1. OBJETIVO

Establecer las actividades para la gestión de control de accesos a la plataforma tecnológica, software de aplicación y servicios de TI por funcionarios, contratistas, proveedores, pasantes y otras partes interesadas del Ministerio de Comercio, Industria y Turismo.

2. ALCANCE

Aplica a todos los procesos institucionales que cuenten con aplicativos, sistemas de información o software específico de apoyo a la gestión, así como los servicios para la gestión tecnológica a cargo de la Oficina de Sistemas de Información. Inicia con el requerimiento de solicitud de acceso a la plataforma tecnológica, servicios de TI y software de aplicación y finaliza con el cierre del requerimiento.

3. DEFINICIONES Y SIGLAS

CATÁLOGO DE SERVICIOS TI: Es un inventario detallado y documentado de los servicios de TI que la institución tiene implementados y que se encuentran activos, incluyendo los que están disponibles para ser desplegados. El catálogo de servicios de TI es el subconjunto del portafolio de servicios publicado para los usuarios. Definiciones del Marco de Referencia de Arquitectura Empresarial.

CONTRASEÑA: Medida de seguridad para restringir los nombres de inicio de sesión a cuentas de usuario y el acceso a los sistemas y recursos. Una contraseña es una cadena de caracteres, que hay que suministrar para obtener la autorización para un acceso o un nombre de inicio de sesión. Puede estar formada por letras, números y símbolos, y distingue mayúsculas de minúsculas.

CONTROL DE ACCESO: Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos (2.63) de negocio y de seguridad.

CUENTA DE USUARIO: Una cuenta de usuario es una asignación de dirección electrónica que está conformada por un nombre usuario, contraseña y dirección de correo electrónico.

MESA DE AYUDA: Herramienta virtual que permite el registro, asignación y cierre de solicitudes de soporte técnico mediante el uso de tickets asignados a cada requerimiento. CENTRO DE ATENCIÓN AL USUARIO - HELP DESK ITIL V3 (Operación del Servicio). Punto de contacto para Usuarios para registrar Incidentes, está normalmente más técnicamente focalizado que un Centro de Servicio al Usuario y no proporciona un Punto Único de Contacto. El término Centro de Atención al Usuario es a menudo usado como sinónimo del Centro de Servicio al Usuario.

SERVICIOS TECNOLÓGICOS: Es un caso particular de un servicio de TI que consiste en una facilidad directamente derivada de los recursos de la plataforma tecnológica (hardware y software) de del Ministerio de Comercio, Industria y Turismo. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos de calidad como disponibilidad, seguridad, confiabilidad, etc.

USUARIO DE EQUIPO: Persona que utiliza un equipo. Si el equipo está conectado a una red, un usuario puede tener acceso a los programas y archivos del equipo, así como a los programas y archivos que se encuentran en la red (en función de las restricciones de cuenta determinadas por el administrador de la red). En definitiva, es cualquier persona que precise o utilice un sistema de proceso de datos.

4. GENERALIDADES

4.1 NORMATIVIDAD

Normas consideradas en la ejecución del procedimiento:

- Resolución 990 de 2008. Reglamenta el Manejo, Uso y Registro de los elementos informáticos del Ministerio. Artículo 17. Asignación de Dirección Electrónica.
- Resolución 3892 de 2011. Modifica la Resolución 990 de 2008 en sus Artículos 17. Asignación de Dirección Electrónica y 22. Cancelación de Direcciones Electrónicas.
- Resolución 387 de 2012. Modifica parágrafo 1, Artículo 2. Asignación Dirección Electrónica y adiciona parágrafo 4 del Artículo 2 la Resolución 3892 de 2011.

4.2. GESTIÓN DE ACCESO A LOS SERVICIOS TI

La Gestión de Acceso a los Servicios TI es el proceso por el cual se brinda a los usuarios institucionales los permisos necesarios para hacer uso de los servicios tecnológicos, plataformas corporativas, aplicaciones y sitios web del Ministerio con la aplicación de los controles de seguridad informática y de ciberseguridad desde el otorgamiento hasta la derogación o retiro de los permisos de acceso con acorde con la función o labor del usuario.

Son parte de la Gestión de Acceso a los Servicios TI las actividades relacionadas con solicitud de acceso, verificación y monitoreo de los accesos.

1. Gestión de Accesos: Se realizada mediante correo o memorando electrónicos o solicitud de soporte técnico, adjuntándose el soporte pertinente y la información requerida para la creación, retiro, habilitación o deshabilitación de la cuenta de usuario, para el acceso a los servicios tecnológicos, plataformas corporativas, aplicaciones y sitios web del Ministerio. Los solicitantes pueden ser:

- El Grupo de Talento Humano de la Secretaría General para funcionarios nuevos y pasantes
- El Grupo de Contratos de la Secretaría General para personal contratista por prestación de servicios.
- Supervisores de Contratos de Proveedores de Servicios para prestadores de servicios y profesionales contratistas.
- Líderes de Procesos para funcionarios o contratistas en relación con aplicaciones o sistemas de información a las que requieran acceso.
- Coordinador de Desarrollo y Mantenimiento de Aplicaciones, como parte de la funcionalidad de los servicios de aplicación que conforman el Catálogo de Servicios de TI del Ministerio.
- Coordinador de Ingeniería y Soporte Técnico, como parte de la funcionalidad de los servicios de TI que conforman el Catálogo de Servicios de TI del Ministerio.

2. Verificación de accesos: Se realiza comprobación de la identidad del usuario institucional al momento de otorgar, retirar, habilitar o deshabilitar el acceso, mediante:

- Comprobar las motivaciones funcionales para otorgar el acceso pertinente a los usuarios.
- Comprobación en el DNS de los accesos mediante el mecanismo de autenticación cuenta de usuario versus contraseña.
- Remitir funcionario, Pasante, Contratista, Proveedor o Ingeniero encargado de aplicación o sistema de información el "usuario y contraseña genérica" para su registro por primera vez y cambio de contraseña.

- Confirmar de acuerdo con las funcionalidades de administración de usuarios en aplicativos y Sistemas de Información y demás servicios tecnológicos.

3. Monitorización de identidad de Usuarios Institucionales:

Mediante el seguimiento al registro y monitoreo de accesos, en relación con:

- Cambios en la asignación de permisos a usuarios institucionales ante retiro de la entidad, cambio de área funcional o cambio de perfil ante un aplicativo o sistema de información o sitio web o plataforma corporativa.
- Comprobación de la seguridad informática y ciberseguridad del usuario a través del monitoreo a la seguridad digital de la cuenta asociada al usuario institucional.

4.2.1. Cuenta de Usuario Institucional

Una cuenta de usuario es una asignación de dirección electrónica que está conformada por un nombre usuario, contraseña y dirección de correo electrónico, la cual se establece de acuerdo con el siguiente formato general xprimerapellido@dominio.gov.co donde X es la inicial del nombre y el dominio es el dominio institucional.

Las cuentas de usuario institucionales se crean asociadas a los dominios institucionales: www.mincit.gov.co, www.vuce.gov.co y mcomercio.gov.co.

El nombre de usuario y dirección de correo electrónico se conforman como se indica a continuación:

- Para funcionarios:

Formato	Usuario ejemplo	Asignación nombre de Usuario	dirección de correo electrónico
xprimerapellido	*Aura Lizarazo*	*alizarazo*	*alizarazo@mincit.gov.co*
xprimerapellido	*Tadeo Niño Perez*	*tninop*	*tninop@mincit.gov.co*

- Para Pasantes, Contratistas:

Formato	Usuario ejemplo	Asignación nombre de Usuario	dirección de correo electrónico
xprimerapellido-pasante	*Aura Lizarazo*	*alizarazo-pasante*	*Alizarazo-pasante@mincit.gov.co*
xprimerapellido-Cont	*Tadeo Niño Perez*	*tninop- Cont*	*Tninop-Cont@mincit.gov.co*

- Para Servicios de aplicación o sistemas de información y Servicios TI:

Tipo	Funcionalidad	Asignación nombre de Usuario	dirección de correo electrónico
Aplicación o Sistema de Información	*Encuestas*	*encuestas*	*encuestas@mincit.gov.co*
Servicio Tecnológico	*Mesa de Ayuda*	*Soporte Tecnico Sistemas*	*soportetecnico@mincit.gov.co*
Servicio Tecnológico	*Notificación Radiación*	*radicacion*	*radicacion@vuce.gov.co*
Servicio Tecnológico	*Notificaciones Noticias*	*notificaciones*	*notificaciones@mcomercio.gov.co*

4.2.2. Gestión de Usuarios y Contraseñas

La Gestión de Contraseñas tiene como propósito el control informático de acceso a los servicios de TI, aplicaciones y sistemas de información por parte de un usuario (funcionarios, pasantes, contratistas, proveedores o encargado de un servicio TI).

A. DNS - Administrador de Dominio - Control de Usuarios y Contraseñas

Por medio del DNS se controla la asignación de cuentas de usuario, registro de contraseña y vigencia de estas, teniendo en cuenta las siguientes condiciones:

a. La contraseña inicial, es una "contraseña genérica", con una vida útil de 12 horas, tiempo en el cual el destinatario de la cuenta deberá autenticarse y cambiar la "contraseña genérica", por la "contraseña personal", de conocimiento solo del usuario (funcionarios, pasantes, contratistas, proveedores o encargado de un servicio TI) y bajo su responsabilidad está el uso de esta.

b. La estructura de la contraseña personal deberá cumplir con los siguientes requisitos:
- No tener nombres ni apellidos o el nombre de la cuenta.
- No tener su número de cédula o documento de identificación del usuario.
- Debe contener mínimo 8 caracteres
- Tener al menos una letra mayúscula
- Un símbolo ya sea: -, * & % / #

c. La vigencia de la contraseña personal, es de 90 días calendario.

d. El cambio de contraseña se informa automáticamente al usuario con 10 días de antelación a su vencimiento, a través del servicio de notificaciones de Windows o al momento de autenticarse en la red.

e. El restablecimiento o habilitación de la contraseña personal por bloqueo de la misma, deberá ser informada por el usuario a Mesa de Ayuda a través del correo soportetecnico@mincit.gov.co.

B. Sistemas de Información y Aplicaciones - Control de Contraseñas

a. Acceso a sistemas de información y aplicaciones con autenticación DNS

Los usuarios con acceso a sistemas de información o aplicaciones con la funcionalidad de autenticación contra el DNS - Controlador de Dominio y que se encuentren conectados a la red institucional, no requieren doble autenticación; los accesos a través de redes externas requieren realizar doble autenticación, con el usuario y contraseña con el fin de validar el ingreso y usuarios ante el DNS.

b. Acceso a sistemas de información y aplicaciones sin autenticación DNS

Para los sistemas de información o aplicaciones que cuentan con administración de usuarios y contraseñas propios, el usuario previamente registrado ante la aplicación o sistema de información realiza la solicitud de contraseña registrando el correo electrónico al cual se le notifica a través del correo notificaciones@mincit.gov.co informando la Contraseña de 6 dígitos conformada por letras y números o un enlace donde podrá ingresar la nueva contraseña y confirmarla.

c. Infraestructura Tecnológica - Control de Contraseñas

El equipo de Infraestructura Tecnológica (proveedor) que hace uso de los usuarios y cuentas de correo asignados por el Grupo de Ingeniería y Soporte para la administración de servidores, consolas de administración y dispositivos de red.Los Usuarios y Contraseñas de Servicios Tecnológicos de Proveedores (ejemplo: Proveedores de Canales de Internet, Appliance para servicios de administración de redes, entre otros), son gestionadas por el Proveedor, previa confirmación del responsable y datos institucionales de contacto.

d. Monitoreo Plataforma Tecnológica - Control de Contraseñas

El equipo de Monitoreo de Plataforma Tecnológica (proveedor) hace uso de los usuarios y cuentas de correo asignados por el Grupo de Ingeniería y Soporte Técnico para la administración de equipos de seguridad de la entidad. Los Usuarios y Contraseñas de Servicios Tecnológicos de Proveedores (ejemplo: Proveedores de Appliance para el monitoreo de seguridad digital de la infraestructura tecnológica, entre otros), son gestionadas por el Proveedor, previa confirmación del responsable y datos institucionales de contacto.

e. Proveedores de Mantenimiento de Servicios de Soporte - Control de Contraseñas

El Grupo de Ingeniería y Soporte Técnico asignará los usuarios y cuentas de correo requeridos por el proveedor para la administración de equipos de administración de la Planta Eléctrica y Aires Acondicionados.

4.3. ROLES Y RESPONSABILIDADES DE LA GESTIÓN DE ACCESO A LOS SERVICIOS TI

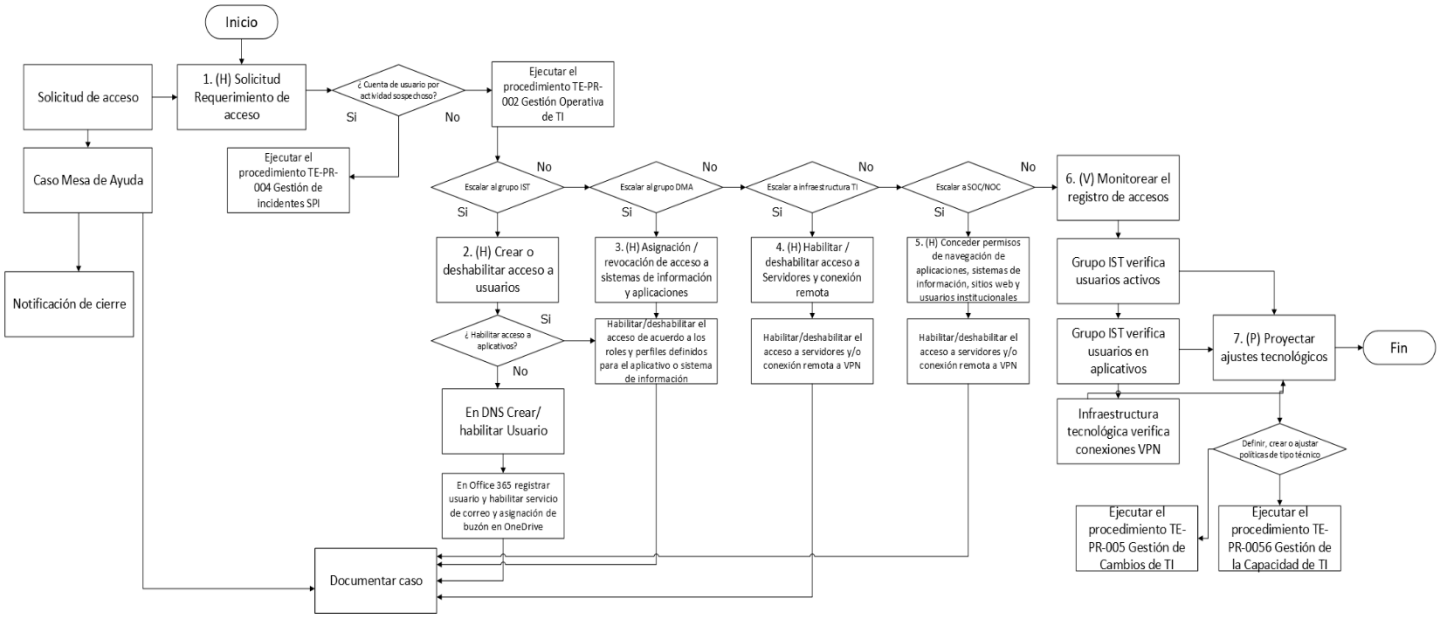
ROLES R – Responsible - Responsable / Encargado A – Accountable - Aprobador C – Consulted - Consultado I - Informed - Informado		Actividades																											
RESPONSABLES		1 (H) Solicitud Requerimiento de acceso				2 (H) Crear o deshabilitar acceso a usuarios				3 (H) Asignación / revocación de acceso a sistemas de información y aplicaciones				4 (H) Habilitar / deshabilitar acceso a Servidores y conexión remota				5 (H) Conceder permisos de navegación de aplicaciones y sistemas de información				6 (V) Monitorear el registro de accesos				7 (P) Proyectar ajustes tecnológicas			
Funcionario Grupo Talento Humano		R							I																				
Funcionario Grupo Contratos		R							I																				
Supervisores		R							I																				
Jefe Oficina de Sistemas de Información		R																A								A		I
Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones		R		C	I			C	I	R	A				A	C			A	C	I	R		I	R		C	
Coordinador Grupo Ingeniería y Soporte Técnico		R		C	I	R	A	C				C				C			A	C	I	R		I	R		C	
Profesional TI (Gestor Sistema Información o Aplicativo)									I				I																
Personal Tercerizado	Soporte Técnico Mesa de Ayuda	R			I			C														R		I	R		C	
	Monitoreo SOC/NOC	R			I			C					I			C	I	R	A			R		I	R		C	
	Infraestructura Tecnológica	R			I			C					I	R			I					R		I	R		C	

4.4 RIESGOS

- Los riesgos del proceso se encuentran documentados en la matriz de riesgos institucionales.
- Los controles aplicables a cada riesgo se relacionan en las actividades descritas en los documentos y se identifican por medio del código del control.

5. DIAGRAMA DE FLUJO

(A continuación se visualiza de manera gráfica y secuencial las actividades descritas en el numeral 6)



6. DESCRIPCIÓN DE ACTIVIDADES

(A continuación se detallan las actividades graficadas en el numeral 5)

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
1		Jefe Oficina de Sistemas de Información, Coordinador (a) Grupo de Contratos, Jefe Inmediato o Supervisor del contrato., Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico, Personal Tercerizado.	Registrar la solicitud de acceso se realiza en la Mesa de Ayuda por medio de: - Mintranet> Servicios> Soporte Técnico (http://helpdesk.mincit.gov.co/ASDKV8/Login.aspx) - Correo electrónico soportetecnico@mincit.gov.co - Comunicándose a la extensión número 2291 La herramienta Mesa de Ayuda genera automáticamente un número de CASO para requerimiento. En ejecución del procedimiento Gestión Operativa de TI, el Analista de Soporte Técnico, revisa la información del requerimiento para determinar el tipo de requerimiento:	Registro de Caso en la Herramienta de Mesa de Ayuda

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
	(H) Solicitud Requerimiento de acceso		Si corresponde a un evento relacionado con una cuenta de usuario por actividad sospechosa, escala a SOC/NOC para que ejecute el procedimiento Gestión de Incidentes de Seguridad y Privacidad de la Información. Ir actividad 2. Sí corresponde a un requerimiento de solicitud de acceso, escala en el Grupo Ingeniería y Soporte Técnico - Meso de Ayuda para acceso a la red, correo electrónico, plataformas corporativas y/o aplicaciones o sitios web en producción. Ir actividad 3. Sí corresponde al Grupo Desarrollo y Mantenimiento de Aplicaciones para acceso a los aplicativos y Sistemas de Información conforme a los roles y perfiles definidos. Ir actividad 4. Sí corresponde al Equipo de Infraestructura Tecnológica para el acceso a servidor de datos, servidores de desarrollo, producción, consolas de administración, accesos remotos a través de VPN. Ir actividad 5. Sí corresponde al Equipo de Monitoreo y Seguridad Perimetral para la navegación a internet y accesos remotos a través de VPN a servicios de aplicaciones, sistemas de información, sitios web y usuarios institucionales. **Tiempo:** Permanente **Control GTI-R4,** **Control GTI-RC-12**	
2	(H) Crear o deshabilitar acceso a usuarios	Coordinador Grupo Ingeniería y Soporte Técnico, Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Profesional Designado, Profesional Especializado, Personal Tercerizado.	Proceder a: i. En la Consola del DNS - Directorio Activo, crear el usuario nuevo o inhabilitar usuario si es retirado. ii. En la Consola de Office 365, registrar el usuario y habilitar el servicio de correo y asignación de buzón en OneDrive del Ministerio. iii. Para aplicaciones, sistemas de información y sitios web del Catálogo de Servicios de TI, coordinar con el Ingeniero (Gestor Sistema Información o Aplicativo) encargado en el Grupo Desarrollo y Mantenimiento de Aplicaciones para habilitar el acceso al usuario solicitante. Ir actividad 3. **Tiempo:** Permanente	Herramienta Mesa de Ayuda
3	(H) Asignación / revocación de acceso a sistemas de información y aplicaciones	Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico, Personal Tercerizado., Profesional Universitario, Profesional Designado,	Coordinar con el Ingeniero - gestor para crear, eliminar, habilitar/deshabilitar el acceso de acuerdo con los roles y perfiles definidos para el aplicativo o sistema de información o sitio web. **Tiempo:** Permanente	Herramienta Mesa de Ayuda

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
		Profesional Especializado		
4	(H) Habilitar / deshabilitar acceso a Servidores y conexión remota	Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico, Profesional Designado, Profesional Especializado, Personal Tercerizado.	Proceder a verificar el alcance del acceso y/o conexión remota i. Habilitar o deshabilitar el acceso a servidores y/o conexión remota requerida por el Grupo Desarrollo y Mantenimiento de Aplicaciones y Proveedores de Desarrollo o a los usuarios que requieren acceso a servidores de datos. ii. Habilitar o deshabilitar el acceso a VPN. **Tiempo:** Permanente	Herramienta Mesa de Ayuda
5	(H) Conceder permisos de navegación de aplicaciones, sistemas de información, sitios web y usuarios institucionales	Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico, Personal Tercerizado.	Proceder de acuerdo con las indicaciones del: i. Coordinador del Grupo de Desarrollo y Mantenimiento de Aplicaciones: - Registrar en los equipos de seguridad perimetral la URL y habilitar IP pública para la navegación a internet del servicio de aplicación, sistemas de información y sitios web, acceso remotos y VPN. - Validar en los equipos de seguridad las permisos y restricciones para cada caso. ii. Coordinador con Ingeniería y Soporte Técnico. - Si se requiere ajuste a las políticas de seguridad informática y de ciberseguridad implementadas para el acceso a servicios tecnológicos. - Aplicar ajuste a las políticas para habilitar o retirar/inhabilitar el acceso de acuerdo con los roles y perfiles de navegación de servicios tecnológicos y de usuarios institucionales. **Tiempo:** Permanente	Herramienta Mesa de Ayuda
6	(V) Monitorear el registro de accesos	Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico, Personal Tercerizado.	Realizar el seguimiento periódico a usuarios - permisos y revocación de acceso de la siguiente manera: i. Grupo de Ingeniería y Soporte Técnico Realiza el monitoreo de los usuarios que no presenten actividad mayor a un (1) mes, verifica se encuentran activos como funcionarios, pasantes o contratistas y procede a deshabilitarlos del DNS y deshabilitar el uso de la plataforma corporativa. ii. Grupo de Desarrollo y Mantenimiento de Aplicaciones El Ingeniero - gestor encargado del aplicativo o sistema de información o sitio web verifica que los usuarios - funcionarios, pasantes o contratistas - se encuentran habilitados de acuerdo con el perfil asignado y cuenten con los permisos para la captura, consultan, modificación o eliminación y almacenamiento.	Reporte

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
			iii. Infraestructura Tecnológica Realiza el monitoreo de la actividad de servicios de aplicaciones, servicios tecnológicos y servicios de conexión remota, determina que servicios requieren ser verificados con Grupo de Ingeniería y Soporte Técnico y Grupo Desarrollo y Mantenimiento de Aplicaciones para establecer los servicios que deben ser deshabilitados. iv. Monitoreo y Seguridad Perimetral Realiza el monitoreo de la actividad de navegación y conexión remota de servicios de los servicios tecnológicos, usuarios institucionales acorde con el perfil de navegación. **Tiempo:** Permanente **Control GTI-R4** **Control RC-12**	
7	(P) Proyectar ajustes tecnológicos	Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones., Coordinador Grupo Ingeniería y Soporte Técnico, Personal Tercerizado.	Determinar las acciones pertinentes que orienten la gestión de los requerimientos de acceso de usuarios institucionales o servicios de aplicación, sistemas de información, sitios web o servicios tecnológicos, a través del procedimiento TE-PR-005 Gestión de Cambios de Tecnologías de la Información. Definir, crear o ajustar políticas de tipo técnico o de incorporación de nuevas tecnologías o plataformas corporativas que requieran implementar institucionalmente el control informático de acceso. **Tiempo:** Permanente	TE-FM-013 Gestión de Cambios

7. FORMATOS DEL PROCEDIMIENTO

No.	CODIGO	NOMBRE DEL FORMATO
1	No aplica	Registro de Caso en la Herramienta de Mesa de Ayuda
2	TE-FM-013	Gestión de Cambios

8. HISTORIAL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
12/06/2026	0	Primera versión del documento para el nuevo Mapa de procesos. Código anterior: GTI-PR-014. V02. Para efectos de trazabilidad y soporte de la migración al nuevo aplicativo de administración de la documentación del Modelo Institucional de Operación (MIO), los siguientes fueron los responsables de la revisión y aprobación del documento migrado: REVISÓ: MARIA DEL ROSARIO CHACÓN Cargo: Profesional especializado OSI APROBÓ: IVÓN CAROLINA RODRIGUEZ Cargo: Jefe OSI Desde la OAPS se asegura que el contenido corresponde a la última versión vigente en ISOlución al momento de la migración a MIOsoft.

9. FLUJO DE APROBACIÓN

ELABORÓ		APOYO OAPS		REVISÓ		APROBÓ	
Nombre:		Nombre:	Jefferson López Saavedra	Nombre:		Nombre:	
Cargo:		Cargo:	Profesional Especializado	Cargo:		Cargo:	