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 al Anexo 28 del SAT.
02	06-03-2019	- Se agregó los accesos a cuentas privilegiadas punto 6.6. - Se agregó el programa anual de auditoria interna punto 6.11. - Se agregó punto 9 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 realizó actualización anual de la política.
06	20-04-2022	- Se realizó la revisión anual del documento. - Se actualizó el número de control del documento y se estructuró bajo el nuevo formato organizacional.
07	19-04-2023	- Se realizó la revisión anual del documento.
08	18-04-2024	- 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.

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

1. Objetivo

1.1 Establecer el mecanismo para controlar el alta de usuarios y acceso a los aplicativos con los que cuente la Organización, de manera que se preserve la seguridad de la información del Monedero Electrónico XIGA.

2 Alcance

2.1 El procedimiento aplica para todo acceso a los aplicativos con los que opere la Organización a nivel nacional.

3 Políticas

3.1 Responsable del proceso.

3.1.1 Administrador del aplicativo.

3.2 Sistema de control de acceso.

3.2.1 Mecanismo en el que, mediante una identificación y autentificación, permita al usuario acceder a datos o recursos de la Organización.

3.3 Definición de acceso a los sistemas.

3.3.1 Es el conjunto de permisos otorgados a un usuario para consultar modificar o agregar información en los sistemas informáticos que soportan el Monedero Electrónico XIGA.

3.4 Directrices para el uso y operación del sistema.

3.4.1 Acceso: el acceso a los sistemas está restringido para todos los usuarios, a menos que exista una solicitud explicita por parte de la Gerencia de su área donde se detalle el nivel de acceso según las responsabilidades de su perfil.

3.4.2 La información contenida en los sistemas será de carácter confidencial y los operadores no podrán hacer uso de ella para otros fines que no sean los requeridos por las responsabilidades de su puesto.

3.4.3 Al terminar la relación laboral de un operador, la Gerencia del área deberá de solicitar la cancelación de dichos accesos.

3.5 El alta de usuarios a los aplicativos, creación de correos electrónicos, solicitud de acceso a menús adicionales y/o revocación de usuarios deberán solicitarse por medio del sistema GLPI al área de TI.

3.5.1 Toda creación de correo electrónico y alta del usuario en GLPI deberá ser solicitada por el Jefe Inmediato del colaborador, adjuntando el formato **XIGA-A28-F-01 Solicitud de acceso**.

3.6 En la solicitud se deberá adjuntar el formato **XIGA-A28-F-01 Solicitud de acceso**, en el cual se indicará la siguiente información:

- Fecha de solicitud.
- Sistema(s) o módulo(s): a los que se requerirá el acceso.
- Nombre a quien se le asigna el acceso.
- No. de empleado.
- Área a la que pertenece el solicitante.
- Cargo que ocupa el solicitante.
- Corto/Extensión.
- Especificación de menús/privilegios en el sistema o módulo: cuando sea más de un acceso se deberá indicar para cada sistema.

- Correo electrónico: Sólo llenar cuando el usuario ya cuente con uno.
- Fecha de vencimiento.
- Nombre y firma del solicitante.
- Nombre y firma del Gerente.

3.7 El área responsable enviará al administrador del aplicativo la solicitud de alta de usuario y/o acceso.

3.8 El administrador del aplicativo asignado para otorgar el permiso recibirá la solicitud y deberá revisar lo siguiente:

- Que en la solicitud se encuentre adjunto el formato **XIGA-A28-F-01 Solicitud de acceso** debidamente llenado y firmado por el Gerente del área.
- Revisar que el usuario para el cual se solicita el acceso cuente con el nivel de responsabilidad para poder hacer uso de los módulos.

Nota: Si el formato **XIGA-A28-F-01 Solicitud de acceso** no cuenta con la firma calígrafa del Gerente de área no se podrá dar de alta el usuario y/o el acceso al aplicativo.

3.9 Las cuentas de acceso privilegiadas son con base a los perfiles establecidos para el ERP, en el caso de los permisos a las operaciones, el responsable de asignarlos es el administrador del sistema, con base en la solicitud enviada por un superior debidamente autorizado.

3.10 Si el usuario para el cual se solicita el acceso cuenta con el nivel de responsabilidad necesario, se crea la cuenta de usuario con los datos generales enviados en la solicitud y se activan los accesos solicitados.

3.10.1 El administrador del aplicativo asignado para otorgar el permiso deberá enviar por correo electrónico el nombre de usuario y contraseña para el acceso al aplicativo solicitado.

3.10.2 Una vez otorgado el usuario y contraseña es responsabilidad del colaborador cambiar la contraseña de manera que cumpla con los puntos de seguridad indicados en la política **XIGA-A28-POL-15 Servicios de TI**.

3.10.2.1 El colaborador para el cual se le brindó el acceso, deberá cumplir con todas las políticas de seguridad indicadas en el documento **XIGA-A28-POL-15 Servicios de TI**, en el cual se indica que el usuario y clave es intransferible quedando bajo responsabilidad de este, conservando estos datos en secreto y en su uso personal exclusivo.

3.11 Cuando el colaborador para el cual se solicita el alta no cuente con el nivel de responsabilidad para el acceso solicitado el Gerente del área deberá justificar la solicitud de dicho acceso.

3.11.1 Una vez justificado el acceso el administrador del aplicativo asignado procederá a dar el alta, quedando en el entendido que el Gerente del área asume la responsabilidad del uso que dé él colaborador a la información que tenga acceso.

3.12 Es responsabilidad del administrador del aplicativo revocar los accesos al aplicativo o menú de algún sistema cuando en la solicitud se haya indicado una vigencia para el acceso.

3.13 Cuando algún colaborador deje de laborar en la Organización es responsabilidad del Gerente de área solicitar la revocación del usuario de manera inmediata.

3.14 De acuerdo al programa anual de auditoria interna se asegura con pruebas de cumplimiento que se encuentren alienados los privilegios del sistema con las funciones, roles y responsabilidades del usuario.

3.15 Penalizaciones.

3.15.1 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.

3.16 Lineamientos de atención a situaciones fortuitas.

3.16.1 Cualquier incidente que afecte la confidencialidad, integridad o disponibilidad del acceso a los aplicativos debido a una situación fortuita se debe avisar al Administrador de Aplicativos, para que se le dé el tratamiento de acuerdo al procedimiento de respuesta a incidentes de seguridad de la información.

3.17 Periodicidad de la revisión de la política.

3.17.1 Se hará revisión de la política cuando:

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

3.17.1.2 Se presente algún incidente referente al control de accesos.

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

3.17.3 Se dará un periodo mínimo de maduración a la política establecido por la Gerencia de XIGA.

4 Documentos de referencia

Código	Documentos
XIGA-A28-POL-15	Servicios de TI

5 Registro

Código	Registros	Tiempo de Conservación	Responsable de Conservarlo	Lugar de Almacenamiento
XIGA-A28-F-01	Solicitud de acceso	5 años	TI	Archivo físico y digital

6 Glosario

6.1 N/A.

7 Anexos

7.1 N/A.