versiones de los parches sugeridos por el fabricante.
- La información que se encuentra en ordenadores portátiles debe estar encriptada para todos los equipos portátiles.
- La protección de datos sensibles debe ser implementada de acuerdo con la política **XIGA-A28-POL-10 Política de clasificación y etiquetado de la información**.
- En el caso que el equipamiento de computación móvil sea desatendido, por más de 5 minutos se debe de aplicar una política de bloqueo de pantalla.

3.15. **Conexión Remota.**

3.15.1. Conexión Remota, significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la Organización. No incluye el uso de teléfonos móviles fuera de las instalaciones de la Organización.

3.15.2. Debe ser solicitado al área de TI y autorizado por la Gerencia de TI.

3.15.3. El uso estará regido por el **XIGA-A28-POL-05 Conexión remota.**

3.16. **Supervisión del uso de sistemas de información y comunicación.**

3.16.1. Los usuarios aceptan que personas autorizadas de la Organización puedan acceder a todos los datos y que el acceso de dichas personas no será considerado una violación de privacidad del usuario.

3.16.2. La Organización puede utilizar herramientas especializadas para identificar y bloquear métodos prohibidos de comunicación y para filtrar contenidos prohibidos.

3.17. **Incidentes.**

3.17.1. Cada empleado, proveedor o tercero que esté en contacto con datos y/o sistemas de la Organización debe reportar toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente.

3.18. **Penalizaciones.**

3.18.1. Cualquier violación a esta política por parte de empleados, socios o proveedores puede resultar en una acción disciplinaria, incluso hasta la terminación de contrato o servicio. La Organización se reserva el derecho de notificar a las autoridades correspondientes de cualquier actividad ilícita y de cooperar en cualquier investigación de dicha actividad.

3.19. **Lineamientos a Situaciones fortuitas.**

3.19.1. Cualquier incidente que afecte la confidencialidad, integridad o disponibilidad de la información de nuestros clientes debido a una situación fortuita se debe avisar al área de Sistemas y al Comité, para aplicar el proceso que corresponda.

3.20. **Periodicidad de revisión de la política.**

3.20.1. Se hará revisión de la política cuando:

3.20.1.1. Exista cambio de tecnología, equipos y/o procesos.

3.20.1.2. La utilización y/o activos sean modificados considerablemente.

3.20.1.3. Se presente algún incidente derivado de la utilización del activo.

3.20.2. Es responsabilidad del dueño de este documento revisar al menos una vez al año que este se encuentra actualizado y revisado.

3.20.3. Se dará un periodo mínimo de maduración a la política establecido por el área de Infraestructura y/o Gerencia de TI.

4. Documentos de referencia

Código	Documentos
XIGA-A28-POL-05	Conexión remota
XIGA-A28-POL-10	Política de clasificación y etiquetado de la información

5. Registros

Código	Registros	Tiempo de Conservación	Responsable de Conservarlo	Lugar de Almacenamiento
N/A	-	-	-	-

6. Glosario

6.1. N/A.

7. Anexos

7.1. N/A.