1. OBJETIVO

Controlar el acceso de usuarios a las plataformas tecnológicas, soluciones tecnológicas y/o redes de comunicaciones de la UAE DIAN, para preservar la disponibilidad, integridad y confidencialidad de la información de la Entidad.

2. ALCANCE

Inicia con la recepción de la solicitud de acceso y/o inactivación de usuarios y/o roles de las plataformas tecnológicas, soluciones tecnológicas y/o redes de comunicaciones, se realiza verificación y gestión de la solicitud a través de la herramienta de mesa de servicio y finaliza con la asignación o inactivación del usuario y/o rol solicitado y monitorización del acceso otorgado.

3. CONDICIONES GENERALES

La Gestión de accesos involucra a todos los usuarios internos de la UAE DIAN, contratistas, proveedores, entes de control y terceros, que requieran acceder a la información, instalaciones de procesamiento de información y/o a la información disponible en la infraestructura tecnológica de la Entidad.

La Subdirección de Soluciones y Desarrollo realiza revisión de manera trimestral de las actividades ejecutadas por la Coordinación de Soporte Técnico al Usuario para la creación e inactivación de usuarios y roles con el fin de identificar oportunidades de mejora en el proceso.

3.1 Usuarios y contraseñas

- Se debe cumplir con las políticas emitidas por la Oficina de Seguridad de la Información o quien haga sus veces, para minimizar los riesgos en materia de seguridad de la información y para garantizar la disponibilidad, integridad, confidencialidad, privacidad y no repudio de la información.

- Las credenciales de autenticación de usuario son personales e intransferibles, estas ofrecen garantía y trazabilidad en el acceso y/o modificación de la información contenida en las bases de datos y/o soluciones tecnológicas.

- Las contraseñas asignadas a los servidores públicos de la UAE DIAN deben ser cambiadas periódicamente y memorizadas o almacenadas en aplicaciones de gestión de contraseñas, se debe evitar escribirlas en papel ya que esto aumenta el riesgo de ser vulneradas.

- Todos y cada uno de los servidores públicos de la UAE DIAN, contratistas, proveedores, entes de control y terceros, son responsables administrativamente, disciplinariamente y/o penalmente por el uso que se haga de sus credenciales de autenticación en cualquier aplicación, sistema, base de datos, entre otros.

- Las contraseñas son auto gestionadas por el usuario en el momento en que se habilita el acceso, para lo cual debe realizar el cambio de las mismas en el primer inicio de sesión o posterior a un restablecimiento solicitado por el usuario.

- Las solicitudes de restablecimiento de contraseña de dominio deben ser registradas por el jefe inmediato, superior jerárquico, líder informático o asistencial del área, el cual debe contener el nombre y usuario de red del colaborador de la UAE DIAN que requiere dicho servicio.

- Cuando se adquiere software desarrollado por un tercero, una vez es instalado y configurado en la red interna de la entidad, el administrador y/o supervisor del contrato debe modificar la información de autenticación predeterminada por el proveedor.

- Los accesos concedidos a los usuarios de las soluciones tecnológicas garantizan la trazabilidad completa de las acciones realizadas por ellos, para posteriores investigaciones o procesos de auditoría. Esta trazabilidad queda registrada en los logs transaccionales, los cuales se consultan y controlan a través del acceso a las bases de datos y/o soluciones tecnológicas.

- Toda cuenta debe ser nombrada y asignada a un único usuario responsable, por lo cual no es permitido el uso de cuentas genéricas.

- Las solicitudes de restablecimiento de contraseña de roles tecnológicos se deben realizar por la herramienta de gestión de la mesa de servicio. Estas solicitudes las puede realizar el usuario o su jefe inmediato, indicando la cuenta de usuario de ingreso a la solución tecnológica y el número de cédula.

- La Dirección de Gestión, Innovación y Tecnología implementa mecanismos de doble factor de autenticación en las soluciones tecnológicas, con el fin de preservar la integridad y el no repudio sobre los mismos.

- La Subdirección de Soluciones y Desarrollo cuenta con la posibilidad de crear usuarios de dominio y cuentas de correo electrónico a través de la mesa de servicio, para lo cual la Subdirección de Infraestructura Tecnológica y Operaciones crea los permisos requeridos sobre dichas plataformas, así mismo adelanta seguimiento y control diario de las cuentas asignadas.

- Para la gestión (custodia, uso, actualización de contraseña, monitoreo, entre otros) de usuarios privilegiados se realiza de acuerdo con lo definido en el anexo protocolo para manejo de cuentas de usuario privilegiadas.

3.1.1. Uso de contraseñas.

La generación, asignación y manejo de contraseñas sobre las soluciones tecnológicas y/o bases de datos institucionales se debe realizar de acuerdo con las siguientes recomendaciones:

- La contraseña debe ser alfanumérica, es decir debe contener mínimo una mayúscula, una minúscula y un carácter especial (! , _ ? $ % &).
- La longitud de la contraseña debe ser de mínimo 8 caracteres.
- No deben utilizarse contraseñas genéricas y deben ser de fácil recordación para el usuario.
- Cada colaborador de la Entidad debe realizar el cambio de contraseña cada 60 días, el cual podrá ser de manera automatizada.
- No dejar expuesta la contraseña a personal ajeno.
- La contraseña es de uso personal e intransferible.

3.2 Novedades administrativas

- La Subdirección de Gestión del Empleo Público, la división Talento Humano y/o el GIT de Talento Humano o quien haga sus veces en el nivel local, deben reportar a través de la herramienta de mesa de servicio, cada vez que se presente una novedad administrativa de los servidores públicos de la Entidad, que implique la separación de funciones por un tiempo mayor o igual a 15 días calendario, la vinculación a la Entidad y/o cambios de dependencia, con el fin de otorgar o retirar los accesos y roles a las soluciones tecnológicas y/o bases de datos institucionales de manera oportuna.

- La Subdirección de Gestión del Empleo Público debe generar y remitir un reporte mensual a la Coordinación de Soporte Técnico al Usuario en donde se registre los datos básicos y fechas de las personas que presentaron novedades administrativas iguales o superiores a 15 días calendario, como: vacaciones, licencias, incapacidad, retiro, comisiones, entre otros, durante el mes previo, con el fin de mantener revisión y control posterior del proceso de activación e inactivación de usuarios y/o roles.

- La Subdirección de Gestión del Empleo Público con acompañamiento de la Subdirección de Soluciones y Desarrollo efectúa las gestiones necesarias con el proveedor de la solución tecnológica de administración de planta de personal, con el fin de implementar procesos automatizados con las plataformas Muisca y SIAT para la gestión de usuarios y roles.

3.2 Roles de soluciones tecnológicas

- Cuando se presente alguna situación administrativa como traslado de área, encargo, comisión, vacaciones, licencia, entre otras, de un usuario que tenga asignado(s) rol(es) de soluciones tecnológicas en plataforma Muisca y no son inactivados por la solución tecnológica de la Administración de Planta de Personal, la Subdirección de Gestión del Empleo Público, la división Talento Humano y/o el GIT de Talento Humano o quien haga sus veces en el nivel local, debe reportar dicha novedad a través de la herramienta de mesa de servicio, anexando el acto administrativo correspondiente, con el fin de que se realice la inactivación de el/los rol(es) asignado(s) hasta el momento del reintegro del servidor público. Para el caso de los Directores de Gestión y Directores Seccionales se debe prever la gestión de la solicitud de inactivación de sus roles y de sus Subdirectores y/o Jefes de División.

- Cuando se presente prorroga y/o terminación anticipada de contratos de prestación de servicios el supervisor del contrato debe reportar dicha novedad a través de la herramienta de mesa de servicio, anexando el acta de terminación u otrosí del contrato, con el fin de que se realice la extensión o inactivación del (los) rol(es) asignado(s) según corresponda.

- La Subdirección de Compras y Contratos debe reportar por correo electrónico a la Coordinación de Soporte Técnico al Usuario cada vez que se designe un supervisor para contratos de prestación de servicios.

- El rol de la solución tecnológica estará activo siempre que el usuario mantenga las condiciones iniciales que dieron origen a la asignación, en caso de presentarse reasignación de actividades en la misma dependencia el Jefe Inmediato debe solicitar su inactivación y asignación de nuevos roles.

- Previo a la asignación de los accesos privilegiados se deberá contar con la plena identificación del servidor o usuario, para corroborar la idoneidad del ejercicio de las funciones a su cargo, las

necesidades del acceso con relación a las actividades fijadas, su ubicación y demás funciones asignadas, así mismo, se debe validar en la base de datos de acuerdos de confidencialidad de la OSI que el servidor público este registrado. Los accesos privilegiados deben revisarse mensualmente por parte de la Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, para identificar cambios y privilegios no autorizados de acuerdo con las competencias del cargo.

- Los accesos privilegiados deben asignarse a un usuario de red diferente de los utilizados para las actividades misionales de la entidad.

- Cada usuario es responsable del manejo y confidencialidad de la información de acuerdo con el acceso concedido.

- Los servidores públicos deben usar diferentes perfiles de usuario para los ambientes de producción y los ambientes de prueba.

- Cada usuario es responsable de verificar los roles que tiene activos en el documento "Roles activos usuarios DIAN", así como reportar oportunamente a su jefe inmediato cualquier tipo de inconsistencia. De igual forma, debe garantizar que solo tiene activos los roles necesarios para el desempeño de sus labores asignadas.

- Como parte del cierre de una solución tecnológica (Sistema de Información) en producción, el responsable funcional debe registrar caso a través de la herramienta de gestión de la mesa de servicio informando la inactivación de la misma, esto con el fin de que se inactiven los roles de todos los funcionarios y/o contratistas activos, así mismo, se debe indicar si se mantendrán roles de consulta y las personas a las que les persistirá dichos roles.

- Para los Directores de Gestión, Directores Seccionales, Subdirectores, Jefes de División, y/o Coordinadores se asignan los roles en las soluciones tecnológicas y/o bases de datos de acuerdo con lo definido en el anexo matriz de roles y cargos.

- Cuando se detecte alguna irregularidad en los roles asignados a un usuario, la Subdirección de Gestión del Empleo Público, la división Talento Humano y/o el GIT de Talento Humano o quien haga sus veces en el nivel local o la Oficina de Seguridad de la Información – OSI o quien haga sus veces, podrán solicitar la inactivación de los roles que no estén debidamente autorizados o que no correspondan a funciones propias del cargo que desempeña a través de la herramienta de gestión de la mesa de servicio.

- Cuando se requiera la recolección de información con ocasión de requerimientos, visitas, inspecciones y demás actividades desarrolladas por entes externos de control, en ejercicio de la función de control externo, esta información será entregada directamente por el dueño y/o responsable del activo de información previa validación del jefe inmediato de la dependencia. Solo en casos excepcionales, en los que sea indispensable el acceso directo a las soluciones tecnológicas de la Entidad, se crearán cuentas de usuario y se asignarán roles exclusivamente de consulta en las aplicaciones o infraestructuras para los entes externos que realicen este tipo de actividades, la vigencia de las mismas será igual al periodo de las investigaciones y/o auditorías que se vayan a realizar; estas solicitudes deberán ser firmadas por el ente externo, llevar un aval del jefe inmediato responsable del activo de información que va a ser consultada y del jefe de la Oficina de Seguridad de la Información.

- El Director de la dependencia o área auditada o responsable del proceso de auditoría para el nivel central y el Director Seccional en el nivel local y delegado, registran y aprueban la solicitud de cuentas y roles para el ente de control externo de acuerdo con lo establecido en el anexo de roles hoja entes de control. De igual forma, el colaborador que recibe la información solicitada para ser entregada a los entes externos de control se encarga de verificar si la información tiene una expresa reserva legal con el dueño del activo de información, fundada en razones de orden público, seguridad nacional o protección de derechos fundamentales, en cuyo caso informará al jefe de la Oficina de Control Interno o quien haga sus veces, o al Director Seccional. Así mismo, el Director de la dependencia o área auditada o responsable del proceso de auditoría para el nivel central o el Director Seccional para el nivel local o el colaborador de la UAE DIAN delegado es responsable de garantizar que posterior al tiempo asignado este sea inhabilitado o retirado según sea el caso.

- En situaciones atípicas donde la seguridad de la información o de la infraestructura esté en riesgo debido a que se detecta algún comportamiento anómalo o sospechoso o cuando se presente una alerta sobre la materialización de un riesgo de seguridad de la información, la Oficina de Seguridad de la Información OSI o quien haga sus veces, o el jefe inmediato del usuario afectado, podrán solicitar la inactivación del rol.

- La Oficina de Seguridad de la Información - OSI o quien haga sus veces, realiza seguimiento periódico de los usuarios y roles existentes en las soluciones tecnológicas, para verificar la correcta ejecución de este procedimiento, en caso de encontrar usuarios y/o roles activos sin el cumplimiento de los requisitos, procederá a solicitar la suspensión de los mismos y a realizar una evaluación del impacto de las soluciones tecnológicas y/o bases de datos teniendo en cuenta los riesgos de seguridad de la información, con el fin de determinar si se genera reporte a la Subdirección de Asuntos Disciplinarios o quien haga sus veces.

- En caso de que se requiera mantener activo el usuario y/o rol por un tiempo adicional debido a finalización del proceso de la entrega del cargo, prórroga del convenio y/o contrato de prestación de servicios, se debe informar a través de la herramienta de mesa de servicio, antes de la fecha inicialmente establecida con el fin de que dicho usuario y rol no sea suspendido en las soluciones tecnológicas y/o bases de datos.

- La Subdirección de Soluciones y Desarrollo realiza seguimiento diario a las fechas de finalización de los contratos de prestación de servicios y/o convenios y/o entes de control reportados por los responsables y realiza la inactivación preventiva de los usuarios y/o roles, la cual se registra en la herramienta de gestión de la mesa de servicio.

- Es responsabilidad del coordinador del convenio validar periódicamente, por lo menos dos veces al año, los roles asignados al convenio y realizar el registro de los cambios necesarios, velando por que estos siempre estén ajustados a lo requerido y pactado.

- Los accesos a bases de datos de usuarios de menú vencerán el 31 de enero del siguiente año al cual fue solicitado y otorgado el acceso.

- El acceso a base de datos debe ser solicitado por parte del jefe inmediato o subdirector del solicitante.

- La Coordinación de Soporte Técnico al Usuario, envía un reporte a los jefes, de los permisos de acceso concedidos durante el último mes a los funcionarios de su dependencia; si el jefe encuentra alguna inconsistencia debe solicitar el retiro de los mismos.

- Es responsabilidad de talento humano, jefes inmediatos y/o supervisores registrar y notificar, la desvinculación definitiva de un funcionario a su cargo y/o la finalización de un contrato o convenio, con el fin de que sean bloqueados todos los accesos a la red corporativa.

- Es responsabilidad del jefe inmediato solicitar la reactivación temporal del usuario del servidor público en caso de ausencia por fallecimiento y determinar a quien se le transferirá la información contenida en las soluciones tecnológicas, una vez finalizado el proceso se deberá solicitar la inactivación del usuario.

- El diligenciamiento de la información del usuario solicitante del rol (tipo, dependencia, convenio, ente de control, entre otros), información del rol solicitado y el tipo de acceso del rol solicitado, se adelanta a través de las plantillas precargadas en cada servicio durante el proceso de registro del caso en la herramienta de gestión de la mesa de servicio.

- Para el levantamiento inicial de la base de la hoja “roles directivos” del anexo “roles de las soluciones tecnológicas”, la Coordinación de Soporte Técnico al Usuario generará un reporte de los roles que tengan asignados a la fecha los Directores de Gestión, Directores Seccionales, Subdirectores, Jefes de División y/o Jefes de Coordinación, el cual debe ser validado por cada directivo, jefe de división o de coordinación para que posteriormente sea validado por el Jefe de la OSI; una vez completadas las dos validaciones, la Coordinación de Soporte Técnico al Usuario incluirá los roles en el anexo “roles de las soluciones tecnológicas”.

3.3 Acceso a elementos de integración para intercambio de información

- Para accesos a elementos de integración, se debe solicitar por parte del responsable del token físico a través de la herramienta de gestión de mesa de servicio el permiso para uso del mismo, cuya duración puede variar en el tiempo producto de cambios en las políticas internas de la Entidad. Solo deben autorizarse tokens que van a ser utilizados, cuando el token no se requiera más para su uso, deberá revocarse.

- La Dirección de Gestión de Innovación y Tecnología o quien haga sus veces, llevará el registro de los tokens asignados, las personas responsables y el tiempo del convenio. De igual forma, la Oficina de Seguridad de la Información – OSI o quien haga sus veces, realizará seguimiento a la asignación de estos tokens.

- No existen limitaciones para la cantidad de tokens generados por un cliente durante un tiempo particular. Sin embargo, esto no evita que las políticas y reglas en el uso de las API detecten los malos usos y generen restricciones al cliente.

- En caso de presentarse fallas en el funcionamiento del token asignado, las personas responsables del mismo deberán contactar a la mesa de servicio a través de los canales habilitados.

- En los equipos tecnológicos institucionales en donde se haga uso del token para acceso a la plataforma tecnológica deben tener instalado y actualizado el antivirus definido por la OSI.

3.4 Conexiones externas al dominio de la Entidad

- La coordinación de infraestructura definirá el nombre estándar con el cual se matriculará el equipo en el dominio DIAN, según aplique.

- Los equipos para conectar a la red corporativa deben cumplir con las condiciones establecidas en los requisitos con el fin de que no generen riesgos a la infraestructura y/o soluciones tecnológicas de la Entidad.

- En caso de que un equipo no cumpla con las condiciones necesarias para conexión a la red corporativa la Oficina de Seguridad de la Información – OSI evaluará el impacto y determinara la pertinencia o no de la conexión.

3.5 Indicadores

La Coordinación de Soporte Técnico al Usuario debe generar un reporte mensual con los tipos de solicitud, cantidades por estado y el tiempo de solución (por rangos de tiempo), dirigido al Subdirector de Soluciones y Desarrollo a través de correo electrónico.

Tiempo de solución: Mide los tiempos de solución en el mes de los casos registrados en la herramienta de gestión de la mesa de servicio para los diferentes tipos de solicitudes

Tipo de solicitud	Recibidas	Solucionadas (horas hábiles)			No Solucionadas
		De 0 a 16	De 17 a 40	Mas de 40	
Creación					
Prórroga					
Inactivación					
Periodo reportado:	**Desde**:	dd mm Aaaa			
	Hasta:	dd mm Aaaa			

Cantidad de solicitudes de activación: Mide la cantidad de solicitudes en el aprovisionamiento de un usuario en las diferentes plataformas tecnológicas.

Cantidad:

Indicador de cantidad: Total de solicitudes solucionadas / Total de solicitudes recibidas (por correo electrónico + Herramienta de gestión de la mesa de servicio) x 100

Indicador cantidad: (Total de solicitudes registradas en la herramienta de gestión de la mesa de servicio / Total de solicitudes de ingreso reportadas mensualmente por la Subdirección de Gestión del Empleo Público) x 100

Calidad:

Indicador de calidad: (Total de solicitudes solucionadas dentro de ANS en el mes (por correo electrónico + Herramienta de gestión de la mesa de servicio) / Total de solicitudes recibidas en el mes) x 100

Cantidad de solicitudes de inactivación: Mide la cantidad de solicitudes de inactivación de roles de un usuario en las diferentes plataformas tecnológicas.

Cantidad:

Indicador de cantidad: Total de solicitudes solucionadas / Total de solicitudes recibidas (por correo electrónico + Herramienta de gestión de la mesa de servicio) x 100

Indicador cantidad: (Total de solicitudes registradas en la herramienta de gestión de la mesa de servicio / Total de solicitudes de desvinculación de servidores públicos reportadas mensualmente por la Subdirección de Gestión del Empleo Público) x 100

3.6 Datos personales

Si dentro de la descripción de este procedimiento o de alguno de sus documentos relacionados se manejan datos personales y/o sensibles, se deben implementar los instrumentos, lineamientos y parámetros establecidos en la política de tratamiento de datos personales de la UAE DIAN, en el documento "*MN-IIT-0062 Manual para la protección de datos personales*" en especial lo referente al principio de privacidad por diseño y por defecto y su Anexo 1 "*Lineamientos para el tratamiento de datos personales sensibles y de niños, niñas y adolescentes*", y demás normativa interna y/o externa en la materia.

3.7 Interacciones eventuales

En los casos que se presenten interacciones con otros procedimientos que no están relacionadas directamente con el objetivo de este documento y que se dan en circunstancias eventuales, se deberá dar cumplimento a las entradas y requisitos definidos en el procedimiento correspondiente.

4. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Procedimiento	PR-IIT-0153	Gestión de proyectos de tecnología	Digital	Interno
Procedimiento	PR-IIT-0460	Gestión de requerimientos	Digital	Interno
Procedimiento	PR-ADF-0018	Egreso de bienes muebles	Digital	Interno
Instructivo	IN-IIT-0202	Registro de solicitud de roles de soluciones tecnológicas	Digital	Interno
Instructivo	IN-IIT-0203	Aprobación gestión de roles de soluciones tecnológicas	Digital	Interno
Instructivo	IN-IIT-0105	Modificación del Anexo "Roles de las soluciones tecnológicas"	Digital	Interno
Instructivo	IN-IIT-0251	Instalación de cliente VPN	Digital	Interno
Instructivo	IN-IIT-0273	Operaciones para la gestión de accesos	Digital	Interno
Formato	FT-IIT-2271	Autorización a terceros para conectarse a la red	Digital	Interno
Formato	FT-IIT-2719	Gestión de usuarios para bases de datos	Digital	Interno

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Formato	FT-IIT-2206	Solicitud de servicio para soluciones tecnológicas	Digital	Interno
Formato	FT-IIT-2794	Solicitud de acceso a direcciones IP o URL	Digital	Interno

5. DEFINICIONES Y SIGLAS

- **Acceso privilegiado**. Acceso a un sistema de información con privilegios superiores a los otorgados a los usuarios normales del sistema, son los accesos que tiene por ejemplo, los administradores del sistema.

  Fuente. UAE DIAN – Dirección de Gestión de Innovación y Tecnología.

- **API**. Application Programming Interface o en español, Interfaz de Programación de Aplicaciones. Conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el software de las aplicaciones.

  Fuente. SYDLE. (2022). Consultado en https://www.sydle.com/es/blog/api-6214f68876950e47761c40e7/

- **Autenticación basada en token**. es un protocolo que permite a los usuarios verificar su identidad y, a cambio, recibir un token de acceso único. Durante la vida útil del token, los usuarios acceden al sitio web o la aplicación para la que se emitió el token, en lugar de tener que volver a ingresar las credenciales cada vez que regresan a la misma página web, aplicación o cualquier recurso protegido con ese mismo token. Los tokens de autenticación funcionan como un boleto sellado. El usuario conserva el acceso mientras el token siga siendo válido. Una vez que el usuario cierra la sesión o sale de una aplicación, el token se invalida.

  Fuente. OKTA. (2022). Consultado en https://www.okta.com/identity-101/what-is-token-based-authentication/

- **Contraseña**. Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

  Fuente. MINTIC. (2022). Consultado en https://www.mintic.gov.co/portal/inicio/Glosario/

- **Direct Access**. También conocido como acceso remoto unificado, es una tecnología de tipo VPN que proporciona conectividad de intranet a los equipos cliente cuando están conectados a Internet. A diferencia de muchas conexiones VPN tradicionales, que deben iniciarse y terminarse mediante la acción explícita del usuario, las conexiones de DirectAccess están diseñadas para conectarse automáticamente tan pronto como la computadora se conecta a Internet.

  Fuente. MICROSOFT. (2022). Consultado en https://docs.microsoft.com/en-us/windows-server/remote/remote-access/directaccess/directaccess

- **GIT**. Grupo Interno de Trabajo.

- **Intranet**. Red digital de uso interno en una organización.

  Fuente. Real Academia Española. (2022). Consultado en https://dle.rae.es/intranet

- **JSON Web Token** (abreviado JWT). Es un estándar abierto basado en JSON propuesto por IETF (RFC 7519) para la creación de tokens de acceso que permiten la propagación de identidad y privilegios o claims en inglés. Por ejemplo, un servidor podría generar un token indicando que el usuario tiene privilegios de administrador y proporcionarlo a un cliente. El cliente entonces podría utilizar el token para probar que está actuando como un administrador en el cliente o en otro sistema. El token está firmado por la clave del servidor, así que el cliente y el servidor son ambos capaz de verificar que el token es legítimo. Los JSON Web Tokens están diseñados para ser compactos, poder ser enviados en las URLs -URL-safe- y ser utilizados en escenarios de Single Sign-On (SSO). Los privilegios de los JSON Web Tokens puede ser utilizados para propagar la identidad de usuarios como parte del proceso de autenticación entre un proveedor de identidad y un proveedor de servicio, o cualquiera otro tipo de privilegios requeridos por procesos empresariales. El estándar de JWT se basa en otros estándares basados en JSON Web Signature (RFC 7515) y JSON Web Encryption (RFC 7516).

  Fuente. JWT. (2022). Consultado en https://jwt.io/introduction

- **OSI**. Oficina de Seguridad de la Información

- **Polfa**. Policía Fiscal y Aduanera.

- **Situación administrativa.** Es aquella condición en la que un servidor público de la Entidad es separado de sus funciones de manera transitoria, como por ejemplo vacaciones, licencias no remuneradas, comisión de estudios, comisión de servicios, investigaciones disciplinarias, entre otros.

  Fuente: UAE DIAN – Dirección de Gestión de Innovación y Tecnología.

- **Solución tecnológica**. Es una actividad de negocio cuya operación es apoyada por elementos tecnológicos que están dentro o fuera de la Entidad, ya sea a través de uno o varios sistemas de información, bases de datos, servicios tercerizados de procesamiento, almacenamiento, entre otros.

  Fuente. Definición adaptada de “Architecture as Strategy: Creating a Foundation for Business. Execution, J. Ross, P. Weill, D. Robertson, HBS Press, June 2006” G.SIS.04 Guía de Arquitectura de Soluciones Tecnológicas noviembre de 2019 Pag 17. Consultado en https://www.mintic.gov.co/arquitecturati/ 630/articles-117954_recurso_pdf.pdf

- **VPN**. Una red privada virtual (RPV) (en inglés, Virtual Private Network, VPN) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

  Fuente. CISCO. (2022). Consultado en https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

6. DIAGRAMA DE FLUJO

6.1 Entradas

No de actividad	Proveedores	Entradas	Requisitos
1	Procedimiento "*PR-IIT-0460 Gestión de requerimientos*"	Solicitud de gestión de usuarios en las soluciones tecnológicas (A)	**Vinculación de un(a) servidor(a) público(a) a la Entidad para creación de usuario de dominio y asignación de roles básicos en las soluciones tecnológicas**: **Para servidores(as) de planta** • La Subdirección de Gestión del Empleo Público, la división Talento Humano y/o el GIT de Talento Humano o quien haga sus veces en el nivel local, crea requerimiento a través de la herramienta de mesa de servicio, adjuntando copia de la resolución de nombramiento o acta de posesión del nuevo servidor, solicitando la creación de usuario de dominio, correo electrónico y asignación de equipo (si aplica). • Si la solicitud es para Directores de Gestión, Operativo, Directores Seccionales, Subdirectores, Jefes de División, y/o Coordinadores se asignan los roles de acuerdo con el Anexo Matriz de roles y cargos. **Para servidores(as) con contrato de prestación de servicios** • Se crea requerimiento por parte del supervisor del contrato de prestación de servicios a través de la herramienta de mesa de servicio, una vez suscrito el contrato, solicitando la creación de usuario de dominio, correo electrónico y asignación de equipo, es necesario incluir la siguiente información del contrato: número del contrato, fecha de contrato, duración, número de identificación del contratista, nombre del contratista y correo electrónico personal.

No de actividad	Proveedores	Entradas	Requisitos
			Activación de un usuario y/o roles por finalización de la situación administrativa, para activación de usuario de dominio y roles en las soluciones tecnológicas: **Para servidores(as) de planta** • Interfaz – web service entre Kactus, Muisca y SIAT con las novedades de vinculación y ejecución exitosa del proceso. • Usuario y roles inactivos por situación administrativa diferente a retiro. • Recepción de correo automático en la coordinación de soporte técnico al usuario y SITO para registro de caso de activación de usuario en Directorio Activo, correo electrónico y firewall. **Para servidores(as) con contrato de prestación de servicios** • Para contratos de prestación de servicios se crea requerimiento por parte del supervisor del mismo, a través de la herramienta de mesa de servicio, una vez activo nuevamente el contrato, se debe adjuntar acta de reinicio del mismo. **Para asignación de roles avanzados en las soluciones tecnológicas** • El jefe inmediato registra la solicitud a través de la herramienta de gestión de la mesa de servicio, donde se justifique si requiere el rol por un reemplazo, encargo, traslado, en el marco de un contrato, convenio u otro. Adicionalmente debe seleccionar el servicio y/o plataforma para el cual se requiere el rol, y diligenciar los datos requeridos en la plantilla que se carga en el campo descripción de la solicitud. • Que sea solicitado de acuerdo con lo descrito en el "*IN-IIT-0202 Registro solicitud de roles de las soluciones tecnológicas"*.

No de actividad	Proveedores	Entradas	Requisitos
			• Que sea aprobado de acuerdo con lo descrito en el "*IN-IIT-0203 Aprobación gestión de roles de las soluciones tecnológicas"*. • Para los colaboradores de la Subdirección de Análisis de Riesgo y Programas y la Subdirección de Información y Analítica de la Dirección de Gestión Estratégica y de Analítica o quien haga sus veces, la solicitud debe ser autorizada, por el Director de Gestión Estratégica y de Analítica o quien haga sus veces, el jefe de la Oficina de Seguridad de la Información o quien haga sus veces y el jefe del área responsable de la solución tecnológica. • Cuando se requiera la asignación o inactivación de roles de la solución tecnológica para usuarios de la POLFA, es responsabilidad del jefe inmediato registrar dicha solicitud en la herramienta de gestión de la mesa de servicio y del Director de Gestión de la Policía Fiscal y Aduanera o el Director Seccional de la POLFA, según aplique o quien haga sus veces, aprobarla y debe ser autorizado por el jefe de la Oficina de Seguridad de la Información. • Cuando se requiera la asignación de roles de la solución tecnológica para organismos con los que se tienen suscritos convenios y/o entes de control, es responsabilidad de los coordinadores del convenio o el Director de la dependencia o área auditada o responsable del proceso de auditoría para el nivel central y el Director Seccional para el nivel local, según aplique, registrar dicho requerimiento en la herramienta de gestión de la mesa de servicio. En este caso, es necesario incluir la siguiente información sobre el convenio: nombre del convenio, fecha del convenio, duración, número de identificación usuario, nombre completo del usuario y correo electrónico de la persona delegada, sobre el ente de control: nombre de la entidad, fecha de inicio del acceso, duración del acceso, número de identificación usuario, nombre completo del usuario y correo electrónico institucional de la persona del ente de control.

No de actividad	Proveedores	Entradas	Requisitos
			Para inactivación de usuario de dominio y/o roles • La Subdirección de Gestión del Empleo Público, la división Talento Humano y/o el GIT de Talento Humano o quien haga sus veces en el nivel local, crea requerimiento a través de la herramienta de mesa de servicio, solicitando desactivar usuario de dominio y correo electrónico, adjuntando el acto administrativo de la novedad presentada. • En caso de cambio de dependencia o cargo de un servidor, la Subdirección de Gestión del Empleo Público, la división Talento Humano y/o el GIT de Talento Humano o quien haga sus veces en el nivel local, crea requerimiento a través de la herramienta de mesa de servicio, solicitando actualizar la información de ubicación del servidor, adjuntando el acto administrativo de la novedad presentada. • En caso de modificación de actividades dentro de la misma dependencia, el jefe inmediato crea un requerimiento a través de la herramienta de gestión de mesa de servicio, solicitando la inactivación de los roles que tenía asignados el servidor, de acuerdo con lo establecido en el anexo roles de las soluciones tecnológicas. • Se crea requerimiento por parte de Coordinación de Soporte Técnico al Usuario cada vez que se realiza inactivación preventiva de acuerdo con las fechas que se encuentren registradas en el instrumento definido por la Subdirección de Soluciones y Desarrollo para el caso de convenios y/o contratos de prestación de servicios.

No de actividad	Proveedores	Entradas	Requisitos
			Para conexión por VPN • Requerimiento registrado por los superiores jerárquicos (Director de Gestión, Subdirector o Jefe de Oficina) en la herramienta de gestión de la mesa de servicio indicando su justificación y fecha de finalización del acceso. • Adjuntar documento en donde el representante legal designa el empleado o colaborador que está autorizado para establecer las credenciales informáticas para la utilización del canal seguro (aplica para usuarios externos). • Que indique la identificación y número telefónico de contacto de la persona que la DIAN autoriza para hacer uso del usuario remoto (aplica para usuarios externos).
			Para direct Access • Requerimiento a través de la herramienta de gestión de mesa de servicio. • Solicitud donde se deberá incluir: ✓ Justificación que indique la pertinencia de la conexión. ✓ Identificación de la persona que requiere el acceso. ✓ Nombre o dirección IP de las máquinas origen y destino de la conexión. ✓ Autorización del jefe inmediato. ✓ Fecha de retiro del acceso concedido.
			Para activación token físico • Requerimiento a través de la herramienta de gestión de la mesa de servicio. • Solicitud donde se deberá incluir: ✓ Nombre o dirección IP de la máquina en la que se realizará la activación.

No de actividad	Proveedores	Entradas	Requisitos
			✓ Solicitud registrada por la persona responsable del token. ✓ Código o ID del token.
			Para intercambio de información • Requerimiento a través de la herramienta de gestión de la mesa de servicio, la solicitud debe incluir la siguiente información: ✓ Documento en donde el representante legal designa el empleado o funcionario que está autorizado para establecer las credenciales informáticas para la utilización del canal seguro (aplica para usuarios externos). ✓ Indicar el número de identificación y número telefónico de contacto de la persona que la entidad autoriza para hacer uso del usuario (aplica para usuarios externos). ✓ Relacionar el convenio que da origen al acceso (si aplica)
			Para conexiones externas al dominio DIAN • Requerimiento a través de la herramienta de gestión de la mesa de servicio. • Adjuntar el formato “FT-IIT-2271 Autorización a terceros para conectarse a la red” (aplica para usuarios externos). • Claridad en la solicitud donde se deberá incluir: ✓ Justificación que indique la pertinencia de la conexión. ✓ Nombre completo de la persona que requiere el acceso. ✓ Nombre o IP de las máquinas origen y destino de la conexión. **Adicionalmente**

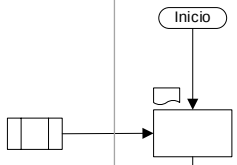
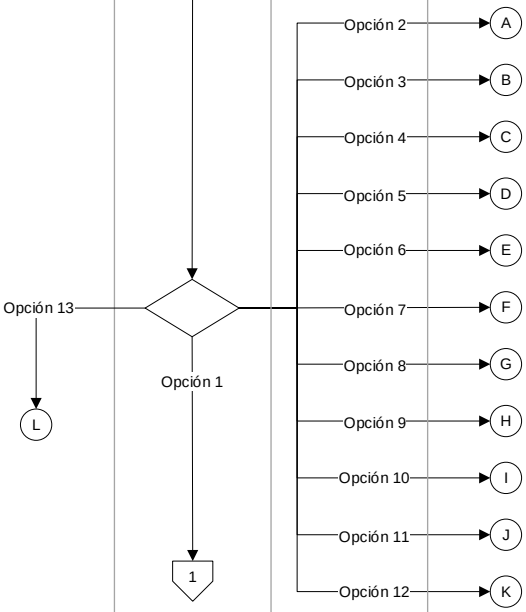
No de actividad	Proveedores	Entradas	Requisitos
			• El software instalado en el equipo a conectar a la red corporativa de la Entidad debe ser oficial y estar debidamente licenciado. • El equipo debe contar con antivirus instalado, actualizable y licenciado en caso de requerir licencia. • Adjuntar resultado de análisis y/o escaneo del antivirus instalado en el equipo con vigencia no superior a un día calendario. • El sistema operativo del equipo se debe encontrar actualizado en su última versión.
			Para acceso a una dirección IP o URL Requerimiento a través de la herramienta de gestión de la mesa de servicio indicando justificación del motivo por el que requiere acceso a la dirección IP o URL, adjuntando formato FT-IIT-2794 Solicitud de acceso a direcciones IP o URL y con la autorización del Jefe Inmediato del solicitante.
			Para acceso a bases de datos • Requerimiento a través de la herramienta de gestión de la mesa de servicio. • Adjuntar el formato “FT-IIT-2719 Gestión de usuarios para bases de datos”. • Solicitud presentada por el jefe inmediato donde se deberá incluir: ✓ Justificación que indique la pertinencia de la asignación. ✓ Identificación de la persona que requiere la asignación del usuario.

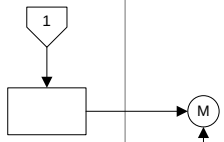
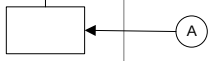
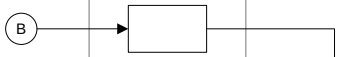
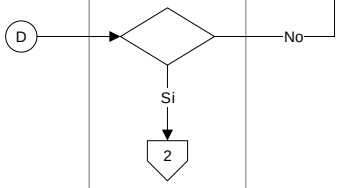
*A (Activo de información)

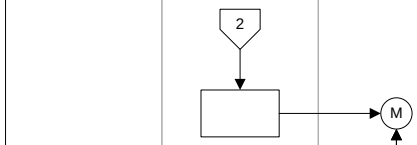
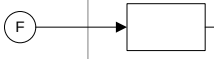
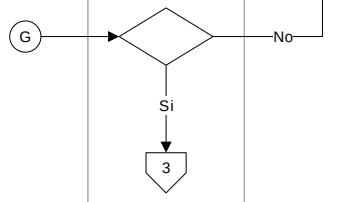
6.2 Descripción de actividades

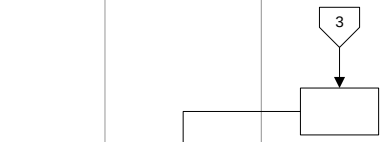
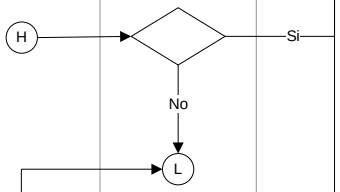
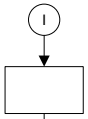
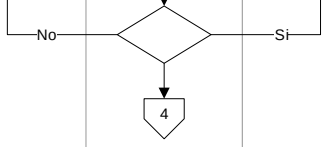
Los símbolos definidos para los flujogramas de la UAE DIAN son los siguientes:

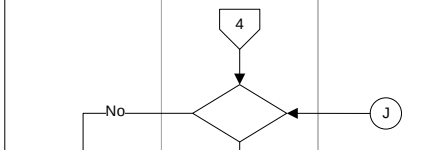
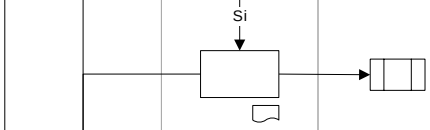
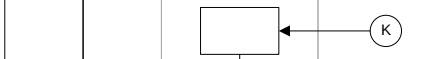
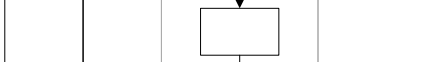
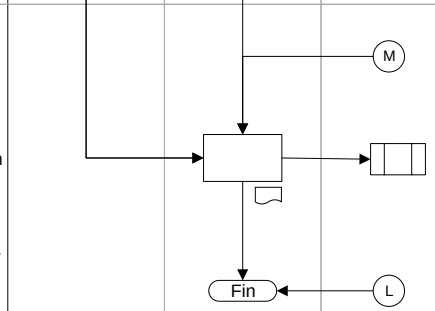
Simbolo	Descripción	Simbolo	Descripción
	INDICA LA SECUENCIA DEL FLUJOGRAMA.		INDICA QUE EL FLUJOGRAMA TIENE VARIAS OPCIONES DE SECUENCIA (máximo 3).
	INDICA LAS ACTIVIDADES REALIZADAS MANUALMENTE.		INDICA LAS ACTIVIDADES REALIZADAS AUTOMÁTICAMENTE.
	INDICA QUE LA ACTIVIDAD ESTA GENERANDO UNA SALIDA A OTRO PROCEDIMIENTO, SUBPROCESO, PROCESO O CLIENTE EXTERNO.		INDICA EL INICIO O EL FIN DEL FLUJOGRAMA.
	INDICA QUE EN LA ACTIVIDAD PRESENTA UNA ENTRADA GENERADA POR OTRO PROCEDIMIENTO, SUBPROCESO, PROCESO O CLIENTE EXTERNO.		INDICA LA CONEXIÓN ENTRE ACTIVIDADES UTILIZANDO CARACTERES ALFABETICOS.
	INDICA QUE UN PROCEDIMIENTO, SUBPROCESO O PROCESO SUMINISTRA O RECIBE INSUMOS.		INDICA LA CONEXIÓN ENTRE PÁGINAS UTILIZANDO CARACTERES NUMÉRICOS.

ACTIVIDAD	RESPONSABLE DE	DEPENDENCIA	REGISTROS
	Agente mesa de servicio		
1. Recibir solicitud de acceso Se reciben solicitudes de acceso a la plataforma tecnológica, en la herramienta de gestión de la mesa de servicio, provenientes del procedimiento "PR-IIT-0460 Gestión de requerimientos". Las solicitudes pueden ser: - Gestión usuarios y roles informáticos. - Accesos por VPN o Direct Access (conexiones por fuera del dominio DIAN). - Acceso elemento de integración para intercambio de información. - Activación de token físico. - Conexiones al interior del dominio DIAN (Acceso a la RED DIAN) o URL restringidas. - Acceso a bases de datos.		Coordinación de Soporte Técnico al Usuario	Registro en la herramienta de gestión de la mesa de servicio.
2. ¿Qué tipo de servicio se está solicitando? Se verifica el cumplimiento de requisitos y si no cumple se cierra el caso en la herramienta de gestión de la mesa de servicio, indicando los motivos por los cuales no es posible atender la solicitud y finaliza el procedimiento, de lo contrario continuar con las siguientes actividades, de la siguiente manera: -Opción 1. Vinculación de un(a) servidor(a) público(a) a la Entidad, continuar con la actividad No. 3. -Opción 2. Novedades administrativas (cambio de cargo o ubicación), continuar con la actividad No. 4. -Opción 3. Gestión de roles avanzados de las soluciones tecnológicas, continuar con la actividad No. 5. -Opción 4. Inactivación de usuarios y roles (inicio de situación administrativa o finalización de contrato, convenio o acceso ente de control), continuar con la actividad No. 6. -Opción 5. Activación de un usuario y/o roles del mismo, por finalización de la situación administrativa, continuar con la actividad No. 7. -Opción 6. Accesos por VPN o Direct Access, continuar con la actividad No. 9. -Opción 7. Activación de token físico, continuar con la actividad No. 11. -Opción 8. Conexiones externas a la red corporativa y/o dominio DIAN, continuar con la actividad No. 12. -Opción 9. Accesos a las bases de datos, continuar con la actividad No. 15. -Opción 10. Acceso a dirección IP o URL restringida, continuar con la actividad No. 16 -Opción 11. Acceso a solución tecnológica para intercambio de información, continuar con la actividad No. 18. -Opción 12. Modificación de anexo de roles, continúa con actividad No. 20. -Opción 13. Se cierra el caso. Finaliza el procedimiento.		Coordinación de Soporte Técnico al Usuario	Registro en la herramienta de gestión de la mesa de servicio.

ACTIVIDAD	RESPONSABLE DE			DEPENDENCIA	REGISTROS
		Agente mesa de servicio y Especialista técnico	Especialista técnico		
3. Consultar datos Se realiza verificación de datos en el acta de posesión y/o contrato de prestación de servicios y se crean tareas en la herramienta de gestión de la mesa de servicio; se debe continuar con los pasos descritos en el instructivo "*IN-IIT-0273 Operaciones para la gestión de accesos*" Capítulo Vinculación de un(a) servidor(a) público(a) y Continuar con la actividad No. 22.				Coordinación de Soporte Técnico al Usuario	Registro en la herramienta de gestión de la mesa de servicio.
4. Asignar roles Se listan los roles asignados al (la) servidor (a) y se crean tareas a los administradores de las soluciones tecnológicas correspondientes, en la herramienta de gestión de la mesa de servicio, con el fin de realizar inactivación de los mismos, se deben mantener los roles básicos, se deben seguir los pasos descritos en el instructivo "*IN-IIT-0273 Operaciones para la gestión de accesos*", capitulo Novedades Administrativas, continuar a la actividad No. 22.				Coordinación de Soporte Técnico al Usuario	Registro en la herramienta de gestión de la mesa de servicio.
5. Gestionar roles avanzados Se identifica el rol solicitado y la dependencia para la que se requiere el rol, de igual forma se valida en la matriz de escalamiento en caso de requerirse, se deben seguir los pasos descritos en el instructivo "*IN-IIT-0273 Operaciones para la gestión de accesos*" Capitulo: Gestión de roles avanzados de las soluciones tecnológicas y continuar con la actividad No. 22.				Coordinación de Soporte Técnico al Usuario	No aplica.
6. Gestionar inactivación de usuarios y roles Se realiza consulta de la fecha de inicio de la novedad administrativa presentada, o fecha fin del contrato de prestación de servicios, o fecha fin del acceso del ente de control o fecha fin del convenio, en el documento anexo, se ajusta a través del campo vigencia del usuario y se registra en el campo definido para registrar la fecha en el directorio activo con el fin de que se genere alerta a través de correo electrónico en la fecha de inactivación, se deben seguir los pasos descritos en el instructivo "*IN-IIT-0273 Operaciones para la gestión de accesos*" Capitulo: Inactivación de usuarios y roles; y continuar con la actividad No. 22.				Coordinaciones de Soporte Técnico al Usuario y Administración Técnica	Registro en Directo Activo
7. ¿Se requiere reintegro anticipado por interrupción de la situación administrativa? En caso de requerir reintegro anticipado por interrupción de una situación administrativa, se validan las fechas de acuerdo con la documentación adjunta en el caso y justificación para la reactivación, y continuar con la actividad No. 8. En caso contrario, una vez recibida la alerta automática de finalización de la situación administrativa por correo electrónico, se realiza activación y/o creación del caso en la herramienta de gestión de la mesa de servicio, continuar con los pasos descritos en el instructivo "*IN-IIT-0273 Operaciones para la gestión de accesos*" Capitulo Activación de usuarios y roles y continuar con actividad No. 22.				Coordinaciones de Soporte Técnico al Usuario, Administración Técnica y SITO	Registro en la herramienta de gestión de la mesa de servicio.

ACTIVIDAD	RESPONSABLE DE	DEPENDENCIA	REGISTROS
	Especialista técnico		
8. Activar manualmente roles Se crean tareas en la herramienta de gestión de la mesa de servicio, a los administradores de las soluciones tecnológicas a las cuales el (la) servidor (a) tenga acceso con el fin de realizar activación de los roles que tenía asignados antes de la novedad administrativa, se deben consultar los roles en la base de datos correspondiente, se debe continuar con los pasos descritos en el instructivo "*IN-IIT-0273 Operaciones para la gestión de accesos*" Capitulo Activación de usuarios y roles, continuando con la actividad No. 22.		Coordinación de Soporte Técnico al Usuario	Registro en la herramienta de gestión de la mesa de servicio.
9. Gestionar acceso por VPN o Direct Access Se asignan permisos de acceso de seguridad en el firewall y permisos en el directorio activo para que el usuario ingrese por acceso remoto.		Subdirección de Infraestructura Tecnológica y de Operaciones	Permiso asignado en firewall y en directorio activo.
10. Remitir instructivo para la instalación del cliente VPN y cerrar caso Se remite instructivo por correo electrónico "*IN-IIT-0251 Instalación de cliente VPN*", en donde se indica la URL para la descarga del aplicativo y el paso a paso para su configuración de la dirección IP o nombre del servidor y su posterior conexión. Posteriormente se cierra el caso en herramienta de gestión de la mesa de servicio y continuar con la actividad No. 22.		Subdirección de Infraestructura Tecnológica y de Operaciones	-Correo electrónico. -Registro en la herramienta de gestión de la mesa de servicio.
11. Gestionar acceso a token físico Se realiza habilitación del acceso a token físico en el equipo de cómputo del servidor público generando la excepción en el antivirus y continuar con la actividad No. 22.		Coordinación de Soporte Técnico al Usuario	Registro de acceso habilitado en equipo de cómputo
12. ¿La validación técnica fue exitosa? Se verifica el cumplimiento de requisitos en la herramienta de gestión de la mesa de servicio y la justificación de la solicitud, comprobando la pertinencia o no de la misma. En caso de aprobarse, continuar con la actividad No. 13; en caso contrario, se solicita la corrección de lo identificado de manera detallada y continuar con la actividad No. 22. **Nota:** La coordinación de Soporte Técnico al Usuario verifica el licenciamiento del equipo que se va a conectar con el fin de determinar la legalidad del software instalado. De encontrarse novedades con el software instalado se solicitará la desinstalación o se debe aportar las licencias autorizadas.		Subdirección de Infraestructura Tecnológica y de Operaciones	Registro en la herramienta de gestión de la mesa de servicio.

ACTIVIDAD	RESPONSABLE DE			DEPENDENCIA	REGISTROS
		Especialista técnico	Agente mesa de servicio		
13. Configurar equipo externo Se configuran los diferentes elementos de la red de acuerdo con la topología y habilitación del punto de red.				Coordinación de Soporte Técnico al Usuario	Configuración de red en equipo externo
14. Conceder acceso a la red Conceder acceso al dominio de la DIAN a la persona autorizada y cerrar el caso. Se cierra el caso en la herramienta de gestión de la mesa de servicio. Continua a la actividad 22.				Subdirección de Infraestructura Tecnológica y de Operaciones	Registro en la herramienta de gestión de la mesa de servicio.
15. ¿Se aprueba la solicitud de acceso a bases de datos? Si se aprueba la solicitud, se revisa el cumplimiento de los requisitos y la pertinencia o no de la misma. Se verifica que esta sea necesaria para ejercer las funciones propias del cargo del colaborador solicitante y seguir los pasos descritos en el instructivo "*IN-IIT-0273 Operaciones para la gestión de accesos*" Capítulo: Acceso a bases de datos, continuando con la actividad No. 22. En caso de no se aprobada la solicitud, se cierra el caso indicando los motivos de la no aprobación y finaliza el procedimiento.				Subdirección de Infraestructura Tecnológica y de Operaciones	Registro en la herramienta de gestión de la mesa de servicio.
16. Validación de listas Se realiza la validación de la dirección IP o URL solicitada en la lista de dominios permitidos y se analiza la justificación de la solicitud verificando que esta sea necesaria para ejercer las funciones propias del cargo del colaborador solicitante.				Subdirección de Infraestructura Tecnológica y de Operaciones	No aplica.
17. ¿Se aprueba la solicitud? Si se aprueba la solicitud, se habilita el acceso a la dirección IP o URL solicitada y continua con la actividad No. 22; de lo contrario, se finaliza el caso en la herramienta de gestión de la mesa de servicio detallando la imposibilidad de habilitar el acceso a la dirección IP o URL y finaliza el procedimiento.				Subdirección de Infraestructura Tecnológica y de Operaciones	-Acceso habilitado. -Registro en la herramienta de gestión de la mesa de servicio.

ACTIVIDAD	RESPONSABLE DE	DEPENDENCIA	REGISTROS
	Especialista técnico		
18. ¿Se requiere desarrollo para el intercambio de información? Se valida la solicitud realizada por el área funcional de acuerdo con la información anexa al caso. En caso de requerir desarrollo, continuar con la actividad No. 19; en caso contrario se debe continuar con los pasos descritos en el instructivo "*IN-IIT-0273 Operaciones para la gestión de accesos*" Capitulo: Acceso para intercambio de información y continuar con la actividad No. 22.		Subdirección de Infraestructura Tecnológica y de Operaciones	No aplica
19. Solicitar desarrollo Se solicita desarrollo del elemento de integración para intercambio de información a través de la herramienta de gestión de la mesa de servicio, opción solicitudes funcionales, adjuntando el formato*"FT-IIT-2206 Solicitud de servicio para soluciones tecnológicas"* continuando con el procedimiento *"PR-IIT-0153 Gestión de proyectos de tecnología"*, continuar a la actividad 22.		Subdirección de Infraestructura Tecnológica y de Operaciones	Registro en la herramienta de gestión de la mesa de servicio.
20. Gestionar modificación del anexo de roles Se realiza seguimiento al reporte de roles activos y si se requiere la modificación del Anexo Roles de las soluciones tecnológicas se valida la justificación anexa al caso.		Subdirección de Soluciones y Desarrollo	No aplica.
21. Modificar anexo roles Se realiza modificación del Anexo Roles de las soluciones tecnológicas de acuerdo con lo descrito en el instructivo *IN-IIT-0105 Modificación del Anexo "Roles de las soluciones tecnológicas*".		Subdirección de Soluciones y Desarrollo	Anexo Roles de las soluciones tecnológicas modificado
22. Documentar en herramienta, enviar respuesta y cerrar caso Se realiza documentación de las actividades desarrolladas en la herramienta de gestión de la mesa de servicio, las cuales pueden estar relacionadas con la gestión de usuarios y roles informáticos, accesos por VPN o Direct Access (conexiones por fuera del dominio DIAN), accesos a elementos de integración para intercambio de información, activación de token físico, conexiones al interior del dominio DIAN (Acceso a la RED DIAN) o IP/URL restringidas, o acceso a bases de datos, teniendo en cuenta los requisitos establecidos en el numeral 6.3 Salidas. Posteriormente se envía respuesta al solicitante indicando la gestión realizada y se cierra el caso. Nota: En el evento de requerir el desarrollo de una solución tecnológica para conceder un acceso, se debe diligenciar el formato *"FT-IIT-2206 Solicitud de servicio para soluciones tecnológicas"* y continuar con el procedimiento *"PR-IIT-0153 Gestión de proyectos de tecnología"*, continuar a la actividad 22. Finaliza el procedimiento.		Subdirección de Soluciones y Desarrollo, Subdirección de Infraestructura Tecnológica y de Operaciones, Coordinación de Soporte Técnico al Usuario y/o Administración Técnica según aplique	Registro en la herramienta de gestión de la mesa de servicio.

6.3 Salidas

No de actividad	Salidas	Clientes	Requisitos
19 y 22	Formato "*FT-IIT-2206 Solicitud de servicio para soluciones tecnológicas*"	Procedimiento "*PR-IIT-0153 Gestión de proyectos de tecnología*"	• Que esté debidamente diligenciado. • Registrado en la herramienta de gestión de solicitudes de la entidad opción "Solicitudes Funcionales". • Estar aprobado por el responsable del proceso. • Que la solución esté registrada en la herramienta de gestión de la mesa de servicio.
22	Respuesta a la solicitud	• Subdirección de Gestión del Empleo Público o quien haga sus veces. • Colaboradores DIAN • Usuarios externos web services • Todas las dependencias • Entes de control • Entes externos	• Debidamente registrada en la herramienta de gestión de la mesa de servicio. • Para usuario (DBA, consulta, aplicación) que se encuentre asignado en la base de datos solicitada con su rol y clave respectiva. • Para usuarios nuevos se debe enviar un esquema de autenticación..

*A (Activo de información)

7. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	10/09/2021	05/01/2023	Versión inicial. Deroga los procedimientos: • PR-SI-0344 Control Accesos y Conexiones Electrónicas • PR-SI-0142 Gestión de roles de los sistemas de información • PR-SI-0357 Habilitación de canal seguro para transferencia de archivos Se modificaron los formatos:	No aplica

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
			• FT-IIT-2271 Autorización a terceros para conectarse a la red • FT-IIT-2596 Solicitud de asignación de roles de las soluciones tecnológicas y compromiso de confidencialidad Se creó el formato: • FT-IIT-2719 Gestión de usuarios para bases de datos Se modifican los instructivos: • IN-IIT-0105 Modificación del anexo de roles de las soluciones tecnológicas • IN-IIT-0202 Registro de solicitud de roles de soluciones tecnológicas • IN-IIT-0203 Aprobación gestión de roles de soluciones tecnológicas Se creó el instructivo: • IN-IIT-0251 Instalación de cliente VPN	
2	06/01/2023	10/08/2023	Versión 2 que reemplaza lo establecido en la versión 1. Se modifica el objetivo, alcance, se actualizan las condiciones generales, se actualiza la tabla de documentos relacionados y se actualizan las definiciones y siglas. Se reestructuran las actividades del flujograma y se actualizan las entradas y salidas. Se crea el instructivo “IN-IIT-0273 Operaciones para la gestión de accesos”.	Esta versión corresponde a Información pública

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
			Se elimina el formato “FT-IIT-2596 Solicitud de asignación de roles de las soluciones tecnológicas compromiso de confidencialidad”, el cual se encontraba asociado al instructivo “IN-IIT-0202 Registro de solicitud de roles de soluciones tecnológicas” Se actualiza la plantilla del presente documento, de acuerdo con la versión 5 del procedimiento “PR-PEC-0001 Documentación del sistema de gestión”.	
3	11/08/2023		Versión 3 que reemplaza lo establecido en la versión 2. Se modifica objetivo. Se modifica las condiciones generales con respecto a las novedades administrativas. Se realizan modificaciones de redacción en todo el documento. Se modifica la entrada para las solicitudes relacionadas con la gestión de usuarios en las soluciones tecnológicas y con direcciones IP y URL. Se crea el formato FT-IIT-2794 Solicitud de acceso a direcciones IP o URL.	Esta versión corresponde a Información pública

Elaboró:	Carlos Arturo Higuera Manrique **Elaboración técnica**	Gestor III	Subdirección de innovación y Proyectos
	Cristian Eduardo Zanguña Ruiz **Elaboración técnica**	Gestor IV	Subdirección de Soluciones y Desarrollo
	Tito Alejandro Menjura Murcia **Elaboración Metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales
	Alfredo Antonio Ahumada Ahumada **Elaboración Metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales
Revisó:	Claudia Patricia Bernal Rivera	Jefe	Coordinación de Soporte Técnico al Usuario

	Divier Javier Alberto Saganome	Subdirector	Subdirección de Soluciones y Desarrollo
	Héctor Leonel Mesa Lara	Subdirector	Subdirección de Infraestructura Tecnológica y de Operaciones
Aprobó:	Julián David Medina Herrera	Director	Dirección de Gestión de Innovación y tecnología

8. ANEXOS

Anexo 1 - Responsables del registro y aprobación de solicitudes de asignación / inactivación de Roles.

Anexo 2 - Roles de las soluciones tecnológicas.
https://diancolombia.sharepoint.com/:x:/s/diannetpruebas/Areas/EeIseQw-dIVAvcScEc1PdE0Bzjsddi5ILyGL5HnEfqeyrA

Anexo 3 - Protocolo para manejo de usuarios privilegiados.