	Aprobación	Revisión Técnica
Firma:	CARMEN ROSA MENDOZA S	Mercedes Yunda
Nombre:	CARMEN ROSA MENDOZA SUÁREZ	**Nombre:** MERCEDES YUNDA MONROY
Cargo:	Director Técnico	**Cargo:** Director Técnico
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones	**Dependencia:** Dirección de Planeación
R.R. No.	047 **Fecha**	28 DIC. 2018

1. OBJETIVO:

Establecer actividades para la administración de cuentas de usuarios asignados a funcionarios, contratistas y terceras partes para gestionar el ingreso seguro a los sistemas de información de la Contraloría de Bogotá.

2. ALCANCE:

Este procedimiento inicia con la solicitud de creación, modificación, inactivación de credenciales de acceso a usuario de red, correo electrónico, sistemas de información de la Contraloría de Bogotá y termina con la atención y solución del requerimiento por parte de la Dirección de Tecnologías de la Información y las Comunicaciones.

3. BASE LEGAL:

NORMA	FECHA	DESCRIPCIÓN
Ley 599	24-jul-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.
Ley 1273	05-ene-2009	Por medio de la cual se modifica el Código Penal. Título VII Bis “De la protección de la información y de los datos”. Artículos 269A a 269J.
Ley 1581	17-Oct-2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712	06-mar- 2014	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.
Decreto 1377	27-jun-2013	Por la cual se reglamenta parcialmente la Ley 1581 de 2012.

NORMA	FECHA	DESCRIPCIÓN
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Capítulo 1, Título 9, Libro 2, Parte 2 subrogado por el Decreto 1008 de 2018.
Decreto 1081	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Presidencia de la República. Parte 1, Titulo 1.
Decreto 1008	14-jun-2018	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. Política de Gobierno Digital.
Acuerdo 658	21-dic-2016	Por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Acuerdo 664	28-mar-2017	Por el cual se modifica parcialmente el Acuerdo 658 del 21 de diciembre de 2016, por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Resolución 305	20-oct-2008	Comisión Distrital de Sistemas. 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.
Resolución 004	28-nov-2017	Por la cual se modifica la Resolución 305 de 2008 de la CDS.
NTC-ISO/IEC COLOMBIANA 27001:2013	11-dic-2013	Norma Técnica Colombiana NTC-ISO-IEC 27001.Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
Guía No 3	25-abr-2016	Procedimientos de Seguridad de la Información, MINTIC.

4. DEFINICIONES:

Ataque de fuerza bruta: Es el método para averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta. Los ataques por fuerza bruta son una de las técnicas más habituales de robo de contraseñas.

Activación de usuario: Se habilita acceso de usuario a la red, correo electrónico, sistemas de información, aplicativos que fueron suspendidos temporalmente por solicitud.

Comunicación Oficial: Son todas aquellas recibidas o producidas en desarrollo de las funciones asignadas legalmente a una entidad, independientemente del medio utilizado.

Cancelación de usuario: Se suspende de manera permanente el acceso del usuario a la red correo electrónico, sistemas de información, aplicativos, dependiendo de la solicitud.

Correo electrónico (Institucional): Servicio de red que permite a los usuarios enviar y recibir mensajes mediante la red de comunicación electrónica de la Contraloría de Bogotá.

Creación de usuario: Se asigna un usuario y contraseña para el ingreso a red, correo electrónico, sistemas de información, aplicativos.

Directorio Activo: Herramienta para la organización y gestión de usuarios de la red de computadoras.

Inactivación de usuario: Se suspende temporalmente el acceso del usuario a la red, correo electrónico, sistemas de información, aplicativos dependiendo de la solicitud.

Mesa de servicios: Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar requerimientos e incidentes relacionados a las Tecnologías de la Información y la Comunicación de manera integral, uno de sus componentes es el sistema de información en el cual se centraliza la recepción de solicitudes de los usuarios internos y externos de la Entidad.

Programas utilitarios privilegiados: Software que permite la administración, solución de problemas y monitoreo de sistemas de información e infraestructura tecnológica.

Sistemas de información: Conjunto de elementos que permiten el ingreso, almacenamiento, procesamiento y salidas de información de forma electrónica, estructurada y automatizada con el fin de apoyar las actividades de la Entidad, Ejemplo SIGESPRO, SIVICOF.

Sistema de atención de requerimientos (**mesa de servicios)**: Punto único de contacto entre el proveedor de servicio y los clientes internos y externos. Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación.

SIVICOF: Sistema de Vigilancia y Control Fiscal, sistema de información que permite rendición de cuenta de a Sujetos de Control.

Usuario de red: Es la identificación y contraseña asignada a un funcionario o contratista para permitirle el ingreso y el acceso a servicios de tecnología de la información en una red de computadoras de la Contraloría de Bogotá.

5. DESCRIPCIÓN DEL PROCEDIMIENTO:

5.1 Gestión de usuarios y contraseña e ingreso seguro a los sistemas de información.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Auxiliar Administrativo Secretario Técnico Operativo Profesional Universitario y/o Especializado Gerente Subdirector Técnico, Financiero o Administrativo Jefe Oficina Director Técnico Asesor Contralor Auxiliar Contralor (Solicitante)	Diligencia en el formato la solicitud de creación, modificación, inactivación, cancelación de acceso a usuario de red, correo electrónico, sistemas de información. **Si la solicitud es inactivación de usuario:** • Gestiona y/o termina las tareas, procesos, registros a su cargo en sistemas de información y/o aplicativos. • Registra la solicitud a través de Sistema de Mesa de Servicios, adjuntando archivo digital del Formato de solicitud y gestión de acceso a usuarios diligenciado correctamente. **Si la solicitud es activación de usuario:** Registra la solicitud a través de Sistema de Mesa de Servicios indicando el número de caso de solicitud de inactivación, sin	Anexo No. 1 Formato de solicitud y gestión de acceso a usuarios PGTI-07-01 Registro en el Sistema de Mesa de Servicios	**Punto de Control** Cuando la novedad administrativa implique entrega puesto de trabajo por retiro del servicio, periodo de prueba en otra entidad, abandono del cargo, muerte o suspensión en el ejercicio del cargo, se deben cancelar todos los accesos informáticos del servidor público. La inactivación del usuario se realizará a partir de la fecha de inicio que establezca la resolución de la novedad administrativa, para lo cual no debe tener tareas o procesos a su cargo en el aplicativo o sistema de información, una vez atendida la solicitud no podrá ingresar al sistema de información o aplicativo. En la activación de usuario, se habilitaran los accesos inactivos que fueron solicitados a través de mesa de servicio, no se crean usuarios o roles. **Observación:** Aplica para solicitudes de

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		adjuntar formato anexo No 1.		vinculación, contratación, terminación de contrato, situaciones administrativas que requieran entrega del puesto de trabajo, cambio de funciones en la dependencia, cambio de roles en sistemas de información o situaciones que implique cambios en el acceso a los sistemas de información.
2	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina. (Jefe de la dependencia).	**Si la solicitud es crear o cancelar usuario y/o roles** Aprueba formato de solicitud y gestión de acceso a usuarios. Registra la solicitud a través de Sistema de Mesa de Servicios, adjuntando archivo digital del *Formato de solicitud y gestión de acceso a usuarios* diligenciado correctamente. **Si la solicitud es cancelación de usuario:** • El usuario debe gestionar y/o terminar las tareas, procesos, registros a su cargo en sistemas de información y/o aplicativos.	Anexo No. 1 Formato de solicitud y gestión de acceso a usuarios PGTI-07-01 Registro en el Sistema de Mesa de Servicios	**Punto de control:** Limitar el acceso a la información de acuerdo a las funciones y cargos que desempeñe el funcionario y/o contratista sin brindar accesos de mayor alcance a los que se requiere. La cancelación del usuario se realizará a partir de la fecha de inicio de la resolución de la novedad administrativa o fecha de finalización de contrato, para lo cual el servidor público no debe tener tareas o procesos a su cargo en el aplicativo o sistema de información, para el caso de situaciones donde no se establezca acto administrativo la fecha debe ser determinada por el jefe de la dependencia. Si la solicitud demanda los derechos de acceso y control de roles de administrador y/o privilegiados a los sistemas de información, a la red, a

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				códigos fuentes de sistemas de información de propiedad de la Contraloría de Bogotá y el uso de programas utilitarios privilegiados, su acceso es únicamente autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones, justificando solicitud del requerimiento por parte del responsable del proceso en el espacio de observaciones del anexo No 1. Se prohíbe el uso de programas utilitarios que estén en capacidad de anular la administración y funcionamiento de los sistemas de información y de la plataforma tecnológica de la Contraloría de Bogotá.
3	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios. la entidad.	Válida el correcto diligenciamiento Formato de solicitud y gestión de acceso a usuarios. Sí el formato se encuentra incompleto o incorrecto, se devuelve al solicitante, se cambia el estado de la solicitud en el sistema de atención de requerimientos a suspendido, registrando la causal de devolución; el trámite continúa cuando el solicitante subsane la solicitud. **Si la solicitud es crear usuario o roles:**	Número de caso en el Sistema de Mesa de Servicios.	**Observación:** Las solicitudes de acceso remoto deben ser asignadas a través Sistema de Mesa de Servicios a Subdirector de Gestión de la Información, para su evaluación y aprobación, antes de ser asignadas a responsable de atención de requerimiento.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		• Valida en el Sistema de Mesa de Servicios que la solicitud provenga del usuario jefe de la dependencia • Verifica en directorio activo la existencia de usuario, en caso de no existir, en el formato debe estar la solicitud de creación de usuario de red. **Si la solicitud es cancelar usuario:** • Valida en el Sistema de Mesa de Servicios que la solicitud provenga del usuario jefe de la dependencia Asigna solicitud a responsable(s) en la Dirección de TIC para atender requerimiento. Activa procedimiento Registro y atención de requerimientos de soporte a los sistemas de información y equipos informático PGTI- 04. La solicitud se debe asignar en orden secuencial a los responsables en el siguiente forma según aplique, hasta atender totalmente la solicitud:		

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		1. Administrador de directorio activo. 2. Administrador de correo electrónico. 3. Administradores de sistemas de información. 4. Administrador de firewall (solicitud de acceso remoto VPN), previa autorización de Subdirector de gestión de la Información. 5. Soporte (configuración de usuario en PC).		
4	Profesional universitario y/o especializado de la Dirección TIC (Responsable de atención de la solicitud)	Ejecuta actividad de acuerdo a la Solicitud. Registra en el sistema de Mesa de Servicios el trámite realizado. Reasigna en el Sistema de Mesa de Servicios al siguiente responsable, si aplica o cambia su estado a "Solucionado" según corresponda, para finalizar el caso se debe verificar que se atendió en su totalidad la solicitud.	Número de caso en el Sistema de Mesa de Servicios Anexo No. 2 Formato entrega de usuario y contraseña sistemas de información PGTI-07-02.	**Punto de control:** No se permite la creación o uso de cuentas genéricas o anónimas a los sistemas de información y/o aplicativos. Para las solicitudes de activación de usuario, se habilitaran los accesos inactivos que fueron solicitados a través de mesa de servicio, no se crean usuarios o roles. **Observación:** Adjuntar a la respuesta de la solicitud en el Sistema de Mesa de Servicios el formato entrega de usuario y contraseña sistemas de información en caso de creación de usuario.
5	Auxiliar Administrativo Secretario Técnico Operativo Profesional Universitario y/o	Consulta respuesta en Sistema de Mesa de Servicios. Aplica anexo No 5. Instructivo para Gestión		**Punto de Control:** El acceso a la red y sistemas de información de un usuario registrado y autorizado en la Entidad, se debe autenticar siempre

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Especializado Gerente Subdirector Técnico, Financiero o Administrativo Jefe Oficina Director Técnico Asesor Contralor Auxiliar Contralor (Solicitante)	de Contraseñas Seguras		con su contraseña personal para acceder a los Sistemas de Información y a los servicios de la plataforma tecnológica. **Observaciones** Es responsable de • Mantener la confidencialidad de la contraseña, no entregarla, ni comunicarla a nadie. • Dar uso adecuado de las claves o contraseñas de acceso asignadas para la utilización de los equipos o servicios informáticos de la Entidad. • Proteger y resguardar toda información institucional reservada y clasificada que se tenga acceso a través de los aplicativos y/o sistemas de información. • Hacer uso de la información institucional de acuerdo a las funciones desempeñadas. • En situaciones administrativas que impliquen ausencia temporal o definitiva en el ejercicio del cargo, debe solicitar inactivación o cancelación de credenciales asignadas de acceso a los sistemas de información de la Entidad.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				• Reportar a la Dirección de Tecnologías de la Información y las Comunicaciones cualquier evento que atente contra la seguridad de la información. • Cumplir con las políticas de seguridad de la información de la Contraloría de Bogotá.
6	Subdirector de Gestión de la Información	Revisa el estado "Solucionado" y la atención **total** de la solicitud en el Sistema de Mesa de Servicios, firma formato PGTH-21-1/2/3 del procedimiento de entrega de puesto de trabajo.	Número de caso en el Sistema de Mesa de Servicio	

5.2 Gestión de Usuarios y contraseñas – revisión de los derechos de acceso

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
7	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC administrador del sistema de información	Genera para revisión de los derechos de acceso a usuarios, reporte trimestral de usuarios y roles **activos** en la red, correo electrónico, sistemas de información, acceso remoto y entrega a Subdirector de Gestión de la Información.	Reporte de usuarios activos	**Observaciones:** El reporte debe contener la siguiente información (según aplique): ✓ Nombre de Sistema de información y/o indicar si es usuario de correo electrónico, acceso red, acceso remoto. ✓ Cédula del usuario. ✓ Nombre y apellidos del usuario. ✓ Dependencia. ✓ Credencial de acceso

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				(usuario). ✓ Rol. ✓ Estado (Activo). ✓ Fecha de creación. ✓ Fecha de modificación. ✓ Fecha ultimo acceso.
8	Subdirector de Gestión de la Información	Remite a Despacho, Dirección, Oficina asesora el listado de usuarios de la dependencia según corresponda.	Comunicación Oficial Interna	
9	Contralor auxiliar, Director, Subdirector, Jefe Oficina (Jefe de la dependencia).	Revisa y depura listado de usuarios y roles de sistemas de información de la dependencia. Remite a Dirección de Tecnologías de la Información y las Comunicaciones la solicitud de depuración de usuarios listando nombre de sistema de información y roles a **cancelar**, o indicar si es usuario de correo electrónico, de acceso red o acceso remoto a **cancelar.**	Comunicación Oficial Interna	**Punto de Control** La solicitud masiva de depuración de usuarios se permite únicamente para cancelar usuarios y/o Roles. La solicitud debe contener la siguiente información: Dependencia ✓ Nombre: Sistema de información, correo electrónico acceso red, acceso remoto ✓ Cédula del usuario. ✓ Nombre y apellidos del usuario. ✓ Dependencia. ✓ Credencial de acceso (usuario). ✓ Rol. **Observación:** En caso de solicitudes de creación y/o modificación, realizar actividades de 5.1. Gestión de usuarios y contraseñas.
10	Subdirector de Gestión de la Información	Recibe la respuesta de los responsables de la actividad anterior, verifica el cumplimiento y entrega solicitud a		**Punto de control:** Las solicitudes que no cumplan con la información requerida para su atención,

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		responsable del Sistema de Mesa de Servicios.		se devuelven a solicitante, no se continúa la atención de requerimiento hasta que se subsane.
11	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios. la entidad.	Registra la información a través del Sistema de Mesa de Servicios, adjuntando memorando SIGESPRO de solicitud. Asigna solicitud a responsable(s) en la Dirección de TIC para atender requerimiento. Activa procedimiento PGTI- 04 Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos PGTI- 04.	Número de caso en el Sistema de Mesa de Servicios.	
12	Subdirector de Gestión de la Información	Responde la solución del requerimiento a responsable de la solicitud.	Comunicación Oficia Interna.	

5.3 Gestión de usuario y contraseña Sujetos de Control – SIVICOF

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Subdirector de Gestión de la Información	Recibe la solicitud de creación, modificación o inactivación de usuario en SIVICOF para sujeto de control con los anexos respectivos	Comunicación Oficia Interna. Anexo No 1. Formato Solicitud y Gestión de Acceso a	**Punto de control** Aplica PVCGF-13 procedimiento para la verificación, análisis, revisión y actualización de la cuenta, Numeral 5.3 – Actualización de los anexos, formatos, documentos, guía

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		debidamente diligenciados para el reporte de la Cuenta. Solicitud proveniente de la Dirección de Planeación.	Usuarios PGTI-07-01.	e instructivos de la cuenta.
2	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios. la entidad.	Registra solicitud a través de Sistema de Mesa de Servicios. Activa procedimiento Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos PGTI-04.	Número de caso en el Sistema de Mesa de Servicios.	
3	Profesional Especializado, Profesional Universitario, Tecnico de la Dirección TIC responsable del sistema SIVICOF	Ejecuta actividad de acuerdo a la Solicitud. Proyecta respuesta de creación de usuario sujeto de control a Director técnico de Planeación.	Comunicación Oficia Interna. Anexo No 1. Formato Solicitud y Gestión de Acceso a Usuarios PGTI-07-01.	**Punto de control:** ANS establecidos por la Dirección TIC para atención de requerimientos.
4	Subdirector de Gestión de la Información	Remite respuesta de creación de usuario de sujeto de control a Dirección de Planeación.	Comunicación Oficial Interna	
5	Subdirector de Gestión de la Información	Remite respuesta de creación de usuario de sujeto de control a Dirección de Planeación.	Comunicación Oficial Interna	
6	Profesional	Genera respuesta	Correo	**Observación**

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Especializado, Profesional Universitario, Técnico de la Dirección TIC responsable del sistema SIVICOF	de acuerdo a Anexo No 4 *Modelo de entrega de usuario SIVICOF a Sujeto de control* y envía a sujeto de control usuario y contraseña a través de correo electrónico registrado en la solicitud. Registra la respuesta a la solicitud y cambia a estado "Solucionado" en el sistema de atención de requerimientos que tenga dispuesta la Entidad.	Electrónico institucional. Anexo No 4 Modelo de entrega de usuario SIVICOF a Sujeto de control Número de caso en el Sistema de Mesa de Servicios.	Archivar respuesta en carpeta compartida designada por la Dirección parar el almacenamiento de correo electrónico.
Cambio de contraseña sujetos de control - SIVICOF				
7	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC responsable del sistema SIVICOF	Recibe la solicitud de cambio de contraseña correo institucional de Sujeto de Control a correo electrónico designado por la Contraloría de Bogotá para tal propósito. Registra solicitud a través del sistema de atención de requerimientos que tenga dispuesta la entidad. Activa procedimiento Registro y atención de requerimientos	Anexo No. 3 Modelo de solicitud de cambio de contraseña de SIVICOF para sujetos de control.	**Punto de Control** El representante debe estar registrado en SIVICOF, en caso contrario remitir acto administrativo de nombramiento. **Observación** Archivar solicitud en carpeta compartida designada por la Dirección para el almacenamiento de correo electrónico.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		de soporte a los sistemas de información y equipos informáticos PGTI-04.		
8	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC responsable del sistema SIVICOF	Modifica contraseña de acuerdo con la Solicitud. Informa a Sujeto de Control a través de correo electrónico registrado en SIVICOF, desde correo electrónico designado por la Contraloría de Bogotá para tal propósito. Registra la respuesta a la solicitud y cambia a estado "Solucionado" en el Sistema de Mesa de Servicios.	Correo electrónico institucional Anexo No. 4 Modelo de entrega de Usuario SIVICOF Número de caso en el Sistema de Mesa de Servicios.	**Punto de control:** ANS establecidos por la Dirección TIC para atención de requerimientos **Observación** Archivar respuesta en carpeta compartida designada por la Dirección parar el almacenamiento de correo electrónico (el cual hace parte de la tabla de retención documental TRD).

5.4 Gestión de usuario y contraseña de servidores, equipos de redes y comunicaciones de tecnologías de la Información.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional Especializado, Profesional universitario, Técnico de la Dirección TIC administrador de sistema de información o elemento de la infraestructura	Realiza cambio trimestral de contraseña de rol administrador a sistema de información o a elemento de infraestructura tecnológica administrable (servidores, switch,		**Punto de control** Garantiza la asignación de contraseñas seguras. Debe proteger y resguardar contraseñas, estas son carácter confidencial. **Observaciones**

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	de redes y comunicaciones de TI.	router, Access point, firewall, antivirus, dispositivos biométricos entre otros). Entrega información de clave en sobre cerrado a Subdirector de Gestión de la Información o a Subdirector de Gestión de Recursos Tecnológicos según corresponda		La información a entregar a Subdirectores Comunicaciones en sobre cerrado debe contener :: ✓ Nombre de SI o elemento de infraestructura tecnológica ✓ Dirección IP ✓ Fecha de asignación y periodo de vigencia de la contraseña. ✓ Usuario y Contraseña ✓ Nombres y apellidos de funcionario administrador que realiza cambio de contraseña
2		Subdirector de Gestión de la Información o a Subdirector de Gestión de Recursos Tecnológicos	Recibe, revisa contenido, sella sobre y custodia información de contraseña. Almacena información en lugar seguro garantizado el acceso únicamente a Director y Subdirectores de la Dirección de Tecnologías de la Información y las Comunicaciones. Terminado el periodo de vigencia de contraseñas, destruye información de manera segura.	**Punto de control** La apertura de sobre con información de contraseña únicamente es realizada por Director y/o Subdirectores de Tecnologías de Información y las comunicaciones.

6. ANEXOS

ANEXO 1. Formato Solicitud y Gestión de Acceso a Usuarios

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato Solicitud y Gestión de Acceso a Usuarios**	Código formato: PGTI-07-01 Versión:1,0
		Código documento: PGTI-07
		Versión: 1.0
		Página x de y

Fecha de solicitud				
	DD	**MM**	**YYYY**	

INFORMACIÓN DE LA DEPENDENCIA

Indique datos dependencia solicitante

Dependencia:				**Extensión:**	
Jefe de la Dependencia: (Autoriza la solicitud)					
Novedad Administrativa que motiva la solicitud:				**Otro, cuál?**	
Periodo de novedad administrativa: Fecha Inical: DD/MM/YYY (Aplica para entrega temporal del cargo y a novedades administrativas superiores		**Fecha Final Novedad Adm**		**No Resolución**	

INFORMACIÓN DEL FUNCIONARIO / CONTRATISTA/ TERCERO

Indique datos de funcionario a quien se va a realizar solicitud

Nombres y apellidos:			
Número de Cédula:		**Cargo**	
Tipo de vinculación:	☐ **Carrera Administrativa** ☐ **Provisional** ☐ **Contratista** ☐ **Libre nombramiento y remoci´ón** ☐ **Proveedor**		
Nombres y apellidos Supervisor de Contrato: (Aplica para contratistas)			
Fecha inicial Contrato: (Aplica para contratistas)		**Fecha Final Contrato: (Aplica para contratistas)**	

Seleccione de las siguientes opciones cuál aplica para su solicitud

INFORMACIÓN GENERAL DE LA SOLICITUD

CONFIGURAR PC	**USUARIO DE RED**	**CORREO ELECTRÓNICO**	**ACCESO REMOTO VPN**
Requiere configuración de usuario red, correo electrónico o sistemas de información en	☐**Crear** ☐**Modificar** ☐ **Inactivar** **Cancelar**	☐ **Crear** ☐ **Inactivar** ☐ **Cancelar**	☐ **Crear** ☐ **Inactivar** ☐**Cancelar**

PC? ☐ SI ☐NO	Indique modificación usuario:*(aplica para cambios de ubicación, nueva dependencia):*		Dirección IP: Fecha Inicial: Nombre PC/Servidor Fecha Final: Justificaciòn de Solicitud de Acceso Remoto

SISTEMAS DE INFORMACIÓN

No.	SISTEMA DE INFORMACIÓN	SOLICITUD	ASIGNAR ROL			
			ACCIÓN	NOMBRE	GRUPO (Solo aplica para PREFIS)	TRASLADO (Unicamente Sigespro,indique nueva dependencia)
1	Seleccione	Seleccione	Seleccione	Seleccione	Seleccione	Seleccione
2						
3						
4						
5						
6						
7						
8						
9						
10						

OTRO SISTEMA DE INFORMACIÓN *(Si no encuentra en el listado indique la siguiente información)*

No.	SISTEMA DE INFORMACIÓN	SOLICITUD	ASIGNACIÓN ROL		
			ACCIÓN	NOMBRE	OBSERVACIONES
1		Crear Usuario	Activar		
2					

SUJETO DE CONTROL SIVICOF

☐ Crear ☐ Modificar ☐ Cancelar

Razón Social Entidad: _____ **Naturaleza Jurídica:** _____

NIT: _____ **E-Mail:** _____

Nombre Representante Legal: _____ **No. Identificacón Representante Legal:** _____

Dirección: _____ **% Participación pública:** _____

Telefóno: _____ **Resolución Reglamentaria:** _____

OBSERVACIONES (Información adicional, breve de la solicitud)

INSTRUCCIONES DE DILIGENCIAMIENTO

Fecha Solicitud:	Fecha en que se realiza la solicitud formato día, mes, año. Campo diligenciado por solicitante.
Información de la dependencia	
Dependencia:	Nombre de Despacho, Dirección, Oficina que hace la solicitud.
Jefe de la dependencia:	Nombres y apellidos de Contralor, Director, Jefe de Oficina, Subdirector que autoriza la solicitud.
Extensión:	Número de extensión de la dependencia donde se pueda localizar a solicitante.
Novedad Administrativa que motiva la solicitud:	Selecciona de listado la novedad administrativa que motiva la solicitud.
Otro, cuál?:	Si no se encuentra en listado de novedades administrativas la situación que motiva la solicitud, indicarla en este campo.
Periodo de novedad administrativa: Fecha Inicial: DD/MM/YYY - Fecha Final Novedad	Aplica para entrega temporal del cargo y a novedades administrativas superiores a 15 días hábiles
Información del Funcionario / Contratista/ Tercero	
Nombres y apellidos:	Nombres y apellidos del funcionario, contratista, proveedor o tercero a quien se le va a crear, activar o inactivar usuario de sistemas de información, éste no aplica para creación de sujetos de control.
Número de cédula:	Número de Cédula del funcionario, contratista, proveedor o tercero a quien se le va a crear, activar o inactivar usuario de sistemas de información, éste no aplica para creación de sujetos de control.
Cargo:	Cargo del funcionario a quien se le va a crear, activar o inactivar usuario de sistemas de información, no aplica a contratista, proveedor o tercero.
Tipo de vinculación:	Marcar en cuadro según la vinculación del funcionario a quien se le va a crear, activar o inactivar usuario de sistemas de información. - Carrera administrativa. - Provisional - Contratista - Libre nombramiento y remoción - Proveedor
Nombres y apellidos de Supervisor del contrato:	Este aplica cuando la solicitud es contratista, indique nombre, apellidos de supervisor de contrato que avala la solicitu**d.**
Fecha inicial Contrato:	Aplica únicamente para Contratistas - Fecha de inicio de contrato
Fecha Final Contrato:	Aplica únicamente para Contratistas - Fecha de finalización de contrato
Información general de la solicitud	
Configurar PC:	Indique si requiere configuración usuario de red, correo electrónico o sistemas de información que ha sido solicitado en el PC.
Usuario de red:	Este campo se diligencia para solicitar la creación, modificación o inactivación de los usuarios para acceder a la red informática de la Contraloría de Bogotá: **Creación:** Se asigna un usuario y contraseña para el ingreso a red, correo electrónico, sistemas de información, aplicativos, dependiendo de la solicitud. **Inactivación:** Se suspende temporalmente el acceso del usuario a la red, correo electrónico, sistemas de información, aplicativos

	dependiendo de la solicitud. Aplica cuando el funcionario se encuentra en situaciones administrativas que implique la no utilización de la red, sistemas de información y correo electrónico de la Entidad, para la entrega temporal del puesto de trabajo y novedades administrativas superiores a 15 días hábiles que implican la entrega del cargo. **Modificación:** Aplica en caso que el funcionario se encuentre en situación administrativa de traslado o reubicación se debe indicar en el motivo de la modificación de usuario de red la dependencia donde es trasladado o reubicado. **Cancelación:** Se suspende de manera permanente el acceso del usuario a la red correo electrónico, sistemas de información, aplicativos, dependiendo de la solicitud. Aplica cuando en funcionario no requiere el acceso a de forma definitiva a la red, sistemas de información y/o correo electrónico o por situaciones administrativas que impliquen la entrega del puesto de trabajo como retiro del servicio, por periodo de prueba en otra entidad, abandono de cargo, muerte, entre otros.
Correo electrónico:	Este campo se diligencia para solicitar creación, inactivación, cancelación de correo electrónico institucional, este depende de la creación del usuario de red, por lo tanto se debe validar con la Dirección de Tecnologías de la Información y las Comunicaciones que se encuentre activo, de no ser así se debe solicitar su creación en el mismo formato.
Acceso remoto VPN:	Indique si requiere activar, inactivar, cancelar acceso remoto VPV a estaciones de trabajo o servidor, esta solicitud es revisada y aprobada por el Director de Gestión de la Información de la Dirección de Tecnologías de la Información y las Comunicaciones, se requiere información de: **Dirección IP:** Dirección IP de la maquina a la cual se va a habilitar o inactivar la conexión VPN. **Nombre PC/servidor:** Nombre de la maquina a la cual se va a habilitar o inactivar la conexión VPN. **Vigencia del servicio:** Fecha inicial y final en el cual se debe tener activa la VPN, este se diligencia en caso que accesos temporales, en caso que sea permanente indíquelo en esta casilla. **Justificación de Solicitud:** Justifique claramente el motivo de requerir acceso a VPN, si se requiere mayor espacio, utilice el espacio de observaciones.
Sistemas de Información El acceso a todos los sistemas de información de la Contraloría de Bogotá dependen de la creación del usuario de red, por lo tanto se debe validar con la Dirección de Tecnologías de la Información y las Comunicaciones que se encuentre activo, de no ser así se debe solicitar su creación en el mismo formato. Las opciones de solicitud son:	
Sistema de Información:	Seleccione de la lista el nombre del sistema de información.
Solicitud:	Seleccione de la lista una de las siguientes opciones, según aplique:
Creación Usuario:	Aplica cuando al usuario nunca se le ha solicitado de acceso al sistema de información (primera vez), obligatoriamente debe activar

	un rol
Modificación Usuario:	Aplica cuando el usuario ya se encuentra creado en el sistema de información y se requiere cambio de roles en el aplicativo, en esta opción se debe indicar específicamente la acción de activar, inactivar, cancelar el rol.
Asignación ROL Los roles Secretaria Común exigen que el Grupo sea Secretaria Común y el Administrador debe ser del grupo Administrador.	
Acción	Seleccione si se desea activar, inactivar, cancelar un **rol** del sistema de información.
Nombre:	Seleccione de la lista desplegable el nombre del rol, este se despliega según el sistema de información seleccionado.
Grupo:	Aplica únicamente para PREFIS. Campo que permite definir la visualización de información y opciones del sistema a nivel de la dependencia a la que pertenece y los reportes que puede consultar.
Traslado	Aplica únicamente para SIGESPRO. Indique el nombre de la dependencia de ubicación, cuando se presente traslado, encargo, comisión, esta información también debe ser indicada en USUARIO DE RED con la opción modificar.

La descripción de los sistemas de información son los siguientes:

SIVICOF: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema de Vigilancia y Control Fiscal, se debe indicar la acción (activar/inactivar) y el nombre del rol correspondiente.

SIVICOF	
Rol	**Descripción**
Consulta	Permite realizar consultas de la información presentada en formularios y documentos electrónicos en rendición de cuenta por los sujetos de control a través de reportes.
Observatorio	Permite realizar consultas de la información presentada en formularios y documentos electrónicos en rendición de cuenta por los sujetos de control a través de reportes, rol asignado a funcionarios de la Dirección de Planeación que cumplen funciones de análisis de estadísticas e indicadores
Sujeto de Control	Rol asignado a Sujetos de Control, permite acceso para realizar transmisión de la rendición de cuenta a la Contraloría de Bogotá y consulta de información presentada.
Economía y finanzas	Permite realizar consultas de la información presentada en formularios y documentos electrónicos en rendición de cuenta por los sujetos de control a través de reportes, rol asignado a funcionarios de la Dirección de Estudios de Economía y Política Pública que cumplen funciones de análisis de estadísticas presupuestales y financieras

SIGESPRO: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema de Gestión de Procesos y Documentos, se debe seleccionar

SIGESPRO	
Rol	**Descripción**

Correspondencia Interna/Externa	Rol asignado al funcionario de una dependencia u oficina que le permite enviar comunicaciones oficiales internas.
Derechos de petición, copia AZ	Rol asignado al funcionario de una dependencia que el permite el manejo los Derechos de Petición y las copias AZ de una dependencia.
Radicación Correspondencia	Rol asignado a funcionario de Radicación y Correspondencia que radica y escanea las comunicaciones oficinales externas, envío y recepción.
Directivo	Rol asignado a funcionario que tiene permiso para asignar procesos a los funcionarios de una dependencia u oficina. Tiene firma mecánica para las comunicaciones oficiales internas y externas. Adicionalmente tiene habilitada la pestaña de Reparto.
Gerente	Rol asignado a funcionario que tiene firma mecánica para las comunicaciones oficiales, internas y externas. No tiene habilitada la pestaña de Reparto.

ORDENES DE PAGO: Se diligencia para solicitar creación o inactivación de órdenes de pago, seleccionar opción.

RELCO: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema de información de Relatoría, se debe seleccionar la acción de activar, inactivar y el nombre del rol correspondiente.

RELCO	
Rol	**Descripción**
Relator	Permite: • Crear/eliminar/modificar Relatos • Consultar Relatos • Consultar Tesauros • Consultar Narrativas de líneas decisionales • Consultar Árbol de líneas decisionales
Sustanciador	Permite: • Consultar Relatos • Consultar Tesauros • Consultar Narrativas de líneas decisionales • Consultar Árbol de líneas decisionales
Consulta	Permite: • Consultar Relatos • Consultar Tesauros • Consultar Árbol de líneas decisionales • Consultar Narrativas de líneas decisionales
Operador Jurídico	Permite realizar las siguientes acciones en el sistema: • Crear/eliminar/modificar dependencias o localidades • Crear/eliminar/modificar los temas (líneas de decisión) • Crear/eliminar/modificar naturaleza e instancias de los documentos • Crear/eliminar/modificar naturaleza Narrativas de líneas decisionales • Crear/eliminar/modificar Árbol de líneas decisionales • Consultar Relatos • Consultar Tesauros • Consultar Narrativas de líneas decisionales • Consultar Árbol de líneas decisionales

PREFIS: Se diligencia para solicitar crear o inactivar permisos de acceso al Sistema de Información de para el manejo y control del proceso de responsabilidad Fiscal, se debe seleccionar la acción de activar, inactivar y el nombre del rol correspondiente.

PREFIS	
Rol	**Descripción**
Administrador	Permite ejecutar acciones en el sistema asociadas a: • Creación de usuarios, modificación de datos de los funcionarios, implicados, garantes, apoderados y números de procesos. • Creación y modificación de entidades, funcionarios, calendario y actuaciones. • Consulta de usuarios y registros de ingreso. • Creación de backups y generación de reportes.
Profesional sustanciador	Asignado a los abogados que han sido designados o comisionados en la dependencia para adelantar las actuaciones en los expedientes asignados. Sólo puede consultar y registrar información de los procesos en los cuales ha sido asignado en el sistema. Tiene habilitadas las opciones para crear y modificar implicados, garantes, apoderados. Las opciones y visibilidad de información están asociadas únicamente a los procesos asignados.
Secretario Común	Rol que permite realizar la administración de datos de todos los procesos, funcionarios, implicados, garantes, apoderados, entidades que existen en el sistema. Permite la asignación, reasignación y modificación de procesos a los usuarios del sistema. Permite consultar la información de todos los procesos de la dependencia a la que pertenece y de todos los informes especializados dispuestos en el sistema.
Grupo	Campo que permite definir la visualización de información y opciones del sistema a nivel de la dependencia a la que pertenece y los reportes que puede consultar. Los roles Secretaria Común exigen que el Grupo sea Secretaria Común y el Administrador debe ser del grupo Administrador.

SIMUC: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema de Cobro de Multas, se debe seleccionar la acción de activar, inactivar y el nombre del rol correspondiente.

SIMUC	
Rol	**Descripción**
Administrador	Rol que permite administrar toda la información del sistema, recalcular valor a un proceso y administrar toda la información asociada al proceso, el IBC, liquidador, costas, actualización de datos de intereses, ajustar cuantías, generación informe Auditoría general. Rol que tiene habilitadas todas las opciones del sistema.
Liquidador	Rol asignado a los abogados que han sido designados o comisionados en la dependencia para adelantar la representación de la entidad en los expedientes asignados. Sólo puede consultar y registrar información de los procesos en los cuales ha sido asignado en el sistema. Tiene habilitadas las opciones para crear y modificar información de cuotas, ejecutados, acuerdos de pago, pólizas, discriminación de cuantías, revocatorias, medidas cautelares. Permite generar la liquidación de los procesos ajustando las costas al proceso, y la relación de procesos por tipo de multa. Las opciones y visibilidad de información están asociadas únicamente a los procesos asignados.

Subdirector Coactivo	Rol asignado al Jefe de la Subdirección Coactiva para consultar y registrar información de todos los procesos del sistema. Tiene habilitadas las opciones para crear y modificar información de cuotas, ejecutados, acuerdos de pago, pólizas, discriminación de cuantías, revocatorias, medidas cautelares. Permite generar la liquidación de los procesos ajustando las costas al proceso, y la relación de procesos por tipo de multa. Las opciones y visibilidad de información corresponden a todos los expedientes existentes en el sistema.

LIMAY: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema SI CAPITAL modulo Contable Libro Mayor, se debe seleccionar la acción de activar, inactivar y el nombre del rol correspondiente.

LIMAY	
Rol	**Descripción**
Consulta	Permite consulta de todas las funcionalidades de la aplicación y generación de reportes.
Registro / modificación	Permite el ingreso y/o modificación de información contable.

OPGET: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema SI CAPITAL módulo de Operación y Gestión de Tesorería, se debe seleccionar la acción de activar, inactivar y el nombre del rol correspondiente.

OPGET	
Rol	**Descripción**
Consulta	Permite consulta de todas las funcionalidades de la aplicación y generación de reportes
Registro / modificación	Permite el ingreso y/o modificación de información de tesorería.

PREDIS: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema SI CAPITAL módulo de Presupuesto, se debe seleccionar la acción de activar, inactivar y el nombre del rol correspondiente.

PREDIS	
Rol	**Descripción**
Consulta	Permite consulta de todas las funcionalidades de la aplicación y generación de reportes.
Registro / modificación	Permite el ingreso y/o modificación de información de presupuesto.

PERNO: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema SI CAPITAL módulo de Autoliquidación de Nómina y Personal, se debe seleccionar la acción de activar, inactivar y el nombre del rol correspondiente.

PERNO	
Rol	**Descripción**

Administrador	Permite administrar la información asociada a todos los procesos de talento humano y actividades de parametrización de tablas en el sistema. Crea y asigna usuarios en el sistema. Es un súper usuario que tiene acceso a todas las opciones del sistema.
Administrador Capacitación	Permite administrar la información básica y actividades de parametrización de tablas en el sistema únicamente en el módulo de capacitación.
Administrador Bienestar	Permite administrar la información básica y actividades de parametrización de tablas en el sistema únicamente en el módulo de bienestar.
Liquidador nómina	Permite controlar, validar y procesar la información de los funcionarios para el pago de sus salarios, sobre un periodo específico, quincenal o mensual. Ejecución de reportes asociados a la liquidación de la nómina y la consulta de información de los funcionarios. Permite administrar dependencias, cargos y posiciones de la planta de personal global de la entidad, contemplando niveles, grados, funciones y perfiles de los cargos.
Generado Autoliquidaciones	Rol del usuario encargado de generar la autoliquidación de aportes a seguridad social. Permite controlar, validar y procesar la información de aportes a Salud, aportes a Pensión y aportes a la ARP para las diferentes entidades prestadoras de estos servicios. Permite generar autoliquidación, restar adicionales, editar incapacidades
Prestaciones Sociales	Rol del usuario encargado de liquidar prestaciones.
Descuentos	Rol del usuario encargado de controlar cupo de endeudamiento y registrar descuentos a los funcionarios.
Jefe de Oficina	Rol del usuario jefe de la unidad de nómina.
Hojas de Vida	Rol del usuario encargado del mantenimiento de hojas de vida de los funcionarios. Permite mantener la información básica de la hoja de vida de los funcionarios de planta y/o Temporales y/o supernumerarios de la Entidad. Permite la administración de novedades y actos administrativos de los funcionarios.
Generador Rel. Autorización	Rol del usuario encargado de generar las relaciones de autorización para pagos de nómina, de aportes y cesantías. Además permite generar los aportes parafiscales y aportes al Fondo Nacional del Ahorro - liquidado en la nómina
Generador Contab Nómina	Rol del usuario encargado de registrar en Limay las transacciones asociadas a los pagos de nómina. Permite realizar el registro contable en el sistema LIMAY de las diferentes nóminas que incluyan algún componente monetario o de valor contable. El proceso de contabilización de la Nómina depende o se inicia una vez se ha generado, aprobado y cerrado una Nómina.

SAE /SAI: Se diligencia para solicitar creación, modificar o inactivar permisos de acceso al Sistema SI CAPITAL módulo de Almacén e Inventarios, se debe seleccionar la acción de activar, inactivar y el nombre del rol correspondiente

SEA / SAI	
Rol	**Descripción**
Almacenista	Rol asignado a funcionario que cumple funciones del cargo de almacenista
Operador	Rol asignado a funcionario que cumple funciones de operador en almacén de la Subdirección de Recursos Materiales

Otro Sistema de Información Estos campos se diligencian en caso que el sistema de información no se encuentre en el listado de selección, se debe diligenciar la siguiente información:	
Sistema de Información:	Digite el nombre del sistema de información

Solicitud:	Selecciones de la lista una de las siguientes opciones, según aplique **Creación Usuario**: Aplica cuando al usuario nunca se le ha solicitado de acceso al sistema de información (primera vez), obligatoriamente debe activar un rol. **Modificación Usuario**: Aplica cuando el usuario ya se encuentra creado en el sistema de información y se requiere cambio de roles en el aplicativo, en esta opción se debe indicar específicamente la acción de activar/inactivar y el nombre del rol.
Asignación ROL	
Acción:	Seleccione si se desea activar o inactivar un rol del sistema de información.
Nombre:	Digite el nombre del rol.
Observaciones:	Digite las observaciones.
Sujeto de Control SIVICOF	

Informacion Creación Usuario Sujeto e Control

Este es utilizado únicamente por la Dirección de Planeación para solicitar la creación, modificación y/o cancelación de un Sujeto de Control del Sistema De Vigilancia y Control Fiscal SIVICOF, se debe especificar:

- Razón social de la Entidad Sujeto de Control.
- Naturaleza Jurídica
- NIT
- E-Mail
- Nombre de Representante Legal
- No Identificación Representante Legal
- Dirección
- % Participación publica
- Teléfono
- Resolución Reglamentaria de creación o inactivación de sujeto de control

Cuando es cancelación de usuario para sujeto de control se debe especificar el número de Resolución Reglamentaria de exclusión, eliminación o cambio del Sujeto de Control.

ANEXO 2. Formato de entrega de usuario y contraseña.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato Entrega de Usuario y Contraseña**	Código formato: PGTI-07-02 Versión:1.0
		Código documento: PGTI-07 Versión:1.0
		Página x de y

Fecha			**Funcionario / Contratista**	
			Nombres y apellidos de funcionario que se asigna usuario y contraseña	
DD	**MM**	**AA**	**Ubicación**	*Despacho / Dirección / Subdirección/ Oficina*

La Dirección de Tecnologías de la información y las Comunicaciones, informa el usuario y contraseña asignado para el acceso a sistemas de información de la Contraloría de Bogotá:

Usuario	**Contraseña**	**Servicio Informático**
Nombre de Usuario	*Contraseña*	*Nombre de servicio informático o sistema de información*
Nombre de Usuario	*Contraseña*	*Nombre de servicio informático o sistema de información*

Por favor aplicar el instructivo para la gestión de contraseña segura y las siguientes indicaciones:

1. La contraseña seleccionada debe tener letras mayúsculas, minúsculas, símbolos, números mínimo 8 caracteres y al menos un número, es importante que no contenga nombres, números de teléfono, palabras, números o letras consecutivas repetidas, utilice contraseñas seguras.
2. Es responsabilidad del funcionario y/o contratista la correcta utilización y no divulgación de la contraseña, siendo esta información secreta, personal, única e intransferible, por tal razón se solicita en el primer ingreso a la red realizar el cambio de contraseña y debe solicitar la inactivación cuando realice entrega del cargo o finalización del contrato.
3. La contraseña de red deberá cambiarse periódicamente a través de la opción Alt+Control+Supr\ cambiar contraseña, las contraseñas de sistemas de información a través de la opción que tenga habilitada cada sistema para tal fin.
4. La vigencia máxima de la contraseña de usuario de red es de 60 días de forma que las contraseñas caducan pasado este periodo de tiempo.
5. La cuenta de usuario se bloquea con tres intentos errados seguidos.

Es responsabilidad del funcionario(a)/contratista que se asigna acceso a los servicios informáticos de la Contraloría de Bogotá:

- Proteger y resguardar toda información institucional de carácter confidencial, reservada y clasificada.
- Hacer uso del de la información institucional de acuerdo a las funciones desempeñadas.

- Reportar cualquier evento que atente contra la seguridad de la información.
- Cumplir con las políticas de seguridad de la información de la Contraloría de Bogotá.
- En situaciones administrativas que impliquen ausencia temporal o definitiva en el ejercicio del cargo se debe solicitar inactivación o cancelación de credenciales asignadas de acceso a los sistemas de información de la Entidad.

Subdirección de Gestión de la Información
Dirección de Tecnologías de la información y las Comunicaciones

INSTRUCCIONES DE DILIGENCIAMIENTO

Fecha:	Fecha de asignación usuario y contraseña para acceso a servicio informatico.
Funcionario/ contratista:	Nombres y Apellidos de funcionario a quien se asigna usuario y contraseña
Ubicación:	Dependencia del funcionario que se asigna usuario y contraseña.
Usuario:	Se indica el usuario asignado para acceso a la red, correo electrónico, sistemas de información, según corresponda.
Contraseña:	Se indica la contraseña asignada para acceso a la red, correo electrónico, sistemas de información, según corresponda.
Servicio Informático:	Se indica el servicio al cual fue asignado el acceso: red, correo electrónico, nombre de sistema de información según corresponda.

ANEXO 3. Modelo solicitud de cambio de contraseña de SIVICOF para Sujetos de Control

MODELO SOLICITUD CAMBIO DE CONTRASEÑA DE SIVICOF PARA SUJETOS DE CONTROL
(Debe ser impreso en papel membretado de la entidad que realiza la solicitud)

Bogotá, Fecha

Señores:
CONTRALORIA DE BOGOTA
Dirección Tecnologías de la Información y las Comunicaciones
Bogotá, D.C.

Asunto: Solicitud de cambio de contraseña para acceso a Sistema de Vigilancia y Control SIVICOF de la Contraloría de Bogotá D.C.

En mi calidad de *representación legal* de *nombre completo de la entidad* con NIT No *número completo de NIT de la entidad***,** de manera atenta solicito que en el Sistema de Vigilancia y Control Fiscal – SIVICOF se realice:

☐ Cambio de contraseña
☐ Cambio de correo electrónico: *registre nuevo correo electrónico*

Esto motivado en _____

Así mismo solicito que la contraseña asignada sea enviada al correo electrónico registrado en la plataforma SIVICOF de la Contraloría de Bogotá.

Agradezco su atención.
Cordialmente,

Nombre Representante Legal
Número y ciudad de expedición de identificación
Nombre de la Entidad
Dirección de la entidad
Teléfono
En caso que el Representante Legal no se encuentre registrado en SIVICOF se debe remitir acto administrativo de nombramiento adjunto a la solicitud.

ANEXO 4. Modelo de entrega de usuario SIVICOF a Sujeto de control

Bogotá, Fecha

Doctor(a):
REPRESENTANTE LEGAL
Nombre de la Entidad
correo electronico@xxxx.xxx
Ciudad

Ref.: Creación de usuario y contraseña / Cambio de contraseña en Sistema de Vigilancia y Control SIVICOF de la Contraloría de Bogotá D.C.

Cordial saludo,

En ocasión a la solicitud presentada por *nombre completo de la entidad* a través de *radicado No / correo electrónico*, la Dirección de Tecnologías de la información y las Comunicaciones, informa el usuario y contraseña asignado a la Entidad en el Sistema de Vigilancia y Control SIVICOF como mecanismo para la presentación de la cuenta (Resolución Reglamentaria N° 011 de 2014 Art 8):

Usuario	Nombre Entidad	Contraseña
Código de Usuario SIVICOF	*nombre completo de la entidad*	*Contraseña*

Es importante mencionar, que le asiste la responsabilidad de mantener el carácter confidencial de la contraseña de la entidad y por esto acepta asumir las implicaciones resultantes de la utilización y/o divulgación de la misma, por tal razón se solicita modificarla después de ingresar al aplicativo por la opción Datos Usuario/Cambiar contraseña.

Subdirección de Gestión de la Información
Dirección de Tecnologías de la Información y las Comunicaciones
Contraloría de Bogotá D.C

ANEXO No 5. Instructivo para la Gestión de Contraseñas Seguras

INSTRUCTIVO PARA LA GESTIÓN DE CONTRASEÑAS SEGURAS

La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá, establece los siguientes lineamientos para que los servidores públicos de la entidad apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

CONDICIONES GENERALES

- La Dirección de Tecnologías de la Información y las Comunicaciones es la encargada de realizar la gestión de acceso de los sistemas de información de la Contraloría de Bogotá, las solicitudes se atienden mediante el Sistema de Mesa de Servicio en aplicación del Procedimiento de Control de Acceso a Sistemas de Información.
- La contraseña es un código único, personal e intransferible, que no debe ser divulgado o compartido con terceras personas.
- La vigencia máxima de la contraseña de usuario de red es de 60 días de forma que las contraseñas caducan pasado este periodo de tiempo.
- La cuenta de usuario se bloquea con tres intentos errados seguidos, para evitar ataques de fuerza bruta.
- El primer ingreso a la red se debe realizar el cambio de contraseña.
- Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

CONTRASEÑA SEGURA O FUERTE

Una contraseña segura, es un código especial para proteger los accesos a los recursos informáticos de la entidad, que debe cumplir los siguientes requisitos.

- Tener letras mayúsculas, minúsculas, símbolos, números mínimo 8 caracteres y al menos un número, es importante que no contenga nombres propios, apellidos, números de teléfono, palabras, números o letras consecutivas repetidas, ni ser frases famosas o refranes.

- Ser de fácil recordación e introducción, aunque difícil de adivinar y de descubrir por terceras personas.
- Utilizar la concatenación de varias palabras para construir contraseñas largas cuya deducción, automática o no, no sea simple, también pueden utilizarse frases cortas sin sentido.
- No debe ser igual a ninguna de las últimas de las contraseñas usadas, ni estar formada por una concatenación de ellas.
- Debe cambiarse ante la evidencia de que hubieren sido vulneradas o comprometidas.
- No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- Evitar apuntarla en papel o elementos no seguros de fácil exposición a terceros.
- No habilitar recordación automática de contraseñas en procesos de registro, por ejemplo almacenadas en una función o formulario de auto llenado.

CAMBIO DE CONTRASEÑA

La contraseña de red deberá cambiarse periódicamente a través de la opción de cambio de contraseña a través del sistema operativo:

Presione simultáneamente las teclas Alt+Control+Supr
Escriba la contraseña anterior.
Escriba la contraseña nueva dos veces, la segunda vez es para reconfirmar la contraseña.

El cambio de contraseñas de los aplicativos y/o sistemas de información debe realizarse a través de la opción que tenga habilitada cada aplicativo /sistema para tal fin.

USO DE LA INFORMACIÓN DE AUTENTICACIÓN SECRETA

- El acceso a la red y sistemas de información de un usuario registrado y autorizado en la Entidad, se debe autenticar siempre con su contraseña personal para acceder a los Sistemas de Información y a los servicios de la plataforma tecnológica.
- No se permite el uso de cuentas genéricas o anónimas.
- No facilitar usuarios o claves de acceso de los sistemas de información y/o aplicativos a terceros.

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0		Versión Inicial