## RESUMEN DE HISTORIA DE CAMBIOS

| Revisión | Fecha | Razón del Cambio |
|---|---|---|
| 00 | 09-03-2015 | - Documento de nueva creación bajo Sistema de administración. |
| 01 | 08-03-2016 | - Se realizó la revisión anual del documento. |
| 02 | 07-03-2017 | - Se realizó la revisión anual del documento. |
| 03 | 06-03-2018 | - Se realizó la revisión anual del documento. |
| 04 | 05-03-2019 | - Se realizó la revisión anual del documento. |
| 05 | 04-03-2020 | - Se realizó modificación del encabezado. |
| 06 | 03-03-2021 | - Se realizó la revisión anual del documento. |
| 07 | 17-01-2022 | - Se actualizó el número de control y se estructuró el documento bajo el nuevo formato organizacional.<br>- Se realizó un cambio en los puntos 4.4.1.4 Alta del personal y 4.5 Convención de nombres de usuario.<br>- Se añadieron imágenes de ejemplo al punto 4.6 Contraseñas.<br>- Se añadieron los puntos 4.8. Confirmación de las Altas, Bajas y Modificaciones, 4.9 y 4.10.<br>- Se eliminó el punto 11 y 12 de la versión 02. |
| 08 | 16-01-2023 | - Se realizó la revisión anual del documento. |
| 09 | 15-01-2024 | - Se realizó la revisión anual del documento. |
| 10 | 14-01-2025 | - Se realizó la revisión anual del documento. |
| 11 | 03-04-2025 | - Se actualizó la tabla de participantes y aprobaciones.<br>- Se remplazó el sistema CONTPAQi por el sistema SAP Business One. |
| 12 | 29-05-2025 | - Se agregó la participación del Gerente de TI en los puntos 3.9.2.1, 3.9.3.1 y 3.9.3.2.<br>- Se actualizó la política 3.4.1.3. mencionando los sistemas ERP/Monedero XIGA y la matriz de PERFILADO DE ACCESOS XIGA. |

| | Elaboró | Revisó | Aprobó |
|---|---|---|---|
| **Nombre** | Merced Ortiz | Miguel Ricario | Isis Curiel |
| **Puesto** | Coordinador de XIGA | Gerente de XIGA | Representante Legal |
| **Firma** |  |  |  |

## 1. Objetivo

1.1. Establecer el procedimiento para el alta, baja y cambios de usuarios en el sistema ERP/Monedero XIGA, así mismo impedir el acceso no autorizado a dichos sistemas de la Organización.

## 2. Alcance

2.1. Dar a conocer al personal de la Organización los datos necesarios para un pedido de alta, baja y/o cambios de cuentas de usuarios.

## 3. Políticas y desarrollo

3.1. **Contactos Claves.**

| Encargados | Sistemas |
|---|---|
| TI | ERP/Monedero XIGA |
| Talento Humano | TRESS |

3.2. **Procedimiento para altas, bajas y modificaciones.**

3.2.1. El área de Talento Humano será responsable de informar a los encargados de los sistemas los movimientos que se produzcan con el personal de la Organización por medio de correo electrónico o GLPI.

3.3. **Para bajas de personal:**

3.3.1. El área de Talento Humano deberá de notificar a las áreas involucradas el mismo día en el que el empleado ha sido dado de baja:

3.3.1.1. Notificar al Área de Infraestructura para aplicar baja en la red, active directory, accesos VPN´s (en caso de que aplique), usuarios para impresora, etc.

3.3.1.2. Notificar al área de Soporte de Sistemas para aplicar baja en la cuenta de correo, así como los accesos a los sistemas que operen, tales como: ERP/MONEDERO XIGA.

3.3.1.3. Notificar a Nóminas para aplicar la baja en el sistema TRESS.

3.4. **Alta de personal:**

3.4.1. El área de Talento Humano deberá notificar a las áreas involucradas el mismo día en el que el empleado ha sido dado de alta, tales como:

3.4.1.1. Infraestructura para aplicar el alta en la red, active directory, accesos a VPN´s (en caso de que aplique), agregar a la línea de avaya, crear usuario para impresora, etc.

3.4.1.2. Soporte Técnico y Sistemas para dar de alta la cuenta de correo y ERP/MONEDERO XIGA. respectivamente y al área de Nóminas para el alta en sistema TRESS.

3.4.1.3. Dar acceso a los sistemas ERP/Monedero XIGA con base en la matriz de PERFILADO DE ACCESOS XIGA, que de forma predefinida indica a qué módulos dentro del sistema tendrá acceso el empleado, dependiendo del área a la que pertenezca y el nivel jerárquico del empleado, esto incluye la generación de cuentas privilegiadas.

3.5. **Convención de nombres de usuario.**

3.5.1. Para asignar nombres de usuario se utilizarán las siguientes convenciones:

3.5.1.1. Primera inicial, seguida del apellido (jperez, cobregon, pramirez, etc.).

3.5.2. En caso de colisión de usuario, se resolverá:

3.5.2.1. Primer nombre separado de un punto y el apellido (Juan.Perez, Raul.Lopez, etc.)

3.6. **Contraseñas.**

3.6.1. El administrador del sistema crea contraseñas por omisión a los usuarios para primera sesión y se le notifica al usuario.

3.6.2. El administrador del sistema a su vez provee de opción para que los usuarios cambien sus propias contraseñas.

3.7. **Para Modificación de Personal.**

3.7.1. Si el empleado fue promovido de cargo, el área de Talento Humano deberá notificar a las áreas involucradas el mismo día en que se ha hecho el cambio.

3.7.2. Si al empleado se le han asignado nuevas tareas que requiera tener nuevos accesos, el coordinador de cada área será responsable de notificar y llenar el **XIGA-A28-F-01 Solicitud de accesos** para que los encargados realicen la modificación solicitada.

3.8. **Confirmación de las Altas, Bajas y Modificaciones.**

3.8.1. Los encargados de los sistemas y demás áreas implicadas deberán notificar por medio de correo electrónico a la Administración de XIGA un día después los movimientos solicitados.

3.9. **Gestión de cuentas privilegiadas.**

3.9.1.1. Generación de cuentas privilegiadas con altos niveles de acceso.

3.9.1.1.1. La generación de cuentas privilegiadas con altos niveles de acceso solo está permitida para Gerentes y Administradores de los sistemas de información (bases de datos), que estén debidamente contratados y con convenio de confidencialidad.

3.9.1.2. Las cuentas privilegiadas que tienen permisos elevados incluyen:

3.9.1.2.1. Cuentas de administrador local o de dominio que administran servidores.

3.9.1.2.2. Cuentas de administrador de dominio que normalmente controlan a los usuarios de Active Directory.

3.9.1.2.3. Cuentas de administrador del sistema que ayudan a administrar las bases de datos.

3.9.1.2.4. Cuentas raíz que gestionan plataformas Unix/Linux.

3.9.1.2.5. Cuentas que ejecutan y administran, servicios y tareas programadas de Windows.

3.9.1.2.6. Grupos de IIS (.NET).

3.9.1.2.7. Cuentas de equipos de red que dan acceso a cortafuegos, enrutadores y conmutadores.

3.9.1.3. Los Gerentes o responsables de área solicitan a TI los accesos y privilegios a los sistemas vía correo electrónico.

3.9.1.4. TI recibe atiende la solicitud.

3.9.1.5. TI crea los accesos requeridos, confirmando por correo y notificando a las áreas los usuarios con privilegios.

3.9.1.6. Las contraseñas de las cuentas deben cambiarse al menos trimestralmente.

3.9.2. Generación de cuentas de Sistemas por perfil de Usuario.

3.9.2.1. El alta de acceso a los sistemas y asignación de perfiles, es solicitada por el Gerente o responsable de área llenando el formato **XIGA-A28-F-01 Solicitud de accesos** y haciéndolo llegar al Gerente de TI quien a su vez generará la cuenta privilegiada de acuerdo con la matriz de perfiles de acceso al aplicativo.

3.9.2.2. El Gerente es el responsable de aprobar las nuevas solicitudes de acceso de los usuarios a los sistemas de información.

3.9.2.3. El acceso a los sistemas y sus opciones se otorga según las funciones laborales de la persona y las responsabilidades establecidas para su rol. (ver perfilado acceso XIGA).

3.9.3. Modificación de los privilegios de acceso del usuario.

3.9.3.1. Los Gerentes o responsables de área, se deberán asegurar cuando un empleado cambie de función dentro de la Organización, que su acceso se modifique para que refleje los requisitos de su nueva función. Para ello envía al Gerente TI vía correo el registro **XIGA-A28-F-01 Solicitud de accesos** con las modificaciones de los privilegios de usuario.

3.9.3.2. El Gerente TI elimina todos los privilegios de acceso de usuario a los sistemas o servicios de información que ya no sean necesarios para el nuevo rol del empleado.

3.9.3.3. El Gerente de área es responsable de aprobar los cambios en el acceso de los usuarios a los sistemas.

3.9.4. Eliminación de los privilegios de acceso del usuario.

3.9.4.1. A los empleados que dejen la empresa, por cualquier motivo, se les desactivan los privilegios de acceso de usuario al causar baja en el sistema de nómina.

3.9.4.2. Talento Humano notifica las bajas.

3.9.4.3. TI y administradores de los sistemas de información, eliminarán el acceso específico de la aplicación para la cuenta de usuario.

3.10. Verificación de permisos y de niveles de acceso a los sistemas.

3.10.1. Para verificar que los permisos y niveles de acceso de los empleados corresponden a sus responsabilidades, TI al menos cada tres meses verifica los accesos y permisos de los sistemas, para garantizar que los privilegios de acceso a los usuarios correspondan a sus funciones según lo establecido a su perfil (ver perfilados accesos XIGA). Lo anterior se realiza mediante las siguientes actividades:

3.10.1.1. TI genera el listado de los empleados que causaron alta, baja, activos y cambios.

3.10.1.2. TI valida los usuarios con acceso al sistema ERP/Monedero.

3.10.1.3. TI verifica que la descripción de los permisos asignados a cada perfil corresponda al puesto definido. (ver perfilado de accesos XIGA).

3.10.1.4. TI obtiene las posibles desviaciones referentes a la asignación de dichos perfiles **(ver XIGA-A28-F-16 Verificación de Permisos y Análisis de perfiles).**

3.10.1.4.1. En la hoja "Análisis" se encuentra el análisis de perfiles realizado a los usuarios de los empleados activos dentro del sistema.

3.10.1.4.2. En la hoja "Perfiles", se encuentra el listado a detalle de los roles de acceso que tiene cada perfil.

3.10.1.4.3. Los archivos adjuntos se encuentran en el listado de empleados Activos, Bajas, Altas y Cambios, los cuales fueron proporcionados por TI.

3.10.2. En caso de ser una auditoria Interna los resultados son notificados por el auditor a la Gerencia de XIGA y a los Encargados de los sistemas.

3.10.3. Las revisiones de acceso de los usuarios deben documentarse y conservarse por los encargados del sistema con fines de auditoría.

3.10.4. TI da seguimiento a las desviaciones hasta el cierre dentro de un plazo inmediato.

3.10.5. TI es responsable de realizar revisiones anuales a los permisos de acceso de usuarios de su área.

## 4. Documentos de referencia

| Código | Documentos |
|---|---|
| - | - |

## 5. Registros

| Código | Registros | Tiempo de Conservación | Responsable de Conservarlo | Lugar de Almacenamiento |
|---|---|---|---|---|
| XIGA-A28-F-01 | Solicitud de accesos | 5 años | Administración de XIGA | Archivo Digital |
| XIGA-A28-F-16 | Verificación de Permisos y Análisis de perfiles | 5 años | Administración de XIGA | Archivo Digital |

## 6. Glosario

6.1. N/A.

## 7. Anexos

7.1. N/A.