| Control de Cambios | | |
|---|---|---|
| **Versión** | **Fecha** | **Descripción de la Modificación** |
| 1 | 29/08/208 | Creación del Procedimiento |
| 2 | 21/10/2013 | Se hace revisión y ajuste a las actividades operacionales del procedimiento por ajuste institucional. |
| 3 | 05/02/2015 | Se actualiza el procedimiento incluyendo elementos de “Control de acceso a sistemas de información y recursos de red” y “Control de acceso al centro de cómputo. |
| 4 | 15/11/2017 | Se actualiza el procedimiento haciendo el cambio de Nombre: Administración de Infraestructura Tecnológica y el código del procedimiento |
| 5 | 28/07/2023 | Inclusión de plantilla, actualización del contenido y puntos de control. |

| Elaboró | Revisó | Aprobó |
|---|---|---|
| Jakeline Sánchez de López<br>Profesional Especializado 222-23 | Claudia Marcela Ladino Herrara<br>Jefe Oficina TIC | Claudia Marcela Ladino Herrara<br>Jefe Oficina TIC<br><br>Nelson Jairo Rincón Martínez<br>Jefe Oficina Asesora de Planeación |

## 1. Objetivo

El presente procedimiento tiene como objetivo establecer las políticas y directrices para la adecuada administración y uso de los elementos de infraestructura de la Oficina de Tecnologías de la Información y las Comunicaciones (TICs) del IDIGER. Este alcance se extiende a todos los profesionales del Equipo de Infraestructura y Sistemas de Información de la Oficina TICs, así como a todos los usuarios del IDIGER, quienes deberán cumplir con las políticas específicas descritas en este documento.

## 2. Alcance

El procedimiento abarca los siguientes elementos de infraestructura:

**Control de acceso**: establecimiento de políticas y mecanismos para garantizar el acceso seguro a los recursos de tecnologías de la información.

**Servidores**: administración, configuración y monitoreo de los servidores utilizados por la Oficina TICs.

**Redes**: Gestión y monitoreo de las redes de datos internas y externas.

**Copias de respaldo**: políticas para la realización de copias de respaldo

**Almacenamiento**: administración y buen uso del almacenamiento de datos.

## 3. Responsables

- Las políticas contenidas en este documento deben ser cumplidas por todos los miembros el equipo de Infraestructura y Sistemas de Información de la Oficina TICs.
- Las políticas sobre Cuentas de usuario, Acceso VPN, Acceso a Redes sociales y Uso del almacenamiento deben ser acatadas por todos los usuarios del IDIGER, independientemente de su rol o posición dentro de la organización

## 4. Definiciones

**Contraseña**: palabra o serie de caracteres que un usuario autorizado crea para iniciar sesión en un sistema o servicio informático.

**Copia de respaldo o backup**: copia de seguridad que puede alojarse en un disco duro o medios externos cuya finalidad es salvaguardar la información en caso de fallos.

**Directorio activo**: servicio donde se gestionan objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas para el acceso de recursos en la red.

**Infraestructura tecnológica**: comprende el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar o soportar los Servicios de TI.

**Logs**: registro oficial de eventos durante un rango de tiempo en particular. Debe registrar datos sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

**Mesa de servicio**: es el punto central de contacto entre la Oficina TICs y los usuarios. Es la encargada de manejar los incidentes y las solicitudes de servicio.

**Monitoreo**: observación repetida de un elemento de configuración, Servicio de TI o Proceso para detectar eventos y asegurarse de que se conoce el estado actual y para detectar cambios.

**NAS**: Network Attached Storage, servidor de almacenamiento en red.

**Principio de mínimo privilegio**: se refiere a la práctica de otorgar los permisos necesarios y suficientes a un usuario para desempeñar sus actividades, por un tiempo limitado, y con el mínimo de privilegios necesarios para la realización de sus tareas.

**Servicio**: Conjunto de actividades realizadas por la entidad para satisfacer las exigencias de sus clientes y/o ciudadanos entregando resultados planificados.

**Herramienta de monitoreo**: son las herramientas tecnológicas usadas por la Oficina TICs para realizar las actividades de seguimiento y verificación.

## 5. Políticas de operación

### 5.1. Control de acceso – Gestión de cuentas de usuarios

La Oficina TICs implementa el control de acceso a las diferentes plataformas tecnológicas de la entidad mediante la identificación de los usuarios mediante cuenta de usuario y contraseña y asignación de roles.

Es responsabilidad del Equipo de Infraestructura tecnológica, la administración de las cuentas de usuario desde su creación hasta su desactivación, para los siguientes entornos:

- Acceso al dominio
- Acceso al Sistema de almacenamiento compartido
- Correo electrónico

#### 5.1.1. Cuentas de administradores

- Las contraseñas de los usuarios de administración de infraestructura, como por ejemplo el usuario administrador o root no tienen fecha de caducidad y deben cambiarse por lo menos 1 vez al año.
- Se debe deshabilitar la cuenta de usuario “guest” o “invitado” de todos los servidores, servicios o dispositivos de comunicaciones.
- Se deben cambiar todas las contraseñas de las cuentas que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware, en cualquier dispositivo conectado a la red.

#### 5.1.2. Cuentas de usuario

- La solicitud de cuentas de usuarios se realizará a través del formato “**TC-FT-31 Formato solicitud de usuarios en tecnología y en sistemas de información**” el cual debe estar debidamente diligenciado y firmado por el supervisor del contrato o jefe inmediato.
- Para la generación o creación de la cuenta de usuario se tendrán en cuenta los lineamientos establecidos al interior.
- Se asignará una cuenta de correo electrónico con el mismo identificador de usuario y

se incluirá en un grupo o lista de distribución.

- Las contraseñas deben cumplir con los siguientes requisitos:
    - No contener el nombre de cuenta del usuario o partes de su nombre ni palabras de diccionario, no utilizar datos personales, tales como números de identificación, teléfonos o direcciones, nombres de familiares o mascotas.
    - Incluir caracteres de las siguientes categorías:
        - Mayúsculas (A-Z)
        - Minúsculas (a-z)
        - Dígitos de base 10 (0-9)
        - Caracteres especiales ($, #, %, *, \)
    - No repetir las últimas 5 contraseñas
    - El usuario puede cambiarla voluntariamente cuando lo desee.
    - La asignación de usuarios y contraseñas debe ser realizada de forma individual, el uso de contraseñas compartidas está prohibido.
- La responsabilidad por el uso indebido del usuario y contraseña es exclusiva del usuario titular.
- La cuenta de usuario será bloqueada si ocurren 5 intentos fallidos de inicio de sesión.
- Si se sospecha que la seguridad de una cuenta de usuario está comprometida, se notificará al usuario para efectuar un cambio de contraseña de manera inmediata.
- Cuando un funcionario o contratista finalice su relación laboral con el IDIGER y no se vaya a realizar prórroga o celebración de un nuevo contrato, se procederá a desactivar las cuentas que tenga asignadas y se realizará una copia de seguridad de su cuenta de correo electrónico. Esto se realiza durante la generación del "**Certificado de sin pendientes"** (Formato TH-FT-101 de Talento Humano).

### 5.1.3. Acceso VPN (Red privada virtual)

- La Oficina TICs proveerá el servicio de conexión remota a la plataforma tecnológica institucional a través de red privada virtual - VPN, así la transferencia de datos entre usuario remoto y red institucional se encontrará debidamente cifrado.
- El acceso remoto vía VPN será habilitado para los usuarios teletrabajadores y aquellos contratistas que así lo requieran previa autorización de su supervisor o jefe inmediato quien debe describir las necesidades de acceso y las herramientas a la que debe acceder.

- La vigencia del permiso de acceso vía VPN estará homologada con la vigencia de la cuenta de dominio a menos que sea expresamente revocada por solicitud del supervisor o jefe inmediato.
- Cada usuario podrá tener activa una única conexión VPN con IDIGER y debe desconectarla una vez concluida las operaciones a realizar en la red interna.
- Los usuarios de la VPN serán automáticamente desconectados de la sesión, una vez que hayan transcurrido 30 minutos de inactividad.
- Los usuarios con acceso VPN son completamente responsables de las actividades realizadas con su cuenta y deben garantizar que ninguna otra persona utilice la misma entendiendo que es de uso personal y que sus computadores, ya sea institucionales o personales, cuando se conectan a la VPN son una extensión de la Red del IDIGER

### 5.1.4. Acceso a redes sociales

- El acceso a redes sociales, desde la red del IDIGER, está restringido a usuarios autorizados por la Oficina TICs previa solicitud por parte del supervisor o jefe inmediato, quien debe justificar la necesidad del acceso a las mismas para el cumplimiento de las funciones u obligaciones contractuales del usuario.

### 5.1.5. Control de acceso a sistemas de información y recursos de red

- El acceso a plataformas, sistemas de información y recursos de red será asignado por el equipo de administración de infraestructura tecnológica y sistemas de información conforme a los requerimientos de cada usuario y/o grupo de trabajo.
- La Oficina TICs controlará el acceso a los servicios de red tanto internos como externos con el propósito de garantizar la seguridad de los usuarios y mantener la estabilidad de los servicios, para lo cual se restringen los puertos de acceso por defecto, salvo casos particulares debidamente justificados.
- Todos los Sistemas de información o aplicaciones administrados por la Oficina TICs deben tener control de acceso a través de autenticación mediante un usuario y contraseña.
- El control de acceso a la información a través de una aplicación, sistema de información o almacenamiento compartido se realizará a través de roles que administren los privilegios de los usuarios y será determinado por el dueño de la información.

- El ingreso para la gestión remota de Sistemas de información o Aplicaciones debe estar restringida, permitiendo solo usuarios conectados a través de la VPN o que estén presencialmente en la entidad y debidamente autorizados.

## 5.2. Gestión de servidores

- El Administrador de infraestructura es el encargado de otorgar permisos de acceso a los sistemas operativos de las máquinas, según el rol de quien los requiere.
- El Administrador de Infraestructura debe revisar periódicamente los archivos de logs de los servidores
- Se deben documentar los componentes de la infraestructura incluyendo permisos de accesos, configuraciones, identificador y función.
- Se debe activar y conservar los registros de auditoría (logs) en todos los dispositivos de comunicaciones, seguridad y servidores.
- El ingreso para la gestión remota de servidores debe estar restringida, permitiendo solo usuarios conectados a través de la VPN o que estén presencialmente en la entidad y debidamente autorizados.
- Los servidores deben tener un esquema de copias de respaldo y recuperación para casos de desastre.
- La gestión de servidores a través interfaz de línea de comando (CLI) se debe realizar sin excepción a través de protocolo seguro. El uso del protocolo Telnet sólo será empleado en los casos en los que el servidor no soporte el protocolo SSH, previa verificación, justificación y aprobación.
- No está permitido el uso de programas inseguros o no licenciados, para la administración remota de ningún servidor dentro de la red.
- El administrador de la infraestructura debe monitorear el procesamiento, la memoria, la capacidad del disco e interfaz de red de los servidores como parte de las operaciones rutinarias, para diagnóstico, mantenimiento o para resolver fallas.

## 5.3. Gestión de red

- El administrador de la red está autorizado para monitorear la red con cualquiera de los métodos existentes con la finalidad de resolver problemas de servicio, como parte de
- las operaciones rutinarias de la red, para diagnóstico, mantenimiento o para resolver

fallas.

- El administrador de la red tiene autoridad para cancelar el servicio a cualquier subred o dispositivo de red que afecte el desempeño de la red y notificar al área responsable para que se identifique la causa.
- Las redes deberán estar separadas en segmentos físicos y/o lógicos aplicando configuraciones de seguridad para cada segmento que permitan el control de tráfico dentro de la red.
- Las configuraciones de los equipos de comunicaciones y de seguridad deben estar debidamente documentadas.
- El administrador de la red debe realizar copias de respaldo de la configuración de los equipos de comunicaciones y seguridad de manera periódica.
- La gestión de los equipos de red a través interfaz de línea de comando (CLI) se debe realizar sin excepción a través del protocolo seguro. El uso del protocolo Telnet sólo será empleado en los casos en los que el dispositivo no soporte el protocolo SSH, previa verificación, justificación y aprobación.
- No está permitido el uso de programas inseguros o no licenciados, para la administración remota de ningún dispositivo dentro de la red.

## 5.4. Copias de respaldo

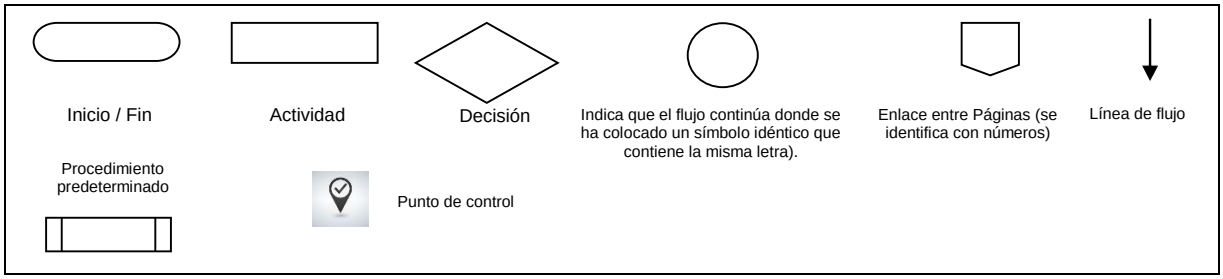
- Las copias de seguridad se administrarán mediante la herramienta de Backups vigente licenciada por la entidad, a excepción de las copias de correo y las copias de configuración de los dispositivos de red debido a que deben realizarse por demanda y manualmente.
- Se deben realizar copias de respaldo a los siguientes componentes:
    - **Configuración de servidores**: Incluyen la configuración del sistema operativo, políticas, reglas configuradas y despliegue de aplicaciones.
    - **Bases de datos**: incluyen Backups de toda la data, completos e incrementales.
    - **Cuentas de correo electrónico**: se realiza a través de la herramienta del proveedor una vez que se requiera suspender o eliminar una cuenta de correo.

## 5.5. Uso del almacenamiento

- El almacenamiento compartido NAS es de uso exclusivo para guardar versiones finales

- de documentos que deban preservarse, por ningún motivo debe utilizarse como almacenamiento de trabajo.
- No está permitido almacenar información personal en las carpetas NAS.
- La información en la NAS debe almacenarse respetando la estructura de las TRDs establecidas por Gestión Documental.
- Para documentos en edición y no finalizados o en edición compartida se debe utilizar el almacenamiento en la nube Google drive provisto por la entidad.
- Los permisos sobre las carpetas compartidas NAS deben ser autorizados por el usuario dueño de la información.

## 6. Desarrollo



## CREACIÓN DE USUARIOS

| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
| Inicio | Inicia el procedimiento | | |
| 1. Recibir el formato TC-FT-31 | Recibir el formato TC-FT-31 firmado por el supervisor del contrato o jefe inmediato | Equipo de trabajo de Infraestructura Tecnológica | Formato TC-FT-31 |
| A<br>2. Estructurar identificador de usuario | Estructurar el identificador de usuario a asignar verificando que no exista como usuario | Equipo de trabajo de Infraestructura Tecnológica | |
| A<br>¿Existe?<br>SI<br>NO | En caso de que ya exista el identificador, regresa a la actividad 2 para asignar un identificador diferente según las reglas descritas en las políticas de operación. Si no existe, continúa a la actividad 3 | Equipo de trabajo de Infraestructura Tecnológica | |
| 3. Crear la cuenta | Crear la cuenta en Directorio activo, NAS y demás Sistemas de información requeridos, así como la cuenta de correo electrónico. | Equipo de trabajo de Infraestructura Tecnológica y Sistemas de Información | BD de usuarios |
| 4. Notificar al usuario | Informar al usuario vía correo electrónico que se encuentra habilitada su cuenta para acceso a aplicaciones y recursos | Equipo de trabajo de Infraestructura Tecnológica | Correo electrónico |
| 5. Archivar solicitud | Archivar la solicitud en la carpeta física de Solicitudes de creación de usuarios si se recibió en físico, o en una carpeta digital si se recibió en ese formato | Equipo de trabajo de Infraestructura Tecnológica | Carpeta física o digital |
| Fin | Termina el procedimiento | | |

## DESACTIVACIÓN DE USUARIOS

| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
| Inicio | Inicia el procedimiento | | |
| 1. Recibir solicitud de Certificado de sin pendientes | Recibir el formato TH-FT-101 por parte del jefe inmediato | Equipo de trabajo de Infraestructura Tecnológica | Formato TH-FT-101 |
| 2. Validar pendientes de usuario | Validar que el usuario no tenga pendientes los respectivos aplicativos | Equipo de trabajo de Infraestructura Tecnológica y de Sistemas de información | |
| B, ¿Tiene pendientes?, SI, NO | En caso de que exista algún pendiente no se desactivará el usuario ni se firma el formato paz y salvo.<br>Si no tiene pendientes, se desactivan las cuentas y se genera el Backup de cuenta de correo electrónico. | Equipo de trabajo de Infraestructura Tecnológica y de Sistemas de información | |
| 3. Desactivar cuentas de usuario | Desactivar la cuenta de usuario en Directorio activo, NAS y demás Sistemas de información requeridos, así como la cuenta de correo electrónico | Equipo de trabajo de Infraestructura Tecnológica y de Sistemas de información | BD de usuarios |
| B, 4. Devolver formato | Devolver formato al área solicitante:<br>a) Firmado si el usuario estaba sin pendientes<br>b) Con la notificación de que el usuario tiene pendientes y por tanto no se firma el formato | Equipo de trabajo de Infraestructura Tecnológica | Formato TH-FT-101 |
| Fin | Termina el procedimiento | | |

## DESBLOQUEO DE USUARIOS

| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
| Inicio | Inicia el procedimiento | | |
| 1. Recibir solicitud de desbloqueo de cuenta de usuario | Recibir la solicitud de desbloqueo de la cuenta a través de la mesa de servicios provista por la Oficina TICs  | Equipo de trabajo de Infraestructura Tecnológica | Caso en la mesa de servicios |
| C<br>2. Verificar servicio bloqueado | Ingresar y verificar cual servicio se encuentra bloqueado | Equipo de trabajo de Infraestructura Tecnológica y de Sistemas de información | |
| 3. Desbloquear la cuenta | Efectuar los procedimientos necesarios para activar las cuentas en el o los servicios bloqueados | Equipo de trabajo de Infraestructura Tecnológica y de Sistemas de información | |
| 4. Validar efectividad de la acción | Notificar y validar con el usuario que la cuenta ya se ha desbloqueado | Equipo de trabajo de Infraestructura Tecnológica | |
| C<br>¿Persiste bloqueo?<br>SI<br>NO | Si el usuario manifiesta que el problema persiste ir nuevamente a la actividad 2.<br><br>Si el usuario manifiesta que ya tiene la cuenta activa continuar a la actividad 5 | Equipo de trabajo de Infraestructura Tecnológica | |
| 5. Cerrar el caso | Documentar y cerrar el caso en la mesa de servicios | Equipo de trabajo de Infraestructura Tecnológica | Caso en la mesa de servicios |
| Fin | Termina el procedimiento | | |

## RESTABLECIMIENTO DE CONTRASEÑAS

| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
| Inicio | Inicia el procedimiento | | |
| 1. Recibir la solicitud para restablecimiento de contraseña | Recibir la solicitud de restablecimiento de contraseña a través de la mesa de servicios provista por la Oficina TICs | Equipo de trabajo de Infraestructura Tecnológica | Caso en la mesa de servicios |
| D<br>2. Verificar las contraseñas a restablecer | Verificar el servicio para el cual se requiere restablecer la contraseña | Equipo de trabajo de Infraestructura Tecnológica y de Sistemas de información | |
| 3. Restablecer las claves solicitadas | Restablecer la clave en el servicio correspondiente | Equipo de trabajo de Infraestructura Tecnológica y de Sistemas de información | |
| 4. Validar efectividad de la acción | Notificar y validar con el usuario que el cambio de clave ha sido efectivo | Equipo de trabajo de Infraestructura Tecnológica | |
| ¿Puede ingresar?<br>D<br>NO<br>SI | Si el usuario manifiesta que el problema persiste ir nuevamente a la actividad 2.<br><br>Si el usuario manifiesta que puede ingresar con la nueva contraseña, continuar a la actividad 5. | Equipo de trabajo de Infraestructura Tecnológica | |
| 5. Cerrar el caso | Documentar y cerrar el caso en la mesa de servicios | Equipo de trabajo de Infraestructura Tecnológica | Caso en la mesa de servicios |
| Fin | Termina el procedimiento | | |

## MONITOREO DE SERVIDORES

| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
| Inicio | Inicia el procedimiento | | |
| 1. Revisar disponibilidad | Revisar disponibilidad de servidores mediante un ping al dispositivo  | Administrador de Servidores | Documento de Checklist |
| 2. Revisar capacidad | Revisar capacidad de servidores mediante el chequeo de los recursos de este | Administrador de Servidores | |
| E<br>¿Encuentra novedades?<br>NO<br>SI | Verificar los parámetros encontrados. Si se encuentra alguna novedad, documentar y planificar la ejecución del correctivo cuando aplique, en caso contrario continua en actividad 4. | Administrador de Servidores | |
| 3. Documentar y ejecutar el correctivo | Documentar y planificar la ejecución del correctivo cuando aplique | Administrador de Servidores | Documento de Checklist |
| E<br>4. Documentar | Documentar y terminar el procedimiento. | Equipo de trabajo de Infraestructura Tecnológica | Documento de Checklist |
| Fin | Termina el procedimiento | | |

## MONITOREO DE CONECTIVIDAD

| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
| Inicio | Inicia el procedimiento | | |
| 1. Monitoreo | Monitorear a través de la herramienta de monitoreo de redes, la disponibilidad y rendimiento de los equipos de Red | Administrador de Redes | Herramienta de Monitoreo |
| F, ¿Encuentra novedades?, NO, SI | Verificar los parámetros encontrados. Si se encuentra alguna novedad, planificar la ejecución del correctivo cuando aplique. En caso contrario, terminar el procedimiento. | Administrador de Redes | |
| 3. Planificar y ejecutar el correctivo | Planificar la ejecución del correctivo cuando aplique | Administrador de Redes | |
| F, Fin | Termina el procedimiento | | |

### VERIFICACIÓN DE BACKUPS

| FLUJOGRAMA | ACTIVIDAD | RESPONSABLE | DOCUMENTO O REGISTRO |
|---|---|---|---|
| Inicio | Inicia el procedimiento | | |
| 1. Revisión de ejecución | Revisar a través de la herramienta de backups la ejecución de las copias de respaldo programadas | Administrador de Servidores | Herramienta de Backups |
| G<br>¿Se realizó el backup?<br>SI<br>NO | Verificar si se ejecutaron correctamente. Si ocurrió alguna falla, ejecutar la copia de backup nuevamente, en caso contrario, termina el procedimiento | Administrador de Servidores | |
| 2. Ejecutar nuevamente la tarea backup | Ejecutar manualmente la copia de backup. | Administrador de Servidores | |
| G<br>Fin | Termina el procedimiento | | |

## 7. Documentos asociados

| Nombre | Fecha de Publicación o Versión | Entidad que lo Emite | Medio de Consulta |
|---|---|---|---|
| | | | |
| | | | |