



## GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

**Código:** GTIC-PD-03

**Fecha:** 2021-11-12

## PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO

**Versión:** 2

**Página:** 1 de 14

### 0. CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Responsable	Descripción de Cambios realizados
1	2018-06-12	Mayra Alejandra Soto Contratista Área de TIC Nestor Ruiz Barragán Contratista Área de TIC Nelson Andres Maldonado Contratista Área de TIC	Emisión Inicial de acuerdo con la actualización del mapa de procesos de la entidad, en LMD anterior corresponde al código: 3AP-GTI-PD-02
2	2021-11-12	OSCAR ALBERTO VARGAS CAMELO	Actualizar los lineamientos para gestionar y administrar las credenciales de autenticación de los diferentes perfiles de usuarios de los recursos tecnológicos para el desarrollo de sus funciones o actividades contractuales.

### 1. LIDER DE PROCESO: CARLOS ALFONSO GAITAN SANCHEZ

**1.1 OBJETIVO DEL PROCEDIMIENTO:** Gestionar y administrar las credenciales de autenticación de los diferentes perfiles de usuarios de los recursos tecnológicos para el desarrollo de sus funciones o actividades contractuales.

**1.2 ALCANCE DEL PROCEDIMIENTO:** El procedimiento está delimitado por el proceso de creación, modificación y hasta el retiro de los usuarios para cumplir con actividades de administración de cuentas de usuarios asignados a funcionarios, contratistas y terceras partes para gestionar el ingreso seguro a los sistemas de información del Idartes

**1.3 RESPONSABLES DEL PROCEDIMIENTO:** 120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN

### 2. GLOSARIO:

- BACKUP: Copia de seguridad o respaldo de la información.
- CREDENCIAL DE AUTENTICACIÓN: Usuario y contraseña para ingresar a un aplicativo o servicio informático.
- CLAVE, CONTRASEÑA, PASSWORD: es la llave asignada por cada usuario para acceder a sus aplicaciones, la cual es personal e intransferible.
- GLPI: Herramienta que gestiona las incidencias o solicitudes de soporte de los usuarios de la entidad. Sus siglas, traducidas de francés a español, significan: Gestión Libre del Parque Informático.
- PLATAFORMA TECNOLÓGICA: Un conjunto de estándares, herramientas de hardware y software que apoyan el desarrollo de los procesos administrativos y misionales de la entidad.
- SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información adicionalmente pueden involucrarse otras propiedades, tales como: autenticidad, responsabilidad, no repudio y confiabilidad.
- USUARIO: Persona vinculada a la entidad, ya sea como funcionario o contratista.
- TIC: Tecnología de Información y Comunicaciones. Se denominan tecnologías de información y comunicaciones, al conjunto de tecnologías que permiten la adquisición, producción almacenamiento, tratamiento, comunicación, registros y presentación de informaciones contenidas en señales de naturaleza acústica (sonidos), óptica (imágenes) o electromagnética (datos alfanuméricos).
- Requerimiento: es una solicitud de soporte TI, sin que haya algún evento que esté interrumpiendo el servicio o reducción en la calidad de dicho servicio.
- Incidencia: Es toda interrupción o reducción de la calidad no planificada del servicio.
- Mesa de Servicios: Punto único de contacto dentro de la organización de TI, para los usuarios.
- Disponibilidad: La habilidad de un servicio de TI u otro elemento de configuración para realizar su función acordada cuando sea requerido.
- Base de datos de gestión de la configuración (CMDB): Base de datos utilizada para almacenar los registros de configuración a lo largo de su ciclo de vida. En la CMDB también se conservan las relaciones entre los registros de configuración.
- Experiencia del cliente (CX): Suma de las interacciones funcionales y emocionales con un servicio y un proveedor de servicios percibidas por el consumidor del servicio.
- Escalamiento: Acto de informar o transferir la propiedad de una problemática a un elemento de trabajo.



**GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**

Código: GTIC-PD-03

Fecha: 2021-11-12

**PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO**

Versión: 2

Página: 2 de 14

- Servicio: Medio para posibilitar la creación conjunta de valor al facilitar las consecuencias que los clientes desean obtener sin que estos asuman costos ni riesgos específicos.
- Práctica de mesa de servicio: Práctica que consiste en registrar peticiones para resolver incidentes y solicitudes de servicio.
- Acuerdo de niveles de servicio (SLA): Acuerdo documentado entre un proveedor de servicios y un cliente, en el que se especifican tanto los servicios requeridos como el nivel de servicio esperado.
- Equipo de soporte: Equipo que tiene la responsabilidad de mantener las operaciones habituales, gestionar las solicitudes de los usuarios, resolver incidentes y problemas relacionados con productos, servicios u otros elementos de configuración concretos.

**3. CONDICIONES GENERALES:**

Para gestionar la solicitud requerida es necesario que la entidad cuente con un herramienta de mesa de ayuda de incidentes tecnológicos.  
 Se requiere contar con un administrador de sistema de mesa de ayuda.  
 Se requiere contar con un administrador de las plataformas de cuentas de usuario.  
 Es necesario que el requerimiento provenga de usuarios con vinculación contractual con la entidad.

**4. RELACIÓN CON OTROS PROCEDIMIENTOS Y PROCESOS: Esquema gráfico de la relación del procedimiento con otros procedimientos y/o procesos del IDARTES.**

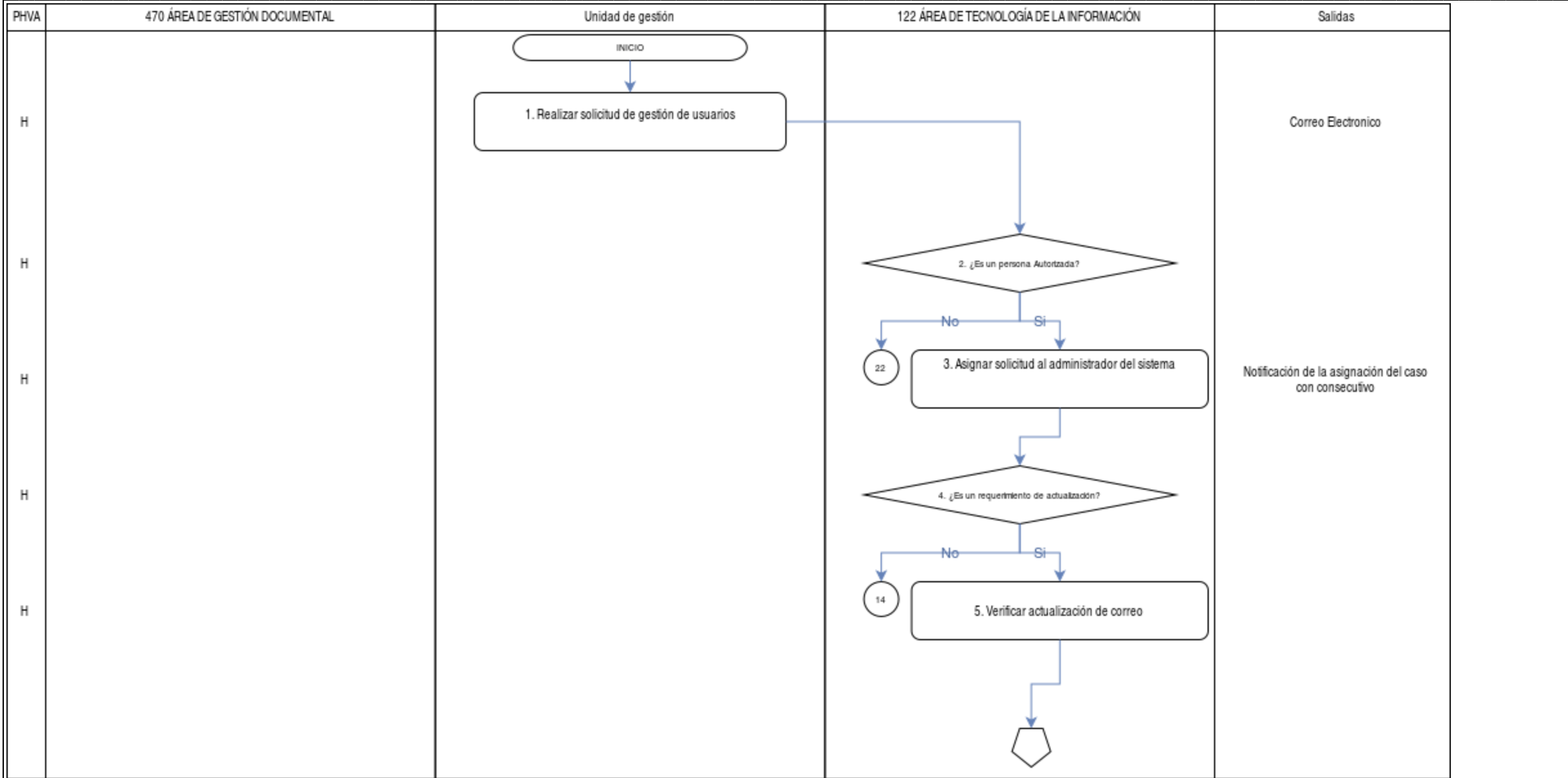
Procesos que se requieren como proveedor	Que insumos requiero del proveedor	Procedimiento	Que se obtiene del procedimiento	Para quien va dirigido el servicio o producto
<ul style="list-style-type: none"> <li>• TODAS LAS ÁREAS</li> </ul>	Solicitud de gestión de cuentas de usuario.	PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO	Credenciales de acceso para los diferentes sistemas solicitados.	<ul style="list-style-type: none"> <li>• TODAS LAS ÁREAS</li> </ul>

**5. ICONOGRAFÍA DEL DIAGRAMA DE FLUJO: Iconografía asociada al diagrama del flujo del procedimiento.**

**5.1 DIAGRAMA DE FLUJO: Secuencia lógica de las actividades establecidas en el procedimiento.**


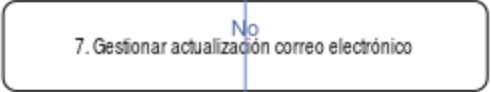
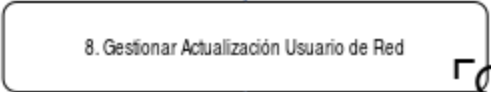
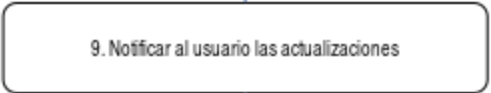



PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO



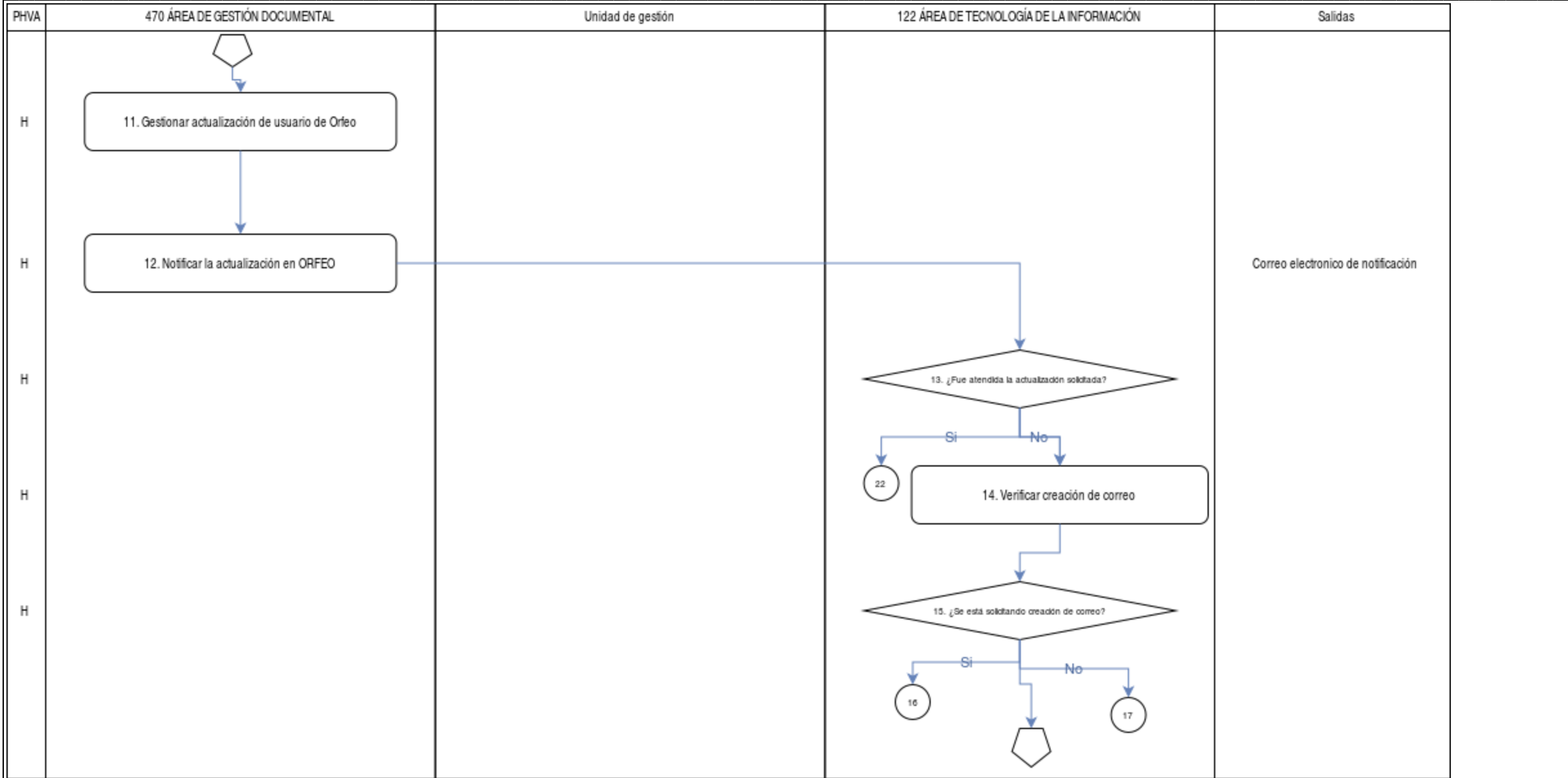


PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO

PHVA	470 ÁREA DE GESTIÓN DOCUMENTAL	Unidad de gestión	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Salidas
H				
H				
H				Base de datos actualizada de Directorio Activo
H				Correo electronico de notificación
H				Correo electronico de notificación mesa de ayuda

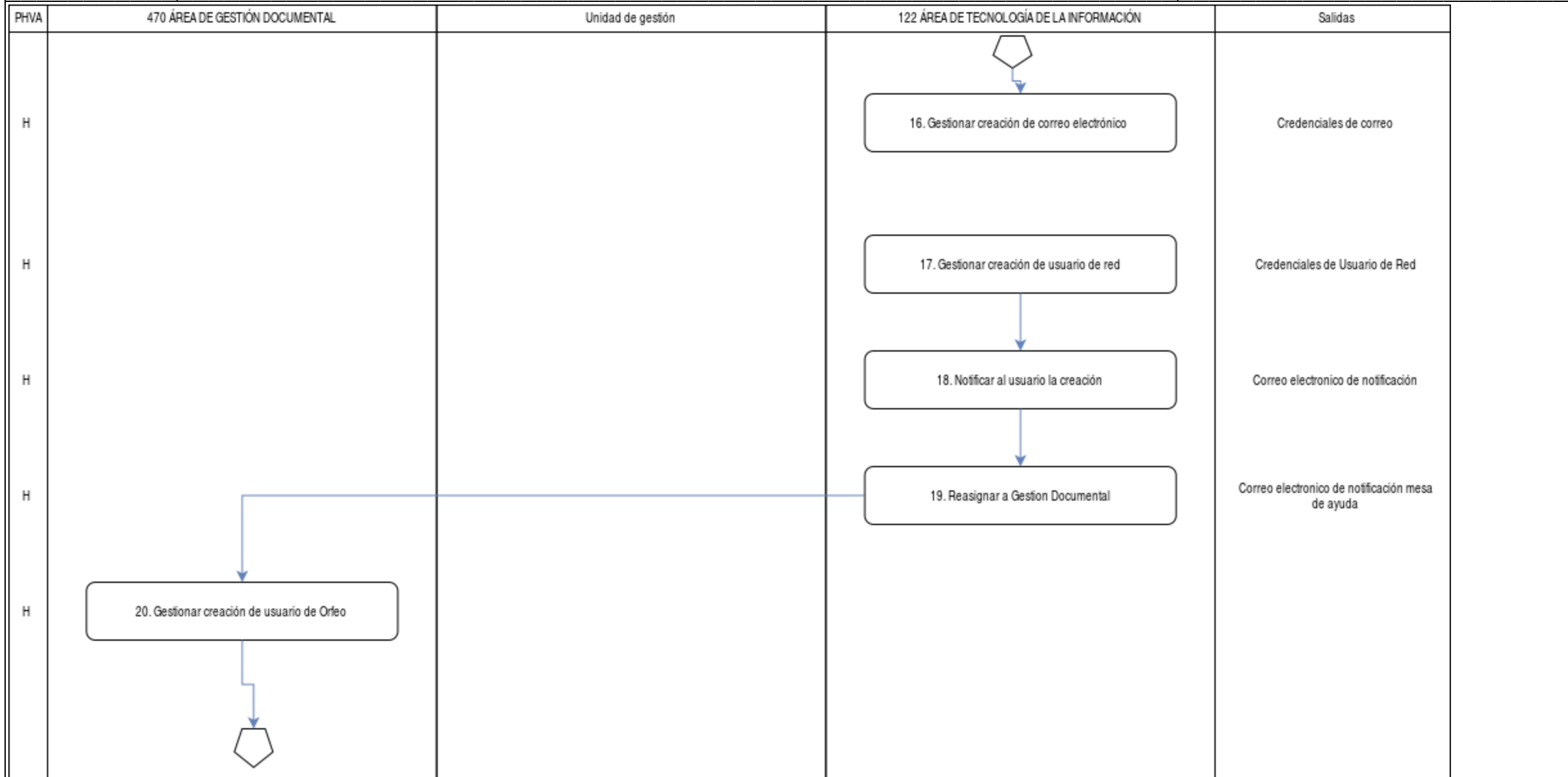


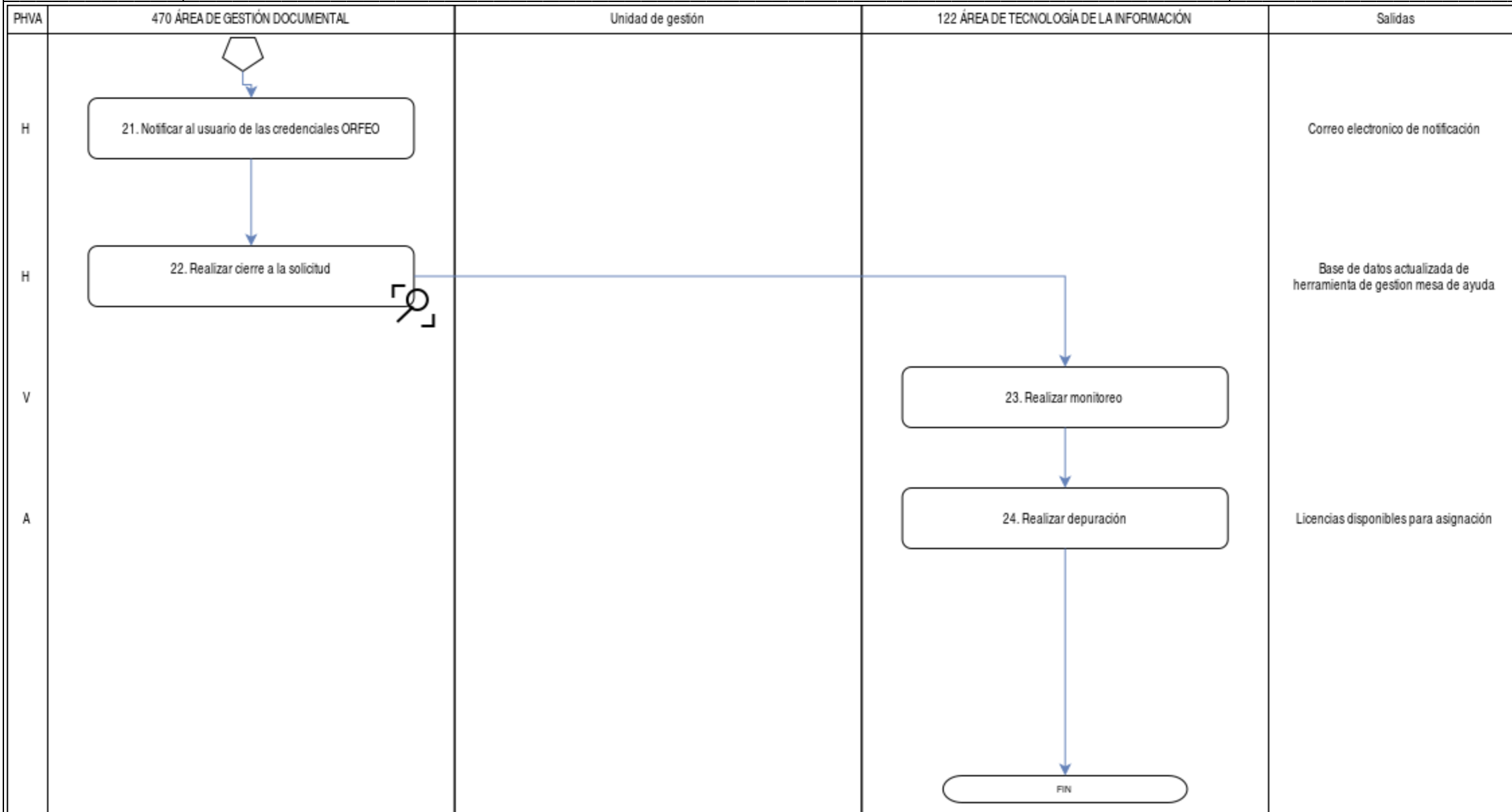
PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO





PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO





5.2. DESCRIPCIÓN DE LAS ACTIVIDADES: Características específicas de las actividades del procedimiento.

PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO

No.	Ciclo PHVA	Ciclo de Gestión	Descripción del Ciclo de Gestión	Actores	Responsable	Tiempo (Horas)	Documento o Registro
1	H	Realizar solicitud de gestión de usuarios	Diligenciamiento del formato digital de la solicitud de creación, modificación, inactivación o cancelación de acceso a usuario de red, correo electrónico, orfeo y de requerirse a sistemas de información; dicho formulario enviará de forma automatizada un registro al aplicativo de mesa de ayuda, por medio del correo soporte.sistemas@idartes.gov.co	Unidad de gestión	Jefe o Gerente de Dependencia, ó designado por él	1 día	Correo Electronico
2	H	¿Es un persona Autorizada?	Realiza validación, identificando si es una persona autorizada para realizar la solicitud.	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Administrador Mesa de Ayuda	1 hora	
3	H	Asignar solicitud al administrador del sistema	Validar la solicitud en la herramienta de mesa de ayuda GLPI y asignar conforme al formato inicial al personal responsable de crear, actualizar, suspender o eliminar la cuenta de usuario en red, correo, orfeo y/o sistema de informacion.	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Administrador Mesa de Ayuda	1 hora	Notificación de la asignación del caso con consecutivo
4	H	¿Es un requerimiento de actualización?	Determina si es un requerimiento para creación ó una actualización(Activación, Inactivación, Actualización).	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	
5	H	Verificar actualización de correo	Valida la existencia de la cuenta para generar la actualización de correo electrónico	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	
6	H	¿El usuario cuenta con correo electrónico creado?	Validar si el usuario cuenta con correo electrónico creado	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	
7	H	Gestionar actualización correo electrónico	Realiza actualización de la información del correo electronico.	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	
8	H	Gestionar Actualización Usuario de Red	Realiza actualización de la información del Usuario de Red	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	Base de datos actualizada de Directorio Activo
9	H	Notificar al usuario las actualizaciones	Una vez creadas las cuentas de usuario, se notifica vía correo electrónico al correo personal registrado en el formato inicial con las credenciales actualizadas en la OAP-TI	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	Correo electronico de notificación
10	H	Reasignar a Gestion Documental	Se reasigna solicitud a Gestion Documental, para atender Usuario de Orfeo	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	Correo electronico de notificación mesa de ayuda
11	H	Gestionar actualización de usuario de Orfeo	Conforme a la informacion del formato, se realiza la acción de actualización de credenciales de Usuario de Orfeo	470 ÁREA DE GESTIÓN DOCUMENTAL	ProfesionalDesignado Gestión Documental	1 hora	
12	H	Notificar la actualización en ORFEO	Una vez creadas las cuentas de usuario, se notifica vía correo electrónico al correo personal registrado en el formato inicial con la actualización realizada al usuario de ORFEO	470 ÁREA DE GESTIÓN DOCUMENTAL	Profesional Designado Gestión Documental	1 hora	Correo electronico de notificación
13	H	¿Fue atendida la actualización solicitada?	Validar si la solicitud de actualización fue atendida por el equipo de TI	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Administrador Mesa de Ayuda	1 hora	



**PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO**

14	H	Verificar creación de correo	Valida la información para generar la creación de correo electrónico	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	
15	H	¿Se está solicitando creación de correo?	Verificar el tipo de solicitud que está realizando el usuario	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	
16	H	Gestionar creación de correo electrónico	Conforme a la información del formato, se realiza la acción de creación de credenciales de correo electrónico	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	Credenciales de correo
17	H	Gestionar creación de usuario de red	Conforme a la información del formato, se realiza la acción de creación de credenciales de Usuario de Red	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	Credenciales de Usuario de Red
18	H	Notificar al usuario la creación	Una vez creadas las cuentas de usuario, se notifica vía correo electrónico con las credenciales creadas	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	4 horas	Correo electrónico de notificación
19	H	Reasignar a Gestion Documental	Se reasigna solicitud a Gestion Documental, para atender Usuario de Orfeo	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	1 hora	Correo electrónico de notificación mesa de ayuda
20	H	Gestionar creación de usuario de Orfeo	Conforme a la información del formato, se realiza la acción de creación de credenciales de Usuario de Orfeo	470 ÁREA DE GESTIÓN DOCUMENTAL	Profesional Gestión Documental	4 horas	
21	H	Notificar al usuario de las credenciales ORFEO	Una vez creadas las cuentas de usuario, se notifica vía correo electrónico con las credenciales de ORFEO	470 ÁREA DE GESTIÓN DOCUMENTAL	Profesional Gestión Documental	1 hora	Correo electrónico de notificación
22	H	Realizar cierre a la solicitud	Soluciona el ticket en la herramienta de Mesa de Ayuda de manera que el caso quede cerrado en el aplicativo.	470 ÁREA DE GESTIÓN DOCUMENTAL	Profesional Gestión Documental	1 hora	Base de datos actualizada de herramienta de gestión mesa de ayuda
23	V	Realizar monitoreo	Semanalmente se realiza un monitoreo del recurso de licenciamiento en la plataforma de correo electrónico, identificando cuentas en desuso	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	48 horas	
24	A	Realizar depuración	Se realiza depuración a las cuentas en desuso, con el objetivo de lograr disponibilidad constante del recurso.	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Profesional Designado de TI	48 horas	Licencias disponibles para asignación

**6. POLÍTICAS DE OPERACIÓN:**

Solo se crearan las credenciales al validar que el formato esta correctamente diligenciado y ha sido remitido por el personal autorizado y definido para esta acción

Toda solicitud de gestión de usuarios se le dará seguimiento a través de la herramienta de mesa de servicio GLPI

Ningún servidor público debe hacer uso de sus credenciales institucionales una vez terminado su contrato o vinculación laboral.

Una vez firmado el paz y salvo se deshabilitará el ingreso a todos los sistemas y los aplicativos que tenga acceso el usuario.

Toda entrega de credenciales debe estar sujeta a la aprobación del usuario de los acuerdos de confidencialidad y el compromiso de cumplimiento a la seguridad de la información.

1. Toda solicitud debe realizarse a través del formulario ubicado en un enlace en la intranet de la entidad, para la solicitud de creación, modificación, inactivación, cancelación de acceso a usuario de red, correo electrónico, sistemas de información, etc, dicho formulario enviará un correo de registro de forma automatizada al aplicativo de mesa de ayuda.

**PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO**

2. Para solicitudes masivas (3 o más personas) de creación de usuario de red, correo electrónico, sistemas de información, etc se deberá descargar el formato para solicitud masiva de creación de usuarios (archivo.xlsx), en la sección mapa de procesos, diligenciar todos sus campos, y nuevamente ser cargado al sitio web destinado para tal fin ó enviarse al correo soporte.sistemas@idartes.gov.co.

3. Las solicitudes de creación de usuario de red, correo electrónico, sistemas de información, etc para personal de planta serán realizadas por el Área de Talento Humano, y para el caso de los Contratistas será responsabilidad del Jefe de Área, Gerente, Subdirector o una persona quien sea designada por escrito al correo soporte.sistemas@idartes.gov.co para dicha actividad.

4. En situaciones especiales como permisos, incapacidades, adición de contrato, suspensión, reactivación o terminación anticipada de contrato o retiro del personal, será responsabilidad del Jefe de Área, Gerente, Subdirector o una persona quien sea designada por escrito al correo soporte.sistemas@idartes.gov.co para dicha actividad, informar la novedad enviando la solicitud de actualización de la información a la Oficina Asesora de Planeación y Tecnologías de la Información a través del formulario y será registrado automáticamente en la herramienta de mesa de ayuda de la Entidad.

Creación: Cuando se va a crear una solicitud para un funcionario nuevo y/o que no ha tenido contratos con el IDARTES.

Adición: Cuando se va a crear una solicitud para un funcionario con adición a su contrato.

Reactivación Terminación: Cuando se crea una solicitud para un funcionario que ya ha tenido contratos con el IDARTES, aplica para 60 días o menos.

Reactivación de una suspensión de contrato: Cuando se va a crear una solicitud para un funcionario que estaba en estado de contrato suspendido y regresa a realizar sus actividades nuevamente.

Suspensión de contrato: Cuando se va a crear una solicitud para desactivar temporalmente una cuenta de un usuario va a suspender contrato.

Terminación: Cuando se va a crear una solicitud para un usuario al que se le termina su contrato.

5. En situaciones como desvinculación laboral, y necesidad de actualización y retiro de los grupos de redistribución (ejemplo: carreraadministrativa@idartes.gov.co, plantapermanente@idartes.gov.co, plantatemporal@idartes.gov.co, etc), para el caso del personal de planta, será responsabilidad del Área de Talento Humano, informar y enviar la solicitud de actualización de la información a la Oficina Asesora de Planeación y Tecnologías de la Información por medio de un correo electrónico a soporte.sistemas@idartes.gov.co. Adicionalmente los grupos de distribución de las diferentes dependencias tendrán una persona con rol de administrador en cada subdirección, o gerencia, etc según la naturaleza de la misma, y a la que pertenezca el grupo, quien será encargado de ingresar o retirar miembros, según la necesidad; esto deberá ser informado a la Oficina Asesora de Planeación y Tecnologías de la Información por medio de un correo electrónico a soporte.sistemas@idartes.gov.co

6. Las cuentas de usuario de red, correo electrónico, sistemas de información, etc junto con las contraseñas que le son asignadas, son de carácter único, personal e intransferible y son consideradas como información privada, con las que se conforman las credenciales.

7. Las contraseñas asignadas por seguridad de la información contendrán las siguientes características:

Tiene una longitud mínima de ocho caracteres

No contiene el nombre de usuario, el nombre real ni el nombre de la empresa.

Es significativamente diferente de las anteriores contraseñas

Contiene letras mayúsculas, letras minúsculas, números y símbolos.

Suspender o bloquear permanentemente al usuario luego de 3 intentos para acceder al sistema con una contraseña incorrecta (deberá pedir solicitar la reactivación a la Oficina asesora de planeación y tecnologías de la información mediante correo a soporte.sistemas@idartes.gov.co)

8 Las cuentas de usuario pueden ser públicas, por lo tanto pueden ser usadas y almacenadas en aquellos repositorios que lo requieran. En contraposición las contraseñas son privadas, son de uso exclusivo del funcionario a quien le fue otorgada, no deben ser divulgadas, su almacenamiento solo debe ser permitido para los mecanismos que ejerzan los procesos de autenticación, que deben velar en todos los casos y por todos los medios posibles la reserva y no divulgación de dicha información.

9. Se realizará el uso de identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo usuario.

**PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO**

10. La mnemotecnia utilizada para definir las credenciales de usuario estará dada por el primer nombre, seguido por un punto (.) y su primer apellido. Si la cuenta ya existe, se agrega la letra inicial de su segundo apellido y en caso de mantenerse la igualdad se utilizará la inicial del segundo nombre de acuerdo al siguiente ejemplo:

Ejemplo para "Cristian Darío López Rátiva": cristian.lopez de existir un usuario con ese usuario previamente se utilizará: cristian.lopezr, de existir un usuario con ese usuario previamente se utilizará: cristiand.lopezr. y se realizará la secuencia hasta que ya no exista igualdad.

11. El uso de identificadores grupales solo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas y toda solicitud de credenciales que requiera nombres impersonales o estructuras especiales, debe ser solicitado y justificado a través del formulario de solicitud, y será responsabilidad del Jefe de Área, Gerente, Subdirector o una persona quien sea designada por escrito al correo soporte.sistemas@idartes.gov.co para dicha actividad, se creará bajo la siguiente estructura: Estará dada por dos palabras separadas por un punto (.). Ejemplo: gestion.documental

12. Las cuentas de correo electrónico que permanezcan en inactividad durante un periodo igual o mayor a 30 días serán suspendidas por el administrador de la plataforma de correos.

13. Se realizará el mantenimiento de un registro formal de todas las personas registradas para utilizar el servicio de la plataforma tecnológica, las cuentas de correo electrónico que permanezcan en estado de suspensión por un periodo igual o mayor a 60 días sin que se reciba solicitud de reactivación con relación contractual serán eliminadas por el administrador de la plataforma de correos.

14. Sin excepción alguna, las personas que no cuenten con relación contractual vigente con la entidad no podrán contar con el servicio de correo ni acceso a los servicios informáticos.

15. En casos que se vea comprometida la seguridad de la información, se podrá modificar las credenciales de una cuenta de usuario y esto a su vez, puede impedir el acceso de los servicios basados en las credenciales de red.

16. Se debe acceder con las credenciales de usuarios asignadas a los servicios de red únicamente para actividades institucionales.

17. Toda solicitud de credenciales que requiera permisos especiales de navegación ó acceso a almacenamiento, carpetas en red, etc debe ser solicitado de forma individual, autorizado por el Jefe de Área, Gerente, Subdirector o una persona quien sea designada y con la respectiva justificación enviada al correo electrónico soporte.sistemas@idartes.gov.co.

18. Ningún servidor público debe hacer uso del correo institucional una vez terminada su relación contractual.

19. Una vez firmado la paz y salvo se deshabilitará automáticamente el ingreso a todos los sistemas y los aplicativos que tenga acceso el usuario.

20. Revisión de los derechos de acceso de usuario. Se debe identificar y autenticar a cualquier usuario que, de manera local o remota, requiera utilizar los recursos tecnológicos del instituto distrital de las artes - Idartes, para lo cual se requiere contar con sistemas de seguridad que cumplan al menos con las siguientes características:

Cada usuario que requiera acceder a la plataforma tiene que identificarse y autenticarse antes de acceder a un recurso tecnológico a través de un usuario y una contraseña, y el usuario debe estar activo.

Una vez se han identificado y autenticado, los usuarios sólo podrán acceder a los recursos sobre los cuales están autorizados.

Debe quedar registro de los eventos de ingreso y autenticación de usuarios, para monitoreo de la Oficina asesora de planeación y tecnologías de la información.

21. Responsabilidades de usuario. El usuario deberá realizar todas las medidas a su alcance para evitar el acceso de usuarios no autorizados, evitar poner en peligro la información del instituto distrital de las artes - Idartes. El compromiso de los usuarios autorizados es fundamental para una seguridad efectiva. Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

22. Uso de contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, que constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a los servicios tecnológicos y de manejo de información de la entidad. Para esto se deben tener en cuenta los siguientes lineamientos:

Mantener las contraseñas en secreto.

Pedir el cambio de las contraseñas siempre que exista un posible indicio de amenaza que comprometa el sistema o la información.

Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas



## GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

**Código: GTIC-PD-03**

**Fecha: 2021-11-12**

## PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO

**Versión: 2**

**Página: 12 de 14**

Cambiar las contraseñas provisionales asignadas en el primer inicio de sesión ("log on").

Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se podrá utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

23. Se realizará la verificación del nivel de acceso otorgado coherente con la Plan de Seguridad y Privacidad de la Información de la entidad

19. Se ha establecido unos tiempos máximos de atención al requerimiento conforme a ANS

### 7. POSIBLES PRODUCTOS O SERVICIOS NO CONFORME:

Actividad	Producto y/o Servicio	Criterio de Aceptación	Corrección	Registro
8. Gestiona Actualización Usuario de Red: Realiza actualización de la información del Usuario de Red	Base de datos actualizada de Directorio Activo	Todos los usuarios de red en estado activo correspondientes a contratistas, deben tener una fecha de vencimiento alineada con la fecha de finalización de sus contratos.	Ajustar la fecha de vencimiento según la la fecha de finalización de sus contratos, la cual se corrobora contra el acta de inicio ó screenshot de secop.	Directorio Activo
22. Da cierre a la solicitud: Soluciona el ticket en la herramienta de Mesa de Ayuda de manera que el caso quede cerrado en el aplicativo.	Base de datos actualizada de herramienta de gestion mesa de ayuda	Todos los casos registrados en la herramienta de gestión de mesa de ayuda, que pasen a estado "Cerrado", deberán registrar una descripción de las acciones realizadas para darle solución al mismo.	Abrir nuevamente el caso, para solicitar el debido registro de las acciones realizadas para darle solución al mismo.	Herramienta de gestion de mesa de ayuda

### 8. DOCUMENTOS ASOCIADOS:

Los documentos asociados del presente procedimiento se pueden acceder a través del mapa de procesos

### 9. NORMATIVA ASOCIADA:

LEY 599 DE 24 JULIO 2000 Por la cual se expide el Código Penal. Título III capítulo séptimo de la violación a la intimidad, reserva e interceptación de comunicaciones. Art 192, 193, 194, 196 y 197.

ACUERDO 57 DE 2002 "Por el cual se dictan disposiciones Generales para la implementación del Sistema Distrital de Información SDI, se organiza la Comisión Distrital de Sistemas"

DECRETO 3816 de 2003 "Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública"

DIRECTIVA 5 de 2005 "Políticas Generales y directrices que orienten el desarrollo tecnológico"

DECRETO 619 de 2007 "Por el cual se establece la Estrategia de Gobierno Electrónico en el Distrito"

RESOLUCIÓN 305 de 2008 "Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre"

LEY 1273 DE 2009 Congreso de la República Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado ""de la protección de la información y de los datos"" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

DECRETO 235 DE 2010 Ministerio del Interior y Justicia Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

CONPES 3701 DE 2011 Conpes Lineamientos de política para la Ciberseguridad y Ciberdefensa



## GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Código: GTIC-PD-03

Fecha: 2021-11-12

## PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO

Versión: 2

Página: 13 de 14

LEY 1581 DE 2012 Congreso de la República Por el cual se dictan disposiciones generales para la protección de datos personales

DECRETO 2364 DE 2012 Ministerio del Interior y Justicia Por medio del cual se reglamenta el artículo 7 de la LEY 527 DE 1999, sobre la firma electrónica y se dictan otras disposiciones

DECRETO 19 DE 2012 Presidencia de Colombia Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública"

RESOLUCIÓN 396 DE 2012 Idartes Por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - IDARTES.

DECRETO 596 DE 2013 Alcaldía Mayor de Bogotá Por el cual se dictan medidas para la aplicación del Teletrabajo en organismos y entidades del Distrito Capital

LEY 1712 DE 2014 Congreso de la República Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones

RESOLUCIÓN 383 DE 2014 Idartes Por la cual se modifica la Resolución No 396 de 2012, "por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - IDARTES"

Conpes 3854 de 2016 Conpes Política Nacional de Seguridad Digital. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo

RESOLUCIÓN 3436 DE 2017: Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.

RESOLUCIÓN 4 DE 2017: Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas – CDS Por la cual se modifica la Resolución 305 de 2008 de la CDS

DECRETO 728 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de las zonas de acceso público a internet inalámbrico

DECRETO 1413 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales

RESOLUCIÓN 2710 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por la cual se establecen lineamientos para la adopción del protocolo IPv6

DECRETO 728 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno

CIRCULAR 30 DE 2017: Alta Consejería de Tics. Implementación CSIRT de Gobierno

CIRCULAR 36 DE 2017: Alta Consejería de Tics. Lineamientos de avance del modelo de seguridad y privacidad de la información

RESOLUCIÓN 3436 DE 2018: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.

DECRETO 612 DE 2018: Departamento Administrativo de la Función Pública. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

DECRETO 1008 DE 2018: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

CIRCULAR 2 DE 2018: Ministerio de Tecnologías de la Información y las Comunicaciones. Cumplimiento legal y normativo respecto a seguridad de la información.

CONPES 3920 DE 2018: Conpes Big Data, la política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.



## GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Código: GTIC-PD-03

Fecha: 2021-11-12

## PROCEDIMIENTO ADMINISTRACIÓN CUENTAS DE USUARIO

Versión: 2

Página: 14 de 14

LEY 1955 DEL 2019: Presidencia de Colombia. Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

DECRETO 2106 DE 2019: Departamento Administrativo De La Función Pública. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva

CONPES 3975 DE 2019: Conpes - Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.

DECRETO 620 DE 2020: Departamento Administrativo De La Función Pública. Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales

RESOLUCIÓN 0500 DE 2021. Ministerio De Tecnologías De La Información y las Comunicaciones. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

### 10. RECURSOS:

Recurso Humano

Sistema GLPI

Equipos de computo

Recursos de conectividad

Plataforma de correo

Plataforma de directorio activo

Recurso humano de administración de plataformas

Elaboró	Aprobó	Validó	Avaló	Código Verificación
OSCAR ALBERTO VARGAS CAMELO 2021-11-12 10:31:00	CARLOS ALFONSO GAITAN SANCHEZ 2021-11-12 12:31:15	AURORA CAMILA CRESPO MURILLO 2021-11-12 10:41:21	CARLOS ALFONSO GAITAN SANCHEZ 2021-11-12 12:32:51	