RESOLUCIÓN DE 2018

CONTRALORÍA DE BOGOTÁ, D.C.

Resolución Reglamentaria Número 047

(Diciembre 28 de 2018)

"Por la cual se adoptan y actualizan procedimientos que conforman el Proceso Gestión de Tecnologías de la Información en la Contraloría de Bogotá, D.C."

EL CONTRALOR DE BOGOTÁ, D.C.
En ejercicio de sus atribuciones constitucionales y legales, en especial las conferidas por el Acuerdo No. 658 de 2016, modificado por el Acuerdo 664 de 2017, expedidos por el Concejo de Bogotá, D.C.

CONSIDERANDO:

Que de conformidad con el artículo 269 de la Constitución Política de Colombia, es obligación de las autoridades públicas diseñar y aplicar en las entidades públicas, métodos y procedimientos de control interno, según la naturaleza de sus funciones, de conformidad con lo que disponga la ley.

Que según los literales b) y l) del artículo 4 de la Ley 87 de 1993 *"Por la cual se establecen normas para el ejercicio de control interno en las entidades y organismos del Estado y se dictan otras disposiciones",* se deben implementar como elementos del sistema de control interno institucional los procedimientos para la ejecución de procesos y la simplificación y actualización de normas y procedimientos.

Que mediante Resolución Reglamentaria No 038 de 8 de octubre de 2018, se adoptó la nueva versión del Modelo Estándar de Control Interno –MECI, en la Contraloría de Bogotá, D.C., de conformidad al Decreto 1499 de 2017, modificatorio del Decreto 1083 del 2015 – Decreto Único Reglamentario del Sector Función Pública-, con el fin de incorporar la estructura definida en la dimensión 7ª Control Interno del Manual Operativo del Modelo Integrado de Planeación y Gestión - MIPG.

Que el Concejo de Bogotá D.C., expidió el Acuerdo 658 de 2016, por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., estableciendo en el artículo 6° que: *"En ejercicio de su autonomía administrativa le corresponde a la Contraloría de Bogotá, D.C., definir todos los aspectos relacionados con el cumplimiento de sus funciones en armonía con los principios consagrados en la Constitución, las Leyes y en este Acuerdo".*

Que en los numerales 3,11 y 15 del artículo 40 del precitado Acuerdo, establece entre las funciones de la Dirección de Tecnologías de la Información y las Comunicaciones: "Coordinar la aplicación a todo nivel de la organización de los estándares, buenas prácticas y principios para el manejo de la información", *"Vigilar que en los procesos tecnológicos de la entidad se tengan en cuenta los estándares y lineamientos dictados por el Ministerio de las Tecnologías de la Información y las Comunicaciones, que permitan la aplicación de las políticas que en materia de información expidan las autoridades competentes."* y *"Organizar los procesos internos de producción de información para cumplir con las políticas, los planes, los programas y los proyectos teniendo en cuenta los lineamientos para la información estatal".*

Que mediante Resolución Reglamentaria No. 007 del 16 de febrero de 2018 se adoptan nuevos procedimientos que conforman el Proceso Gestión de Tecnologías de la Información de la Contraloría de Bogotá, D.C.

Que mediante la Resolución Reglamentaria No. 022 del 19 de abril de 2018 la Contraloría de Bogotá,

D.C., modifica las Políticas de Seguridad y Privacidad de la Información.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones, expidió el Decreto 1008 de 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", en el cual se dictan disposiciones en Seguridad de la Información como habilitador transversal de la Política de Gobierno Digital, en aplicación de la Guía No 3 procedimientos de seguridad de la información establecidos en el Modelo de Seguridad y Privacidad de la Información de MINTIC e implementación de estándares internacionales y nacionales establecidos en la norma ISO/IEC 27001:2013.

Que según revisión de la Dirección de Tecnologías de la Información y las Comunicaciones a sus procedimientos en el proceso para la implementación del Subsistema de Seguridad de la Información, se considera necesario ajustar los procedimientos del Proceso Gestión de Tecnologías de la Información, atendiendo los aspectos normativos vigentes.

RESUELVE:

ARTÍCULO PRIMERO. Adoptar los siguientes procedimientos del proceso Gestión de Tecnologías de la Información.

No	Nombre de Procedimiento	Código	Versión
1	**Procedimiento de Control de Acceso a Usuarios.**	**PGTI-07**	**1.0**
2	**Procedimiento para la Gestión de Cambios y Capacidad Tecnológica.**	**PGTI-08**	**1.0**
3	**Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.**	**PGTI-09**	**1.0**
4	**Procedimiento Gestión de Incidentes de Seguridad.**	**PGTI-10**	**1.0**
5	**Procedimiento Gestión de Seguridad en las Comunicaciones y Criptografía.**	**PGTI-11**	**1.0**

ARTÍCULO SEGUNDO. Actualizar los siguientes procedimientos del proceso Gestión de Tecnologías de la Información.

No	Nombre de Procedimiento	Código	Versión
1	Procedimiento Registro y Atención de Requerimientos de Soporte a los Sistemas de Información y Equipos Informáticos.	PGTI-04	2.0
2	Procedimiento Gestión de Recursos y Servicios Tecnológicos.	PGTI-05	2.0
3	Procedimiento Gestion de Seguridad Informática.	PGTI-06	2.0

ARTÍCULO TERCERO. Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina y Gerentes, velar por la divulgación y cumplimiento de los procedimientos adoptados.

ARTÍCULO CUARTO. La presente Resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias, en especial lo señalado en el Artículo 3 de la Resolución Reglamentaria No.007 del 16 de febrero de 2018.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los veintiocho (28) días del mes de diciembre de dos mil dieciocho (2018).

JUAN CARLOS GRANADOS BECERRA
Contralor de Bogotá D. C.

	Aprobación	Revisión Técnica
Firma:		
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 Diciembre 28 de 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.	Valida 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 apliqa 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.xxxx
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	R.R. No. 047 28 Diciembre 2018	Versión Inicial

	Aprobación	Revisión Técnica
Firma:		
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. N°	**047**	**Fecha Diciembre 28 de 2018**

1. OBJETIVO

Establecer las actividades que garanticen que los cambios de tecnología se evalúan, aprueban, implementan y revisan de manera controlada y segura en las operaciones de la Dirección de Tecnologías de la Información, para la Contraloría de Bogotá D.C.

2. ALCANCE

Este procedimiento inicia con la creación del grupo interno de gestión de cambios de la Dirección de TIC (CAB-TIC) y finaliza con la generación del informe de desempeño del documento de Gestión de Capacidad y actualización las líneas base de configuración de los componentes de TI.

3. BASE LEGAL

NORMA	FECHA	DESCRIPCIÓN
Ley 1273	5-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 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 2573	12-dic-2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único 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
CONPES 3701-2011	14 - jul - 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa Estrategia Nacional de Ciberseguridad y Ciberdefensa
NTC-ISO/IEC COLOMBIANA 20000-1:2011	abr-2011	Norma Técnica Colombiana NTC-ISO/IEC 27001 Colombiana. Tecnología de la Información.Gestión de Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio.
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

Acuerdos de Niveles de Servicio (ANS)[1]: Acuerdo documentado entre un prestador de servicios y un cliente, el cual identifica los servicios y los objetivos del servicio.

Cambio[2]: Adición, modificación o eliminación de cualquier elemento y/o activo de información que afecte los servicios de TI.

Cambio Normal: Corresponde a los cambios en los elementos de TI que afectan la disponibilidad y continuidad de los servicios de TI y requieren la valoración y aprobación de Grupo de Cambios.

Cambio de Emergencia: Cualquier interrupción del servicio de alto impacto ya sea en el número de usuarios afectados o porque se han visto involucrados sistemas o servicios críticos, siendo necesario encontrar una respuesta tan pronto como sea posible.

Cambio Mayor: Corresponde a cambios que pueden poner en riesgo a la entidad en caso de falla. Ej. Migración de sistemas, cambios de tecnología, cambios en las topologías de red, entre otros.

Cambio Estándar: Es un cambio pre-aprobado que es de bajo riesgo, relativamente común y sigue un procedimiento o instrucción de trabajo. Ej. Cambios de clave o requerimientos de servicios.

Comité Asesor de Cambios (CAB) – ITIL[3]: Grupo de personas que revisan, clasifican evalúan, priorizan, autorizan y establecen la programación de los cambios en tecnología.

Documento de Gestión de Capacidad: Es un documento que contiene los lineamientos y atributos para gestionar los recursos necesarios para entregar los servicios de TI. Contiene los detalles sobre el uso actual e histórico de los servicios de TI y de sus componentes.

Gestión de cambios: Es el proceso responsable de controlar el ciclo de vida de todos los cambios, permitiendo que se realicen los cambios que son beneficios y minimizando la interrupción de los servicios de TI.

Gestión de capacidad: Es el proceso responsable de asegurar que la capacidad de los servicios de TI y la infraestructura de TI puedan cumplir con los requerimientos relacionados con la capacidad y desempeño de una manera rentable y oportuna; considerando todos los recursos necesarios para proporcionar un servicio de TI y se preocupa de satisfacer las necesidades tanto de la capacidad actual y fututa, así como del desempeño de la entidad.

Grupo Interno de Gestión de Cambios la Dirección de Tecnologías de la Información y las Comunicaciones – (CAB-TIC): Grupo de funcionarios adscritos a la Dirección de TIC de

[1] Tomado: NTC-ISO–IEC COLOMBIANA 20000:2011
[2] Tomado de: Biblioteca ITIL v. 3.0- Conjunto de publicaciones de mejores prácticas para la gestión de los servicios TI.
[3] Ídem

la Contraloría de Bogotá, que cumplen las funciones de un comité asesor de cambios en relación con aspectos tecnológicos de la entidad.

Impacto: Determina la importancia del cambio dependiendo de cómo se ven afectados los procesos de la entidad y/o el número de usuarios afectados.

Línea base de configuración: Es la configuración de un elemento o sistema establecido en un momento concreto en el tiempo, que capta tanto la estructura como los detalles de una configuración, sirve como referencia para más actividades, adicionalmente, proporciona la habilidad de cambiar o reconstruir una versión concreta en una fecha más adelante. Las líneas base de configuración se deben establecer mediante un acuerdo formal en momentos concretos del tiempo y se deben utilizar como puntos de referencia para el control formal de una configuración.

Prioridad: Categoría utilizada para representar la importancia relativa a los requerimientos, y cambios. La prioridad se fundamenta en el impacto y la urgencia y es utilizada para identificar los tiempos en los que se deben tomar las acciones requeridas.

Recurso de software: Software de aplicación, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.

Recurso de hardware: Equipo de cómputo, equipo de comunicación, medios removibles y otro equipo que por su criticidad son considerados activos de información, no sólo activos fijos.

Riesgo Operacional[4]: El potencial impacto en activos, aplicaciones, procesos y/o plataformas clave, incluyendo sus servicios relacionados, que podrían resultar de capacidades insuficientes o procesos internos fallidos, sistemas o tecnologías, o las acciones deliberadas o inadvertidas de personas, o eventos externos.

Roll Back: Actividades previamente establecidas para volver atrás un cambio cuando los resultados esperados del mismo no son satisfactorios y no es conveniente continuar con su implementación.

Sistema de Mesa de servicios: Sistema manual o automatizado donde los funcionarios o entes externos registran las solicitudes e incidencias sobre los servicios que presta la Dirección de TIC.

Solicitud de Cambio[5]: Propuesta formal para que se realice un cambio, incluye los detalles del cambio propuesto y puede ser registrada en papel o en la herramienta para gestionar requerimientos.

[4] Tomado de: Glosario de seguridad cibernética para la comisión interamericana de puertos organización de los Estados Americanos. HA Ciber.2017
[5] Tomado de: Biblioteca ITIL v. 3.0

Urgencia: Medida de cuanto puede esperarse para que un cambio o requerimiento tenga un impacto significativo en la entidad.

DESCRIPCION DEL PROCEDIMIENTO

5.1. GESTIÓN DE CAMBIOS TECNOLÓGICOS

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de Tecnologías de la Información y la comunicaciones	Crea el Grupo interno de gestión de cambios de la Dirección de TIC (CAB-TIC), el cual estará conformado por el Director, los Subdirectores de la Dirección de TIC, el líder de seguridad de la Información y los administradores y/o gestores de infraestructura y/o servicios de TI según el cambio a evaluar.	Comunicación Oficial	**Observación:** Al Grupo interno de gestión de cambios, deben ser invitados funcionarios con funciones asignadas relativas al cambio a realizar, así como el dueño funcional del servicio que se verá afectado con el cambio. Los integrantes del Grupo Interno de Gestión de Cambios tienen derecho a voz y voto, mientras que los invitados solo podrán ejercer el derecho de voz.
2	Servidores públicos de la Contraloría de Bogotá.	Reporta la solicitud de cambio a los servicios de tecnología existentes, siguiendo las actividades del numeral 5.1. del procedimiento PGTI-04 - “Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos”.	Registro en el Sistema de Mesa de Servicios	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
3	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios.	Valida si la solicitud es de cambios en el centro de datos y los centros de cableado y continua con la sección 5.3 Gestión de cambios en el centro de datos y los centros de cableado, del procedimiento "Gestión de Seguridad Informática" PGTI-06 Si no, valida que la solicitud de cambio incluya: • Los servicios afecta el cambio en términos de recursos de hardware y software. • Identifica de las necesidades y/o errores por los cuales es necesario realizar el cambio. • Escala la solicitud al profesional de la Dirección de TIC que puede atender la solicitud.	Sistema de Mesa de Servicios por número de caso.	
4	Profesional Especializado Profesional Universitario, de la Dirección TIC (Responsable Asignado de atención de la solicitud)	Completa la solicitud de cambio con la siguiente información: • Descripción del impacto y urgencia del cambio teniendo en cuenta el servicio afectado. • Clasificación del cambio (Normal, emergencia, mayor	Sistema de Mesa de Servicios por número de caso.	**Observación:** Los cambios que se presentan ante el Grupo Interno de Gestión de Cambios (CAB_TIC) son aquellos cambios mayores o de emergencia que generen impacto

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		o estándar) • Explicación del cambio, motivación, propósito, elementos de TI involucrados, la estimación de recursos necesarios para la implementación y el tiempo estimado.		y/o comprometa la operación de la entidad y/o generen la no disponibilidad del servicio o que tienen una probabilidad significativa de amenazar la seguridad de la información.
5	Grupo Interno de Gestión de Cambios de la Dirección de TIC (CAB_TIC)	Realiza actividades de viabilidad y planificación de la solicitud, así: • Verifica si la solicitud responde a una necesidad de la entidad, si es justificable con relación a la operación de la entidad o es una solicitud de emergencia, es decir que tiene un alto impacto en la prestación del servicio de TI. • Evalúa la prioridad asignada a la solicitud por el profesional responsable y la ratifica o la reasigna. • Realiza un análisis de riesgo frente a los cambios solicitados, identificando los riesgos	Acta de Reunión y Sistema de Mesa de Servicios por número de caso.	**Punto de Control:** Si el cambio es originado en la ejecución de un contrato, el supervisor del mismo, debe diligenciar la de solicitud de cambio, incluyendo el plan de actividades que va a ejecutar el proveedor. Si es un cambio normal o estándar y no genera la no disponibilidad de servicios y/o obedece a labores administrativas y/o afinamiento de los servicios y/o infraestructura de TIC, se realiza con la aprobación del Jefe inmediato, y se deben documentar el al

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		operacionales. • Especifica aspectos como pruebas previas de los cambios, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, y procedimiento de roll back (reversa) entre otros. • Efectúa análisis costo-beneficio. Asigna recursos y evalúa los tipos de cambio, teniendo en cuenta lo siguiente: • Recursos necesarios para llevar a cabo el cambio • Competencia del funcionario que lo tiene asignado para su atención.		hoja de vida del elemento en el Sistema de Información de Control de Elementos Informáticos SICEINFO, actividad que puede realizarse posterior a la implementación del cambio.
6	Grupo Interno de Gestión de Cambios de la Dirección de TIC (CAB_TIC)	Evalúa y priorizan los cambios mayores o de emergencia para aceptarlos o rechazarlos, con base en los siguientes aspectos: • Establece si el cambio puede afectar los niveles de seguridad. • Determina el impacto sobre la infraestructura (recursos tanto de	Acta de Reunión y Sistema de Mesa de Servicios por número de caso. .	**Punto de Control:** Si el cambio tiene impacto de carácter estratégico o afecta las políticas de la entidad, se debe solicitar aprobación de la alta dirección de la Contraloría de Bogotá.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		software como de hardware) y la calidad de los servicios, que incluya: • *Servicios internos de apoyo requeridos* • *Servicios de apoyo suministrados externamente* • *Cambios técnicos requeridos.* Aprueba o rechaza la solicitud de cambio.		
7	Profesional Especializado Profesional Universitario, de la Dirección TIC (Responsable Asignado de atención de la solicitud)	Revisa si el cambio es aprobado, complementa la información de la solicitud de cambio con la siguiente información: • Fecha de aceptación • Evaluación preliminar realizada por el (CAB_TIC) • Categoría asignada • Estado (aprobado, rechazado). • Fecha aprobación • Cuantificación beneficios esperados • Resultados análisis costo beneficios • Recursos asignados	Sistema de Mesa de Servicios por número de caso.	**Observación**: Para los cambios de emergencia algunos de los aspectos descritos en el procedimiento se podrán documentar de manera retrospectiva y se deberá justificar, revisar y verificar si realmente se trató de una emergencia.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		• Riesgos operacionales y de seguridad asociados • Impacto del cambio y continúa con la actividad No.8. Si el cambio es rechazado, se complementa la información de la solicitud de cambio documentando los motivos de rechazo y se informa al funcionario los motivos para rechazar el cambio, se cierra el caso y finaliza el procedimiento.		
8	Grupo Interno de Gestión de Cambios de la Dirección de TIC (CAB_TIC)	Define la estrategia y el cronograma de implementación del cambio, este debe incluir (si se requiere) las actividades de atención para los cambios de emergencias. Convoca el grupo de funcionarios que participaran en el desarrollo e implementación del cambio y designa el líder de la implementación.	Acta de Reunión y Sistema de Mesa de Servicios por número de caso. .	
9	Profesional Especializado, Profesional Universitario,	Lidera y ejecuta la estrategia y el cronograma de implementación del	Sistema de Mesa de Servicios por número de	**Observación:** Los ejecutantes del cambio, deben informar al

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Técnico Operativo de la Dirección TIC designado como líder de la implementación.	cambio teniendo en cuenta todo lo definido por el CAB_TIC.	caso.	responsable del cambio y validan que los servicios intervenidos queden operativos y con las mismas funcionalidades que antes de la aplicación del cambio, para ello se deben tomar todas las medidas de seguridad, con las que se garantice una correcta continuidad de la operación de TI. La gestión del cambio, se realiza coordinando las acciones definidas en el plan de actividades /cronograma, para asegurar un correcto flujo de trabajo en la ejecución del cambio.
10	Profesional Especializado Profesional Universitario, de la Dirección TIC (Responsable Asignado de atención de la solicitud)	Verifica el cumplimiento de los objetivos del cambio. Determina si se presentaron problemas o interrupciones en el servicio con ocasión del cambio implementado. • Genera el concepto final y cierra la	Sistema de Mesa de Servicios por número de caso.	**Observación:** Si tras la validación del cambio el concepto es fallido, el cambio se debe devolver a la actividad No. 5 para proceder con su retiro o remisión al solicitante para la corrección y actualización de la solicitud.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		solicitud de cambio. • Informa el resultado de su implementación al CAB_TIC. • Evalúa la percepción de los usuarios con respecto al cambio y determina si el proceso y los resultados han sido satisfactorios. • Actualiza el registro de cambio con la información de: • Fecha de evaluación • Evaluación final • Fecha de cierre • Estado Finaliza el procedimiento.		

5.2. GESTIÓN DE LA CAPACIDAD

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de TI	Analiza y documenta el rendimiento de la infraestructura TI y evalúa las cargas y consumos de la infraestructura de TI, definidos en los niveles de servicio, ejemplo: capacidad de procesamiento, almacenamiento, ancho de banda, entre otros.	Documento Línea base de configuración por componente de TI.	**Observación:** Se debe analizar y monitorear el rendimiento de la infraestructura tecnológica conforme a los Acuerdos de Niveles de Servicio (ANS) relacionados con la infraestructura de TI, incluyendo aspectos técnicos,

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		Realiza las actividades relacionadas en los numerales: 5.2. Administración de licencias de software; 5.3. Administración de Nuevos Elementos informáticos y 5.5. Mantenimientos Preventivos de Elementos Informáticos y comunicaciones del procedimiento Gestión de Recursos y servicios Tecnológicos PGTI-05; con el fin de establecer las líneas base de configuración de los equipos e infraestructura tecnológica y termina el procedimiento.		entre ellos los relativos a licencias. La documentación generada del monitoreo deberá ser incluida en el ANEXO No.1 "Formato Hoja de Vida de equipos de cómputo y de comunicaciones", del procedimiento "Gestión de Recursos y servicios tecnológicos" PGTI-05 y generar la línea base de la configuración del elemento de TI.
2	Profesional especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de TI	Realiza reporte semestral sobre el estado de la tecnología relevante a los servicios ofrecidos.	Reporte de Análisis de capacidades de la infraestructura.	**Observación:** Este documento debe contener la estrategia de controlar y predecir el uso y las cargas del trabajo final de cada componente de TI que soportan los servicios críticos de la entidad.
3	Profesional especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de TI	Elabora el Documento de Gestión de Capacidad, determinando el rendimiento y necesidades actuales y futuras de la capacidad de los recursos asignados a	Documento de Gestión de Capacidad	**Observación:** Los insumos requeridos para la elaboración de este documento, deben ser producto de la gestión de los funcionarios de la Dirección de

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		la Dirección de TIC, con base en el documento de análisis de capacidades de la infraestructura y en los siguientes aspectos: • Requisitos de los usuarios • Costos asociados a la capacidad • Información de la capacidad utilizada y rendimiento de cada uno de los elementos de configuración de infraestructura • Requisitos para la continuidad de TIC • Sistemas de apoyo para garantizar la disponibilidad. • Estadísticas de los incidentes, problemas y requerimientos diagnosticados/clasificados por causa como problemas de capacidad • Utilización de la capacidad instalada • Identificación de los planes de la entidad que impactan la capacidad instalada		Tecnologías de la Información y las Comunicaciones responsables de administrar algún elemento de la infraestructura de TI.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
4	Director de Tecnologías de la Información y las comunicaciones, Subdirector de Gestión Recursos Tecnológicos, Subdirector de Gestión de la Información y Profesional especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de TI	Analiza y perfecciona el Documento de Gestión de Capacidad.	Acta de reunión	**Observación:** Se debe garantizar que los aspectos y necesidades futuras de la entidad están cuantificados, diseñados y planteados oportunamente en la medida de lo posible de acuerdo al Plan Estratégico Institucional.
5	Grupo Interno de Gestión de Cambios de la Dirección de TIC (CAB_TIC)	Evalúa el Documento de Gestión de Capacidad para su aprobación y/o ajustes y determina según el impacto cuales cambios en la capacidad se pueden tratar como cambios a la infraestructura (Continua en la actividad 2 de la sección 5.1. Gestión de cambios tecnológicos del presente procedimiento) y cuáles entran hacer parte del Documento de Gestión de Capacidad destinadas a mejorar el rendimiento de los servicios de TI y se determina el	Documento de Gestión de Capacidad aprobado y necesidades de TI.	

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		tratamiento de las necesidades.		
6	Director de Tecnologías de la Información y las Comunicaciones	Presenta las necesidades de contratación a la Dirección Administrativa y hace seguimiento a la ejecución de los requerimientos. (Continua en la actividad 6 de la sección 5.1. Gestión de cambios tecnológicos del presente procedimiento).	Comunicación Oficial	**Observación:** Documento de Gestión de Capacidad, debe ser insumo para elaborar el presupuesto para el Proyecto de TIC, el cual se puntualiza en el Plan de Adquisiciones de TIC.
7	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de TI	Genera el informe de desempeño del documento de Gestión de Capacidad y actualiza las líneas base de configuración de los componentes de TI que se intervinieron como producto del Documento de Gestión de Capacidad y cuales se deben incluir producto de nuevas adquisiciones, generando para ellos sus respectivas líneas base de configuración.	Documento de Gestión de Capacidad actualizado	**Observación:** Documento de Gestión de Capacidad se revisará semestralmente frente a datos reales extraídos de la monitorización de los sistemas, el documento de análisis de capacidades de la infraestructura y de las previsiones de la entidad.

6. ANEXOS

No aplica

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	R.R. No. 047 28 Diciembre 2018	Versión Inicial

Aprobación		Revisión Técnica	
Firma:		Firma:	
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 Diciembre 28 de 2018**	

1. OBJETIVO:

Establecer las actividades para la adquisición, desarrollo y mantenimiento de sistemas de información de la Contraloría de Bogotá D.C.

2. ALCANCE:

Este procedimiento inicia con la identificación de la necesidad de un nuevo sistema de información y termina con el soporte y mantenimiento de sistemas de información, cambio de estado en el sistema de atención de requerimientos.

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.
Ley 1915	12-jul-2018	Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 1377	27-jun-2013	Por la cual se reglamenta parcialmente la Ley 1581 de

NORMA	FECHA	DESCRIPCIÓN
		2012.
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 Único 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:

Ambiente de desarrollo: proveer la infraestructura de hardware y software necesaria para realizar la implementación del sistema y la ejecución de pruebas unitarias por parte de cada desarrollador.

Bases de datos: Se refiere a un conjunto de datos o archivos que tiene una estructura en común, la cual está organizada de tal forma que el ordenador pueda fácilmente encontrar la información.

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

Historias de usuario: Son pequeños textos en los que el usuario describe una actividad que desea que haga el sistema, es una herramienta para dar a conocer los requerimientos al equipo de desarrollo.

Iteración: Es utilizada para la creación o modificación de un sistema de información, la cual consiste en dividir en etapas la solución para su realización, en cada iteración se define un módulo o conjunto de historias que se van a implementar, al final de cada iteración se obtiene como resultado la entrega del módulo correspondiente.

Líder Funcional: Corresponde a un funcionario perteneciente al área usuaria, responsable del manejo funcional del sistema de información y/o aplicación o de la solicitud de requerimiento.
Este funcionario requiere:

- Conocer los procesos que soportan el funcionamiento del Sistema de Información y/o aplicación, con el fin de asegurar que los requerimientos funcionales definidos para el desarrollo del Sistema de Información/Aplicación, estén acordes a los procesos que lo apoyará, asimismo:
- Valida que los Sistemas de Información/Aplicaciones estén ajustados a los procesos del área, desde el momento de la definición y ajuste hasta su puesta en producción.
- Lidera el análisis desde el punto de vista funcional de los Sistemas de Información/Aplicaciones que lidera y establecer las necesidades y requerimientos del sistema de información/Aplicación, validados y aprobados por el jefe de la dependencia.
- Participa activamente en las etapas y actividades que hacen parte del desarrollo de Software: exploración, planificación, pruebas funcionales (aceptación), documentación funcional, Puesta en Producción y Evolución/Mantenimiento.
- Informar al Director o Jefe del Área funcional sobre las actividades realizadas en los sistemas de información/ aplicación bajo su responsabilidad.

Líder Técnico: Corresponde a un funcionario perteneciente a la Oficina de Tecnologías de la Información y las Comunicaciones, que tiene el conocimiento técnico necesario para atender

los requerimientos realizados por un área funcional para un determinado sistema de información o aplicación, este funcionario deberá:

- Liderar el proceso de especificación de requerimientos desde el punto de vista técnico, garantizando que se incluyan las necesidades expresadas por el líder funcional y que se genere la documentación requerida para este proceso.
- Liderar cada una de las etapas de desarrollo de Sistemas de Información garantizando el cumplimiento los requerimientos funcionales y técnicos planteados en el requerimiento.
- Garantiza la generación, revisión y aprobación de la documentación técnica requerida para el desarrollo y/o mantenimiento de los sistemas de información.
- Valida que se cumpla con toda la documentación requerida para la entrega a producción de los sistemas de información/aplicaciones nuevos y/o actualizados.

Manual de administración: Documento que presenta una guía de gestión para el rol del administrador para el sistema, donde indica cómo realizar acciones de parametrización, configuración para su correcto funcionamiento; las opciones para crear roles, perfiles, usuarios y acciones necesarias para la administración del sistema de información.

Manual técnico: Documento que explica el desarrollo del sistema de información, como la estructura de datos, funciones, procedimiento, variables, metodología, diccionario de datos entre otras, así como, la información necesaria para la correcta instalación y funcionamiento de los requisitos técnicos de la solución.

Manual de usuario: Documento que explica y da asistencia a los usuarios del funcionamiento del sistema de información.

Mantenimiento de sistema de información: Se realiza con motivo de un problema detectado en el sistema o por la necesidad de una mejora del mismo.

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.

Metodología de programación. Es un marco de trabajo usado para estructurar, planificar y controlar el proceso de desarrollo en sistemas de información. En un proyecto de desarrollo de software la metodología ayuda a definir: Quién debe hacer Qué Cuándo y Cómo debe hacerlo.

Metodología de Programación Extrema XP: Metodología adoptada por la Dirección de Tecnologías de la Información y las Comunicaciones de desarrollo ágil, cuyo objetivo principal es entregar un software de calidad controlado por las necesidades de los usuarios, permite un desarrollo y gestión de proyectos con eficacia, flexibilidad y control, aumenta la productividad a la hora de desarrollar un proyecto software dando prioridad a los trabajos que dan un resultado directo.

Presenta las siguientes fases:

- **Fase de Exploración:** Usuario plantea a grandes rasgos la actividad que desea que haga el sistema y que es de interés para la entrega del producto.
- **Fase del planeamiento:** Se detalla y priorizan las historias de usuario, se acuerda el alcance del reléase o modulo (iteraciones). Los programadores estiman cuánto esfuerzo requiere cada historia y a partir de allí se define el cronograma.
- **Fase de producción:** Etapa de desarrollo, prueba y comprobación extra del funcionamiento del sistema antes de que éste se pueda liberar al cliente. En esta fase, se pueden presentar cambios y debe tomarse la decisión de si se incluyen o no en el reléase actual.
- **Fase de mantenimiento:** Mantener el sistema en funcionamiento al mismo tiempo que desarrolla nuevas iteraciones. Para realizar esto se requiere de tareas de soporte para el usuario.
- **Fase Final:** Ocurre cuando el usuario no tiene más historias para ser incluidas en el sistema. Esto requiere que se satisfagan las necesidades del cliente en otros aspectos como rendimiento y confiabilidad del sistema. Se genera la documentación final del sistema y no se realizan más cambios en la arquitectura.

Pascal Case: Es un estilo de escritura que se aplica a frases o palabras compuestas y se asemejan a las jorobas de un camello. La letra inicial es mayúscula. Ejemplo: SaldoInicial.

Programación individual: Codificación de una funcionalidad elaborada por una persona o programador.

Programación en parejas: Involucra dos programadores trabajando en el mismo equipo; mientras uno codifica haciendo hincapié en la calidad de la función o método que está implementando, el otro analiza si ese método o función es adecuado y está bien diseñado.

Pruebas de aceptación: Los test de aceptación son aquellos destinados a determinar si los requisitos de cierta funcionalidad han sido cumplidos, a fin de determinar si cumplen con las necesidades y/o requerimientos del usuario.

Pruebas de compatibilidad: Son pruebas funcionales realizadas en diferentes entornos como en cada navegador de internet, sistema operativo o dispositivo, para garantizar el correcto funcionamiento de la aplicación en todos los medios. El mismo software puede presentar errores dependiendo de dónde se ejecute: funcionales (botones y enlaces pueden dejar de funcionar, producen errores de sistema o simplemente no realizan la funcionalidad esperada), estéticos –(no cargar imágenes, desaparecer enlaces o botones y textos).

Pruebas de humo: son aquellas pruebas que pretenden evaluar la calidad de un producto de software previo a una recepción formal, ya sea al equipo de pruebas o al usuario final, es decir, es una revisión rápida del producto de software para comprobar que funciona y no tiene defectos que interrumpan la operación básica del mismo.

Pruebas de integración: Las pruebas de integración se definen como las pruebas para evaluar un proceso compuesto por varios componentes o funcionalidades y se deben relacionar en el formato de pruebas de integración.

Pruebas de mantenimiento: Se ejecutan como resultado de modificaciones, migraciones o desincorporación de software. Las pruebas de modificaciones incluyen mejoras planificadas, correctivas o de emergencia, así como cambios en el entorno de sistema operativo, bases de datos, actualizaciones o parches. Las pruebas de migración deben incluir pruebas operativas del nuevo entorno (Sistema operativo, base de datos, etc.), así como, pruebas sobre el software modificado. Si existe migración y conversión de datos, también serán necesarias pruebas sobre estos.

Pruebas de regresión: Se definen el conjunto de pruebas necesarias para validar que ante eventuales cambios en el software, como parches, ajuste en datos, cambios en la configuración, interfaces, orígenes de datos etc. Las características del software se comportan de manera correcta.

Pruebas de rendimiento: Se definen el conjunto de pruebas asociadas al rendimiento del software y los mecanismos por los cuales se realizarán estas pruebas.

Pruebas de seguridad: Se definen el conjunto de pruebas asociadas a la seguridad del software y los mecanismos por los cuales se realizarán estas pruebas.

Pruebas unitarias: Las pruebas unitarias son definidas para comprobar el correcto funcionamiento de un módulo de código. Esto sirve para asegurar que cada uno de los módulos funcione correctamente por separado, en esta sección se definen los módulos o funcionalidades sobre los cuales se deben realizar pruebas unitarias, estos componentes o funcionalidades debe relacionarse en el formato de pruebas unitarias.

Requerimiento funcional: Describe cualquier actividad que este deba realizar, en otras palabras, el comportamiento o función particular de un sistema o software cuando se cumplen ciertas condiciones.

Requerimiento de seguridad de la información: Las condiciones que deben cumplir para garantizar la confidencialidad, integridad y disponibilidad de un sistema o software.

Requerimiento técnico: Son los requisitos de hardware y software, necesarios para implementar una solución a un requerimiento de TIC.

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.

Software: Se refiere al equipamiento lógico de un computador, está compuesto por todos los aplicativos y licencias que están instalados en cada uno de los equipos de cómputo.

Viabilidad técnica: Hace referencia a aquello que atiende a las características tecnológicas involucradas en un proyecto.

5. DESCRIPCIÓN DEL PROCEDIMIENTO:

5.1 Adquisición o Desarrollo de Nuevo Sistema de Información

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina.	Identifica la necesidad del nuevo software Ordena el Registro en el sistema de mesa de servicios.		
2	Director, Subdirector, Jefe de Oficina.	**Fase de exploración** Registra requerimiento o necesidad de nuevo sistema de información en el Sistema de Mesa de Servicios y adjunta el formato de solicitud para nuevos sistemas de información – PGTI-09-01 Activa Procedimiento de registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos PGTI-04.	Registro en el Sistema de Mesa de Servicios. Anexo No 1 Formato de solicitud para nuevos sistemas de información PGTI-09-01.	
3	Subdirector de Gestión de Información.	Analiza la solicitud y apoyado en Funcionarios de la Subdirección de Gestión de la Información determinan si dentro del inventario de aplicaciones y/o sistemas de la Contraloría de Bogotá existe alguno que cumpla de forma parcial o total con los requerimientos planteados, para lo	Número de caso en el Sistema de Mesa de Servicios.	**Punto de Control** En caso de adquisición del sistema de información, superado el proceso contractual se activa Procedimiento gestión de recursos y servicios tecnológicos PGTI - 05 numeral 5.1 Administración de Sistemas de información o

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		cual: ✓ **Si existe** Pasa a numeral 5.2 soporte y mantenimiento de sistemas de información, e informa a usuario solicitante. ✓ **No existe:** Realiza análisis de viabilidad e informa a usuario solicitante, lo correspondiente a: • **Se requiere adquisición:** Se Activa Procedimiento de gestión contractual-PAGF-08, para lo cual la Subdirección de Gestión de información apoyara la elaboración de las especificaciones o requisitos técnicos para los estudios previos de la contratación, aplica numerales 4, 5 y 6 fin del procedimiento. • **Se Desarrolla Internamente** Asigna Líder Técnico a cargo de la solicitud.		Aplicativos, así mismo garantiza la creación de ambientes de desarrollo, pruebas y producción por separado para el sistema adquirido. **Observación** Solicita mayor información de la solicitud en caso de requerirse. Debe asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual o el uso de productos de software patentados. La Dirección de Tecnologías de la Información y las Comunicaciones adopta la Metodología de Programación Extrema XP para el desarrollo de software.
4	Contralor Auxiliar, Director,	Asigna Líder funcional a cargo de la solicitud	Comunicación Oficial Interna	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Subdirector, Jefe de Oficina.			
5	Profesional universitario y/o especializado Dirección TIC (Líder Técnico) Profesional universitario y/o especializado dependencia solicitante (Líder Funcional) Profesional universitario y/o especializado Dirección TIC (Seguridad de la Información)	**Fase de planificación** Definen cronograma de actividades para levantamiento de requerimientos y documentan los requerimientos funcionales, técnicos y de seguridad de la información relacionados con la solicitud. Presentan definición de requerimientos para ser aprobados.	Cronograma de actividades de levantamiento de requerimientos Anexo No 3 Formato de definición de requerimientos de sistemas de información PGTI-09-03.	
6	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina. (Solicitante) Subdirector de Gestión de Información. Subdirector de Recursos Tecnológicos.	Aprueban requerimientos funcionales, técnicos y de seguridad de la información documentados.	Anexo No 3 Formato de definición de requerimientos de sistemas de información PGTI-09-03.	**Punto de control** Jefe de la dependencia solicitante aprueba los requerimientos funcionales. Subdirector de gestión de la información y Subdirector de Gestión de Recursos Tecnológicos: Aprueban los requerimientos técnicos y de seguridad de la información.
7	Profesional universitario y/o	Generan y presentan alternativas de	Documento con propuesta(s) de	**Punto de control** Analizan requisitos

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	especializado Dirección TIC (Líder Técnico) Profesional universitario y/o especializado dependencia solicitante (Líder Funcional)	solución, respecto a los requerimientos aprobados. Diseñan y construyen modelos, prototipos, diagramas para desarrollo de la aplicación. Presentan definición de diseño para ser aprobados.	solución.	de infraestructura (de acuerdo al documento de gestión de capacidad de la Dirección de TIC, generado en el procedimiento de gestión de cambios y capacidad tecnológica PGTI-08), licenciamiento, costo, presupuesto, adaptabilidad, escalabilidad y portabilidad, riesgos, modelo de base de datos e interacción con otros sistemas e impacto según se determine.
8	Director Tecnologías de la Información y las Comunicaciones Subdirector de Gestión de Información Subdirector de Recursos Tecnológicos. Contralor Auxiliar, Director, Subdirector, Jefe de Oficina. (Usuario Solicitante)	Evalúan, seleccionan y aprueban alternativa de solución.	Acta de reunión	**Observación** Evaluar alternativas teniendo en cuenta el impacto en la entidad, tecnológico, organizativo y de operación.
9	Subdirector de Gestión de	Asigna el recurso humano para el		**Punto de control**

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Información	desarrollo de sistema de información, Solicita a Subdirector de Gestión de Recursos Tecnológicos creación de ambientes de desarrollo, pruebas y producción para el sistema de información (aplicación, base de datos y recursos necesarios) y asigna permisos de acceso a estos.	Comunicación Oficial Interna	Garantiza que los ambientes se encuentren creados por separado. Autoriza el acceso a los diferentes ambientes (desarrollo, pruebas y producción) de manera que garantice que sean completamente segregados. Los proveedores, contratistas no deben tener acceso al ambiente de producción, en caso de ser requerido deberá ser autorizado por Subdirector de Gestión de la Información y su acceso será controlado y supervisado por funcionarios la Dirección TIC.
10	Subdirector de Gestión de Recursos Tecnológicos Profesional universitario y/o especializado Dirección TIC administrador de centro de datos	**Separación de ambientes de desarrollo, pruebas y producción** Asigna recurso tecnológico, administra y crea por separado ambientes de desarrollo, pruebas y producción. Informa la creación de ambientes a	Comunicación Oficial Interna	**Punto de control** Garantiza la creación en ambientes seguros y por separado de los ambientes desarrollo, pruebas y producción, y la existencia de backups de cada uno de estos. Aplica controles de seguridad y

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Subdirector de Gestión de la Información.		protección adecuados para garantizar ambientes seguros. Los cambios serán autorizados por el Subdirector de Gestión de la Información, según sea evaluado se activa procedimiento para la gestión de cambios y capacidad tecnológica.
11	Profesional universitario y/o especializado Dirección TIC (Líder Técnico) Profesional universitario y/o especializado de la Dirección TIC (Desarrollador) Profesional universitario y/o especializado dependencia solicitante (Líder Funcional)	Establecen cronograma desarrollo y plan de entregas de la solución	Cronograma de desarrollo e implementación.	**Punto de control** Se debe dividir en etapas (iteraciones), cada iteración define un módulo o conjunto de historias de usuario que se va a implementar teniendo en cuenta a los requerimientos aprobados y el diseño propuesto. Debe contener los siguiente: Objetivo /actividad Tiempo Responsable(s) indicador(es)
12	Profesional universitario y/o especializado de la Dirección TIC -	**Fase Desarrollo y Producción** Desarrolla acorde al diseño y al plan de	Manual técnico y/o de usuario del desarrollo.	**Punto de control** Ejecuta actividades en ambiente seguro de desarrollo.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Desarrollador	entregas aprobado. Realiza reunión y presenta avances y/o entregas a líder funcional y líder técnico para su retroalimentación, verificación y validación. Entrega de desarrollo para pruebas.		Se debe aplicar Anexo No 7. *Buenas prácticas de desarrollo y estándar de codificación de software, en caso que se adquiera sistema de información la Contraloría de Bogotá adopta el estándar de codificación del producto PGTI-09-07.* **Observación:** Si la programación se realiza de manera individual se debe mantener informado a los miembros del equipo de trabajo.
13	Profesional universitario y/o especializado de la Dirección TIC (pruebas) Profesional universitario y/o especializado Dirección TIC (Líder Técnico)	Ejecuta pruebas según se determine en plan de pruebas. Realiza pruebas confiables en ambiente de pruebas realistas y actualizadas.	Anexo No 4 Formato Pruebas de Sistemas de Información PGTI-09-04	**Punto de control** Ejecuta actividades en ambiente de pruebas. En la ejecución de las pruebas evitar el uso de datos que contengan información personal o cualquier otra información confidencial, reservada o clasificada en caso de ser utilizados se deben proteger eliminándolos o modificándolos inmediatamente
14	Profesional universitario y/o especializado dependencia solicitante	Ejecuta pruebas de aceptación según se determine en plan de pruebas.	Anexo No 4 Formato Pruebas de Sistemas de Información	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	(Líder Funcional).		PGTI-09-04	finalizada la prueba. Debe seleccionar, proteger y controlar cuidadosamente los datos de prueba. Las pruebas se realizan respecto a las especificaciones funcionales aprobadas.
13	Profesional universitario y/o especializado de la Dirección TIC (pruebas) Profesional universitario y/o especializado Dirección TIC (Líder Técnico)	Ejecuta pruebas según se determine en plan de pruebas. Realiza pruebas confiables en ambiente de pruebas realistas y actualizadas.	Anexo No 4 Formato Pruebas de Sistemas de Información PGTI-09-04	**Punto de control** Ejecuta actividades en ambiente de pruebas. En la ejecución de las pruebas evitar el uso de datos que contengan información personal o cualquier otra información confidencial, reservada o clasificada en caso de ser utilizados se deben proteger eliminándolos o modificándolos inmediatamente finalizada la prueba. Debe seleccionar, proteger y controlar cuidadosamente los datos de prueba. Las pruebas se realizan respecto a las especificaciones funcionales aprobadas.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
14	Profesional universitario y/o especializado dependencia solicitante (Líder Funcional).	Ejecuta pruebas de aceptación según se determine en plan de pruebas.	Anexo No 4 Formato Pruebas de Sistemas de Información PGTI-09-04	
15	Profesional universitario y/o especializado Dirección TIC (Seguridad de la Información)	Realiza pruebas de seguridad de la información según se determine en plan de pruebas. Entrega resultados a líder técnico.	Anexo No 4 Formato Pruebas de Sistemas de Información PGTI-09-04	
16	Profesional universitario y/o especializado Dirección TIC (Líder Técnico)	Recibe resultados de pruebas ejecutadas. En caso de no superar las pruebas devuelve a profesional TIC que realizó el desarrollo. Superadas las pruebas informa a Subdirector de Gestión de información.	Anexo No 4 Formato Pruebas de Sistemas de Información PGTI-09-04	**Punto de control** La totalidad de las pruebas deben ser exitosas para solicitar paso a producción.
17	Director TIC y/o Subdirector de Gestión de Información	Autoriza liberación de paso a producción.	Anexo No 5 Formato paso a producción PGTI-09-05	**Punto de control** Bajo ninguna circunstancia autorizará paso a producción sin haber pasado por los ambientes de desarrollo y pruebas.
18	Profesional universitario y/o especializado de la Dirección	Entrega aplicaciones, reportes, ejecutables, base de datos, parametrización, manuales técnicos y de	Manual técnico y/o de usuario del sistema	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	TIC - Desarrollador	usuario y elementos necesarios para la puesta en producción.		
19	Profesional universitario y/o especializado Dirección TIC (Administrador de centro de datos) Subdirector de Gestión de Recursos Tecnológicos	Instala en ambiente de producción las aplicaciones para la ejecución de la solución. Registra el Sistema de Información en el Formato Registro de Aplicación y Sistema de Información. Informa a Subdirector de Gestión de Información. Almacena copia del sistema en una unidad destinada para este fin	Anexo No.6 Formato Registro de Aplicación y Sistema de Información - PGTI-09-06	**Punto de control** Debe garantizar almacenamiento seguro y backup de elementos puestos en ambiente de producción Bajo ninguna circunstancia se rrealizarán despliegues en ambiente de producción sin pasar por los otros dos ambientes ni por el control de cambios respectivo.
20	Director TIC y Subdirector de Gestión de Información	Informa al área solicitante la puesta en producción de la solución. • **Se Desarrolló Internamente** Realiza solicitud para que la solución sea registrada en los inventarios de la entidad.	Comunicación Oficial Interna	**Punto de control** Verifica que la solución se registre o en los inventarios de la entidad.
21	Profesional universitario y/o especializado de la Dirección TIC	Cambia a estado solucionado en el Sistema de Mesa de Servicios.	Registro en el Sistema de Mesa de Servicios	

5.2 Soporte y/o Mantenimiento de Sistema de Información

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, Asesor, Profesional universitario y/o especializado, Técnico de la dependencia solicitante.	Registra requerimiento o necesidad de soporte y/o mantenimiento en el Sistema de Mesa de Servicios. Activa Procedimiento de registro y atención de requerimientos de soporte mantenimiento a los sistemas de información y equipos informáticos PGTI-04.	Registro en el Sistema de Mesa de Servicios	**Punto de control** En caso de requerir desarrollo de nueva funcionalidad, el registro en el Sistema la Mesa de Servicio lo debe realizar el jefe de la dependencia adjuntado formato diligenciado de solicitud para desarrollo nuevas funcionalidades PGTI-09-02.
2	Profesional universitario y/o especializado de la Dirección TIC - Desarrollador (Responsable de atención de la solicitud)	Recibe solicitud de servicio asignada a través de Sistema de Mesa de Servicios. Evalúa el tipo de solicitud, la viabilidad de solución por parte del funcionario TIC o requiere ser escalada a proveedor o contratista. Si la solución requiere desarrollo de una nueva funcionalidad, continua actividad 3 del numeral 5.2 ✓ **Sí es solucionada por funcionario TIC**: Evalúa el grado de complejidad de la	Número de caso en el Sistema de Mesa de Servicios.	**Punto de control** Ejecuta actividades en ambiente seguro de desarrollo. Se debe aplicar Anexo No 7. *Buenas prácticas de desarrollo y estándar de codificación de software, en caso que sea sistema de información adquirido por la Contraloría de Bogotá se adopta el estándar de codificación del producto PGTI-09-07.* **Observación** En caso de no viabilidad o

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		solicitud y determina si se activa o no el Procedimiento de Gestión de Cambios y Capacidad Tecnológica PGTI-08. Atiende solicitud y registra en el Sistema de Mesa de Servicios las acciones realizadas que dieron solución al servicio y asigna estado solucionado al número de caso. Solicita a usuario calificación del servicio por el medio del Sistema de Mesa de Servicios. Sí la solución es satisfactoria para el usuario asignar estado cerrado al número de caso. Sí la solución no es satisfactoria asignar estado reabierto al número de caso. Fin de procedimiento. ✓ **Sí es escalada a proveedor o contratista:** Evalúa el grado de complejidad de la solicitud y determina si se activa o no el Procedimiento de Gestión de Cambios y Capacidad Tecnológica PGTI-08. Informa a proveedor o		aprobación, se informa a usuario solicitante a través de Sistema de Mesa de Servicios. Las actividades de prueba se realizan en ambiente de pruebas.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		contratista a través de aplicativo dispuesto para tal fin o mediante comunicación escrita las especificaciones técnicas y/o requerimientos de la solicitud. Recibe de Proveedor o Contratista la solución y la documentación de ésta, según los ANS pactados Ejecuta pruebas según se determine en plan de pruebas. En caso de no superar alguna de las pruebas se devuelve a proveedor o contratista para su ajuste. Superadas las pruebas registra en el Sistema de Mesa de servicios la solución al servicio y asigna estado *solucionado* al número de caso. Solicita a usuario calificación del servicio por el medio del Sistema de Mesa de Servicios. Sí la solución es satisfactoria para el usuario asignar estado cerrado al número del caso. Sí la solución no		

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		es satisfactoria asignar estado reabierto al número del caso. Fin de procedimiento.		
3		**Para desarrollo de nueva funcionalidad:** Revisa en el Sistema de Mesa de Servicio que la solicitud provenga del jefe de la dependencia y tenga adjunto el Formato diligenciado *de solicitud para desarrollo nuevas funcionalidades* para dar atención a la solicitud, en caso contrario informa a solicitante para subsanar la solicitud. Define y documenta con usuario solicitante requerimientos funcionales, técnicos y de seguridad de la información de la solicitud, Diligencia *Formato de Definición de Requerimientos de Sistema de Información*. Determina si es solucionado por funcionario TIC, proveedor o contratista. ✓ **Sí es solucionada por funcionario TIC**: Evalúa el grado de	Anexo No 2 Formato de solicitud para desarrollo nuevas funcionalidades PGTI-09-02 Anexo No 3 Formato de Definición de Requerimientos de Sistema de Información PGTI-09-03	

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		complejidad de la solicitud y determina si se activa o no el Procedimiento de Gestión de Cambios y Capacidad Tecnológica PGTI-08. Solicita a Subdirector de Gestión de la información la aprobación para el desarrollo, en caso de tener requerimientos de infraestructura tecnológica se requiere aprobación de Subdirector de Gestión de Recursos Tecnológicos. ✓ **Sí es escalada a proveedor o contratista:** Evalúa el grado de complejidad de la solicitud y determina si se activa o no el Procedimiento de Gestión de Cambios y Capacidad Tecnológica PGTI-08. Informa a proveedor o contratista a través de aplicativo dispuesto para tal fin o mediante comunicación escrita las especificaciones técnicas y/o requerimientos de la solicitud. Solicita a Proveedor o contratista propuesta		

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		de solución con las actividades a realizar, tiempo, costo (si aplica), cargo a horas (si aplica) y fecha estimada de entrega de la solución de acuerdo con las obligaciones contractuales y alcance de los ANS pactados. Entrega a Subdirector de Gestión de la Información la propuesta de solución presentada por proveedor o contratista para su aprobación, Si no es aprobada se informa al proveedor o contratista para ajustes.		
4	Subdirector de Gestión de la Información	Aprueba desarrollo para nueva funcionalidad. Aprueba propuesta de solución de proveedor o contratista.		**Punto de control** Analizan requisitos de infraestructura (de acuerdo al documento de gestión de capacidad de la Dirección de TIC, generado en el procedimiento de gestión de cambios y capacidad tecnológica PGTI-08).
5	Profesional universitario y/o especializado de la Dirección TIC - Desarrollador (Responsable	**Sí es atendida por funcionario TIC**: Diseña la solución y la valida con usuario solicitante.		**Punto de control** Ejecuta actividades en ambiente de desarrollo. Se debe aplicar Anexo No 7. *Buenas*

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	de atención de la solicitud)	Desarrolla la solución. Documenta la solución y genera y/o actualiza manuales técnico, administración y de usuario, según aplique. Entrega solución para ejecución de pruebas, actividad 7 del numeral 5.2.		*prácticas de desarrollo y estándar de codificación de software, en caso que sea sistema de información adquirido por la Contraloría de Bogotá se adopta el estándar de codificación del producto PGTI-09-07.*
6	Profesional universitario y/o especializado de la Dirección TIC - Desarrollador (Responsable de atención de la solicitud)	**Sí atendida por proveedor o contratista:** Recibe de Proveedor o Contratista la solución y la documentación técnica y/o de usuario. Ejecuta pruebas según se determine en plan de pruebas. Requiere a usuario solicitante realizar pruebas de aceptación (Actividad 8 del numeral 5.2) En caso de no superar alguna de las pruebas se devuelve a proveedor o contratista para su ajuste. Superadas las pruebas informa a Subdirector de Gestión de información, continua actividad No 9 del numeral 5.2.		**Punto de Control** Ejecuta actividades en ambiente de pruebas. En la ejecución de las pruebas evitar el uso de datos que contengan información personal o cualquier otra información confidencial, reservada o clasificada en caso de ser utilizados se deben proteger eliminándolos o modificándolos inmediatamente finalizada la prueba. Debe seleccionar, proteger y controlar cuidadosamente los datos de prueba. Las pruebas se realizan respecto a las especificaciones funcionales

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
7	Profesional universitario y/o especializado de la Dirección TIC (pruebas)	Ejecuta pruebas según se determine en plan de pruebas. Requiere a usuario solicitante realizar pruebas de aceptación (Actividad 8 del numeral 5.2). En caso de no superar alguna de las pruebas se devuelve a profesional TIC que realizó el desarrollo o responsable de atención del requerimiento. Superadas las pruebas informa a Subdirector de Gestión de información, continua actividad No 9 del numeral 5.2		aprobadas.
8	Usuario solicitante	Ejecuta pruebas de aceptación y entrega resultados a funcionario TIC responsable de la atención de pruebas	Anexo No 4 Formato pruebas sistemas de información PGTI-09-04	
9	Director TIC y/o Subdirector de Gestión de Información	Autoriza liberación de paso a producción.	Formato paso a producción Anexo No 5	**Punto de control** Bajo ninguna circunstancia autorizará paso a producción sin haber pasado por los ambientes de desarrollo y pruebas.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
10	Profesional universitario y/o especializado de la Dirección TIC – Desarrollador (Responsable de atención de la solicitud)	Entrega aplicaciones, reportes, ejecutables, base de datos, manuales técnicos y de usuario, parametrización y elementos necesarios para la puesta en producción.	Manual técnico y/o de usuario del desarrollo	
11	Profesional universitario y/o especializado Dirección TIC (Administrador de centro de datos)	Instala en ambiente de producción las aplicaciones para la ejecución de la solución. Informa a Subdirector de Gestión de Información. Actualiza Formato Registro de Aplicación y Sistema de Información. Almacena copia de las versiones generadas en una unidad destinada para este fin.	Anexo No.6 Formato Registro de Aplicación y Sistema de Información-PGTI-09-06	**Punto de control** Debe garantizar almacenamiento seguro y backup de elementos puestos en producción. Bajo ninguna circunstancia se rrealizarán despliegues en ambiente de producción sin pasar por los otros dos ambientes ni por el control de cambios respectivo.
12	Profesional universitario y/o especializado de la Dirección TIC	Cambia a estado solucionado en Sistema de Mesa de Servicios.	Número de caso en el Sistema de Mesa e Servicios.	

6. ANEXOS

ANEXO 1. Formato de Solicitud para Nuevo Sistema de Información

CONTRALORÍA DE BOGOTÁ, D.C.	Formato Solicitud para Nuevo Sistema de Información	Código formato: PGTI-09-01 Versión: 1.0
		Código documento: PGTI-09 Versión 1.0
		Página x de y

Fecha de solicitud		
DD	MM	AA

Número solicitud (Diligencia Dirección TIC)

NFORMACIÓN DEL SOLICITANTE	
Nombre y apellidos del solicitante	*Nombre y apellido de funcionario solicitante*
Cargo	*Cargo de funcionario solicitante*
Jefe de la Dependencia	*Nombre de Director o Jefe de Oficina*
Dependencia	*Nombre de la dependencia*

DESCRIPCIÓN DE LA SOLICITUD (Historia de Usuario)

Describa el requerimiento del sistema de información de forma detallada, respondiendo lo siguiente:

Problemática Actual	*Descripción de la situación que genera la solicitud, Indique sí es un requerimiento normativo y cite la norma que lo exige*
Definición del Requerimiento, Qué necesito?:	*Descripción del requerimiento de forma general y clara, Necesito que haga,… quiero que…*
Objetivo:	*Para…*
Criterios de validación	*Indique todos los criterios de validación, debe...*
Tipo de usuario	*Usuario o rol …*
Anexos	*Adjuntar imagen, prototipo de lo que se requiere*
Observaciones	

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Fecha Solicitud	Día, mes, año de la solicitud.
Número solicitud	No. asignado por la Dirección de Tecnologías de la Información.
Nombre y apellidos del solicitante	Nombre y apellido de funcionario solicitante.
Cargo	Cargo de funcionario solicitante
Jefe de la Dependencia	Nombre de Contralor, Contralor Auxiliar, Director, Subdirector
Dependencia	Nombre de la dependencia.
Problemática Actual	Descripción de la situación que genera la solicitud, Indique sí es un requerimiento normativo y cite la norma que lo exige.
Definición del Requerimiento Qué necesito?	Redactar de forma clara qué se necesita. Ejemplo: Necesito consultar en pantalla los datos de los funcionarios por número de cedula o por nombres o apellidos.
Objetivo	Describir para que se necesita, Ejemplo: para facilitar la consulta de los funcionarios y permitir su búsqueda por cualquier criterio de identificación en el sistema de información.
Criterios de validación	Indique que validaciones debe tener. Ejemplo: • Generar reporte • Validar fecha de la transacción • El listado salga al pulsar un botón
Tipo de usuario	Indique el tipo de usuario que va a aplicar la solución: Ejemplo: Como secretaria, auditor, administrador.
Anexos	Adjunte documentos, imágenes o prototipo que sea necesario para mayor entendimiento de la solución requerida.
Observaciones	Indique observaciones del requerimiento.

ANEXO 2. Formato de Solicitud para Desarrollo Nuevas Funcionalidades

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato de Solicitud para Desarrollo Nuevas Funcionalidades**	Código formato: PGTI-09-02 Versión: 1.0
		Código documento: PGTI-09 Versión 1.0
		Página x de y

Fecha de solicitud				**Número solicitud** (Diligencia Dirección TIC)
DD	**MM**	**AA**		

INFORMACIÓN DEL SOLICITANTE	
Nombre y apellidos del solicitante	*Nombre y apellido de funcionario solicitante*
Cargo	*Cargo de funcionario solicitante*
Director Técnico/Jefe de Oficina	*Nombre de Director o Jefe de Oficina*
Sistema de información (SI)	*Nombre de sistema de información al cual se solicita el desarrollo de la nueva funcionalidad*
Módulo de SI	*Nombre del módulo de sistema de información al cual se solicita el desarrollo de la nueva funcionalidad*
Nombre de la funcionalidad	*Nombre de la nueva funcionalidad*

DESCRIPCIÓN DE LA SOLICITUD (Historia de Usuario)

Describa el requerimiento del sistema de información de forma detallada, respondiendo lo siguiente:

Problemática Actual	*Descripción de la situación que genera la solicitud, Indique sí es un requerimiento normativo y cite la norma que lo exige*
Definición del Requerimiento, Qué necesito?	*Descripción del requerimiento de forma detallada y clara, Necesito que haga,… quiero que…*
Objetivo:	*Para…*
Criterios de validación	*Indique todos los criterios de validación (restricciones), debe...*
Prototipo	*Inserte imagen de las pantallas y o reportes de la nueva funcionalidad*
Explicación de prototipo	*Explique el funcionamiento que desea obtener de los campos, botones, columnas, reportes, etc ,mostrados en el prototipo*
Se integra con otro aplicativo?, cuál?	*Diligencie sí la nueva funcionalidad consulta, inserta, elimina o modifica información de otro(s) aplicativo(s), indique en cual(es)?*

DEFINICIÓN DE USUARIOS

Descripción del perfil y responsabilidades de los usuarios que tendrán interacción con la nueva funcionalidad

PERFIL	RESPONSABILIDAD
Nombre del perfil	*Responsabilidades en la ejecución de la nueva funcionalidad*

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCION DEL CAMPO
Fecha Solicitud	Día, mes, año de la solicitud.
Número solicitud	No asignado por la Dirección de Tecnologías de la Información.
Nombre y apellidos del solicitante	Nombre y apellido de funcionario solicitante.
Cargo	Cargo de funcionario solicitante

NOMBRE DEL CAMPO	DESCRIPCION DEL CAMPO
Director técnico/jefe de oficina	Nombre de Director o Jefe de Oficina.
Sistema de información (si):	Nombre de sistema de información al cual se solicita el desarrollo de la nueva funcionalidad.
Módulo de si	Nombre del módulo de sistema de información al cual se solicita el desarrollo de la nueva funcionalidad.
Nombre de la funcionalidad	Nombre de la nueva funcionalidad.
Problemática actual	Descripción de la situación que genera la solicitud, Indique sí es un requerimiento normativo y cite la norma que lo exige.
Definición del requerimiento, Qué necesito?	Redactar de forma clara qué se necesita. Ejemplo: Necesito consultar en pantalla los datos de los funcionarios por número de cedula o por nombres o apellidos.
Objetivo	Describir para que se necesita, Ejemplo: para facilitar la consulta de los funcionarios y permitir su búsqueda por cualquier criterio de identificación en el sistema de información.
Criterios de validación	Indique que validaciones debe tener. Ejemplo: • Generar reporte. • Validar fecha de la transacción. • El listado salga al pulsar un botón.
Prototipo	Inserte imagen de las pantallas y o reportes de la nueva funcionalidad.
Explicación de Prototipo	Explique el funcionamiento que desea obtener de los campos, botones, columnas, reportes, etc, mostrados en el prototipo.
Se integra con otro aplicativo?, cuál?	Diligencie sí la nueva funcionalidad consulta, inserta, elimina o modifica información de otro(s) aplicativo(s), Cual(es)?
Definición de usuarios	Descripción del perfil y responsabilidades de los usuarios que tendrán interacción con la nueva funcionalidad.
Perfil	Nombre del perfil.
Responsabilidad	Responsabilidades en la ejecución de la nueva funcionalidad, (ej. ingresar información, aprobar la transacción.)

ANEXO 3. Formato de definición de requerimientos de sistema de información

CONTRALORÍA DE BOGOTÁ, D.C.	Formato para la Definición de Requerimientos de Sistema de Información	Código formato: : PGTI-09-03 Versión: 1.0
		Código documento: PGTI-09 Versión 1.0
		Página x de y

Fecha		
DD	MM	AA

Número solicitud	*Este número corresponde al número asignado por TIC al Formato de solicitud de sistema de información*
Sistema Información	*Nombre sistema de información*

DESCRIPCIÓN DE LA SOLICITUD (Historia de Usuario)

Numero Historia	*No*	**Prioridad**	*Alta/Media/Baja*	**Iteración asignada**	
Tiempo proyectado desarrollo	*Indique en No días*	**Fecha Inicial**	*Fecha inicial*	**Fecha Final**	*Fecha Final*
Título	*Nombre de la historia de usuario o funcionalidad.*				
Tipo de usuario	*Usuario o rol …*				
Qué necesito?	*Necesito que haga, … quiero que…*				
Objetivo	*Para…*				
Criterios de validación	*Debe...*				
Anexos	*Adjuntar imagen, prototipo de lo que se requiere.*				

REQUERIMIENTOS FUNCIONALES

Describa detalles del requerimiento funcional No 1

Entrada	*Indique la información (datos de entrada y/o funcionalidades que dependa) para la iniciar el proceso que ejecuta.*
Proceso	*Descripción detallada de los pasos que debe para cumplir con los resultados e separados (especifique condiciones, cálculos matemáticos, datos.*
Salida	*Resultado de la ejecución del proceso, la respuesta o salida requerida (ej: reporte, archivo plano, mensaje de ejecución del proceso, información almacenada, correo electrónico).*

REGLAS DEL NEGOCIO:

REQUISITOS DE CONDUCTA DEL SISTEMA:

REQUISITOS DE INTEGRACIÓN:

Describa detalles del requerimiento funcional No 2

Entrada	*Indique la información (datos de entrada y/o funcionalidades que dependa) para la iniciar el proceso que ejecuta.*
Proceso	*Descripción detallada de los pasos que debe para cumplir con los resultados e separados (especifique condiciones, cálculos matemáticos, datos).*
Salida	*Resultado de la ejecución del proceso, la respuesta o salida requerida (ej: reporte, archivo plano, mensaje de ejecución del proceso, información almacenada, correo electrónico).*

REGLAS DEL NEGOCIO:

REQUISITOS DE CONDUCTA DEL SISTEMA:

REQUISITOS DE INTEGRACIÓN:

REQUERIMIENTOS TÉCNICOS

Describa los requerimientos técnicos.

REQUERIMIENTOS DE SEGURIDAD

Indique los requerimientos de seguridad que apliquen, seleccione según aplique requerimientos de seguridad de la información según Anexo No 7: Buenas prácticas de desarrollo, estándar de codificación de software y seguridad de la información, de procedimiento de sistemas de información, sí presenta más requerimientos que no se encuentre en anexo, indíquelos.

TIPO DE PRUEBAS REQUERIDAS

☐ Aceptación	☐ Integración	☐ Rendimiento
☐ Compatibilidad	☐ Mantenimiento	☐ Seguridad
☐ Humo	☐ Regresión	☐ Unitaria

FUNCIONARIOS QUE PARTICIPARON EN LA DEFINICIÓN DE LOS REQUERIMIENTOS

Nombres y Apellidos	*Rol Desempeñado* (*Líder Funcional, técnico, Seguridad Inf*)	*Firma*

_____

VoBo Jefe dependencia solicitante

Nombre y Apellidos:

_____ ***VoBo Subdirector Gestión de la Información*** ***Nombre y Apellidos:***	_____ ***VoBo Subdirector Gestión de Recursos Tecnológicos*** ***Nombre y Apellidos:***

INSTRUCTIVO DE DILIGENCIAMIENTO

Este anexo se diligencia con el objetivo de realizar un levantamiento detallado las especificaciones de los requerimientos funcionales, técnicos y de seguridad de la información de los sistemas de información, se inicia a partir de la historia de usuario descrita en la solicitud de sistema de información, lo diligencian en conjunto líder funcional, líder técnico y líder de seguridad de la información, debe tener aprobación de:

- Jefe dependencia solicitante: Para aprobar los requerimientos funcionales.

- Subdirector de gestión de la información y Subdirector de Gestión de Recursos Tecnológicos: Aprueban los requerimientos técnicos y de seguridad de la información.

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Fecha	Día, mes y año de cuando se realizó el levantamiento de diligenciamiento del formato.
Número solicitud	Corresponde al número asignado por TIC al Formato de solicitud de sistema de información.
DESCRIPCIÓN DE LA SOLICITUD (Historia de Usuario)	
Numero	Numero consecutivo que indica el orden de la historia de usuario, una iteración o conjunto de historias de usuario que conforman el modulo.
Prioridad	Que tan importante es: Alta o Media o Baja.
Iteración asignada	Numero de iteración a la que pertenece la historia de usuario.
Tiempo desarrollo	Indique en No días proyectados de desarrollo.
Fecha Inicial	Indique fecha de inicio de desarrollo.
Fecha Final	Indique fecha de final de desarrollo.
Titulo	Nombre de la historia de usuario o funcionalidad.
Tipo de usuario	Indique el tipo de usuario que va a aplicar la solución: Ejemplo: Como secretaria, auditor, administrador.
Qué necesito?	Redactar de forma clara se necesita. Ejemplo: Necesito consultar en pantalla los datos de los funcionarios por número de cedula o por nombres o apellidos.
Objetivo:	Describir para que se necesita, Ejemplo: para facilitar la consulta de los funcionarios y permitir su búsqueda por cualquier criterio de identificación en el sistema de información.
Criterios de validación	Indique que validaciones debe tener. Ejemplo: • El listado salga al pulsar un botón. • sean ordenados por orden ascendente por número de cedula.
Anexos	Adjunte documentos, imágenes o prototipo que sea necesario para mayor entendimiento de la solución requerida.
Requerimientos Funcionales	Esta sección debe contener los requisitos funcionales del sistema que se hayan identificado a partir de los requisitos de la solicitud planteada, descrita en: **Entrada**: Indique la información (datos de entrada y/o funcionalidades que dependa) para la iniciar el proceso que ejecuta. **Proceso**: *D*escripción detallada de los pasos que debe para cumplir con los resultados esperados (especifique condiciones, cálculos matemáticos, datos). **Salida**: Resultado de la ejecución del proceso, la respuesta o salida requerida (ej: reporte, archivo plano, mensaje de ejecución del proceso, información almacenada, correo electrónico). **Reglas de Negocio:** Esta sección debe contener las reglas de

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
	negocio, normatividad que deba cumplir la solución a desarrollar. **Requisitos de Conducta del Sistema:** Debe contener los requisitos de conducta que se hayan identificado. Estos requisitos deben especificar cualquier otro comportamiento deseado del sistema que no se haya especificado, como rendimiento disponibilidad, etc. **Requisitos de Integración:** Debe contener los requisitos de integración que se hayan identificado. Estos requisitos deben identificar aquellos servicios disponibles en el entorno tecnológico de producción o componentes software (por ejemplo, librerías enlazables, otros sistemas de información) cuya funcionalidad sea relevante para el sistema a desarrollar y deban ser consumidos por el mismo.
Requerimientos Técnicos:	Especifique que requerimientos técnicos de hardware, software, arquitectura que son necesarios, ejemplo: Base De Datos Servidor de Aplicaciones Navegador Web Máquina Virtual De Java, etc
Requerimientos de Seguridad	indique los requerimientos de seguridad que apliquen, seleccione según aplique requerimientos de seguridad de la información según Anexo No 7: Buenas prácticas de desarrollo, estándar de codificación de software y seguridad de la información, de procedimiento de sistemas de información, sí presenta más requerimientos que no se encuentre en anexo, indíquelos
Tipo de pruebas requeridas	Seleccione las pruebas requeridas para verificar el correcto funcionamiento.
Funcionarios que participaron en la definición de los requerimientos	Relacione los funcionarios que participaron en la definición de los requerimientos.
VoBo jefe dependencia solicitante	Firma de Contralor, Contralor Auxiliar, jefe de Oficina, Director o Subdirector aprueba los requerimientos funcionales.
VoBo Subdirector de Gestión de la Información	Firma de Subdirector de Gestión de la Información aprueba los requerimientos técnicos y de seguridad de la información.
VoBo Subdirector Gestión de Recursos Tecnológicos	Firma de Subdirector de Gestión de Recursos Tecnológicos aprueba los requerimientos técnicos y de seguridad de la información, aplica en caso que la solución requiera recursos de infraestructura tecnológica.

ANEXO 4. Formato de pruebas sistemas de información.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato de Pruebas Sistemas de Información**	Código formato: : PGTI-09-04 Versión: 1.0
		Código documento: PGTI-09 Versión 1.0
		Página x de y

Funcionario responsable prueba		**Dependencia**	
Sistema de Información o aplicativo		**Módulo**	
Componente/ Funcionalidad			
SISTEMA DE INFORMACIÓN O APLICATIVO ADQUIRIDO			
No Licencia		**Fecha Adquisición**	
Versión		**Fecha Caducidad**	
Software Requerido			
SISTEMA DE INFORMACION DESARROLLADO O EN MANTENIMIENTO POR CB			
Número de servicio		**Fecha de entrega para prueba**	
Número de historia de usuario		**Funcionario desarrollador**	
TIPO DE PRUEBAS			
☐ Aceptación	☐ Integración	☐ Rendimiento	
☐ Compatibilidad	☐ Migración	☐ Seguridad	
☑ Humo	☐ Regresión	☐ Unitaria	
EJECUCIÓN DE PRUEBAS			
	PRUEBA No	**FECHA**	
Tipo de prueba		Estado Final Prueba	
Escenario Prueba			
Consideraciones técnicas	**Servidor Aplicaciones**	**Servidor Base Datos**	
	Motor BD	**Instancia de BD**	
	Otras		

Detalles de la prueba				
No	**Descripción**	**Resultado esperado**	**Resultado actual**	**Resultado**
Evidencias				
Observaciones				

			PRUEBA No		**FECHA**
Tipo de prueba			Estado Final Prueba		
Escenario Prueba					
Consideraciones técnicas	**Servidor Aplicaciones**		**Servidor Base Datos**		
	Motor BD		**Instancia de BD**		
	Otras				

Detalles de la prueba

No	Descripción	Resultado esperado	Resultado actual	Resultado

Evidencias

Observaciones

FIRMA RESPONSABLE DE LA(S) PRUEBA(S)

Informo que la(s) prueba(s) realizada(s) al Sistema de Información o Aplicativo relacionado en el presente documento fue (ron) ----Seleccione--- para puesta en producción.

Firma Responsable Prueba(s)

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCION DEL CAMPO
Funcionario responsable de la prueba	Nombres y apellidos de funcionario que realiza de la prueba.
Dependencia	Despacho, Dirección, Dirección, Subdirección, Oficina que pertenece el funcionario responsable de la prueba.
Sistema de Información o aplicativo	Nombre de sistema de información, software o aplicativo a realizar la prueba.

Modulo	Nombre del módulo del sistema de información o aplicativo a realizar la prueba (si aplica).
Componente/ Funcionalidad	Nombre del formulario, reporte, plantilla, componente o funcionalidad del sistema de información o aplicativo a realizar la prueba (si aplica).
SISTEMA DE INFORMACION O APLICATIVO ADQUIRIDO	Refiere a la información de sistemas de información que son comprados o adquiridos por la Contraloría de Bogotá (no desarrollados o que se le dé directamente soporte de desarrollo los funcionarios de la Contraloría de Bogotá)
Licencia	Número o serie de la licencia.
Fecha apertura formato control de cambios	Fecha en la que se abre el formato control de cambios.
Fecha de adquisición	Fecha en la cual se adquirió la licencia.
Fecha de caducidad	Fecha en la cual vence la licencia.
Versión	Releáse de software o sistema de información.
Servidor	Lugar de alojamiento de software o sistema de información.
Software requerido	Lista los requerimientos de software que requiere el sistemas de información o aplicativo o la licencia de software para su funcionamiento.
SISTEMA DE INFORMACION DESARROLLADO O EN MANTENIMIENTO POR CB	Refiere a la información de sistemas de información que son desarrollados o que se le da mantenimiento de desarrollo por parte de los funcionarios de la Contraloría de Bogotá.
Numero de servicio	Numero asignado por la Dirección a la atención del requerimiento (Mesa de servicio).
Fecha de entrega para prueba	Fecha en que es entregado por el desarrollador o responsable de la atención del requerimiento para realizar la(s) prueba(s).
Numero de Historia de usuario	Numero de historia asignado en la descripción de la solicitud ubicado en el formato para la definición de requerimientos de Sistema de Información.
Funcionario desarrollador	Nombres y apellidos de funcionario que realizó el desarrollo.
TIPO DE PRUEBAS	Seleccione el tipo de pruebas a realizar.
Prueba No	Asigne número consecutivo de ejecución de la prueba.
Fecha	Fecha en que se realiza la prueba formato DD/MM/AA.
Estado Final Prueba	Seleccione si fue exitosa o fallida.
Escenario Prueba	Indique las condiciones de para ejecutar la prueba.
Consideraciones técnicas	Indique nombre del servidor de aplicaciones, de base de datos, motor e instancia de base datos en la que se realiza la prueba y otras consideraciones técnicas que se requieran especificar.
Detalle de las pruebas	Indique los pasos que realizó para ejecutar las pruebas con numero consecutivo, descripción de la acción, resultado esperado, resultado generado después de ejecutar la prueba y si fue exitosa o fallida.

Evidencias	Indique las imágenes, pruebas o evidencias de las pruebas realizadas.
Observaciones	Si hay observaciones, indíquelas en este espacio.
los campos Prueba No, Fecha, Estado Final Prueba, Escenario Prueba, Consideraciones técnicas, Detalle de las pruebas, Evidencias y Observaciones se pueden repetir en el formato cuantas pruebas se requiera realizar, teniendo en cuenta que estas aplican para un único funcionario responsable de las pruebas.	
FIRMA RESPONSABLE DE LA(S) PRUEBA(S)	Firma de funcionario que realizó las pruebas, registrado inicialmente en el formato, tener en cuenta que sí se agregan más campos de los descritos en el ítem anterior, la sección de éste formato debe finalizar con la firma del responsable.

ANEXO 5. Formato de paso a producción.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato de Paso a Producción**	Código formato: : PGTI-09-05 Versión 1.0
		Código documento: PGTI-09 Versión 1.0
		Página X de Y

Nombres y apellidos Subdirector de Gestión de la Información			
Funcionario Responsable puesta en producción			
Sistema de Información o aplicativo		**Módulo**	
Componente/ Funcionalidad			
SISTEMA DE INFORMACIÓN O APLICATIVO ADQUIRIDO			
No Licencia		**Fecha Adquisición**	
Versión		**Fecha Caducidad**	
Software Requerido			
SISTEMA DE INFORMACIÓN DESARROLLADO O EN MANTENIMIENTO POR CB			
Número de servicio		**Funcionario desarrollador**	
Número de historia de usuario		**Funcionario desarrollador**	
APROBACIÓN PASO A PRODUCCIÓN			
Aceptación de pruebas			

☐ Aceptación	☐ Integración	☐ Rendimiento
☐ Compatibilidad	☐ Migración	☐ Seguridad
☑ Humo	☐ Regresión	☐ Unitaria

Funcionarios que realizaron y aprobaron pruebas			
Fecha aceptación	**Nombres y apellidos**	**Dependencia**	**Firma**

Componentes de instalación		
Nombre	**Tipo**	**Servidor de ubicación**

Fecha autorización paso a producción: DD _____MM _____AA_____		
Firma autorización paso a producción - Subdirector Gestión Información		

INSTRUCTIVO DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCION DEL CAMPO
Nombres y apellidos Subdirector de Gestión de la Información	Nombres y apellidos de Subdirector de Gestión de la Información, autoriza la el paso a producción.
Funcionario responsable de puesta en producción	Nombres y apellidos de funcionario que realiza de puesta en producción.
Sistema de Información o aplicativo	Nombre de sistema de información, software o aplicativo a realizar paso a producción.
Módulo	Nombre del módulo del sistema de información o aplicativo a realizar paso a producción (si aplica).
Componente/ Funcionalidad	Nombre del formulario, reporte, plantilla, componente o funcionalidad del sistema de información o aplicativo a realizar paso a producción (si aplica).
Sistema de información o aplicativo adquirido	Refiere a la información de sistemas de información que son comprados o adquiridos por la Contraloría de Bogotá (no desarrollados o que se le dé directamente soporte de desarrollo los funcionarios de la Contraloría de Bogotá).
Licencia	Número o serie de la licencia.
Fecha apertura formato control de cambios	Fecha en la que se abre el formato control de cambios.
Fecha de adquisición	Fecha en la cual se adquirió la licencia.
Fecha de caducidad	Fecha en la cual vence la licencia.
Versión	Reléase de software o sistema de información.
Servidor	Lugar de alojamiento de software o sistema de información.
Software requerido	Lista los requerimientos de software que requiere el sistemas de información o aplicativo o la licencia de software para su funcionamiento.
sistema de información desarrollado o en mantenimiento por CB	Refiere a la información de sistemas de información que son desarrollados o que se le da mantenimiento de desarrollo por parte de los funcionarios de la Contraloría de Bogotá.
Numero de servicio	Numero asignado por la Dirección a la atención del requerimiento (Mesa de servicio).
Numero de Historia de usuario	Número de historia asignado en la descripción de la solicitud ubicado en el formato para la definición de requerimientos de Sistema de Información.
Funcionario desarrollador	Nombres y apellidos de funcionario que realizó el desarrollo

APROBACIÓN PASO A PRODUCCIÓN	Esta sección del formato es diligenciado por Líder Técnico o funcionario responsable de atención del requerimiento para solicitar aprobación a Subdirector de Gestión de la Información para paso a producción del desarrollo.
Aceptación de pruebas	Se selecciona el compendio de pruebas que se ejecutaron, estas deben de estar con los soportes correspondientes firmados por los que ejecutaron las pruebas.
Funcionarios que realizaron y aprobaron pruebas	Fecha del formato donde se registra la aceptación de la(s) prueba(s), nombres, apellidos, dependencia y firma de funcionarios que realizaron e informaron el éxito de las pruebas y observaciones, estas deben de estar con los soportes correspondientes firmados por los que ejecutaron las pruebas.
Componentes de instalación	Relación de los elementos o componentes para paso a producción (formularios, reportes, dll, etc), se describe el nombre, tipo y el servidor en donde quedo ubicada la solución.
Fecha autorización paso a producción	Fecha autorización paso a producción en formato DD, MM, AAA.
Firma autorización paso a producción - Subdirector Gestión Información	Firma de Subdirector de Gestión de la Información que aprueba paso a producción.

ANEXO 6. Formato Registro de Aplicación y Sistema de Información

CONTRALORÍA DE BOGOTÁ, D.C.	Formato Registro de Aplicación y Sistema de Información	Código formato: : PGTI-09-06 Versión 1.0
		Código documento: PGTI-09 Versión 1.0
		Página x de y

FECHA DILIGENCIAMIENTO		**FECHA DE ADQUISICIÓN**		**FECHA DE CADUCIDAD**	
SISTEMA DE INFORMACIÓN (O APLICATIVO)			**LICENCIA (Número de licencia- Cantidad de usuarios que cubre - Tipo)**		
USUARIOS					
VERSIÓN INICIAL					
SERVIDOR					
MOTOR BASE DE DATOS			**INSTANCIA DE BASE DATOS**		
MÓDULOS					

CONTROL DE CAMBIOS Y/O VERSIONAMIENTO						
No. Cambio	**Módulo**	**Componente**	**Fecha Implementación**	**Motivación del cambio**	**Versión**	**Descripción de la modificación**
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

INSTRUCTIVO DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCION DEL CAMPO
Fecha diligenciamiento	**Fecha en la que se abre el formato.**
Fecha de adquisición	**Fecha en la cual se adquirió la licencia.**
Fecha de caducidad	**Fecha en la cual vence la licencia.**
Sistema de información	**Nombre de software o sistema de información.**
Licencia	**Número o serie de la licencia - Cantidad de usuarios que cubre, tipo de licencia.**
Usuarios	**Dependencia o nombre de usuarios que usan el sistema.**
Versión	**Release de software o sistema de información inicial.**
Servidor	**Lugar de alojamiento de software o sistema de información.**
Motor de Base de Datos	**Servicio principal para almacenar, procesar y proteger los datos de sistema de información.**
Instancia de Base de Datos	**Nombre de la base de datos.**
Módulo	**Nombre del módulo de software o sistema de información (si aplica).**
Componente	**Nombre del formulario, reporte, plantilla sobre el cual se va realizar la prueba.**
Fecha Implementación	**Fecha de puesta en producción de software o sistema de información.**

Motivación del cambio	**Descripción del motivo del cambio.**
Versión	**Release de software o sistema de información con el cambio realizado.**
Descripción de la modificación	**Breve descripción de la modificación o ajuste del software o sistema de información.**

ANEXO 7. Buenas Prácticas de Desarrollo, Estándar de Codificación de Software y Seguridad de la Información

1. BUENAS PRÁCTICAS DE DESARROLLO

- Utilizar nombres descriptivos para la definición de variables, métodos, funciones, clases.
- No repetir código: Funciones, métodos, clases, no repetir librerías ni documentación.
- Mantener al mínimo el número de niveles en las instrucciones anidadas.
- Hacer test unitarios.
- Evitar usar métodos con muchos parámetros.
- Comentar el código, funciones, definiciones y lógica compleja.
- Evitar comentarios innecesarios
- Las librerías, Componentes, Servicios o bibliotecas de uso general deben estar debidamente documentadas explicando su propósito, funciones, parámetros de entrada y salida, etc. La documentación de estos componentes debe ser almacenada en el repositorio designado por la Subdirección de Gestión de la Información.
- Proteger a las variables y los recursos compartidos de acceso concurrente inapropiados.
- Impedir que los usuarios generen nuevo código o alteren el código existente.
- La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

1.1 BUENAS PRÁCTICAS PARA UNA CODIFICACION SEGURA:

Las practicas referenciadas en este numeral son extractadas "*Prácticas seguras de codificación OWASP-Guia de referencia rápida*" https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf.

✓ **Validación de entradas:**

- Validar los tipos, rangos, longitud de datos esperados.

- Validar todas las entradas en una lista "blanca" de caracteres permitidos, siempre que sea posible.
- Todos los errores de validación deben resultar en el rechazo de entrada.
- Validar todos los datos de usuario proporcionados antes del procesamiento, incluyendo todos los parámetros, URL y contenido de la cabecera HTTP.
- Validar los tipos de datos esperados.

✓ **Codificación de salidas:**

- Depurar toda la salida de los datos no confiables a las consultas de SQL, XML, y LDAP.
- Utilizan un estándar, la rutina probada para cada tipo de codificación de salida.

✓ **Autenticación y gestión de contraseñas:**

- Requerir la autenticación de todas las páginas y los recursos, salvo los destinados específicamente a ser pública.
- Todos los controles de autenticación deben aplicarse en un sistema de confianza (LDAP).
- Si la aplicación gestiona un almacén de credenciales, se debe garantizar que la tabla o archivo que almacena las contraseñas y claves contengan controles criptográficos y sean manejados únicamente por la aplicación.
- Validar los datos de autenticación.
- Hacer cumplir los requisitos de complejidad y longitud de contraseñas establecidas por la política aplicada por la Contraloría de Bogotá.
- La introducción de contraseña se deberá cubrir en la pantalla del usuario.
- Forzar desactivación de la cuenta o sesión después de un número establecido de intentos de acceso no válidos.
- Restablecimiento de contraseñas y operaciones de cambio requiere el mismo nivel de control como la creación de cuentas y la autenticación.
- Las contraseñas temporales y enlaces deben tener un tiempo de caducidad corta.
- Prevenir reutilización de contraseña.

✓ **Gestión de sesión:**

- El identificador de sesión debe realizarse siempre en un sistema de confianza (LDAP).
- La funcionalidad de cierre de sesión debe terminar completamente la sesión o conexión asociada.
- Establecer un tiempo de espera de inactividad de la sesión que sea lo más corto posible.
- No permitir conexiones persistentes y hacer cumplir las terminaciones de sesiones periódicas, incluso cuando la sesión está activa.
- No permitir conexiones simultáneas con el mismo ID de usuario.

✓ **Control de acceso:**

- Utilizar un único componente de todo el sitio para comprobar la autorización de acceso (LDAP). Esto incluye las bibliotecas que requieren servicios de autorizaciones externos
- Denegar el acceso si la aplicación no puede acceder a la información de la configuración de seguridad.
- Restringir el acceso a direcciones URL, funciones, objetos, servicios, datos protegidos sólo a los usuarios autorizados.
- Implementar auditoría de cuentas y hacer cumplir la desactivación de cuentas no utilizadas.

✓ **Manejo de log de cambios**
- No revelar información confidencial en las respuestas de error, incluyendo detalles del sistema, los identificadores de sesión o información de la cuenta.
- Restringir el acceso a los registros de sólo las personas autorizadas.
- Registrar todos los intentos de autenticación, especialmente los fracasos.
- Registrar todas las fallas de control de acceso.
- Registrar todos los eventos de alteración aparentes, incluyendo cambios inesperados en el estado de los datos
- Registrar sesiones de tokens no válidos o caducados.

✓ **Protección de datos:**
- Implementar los privilegios para restringir a los usuarios sólo la funcionalidad, datos e información del sistema que se requiere para llevar a cabo sus tareas
- Proteger de acceso no autorizado los datos confidenciales almacenados en caché o temporales almacenados en el servidor.
- No almacenar contraseñas, cadenas de conexión u otra información confidencial en texto claro o de cualquier manera segura en el lado del cliente.
- No incluya información confidencial en parámetros de la petición.
- Desactivar las funciones de auto completar en los formularios que se espera que contengan información sensible, incluyendo la autenticación.

✓ **Seguridad de comunicación:**
- Implementar mecanismos de cifrado para la transmisión de la información clasificada como reservada, privada, semiprivada, sensible, confidencial.

✓ **Base de datos**
- Utilizar consultas con parámetros fuertemente tipadas.
- Implementar el cifrado para la transmisión de toda la información sensible.
- Las cadenas de conexión no deben estar codificado dentro de la aplicación.
- Cerrar la conexión tan pronto como sea posible.
- Eliminar o cambiar todas las contraseñas administrativas de base de datos por defecto. Utilizar contraseñas fuertes / frases o implementar autenticación de múltiples factores.

✓ **Manejo de archivos:**

- Requerir autenticación antes de permitir que un archivo para ser cargado.
- Desactivar privilegios de ejecución en los directorios de subida de archivos.
- Explorar los archivos subidos en busca de virus y malware.

✓ **Manejo de memoria**
- Libere adecuadamente la memoria asignada a la finalización de funciones y en todos los puntos de salida.

2. ESTÁNDAR DE CODIFICACIÓN DE SOFTWARE

2.1 Prefijos

Es obligatorio utilizarlos para denominar cada tipo de elemento, su función es identificar diferentes tipos de campos, objetos, datos. Se puede aplicar para: directorios y estructura de archivos, archivos, clases, interfaces, servicios, formularios, funciones, etc.

Los prefijos deben estar compuestos por 2 letras y los nombres de los elementos que acompañan el prefijo deben reflejar de manera precisa su contenido y función, los prefijos se toman como una nueva palabra adicionada al elemento que se quiere describir y por lo tanto deben respetar la sintaxis del elemento.

Reglas de Generación de prefijos:

Determinar el prefijo según las siguientes condiciones:

✓ Si la palabra empieza en letra y tiene al menos 2 consonantes, se escogen las dos primeras consonantes, ejemplo:
- Texto : Tx_Nombre
- Combo: Cm_Listado

✓ Si la palabra inicia en vocal y tiene al menos una consonante, se escoge la primera vocal y consonante, ejemplo:
- Update : Up

✓ Si la palabra tiene menos 2 consonantes, se escogen las consonantes y/o vocales en el orden que aparezcan
- Aro: Ar_Centro

✓ En caso que se repita la nomenclatura se debe escoger la primera y tercera consonante o vocal en el orden que aparezcan evitando duplicidad de prefijos, ejemplo: **U**pdatePanel – Prefijo: Up y **Up**d**a**teProgress: Ud, esto se debe documentar en comentario.

2.2 Nomenclatura para elementos de base de datos.

El prefijo: debe estar en mayúscula, separado del nombre por guion bajo (_).
El nombre: debe reflejar de manera precisa y exacta el contenido y su función, no debe usar tildes y se utiliza la nomenclatura Pascal Case.

Prefijos a utilizar:

TIPO	PREFIJO	EJEMPLO
Esquema	SC_	[Servidor].[SC_Nomina_Cb].[Base_datos]
Base de datos	BD_	[Servidor].[Schema].[BD_Nomina]
Tablas	TB_	[Servidor].[Schema].[Base_Datos].[TB_Funcionarios]
Vistas	VW_	[Servidor].[Schema].[Base_datos].[VW_Funcionarios_Pensionados]
Llave Primaria	PK_	PK_CodFuncionario
Llave Foránea	FK_	FK_CodCiudad
Llaves Unique	UK_	UK_CodDepartamento
Store procedures	SP_	SP_ReporteSalidasFuncionarios
Trigger	TR_	TR_AuditoriaEstado

En caso de la existencia de un elemento de la base de datos que no se encuentra en este listado se debe utilizar las reglas de generación de prefijos, antes descrita.

2.2.1 Llaves o Clave

Los índices se nombran considerando la tabla a la que están relacionados y el propósito del índice.
• Las claves primarias utilizan el prefijo “PK”.
• Las claves foráneas utilizan el prefijo “FK”.

2.2.2 Campos:

Cada nombre de campo debe ser único dentro de su tabla correspondiente y utiliza nomenclatura Pascal Case, deben venir precedido del prefijo **PK o FK** seguido por el carácter **(_)** guion bajo cuando sean llaves primarias o foráneas.
No se deben utilizar palabras reservadas como nombres de los campos.
Ejemplo: PK_CedFuncionario, FK_CodCiudad.

2.3 Nomenclatura de programación

2.3.1 Elementos de programas:

Nomenclatura Pascal Case**.**
El nombre: debe reflejar de manera precisa y exacta el contenido y su función, no debe usar tildes.

TIPO	PREFIJO	Estructura	EJEMPLO
Formulario	Fm_	Fm_NombreFormulario	Fr_Funcionarios

Reportes	Rp_	Rp_NombreReporte	Rp_Vacaciones
WebServices	Ws_	Ws_NombreWebService	Ws_Pila
Proyecto	Pr_	Pr_NombreProyecto	Pr_Personal

2.3.2. Definición nombre de Variables

Nomenclatura Pascal Case**.**

Comience el nombre de la variable con una letra.

Debe describir claramente el propósito de la variable.

Utilizar el prefijo que indique el tipo de dato.

TIPO DE DATO	PREFIJO	Estructura	EJEMPLO
Integer (entero)	In	InNombreVariable	InTelefono
doble	Db	DbNombreVariable	DbValor
Long (entero largo)	Ln	LnNombreVariable	LnTotal
Float	Fl	FlNombreVariable	FlSubtotal
Decimal	Dc	DcNombreVariable	DcPago
Char	Ch	ChNombreVariable	ChDato
Varchar	Vr	VrNombreVariable	VrNombre
String	St	StNombreVariable	StNombreFun
boolean	Bl	BlNombreVariable	BlRespuesta
Byte	By	ByNombreVariable	ByByte
Date time	Dt	DtNombreVariable	DtFechaIncial

2.3.3. Definición de Procedimientos

Nomenclatura: Pascal Case**.**

Nombre: Describe la acción

2.3.4. Definición de Funciones

Nomenclatura: Pascal Case**.**

Nombre: Debe ser tan largos como sea necesario para describir su funcionalidad, la Primera letra del nombre en Mayúscula.

Usar el sufijo: Tipo de dato que retorna, sí la función no retorna nada no se usará sufijo (El sufijo utiliza la misma sintaxis del prefijo).

TIPO	PREFIJO	EJEMPLO
Procedimiento	Pr	*PrCalcularExcedente()*
Funciones	Fn	*FnCalcularPorcentajeDb, fnEnviarEmail*
Clases	Cl	ClCuenta

2.3.5. Definición de Objetos

Tipo	Prefijo	Ejemplo
Button	Bt	BtNombre
Calendar	Cn	CnNombre
CheckBox	Ch	ChNombre
ComboBox	Cb	CbNombre
DataGrid	Dg	DgNombre
GroupBox	Gb	GbNombre
ImageList	Il	IlNombre (il)
Label	Lb	LaNombre
LinkLabel	Ll	LlNombre
ListBox	Lb	LbNombre
ListView	Lv	LvNombre
MainMenu	Mm	MmNombre
PictureBox	Pb	PbNombre
ProgressBar	Pr	PrNombre
RadioButton	Rb	RbNombre
RichTextBox	Rt	RtNombre
StatusBar	Sb	SbNombre
TabControl	Tc	TcNombre
TextBox	Tb	TbNombre

En caso de la existencia de un objeto que no se encuentra en el listado se debe utilizar las reglas de generación de prefijos descrita inicialmente, con las siguiente excepción:

- Cuando el nombre está compuesto por dos o más palabras unidas se debe seleccionar la primera letra de cada palabra, por ejemplo: **R**ich**T**extBox - Prefijo: Rt.

3. REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

REQUERIMIENTO SEGURIDAD DE LA INFORMACIÓN
Autenticación y gestión de contraseñas.
Todos los controles de autenticación se deben aplicar en un sistema de confianza (LDAP).
El ingreso al sistema de información debe permitir autenticación de usuario, gestión de contraseña y control de sesiones seguras, cumpliendo con los requisitos aplicados por la Contraloría de Bogotá en cuanto a complejidad y longitud de contraseñas.
Debe forzar desactivación de la cuenta o sesión después de un número establecido de intentos de acceso no válidos.
Debe permitir la gestión de seguridad de usuarios, roles y perfiles, permitiendo asociarlo según los roles y responsabilidades del usuario.
No debe permitir conexiones simultaneas con el mismo ID de usuario.
Control de acceso.
La asignación de permisos o denegación de acceso al sistema de información para los usuarios, solo podrán ser aplicados por el administrador del sistema.
Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación del sistema se muestren o desplieguen dependiendo de las acciones asociadas a cada rol de

usuario, la autenticación del usuario permite el acceso a roles Y/o perfiles asignados otorgando únicamente las acciones autorizadas a realizar.
Requiere del uso de herramientas criptográficas como dispositivos biométricos, tarjetas inteligentes, certificados electrónicos, toquen de seguridad, entre otros.
Debe generar registros de auditoria de ingreso a usuarios y acciones ejecutadas en el sistema de información
Manejo de Log y Eventos
Registrar todos los eventos de alteración aparentes, incluyendo cambios inesperados en el estado de los datos y del sistema de información.
El sistema de información debe estar sincronizado con la Hora Legal Colombiana del Instituto Nacional de Metrología de la Superintendencia de Industria y Comercio, el ingreso de los usuarios y las transacciones realizadas deben quedar registradas con esta fecha y hora.
Seguridad de comunicación:
Implementar mecanismos de cifrado para la transmisión de toda la información clasificada como reservada, privada, semiprivada, sensible, confidencial.
Debe cumplir con controles de seguridad de conexión segura a través de redes públicas y privadas, garantizando la confidencialidad, integridad y disponibilidad de la información y acceso a ella.

4. PRÀCTICAS DE SEGURIDAD [1]

PRÁCTICAS DE SEGURIDAD A TENER ENCUENTA EN EL DESARROLLO DE SISTEMAS DE INFORMACIÒN
Revisión de diseño
• **Identificar posibles ataques de software:** Por medio de diagramas, compruebe el modelo para verificar una consistencia a nivel de diseño para ver cómo se aseguran las interfaces con acceso similar, cualquier ruptura en la consistencia puede ser anotada como un fallo en la evaluación.
• **Analizar el diseño contra requisitos de seguridad conocidos:** Verificar que cada requerimiento de seguridad conocido haya sido solucionado en el diseño del sistema.
Revisión de código
• **Crear listas de verificación para la revisión de los requisitos de seguridad conocidos** basándose en el punto 3. REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN.
• **Realizar revisiones en código de puntos de alto riesgo:** Revisar módulos de alto riesgo por vulnerabilidades comunes, las funcionalidades de alto riesgo incluyen módulos de autenticación, puntos de reforzamiento de controles de acceso, esquemas de manejo de sesión, interfaces externas, validadores de entradas, y analizadores de datos, etc.
• **Establecer puntos de control para la liberación de las revisiones de código:** Para establecer lineamientos de seguridad a nivel de código a todos los proyectos de software, un punto en particular en el ciclo de desarrollo de software puede ser establecido como un punto de control donde el estándar mínimo para los resultados de las revisiones de código deben ser cumplidos para poder hacer la liberación
Pruebas de seguridad
• **Deducir casos de prueba desde los requisitos de seguridad conocidos**: De los requisitos de seguridad conocidos para un proyecto, identificar un conjunto de casos de prueba para comprobar la correcta funcionalidad del software

[1] Basado en el Software Assurance Maturity Model – Una guía para integrar en el desarrollo de software Versión - 1.0. OWASP THE Open Web Application Security Project.

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	**Descripción de la modificación**
1.0	R.R. No. 047 28 Diciembre 2018	Versión inicial.

	Aprobación	Revisión Técnica
Firma:		
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. N°	**047**	**Fecha Diciembre 28 de 2018**

1. OBJETIVO

Gestionar los incidentes y/o eventos de seguridad que se presenten en los activos de información de la Contraloría de Bogotá D.C., y que atenten contra sus características de Confidencialidad, Integridad y Disponibilidad, así como la atención eficaz y oportuna de éstos.

2. ALCANCE

El procedimiento inicia con la creación del Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT) y termina con la documentación y cierre del incidente.

3. BASE LEGAL

NORMA	FECHA	DESCRIPCIÓN
Ley 1273	5-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 el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886	13-may-2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 2573	12-dic-2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

NORMA	FECHA	DESCRIPCIÓN
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único 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
CONPES 3701-2011	14-jul-2018	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 - 2016	11-Abr-2016	Política Nacional de Seguridad Digital.
NTC-ISO/IEC COLOMBIANA 20000-1:2011	abr-2011	Norma Técnica Colombiana NTC-ISO/IEC 27001 Colombiana. Tecnología de la Información.Gestión de Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio.
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.

NORMA	FECHA	DESCRIPCIÓN
Guía No 3	25-abr-2016	Procedimientos de Seguridad de la Información, MINTIC.

4. DEFINICIONES

Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.

Código malicioso: Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Contención: Son aquellas acciones tendientes a evitar la propagación de la amenaza que ocasiono el incidente de seguridad de la información detectado.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT): Es un grupo de profesionales que buscan restituir las actividades con el impacto mínimo aceptable para la entidad, así mismo brindan apoyo al funcionario u área afectada en la respuesta rápida para contener un incidente de seguridad de la información de igual manera recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas.

Erradicación: Una vez el incidente de seguridad de la información es contenido, este debe erradicarse, es decir, eliminar cualquier tipo de rastro que pudiera existir con ocasión de comportamiento inusual sobre los activos de información y/o infraestructura de TI.

Incidente de Seguridad[1]: Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Log (Registro): es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

[1] http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Mesa de servicios: Sistema manual o automatizado donde los funcionarios o entes externos registran las solicitudes e incidencias sobre los servicios que presta la Dirección de TIC.

Recolección y Análisis de Evidencia: Actividad referente a la toma, preservación, documentación y análisis de evidencia.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

5. DESCRIPCIÓN DEL PROCEDIMIENTO

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de Tecnologías de la Información y la comunicaciones	Crea el Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT), el cual estará conformado por el Director, los Subdirectores de la Dirección de TIC, el líder de seguridad de la Información y los administradores y/o gestores de infraestructura y/o servicios de TI según el incidente a considerar.	Comunicación Oficial	**Observación:** Al Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT), deben ser convocados funcionarios con funciones asignadas relativas al incidente a atender, así como el dueño funcional del servicio que está afectado (Si aplica). Los integrantes del Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT) tienen derecho a voz y voto, mientras que los invitados solo podrán ejercer el derecho de voz.
2	Servidores públicos de la Contraloría de Bogotá.	Reporta el evento, siguiendo las actividades del numeral 5.1. del procedimiento PGTI-04 - "Registro y	Sistema de Mesa de Servicios por número de caso.	

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		atención de requerimientos de soporte a los sistemas de información y equipos informáticos".		
3	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios.	Evalúa si el evento y/o incidente reportado es una falsa alarma o es un incidente de seguridad que afecta la disponibilidad, integridad y/o confidencialidad de la información. En caso de que el incidente no sea catalogado como de seguridad de la información, se continuará el numeral 5.1. Del procedimiento PGTI-04 - "Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos".	Sistema de Mesa de Servicios por número de caso.	
4	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios.	Clasifica el Incidente tomando como referencia la tabla de clasificación de los incidentes y/o eventos de seguridad (Ver. ANEXO No.1 - Clasificación de Incidentes de Seguridad).	Sistema de Mesa de Servicios por número de caso.	**Observación:** El incidente deberá ser estimado estableciendo el impacto causado a cualquier activo de Información de la Contraloría de Bogotá y a los tiempos de respuesta por parte de la Dirección de TIC. Todo esto, deberá ser documentado en el registro de la Mesa de Servicio.

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
5	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT)	Verifica la situación actual del incidente (finalizó, está en proceso, ya se tiene bajo control), obteniendo la mayor cantidad de información del incidente, complementando el registro del Incidente, como resultado de la verificación puede reclasificar y reasignar el incidente.	Sistema de Mesa de Servicios por número de caso.	**Observación:** Se deberá validar la situación reportada realizando visita en sitio de ser necesario y se da inicio al análisis del incidente, posibles causas, daños, y demás datos necesarios para realizar el análisis. Es necesario que se recoja la mayor cantidad de información de lo ocurrido o de lo que llevó al reporte teniendo en cuenta el antes, durante y después de cada acción o comportamiento para identificar la causa de manera rápida y apropiada. Así como analizar el material complementario como logs, archivos, código malicioso entre otros. Determina si es necesario reportar el caso la Oficina de Asuntos Disciplinarios en caso de existir una presunta conducta disciplinaria.

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
6	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT)	Verifica si el incidente puede ser manejado por los responsables de la actividad o se hace necesario el apoyo de un proveedor o Entidad externa. Si es necesario el apoyo de un proveedor para el manejo, se continúa con las actividades del procedimiento PGAF-08 - Gestión Contractual.	Sistema de Mesa de Servicios por número de caso.	**Punto de Control:** Si el incidente es originado en la ejecución de un contrato, el supervisor del mismo, debe diligenciar la información requerida en el incidente, incluyendo el plan de actividades que va a ejecutar el proveedor.
7	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT)	Planea las estrategias a seguir las actividades que se deben ejecutar para la gestión del Incidente de Seguridad y posteriormente, si es necesario recurrir a una recolección de evidencias. Identifica las causas del incidente, las plataformas afectadas y el detalle técnico de los activos afectados.	Documento de la estrategia para de atención del incidente	**Punto de Control**: El Director de las TIC, junto con los Subdirectores de acuerdo a la clasificación del Incidente, evalúan y aprueban la realización de las actividades propuestas en la estrategia de atención al incidente. **Observación:** Dentro de la planeación para la atención del incidente y/o evento de seguridad, deberá tener en cuenta los tiempos, así como aquellas necesidades de recursos logísticos, humanos, áreas que deben involucrarse, entre otros aspectos.

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
8	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información y Profesionales de la Dirección TIC – con roles de Administradores de infraestructura y/o servicios de TI.	Ejecuta las acciones orientadas a la contención y corrección inmediata buscando salvaguardar la información principal que está siendo afectada.	Sistema de Mesa de Servicios por número de caso.	**Observación**: Los esfuerzos se deben enfocar en detener el incidente de seguridad, evitando la propagación de la amenaza que lo causo y teniendo en cuenta las siguientes prioridades: • Proteger la vida y la seguridad de las personas. • Proteger la información confidencial o del ámbito directivo. • Proteger el hardware y software contra el ataque. • Minimizar la interrupción de los sistemas de información (incluidos los procesos).
9	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información y Profesionales de la Dirección TIC – con roles de Administradores de infraestructura y/o servicios de TI.	Ejecuta actividades de mitigación y remediación del incidente que se plantearon en el documento de la estrategia de atención al incidente con el fin de controlar la vulnerabilidad explotada y activando o implementado controles y/o eliminando o contralando la amenaza.	Sistema de Mesa de Servicios por número de caso.	**Observación:** Dentro de las actividades de remediación, se deberán tener en cuenta actividades de inspección, si es el caso, a todos aquellos activos de información que pudieron estar impactados, con la finalidad de poder cerrar las vulnerabilidades detectadas.

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
10	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información y Profesional Especializado, Profesional Universitario de la Dirección TIC con roles de Administradores de infraestructura y/o servicios de TI.	Ejecuta actividades de recuperación de sistemas de información, de información o restauración, para lo cual, si se requiere cargar la copia de respaldo actualizada del sistema de información, configuración y/o base de datos, se ejecuta el numeral 5.2 Restauración de copias de respaldo del procedimiento Realización y Control de Copias de Respaldo (backups) – PGTI-03.	Sistema de Mesa de Servicios por número de caso.	**Observación:** Dentro de las actividades de recuperación se puede contemplar: • Creación nuevamente de la información digital o física, configuración de sistemas operativos, sistemas de información y carga manual de la información. • Actualización o instalación de parches de seguridad a los sistemas que se vieron comprometidos. • Actualización en lote del antivirus.
11	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT)	Comprueba la eficacia y oportunidad de la solución al incidente de seguridad de la información.	Sistema de Mesa de Servicios por número de caso.	**Observación:** Como parte de la comprobación, se debe realizar un análisis que ocasionó la no disponibilidad de los servicios, o el daño de los activos de información afectados por el incidente de seguridad, teniendo en cuenta la criticidad que estos representan para la entidad.
12	Asesor y/o Profesional Especializado	Documenta y cierra el incidente con indicación del análisis	Sistema de Mesa de Servicios por número de caso.	

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	con funciones de Oficial de Seguridad de la Información	de sitio, fecha, descripción del hecho y cuáles fueron las causas, la estrategia de atención, las acciones preventivas, acciones correctivas, conclusiones y recomendaciones.		

6. ANEXOS

ANEXO No.1 - Clasificación de Incidentes de Seguridad

La clasificación de los incidentes de seguridad se debe realizar teniendo en cuenta la siguiente tabla:

Tabla 1 - Niveles de criticidad de los incidentes y/o eventos de Seguridad

NIVEL	NOMBRE	TIEMPO DE ATENCIÓN
1	BAJO	1 SEMANA
2	MEDIO	2 DÍAS
3	ALTO	12 HORAS
4	CRÍTICO	1 HORA

Fuente: Elaboración propia – con base en el catálogo de servicios de la Dirección de TIC de la Contraloría de Bogotá.

La ponderación para la clasificación de estos niveles es la siguiente:

Bajo o Nulo: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados como posibles amenazas para los activos de información, es decir, que pueden impactar sus características de integridad y/o confidencialidad y/o disponibilidad, sin embargo, los controles de seguridad resultan efectivos anulando cualquier impacto para la Contraloría de Bogotá.

Medio: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados como posibles amenazas, que pueden afectar los activos de información de la entidad, impactando de modo limitado sus características de integridad y/o confidencialidad y/o disponibilidad frente a un activo no crítico para la Contraloría de Bogotá.

Alto: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de un activo no crítico o critico para la Contraloría de Bogotá.

Crítico: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de un activo crítico la Contraloría de Bogotá.

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	R.R. No. 047 28 Diciembre 2018	Versión Inicial

Aprobación		Revisión Técnica	
Firma:		Firma:	
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.	**Fecha**		

1. OBJETIVO

Proteger la información por medio de la gestión y aseguramiento de los servicios de red de la Contraloría de Bogotá D.C., así como el establecimiento de actividades para el uso de mecanismos criptográficos para garantizar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Inicia con la verificación y análisis de los registros (logs) de auditoria y eventos de los elementos de red (Routers, switches, firewall, controladores inalámbricos, otros) información y equipos informáticos, y finaliza con la actualización del inventario de los distintos mecanismos criptográficos.

3. BASE LEGAL

NORMA	FECHA	DESCRIPCIÓN
Ley 527	19-ago-1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
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	5-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 1341	30-jul-2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
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.
Decreto 886	13-may-2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074	26-may-2015	Por medio del cual se expide el Decreto único Reglamentario del Sector Comercio, Industria y Turismo.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único 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.
CONPES 3701-2011	14 - jul - 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2016	11-abr-2016	Política nacional de seguridad digital.
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

Activo de información: Es una pieza de información definible e identificable, almacenada en cualquier medio.

Criptografía: Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

Enrutador: (Router) Dispositivo de comunicaciones encargado de enviar paquetes de datos de una red a otra de acuerdo con las reglas implementadas en la red de la entidad.

Hardening o endurecimiento: Es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuanto más funciones desempeña; el proceso de cerrar las vías para los ataques más típicos incluye el cambio de claves por defecto, desinstalar el software y dar de baja usuarios y accesos innecesarios; también deshabilitar servicios que no serán usados y fortalecer las configuraciones de aquellos que estarán en uso.

Hash: Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Información: Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.

Logs: Huellas o rastros de los sucesos que se han presentado en un equipo de cómputo o de comunicaciones de red con el fin de dar a proteger los equipos que conforman la red de la entidad.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Segmentación de red: proceso a través del cual se divide la red LAN en segmentos o grupos más pequeños con el fin de conseguir un mejor aprovechamiento del ancho de banda, evitar congestión de tráfico.

Transferencia de información: Proceso a través del cual se entrega información en formato digital al interior de la entidad o entidades externas de acuerdo con la solicitud presentada.

5. DESCRIPCION DEL PROCEDIMIENTO

5.1. Aseguramiento de Servicios en la Red

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura	Verifica y analiza los registros (logs) de auditoria y eventos de los elementos de red (Routers, switches, firewall, controladores inalámbricos, otros) En caso de encontrar		

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
	de redes de TI.	alertas que comprometan la red o su seguridad, se inicia con las actividades del Procedimiento Gestión de Incidentes de Seguridad – PGTI-10.		
2	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Realiza actividades de administración y gestión de privilegios de usuarios con acceso al dispositivo de acuerdo a lo descrito en el procedimiento Control de Accesos a Usuarios – PGTI-07 y efectúa acciones de hardening o endurecimiento de dispositivos de ser requerido. Registra actividades en SICEINFO .	Sistema de Información de Control de Elementos Informáticos SICEINFO	
3	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Segmenta redes de acuerdo con las necesidades de distribución y seguridad de la información de la entidad, establece la segmentación de la red. Si existen, revisa y evalúa solicitudes de cambios en temas de organización, segmentación nuevos o modificación de accesos y se inicia el	Diagramación y documentación de la segmentación de la red de la Contraloría de Bogotá.	

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		procedimiento Gestión de Cambios y Capacidad Tecnológica – PGTI-08		
4	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Gestiona y/o configura las redes Inalámbricas autorizadas según la necesidad.		
5	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Configura y gestiona las conexiones de VPN autorizadas según la necesidad.	Registro de VPN	**Observación:** Revisa los parámetros técnicos para la conexión segura sección 5.3 controles criptográficos de este procedimiento en conjunto con el Oficial de Seguridad.
6	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Establece los protocolos de trasmisión y transferencia de información que se manejaran en las diferentes redes.		**Observación:** Teniendo en cuenta el nivel de confidencialidad de la información, a transmitir por las redes establecidas en la Contraloría de Bogotá, se iniciarán las actividades 5.3. Gestión de

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
				Controles criptográficos de este procedimiento
7	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Supervisa y controla cuatrimestralmente los aspectos de configuración en los equipos y sistemas operativos de los elementos de la red que permitan asegurar la disponibilidad, integridad y confidencialidad de la información de acuerdo con las necesidades de la entidad.	Informe de administración y gestión de conexiones de red.	
8	Subdirector de Recursos Tecnológicos	Revisa informe de administración y gestión de conexiones de red.		

5.2. Transferencia de Información digital

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
1	Servidores públicos de la Contraloría de Bogotá Propietario del activo de información	Reporta la solicitud de transferencia o transmisión de información, siguiendo las actividades del numeral 5.1. del procedimiento PGTI-04 - "Registro y atención de requerimientos de soporte a los sistemas de información y	Registro en el Sistema de Mesa de Servicios	**Punto de Control:** Para solicitudes de transferencia de información con entidades externas debe ser solicitado por el jefe de la dependencia propietario de la información. **Observaciones**:

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		equipos informáticos".		Tener en cuenta los acuerdos de confidencialidad establecidos por la Entidad Los servidores públicos de la Contraloría de Bogotá, que traten temas o información clasificada como información pública reservada o información pública clasificada (privada o semiprivada), lo deberán hacer en lugares seguros y/o por medios de comunicación establecidos por la Entidad.
2	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios la Dirección TIC – responsable del registro en el Sistema de Mesa de Servicios	Verifica la necesidad de transferencia de información, establecerá sí es transferencia de información al interior de la entidad o fuera de ella y escala el requerimiento.	Sistema de Mesa de Servicios por número de caso.	**Observación**: La transferencia de información al interior de la Entidad se realizará a través de los medios oficiales de comunicación establecidos por la entidad.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
3	Profesional Especializado, Profesional Universitario – responsable de atención de la solicitud (Asignado)	Complementa la solicitud de transferencia de información teniendo en cuenta los siguientes aspectos en caso que se requiera: **Si es Transferencia a terceros:** • Establecer el acuerdo de transferencia de información con terceros, el cual deberá contener cláusulas donde se establezcan las herramientas a utilizar para asegurar la transferencia de información. • Incluir acuerdos de confidencialidad de la información, compromiso y reserva, el cumplimiento de la normatividad vigente nacional e internacional para el tratamiento de la información, en caso que se requiera. • Método de enrutado y autenticación detallada para la transferencia de información. • Tiempo aproximado	Sistema de Mesa de Servicios por número de caso. Acuerdo de transferencia y confidencialidad de información con terceros.	**Punto de Control:** El Director y subdirectores de Tecnologías de la Información y las comunicaciones, revisan y aprueban la solicitud antes de ser realizada. **Observaciones**: La transferencia de información digital será liderada por la Dirección de Tecnologías de la Información y las comunicaciones así como el control del uso de sistemas de transferencia en coordinación con la dependencia y/o funcionario que manifieste la necesidad. La Dirección de TIC se reservará el derecho de suspender de manera unilateral los servicios que hacen parte del objeto del acuerdo, así como la terminación unilateral del mismo, si llegaré a

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		de utilización de la herramienta para el traspaso de la información. • Especificaciones técnicas especiales como llaves digitales o técnicas de encriptación de acuerdo con la entidad que se esté trabajando y la clasificación de la información Pasa a la actividad No.4 **Si la transferencia es interna:** • Valida que este autorizado por el jefe inmediato. • Evalúa la necesidad y establecer la herramienta apropiada para la atención de la solicitud. • Verifica la clasificación de la información a transferir de ser necesario da inicio a las actividades descritas en la sección 5.3 – Gestión de Controles Criptográficos de este		detectar algún incidente de seguridad que ponga en riesgo la Información de la Contraloría de Bogotá. La Entidad realizará transferencia de información con organizaciones gubernamentales y privadas, basada en la necesidad planteada por la Contraloría de Bogotá.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		procedimiento. Pasa a la actividad No.5		
4	Profesional Especializado, Profesional Universitario de la Dirección TIC – responsable de atención de la solicitud (Asignada)	**Transferencia de información a terceros** Si la transferencia de información obedece a la ejecución de una función de la entidad, se procede a coordinar con la entidad interesada el método de transferencia y si se requiere un cambio en la infraestructura de red, se inicia el procedimiento Gestión de Cambios y Capacidad Tecnológica – PGTI-08.	Sistema de Mesa de Servicios por número de caso	**Punto de control**: Verifica si la transferencia de información hace parte del desarrollo de un contrato, para lo cual deberá verificar que se tenga total claridad del acuerdo de confidencialidad de la información que firmo.
5	Profesional Especializado, Profesional Universitario de la Dirección TIC – responsable de atención de la solicitud (Asignada)	**Transferencia de información interna** Realiza las actividades de transferencia de información interna; para lo cual sí se requiere un cambio en la infraestructura de red, se inicia el procedimiento Gestión de Cambios y Capacidad Tecnológica – PGTI-08. De lo contrario realiza las actividades del procedimiento Registro	Registro en el Sistema de Mesa de Servicios	**Observación:** La Dirección de Tecnologías de la Información y las comunicaciones, implementará las herramientas, y controles para asegurar la transferencia de información al interior de la Entidad.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		y atención de requerimientos de soporte a los sistemas de información y equipos informáticos – PGTI-04, que apliquen de acuerdo a la naturaleza de la solicitud.		
6	Profesional Especializado, Profesional Universitario de la Dirección TIC – responsable de atención de la solicitud (Asignada)	Valida el método de transferencia. En caso de ser por el protocolo de transferencia de archivos FTP o almacenamiento en la nube o correo electrónico, se inicia las actividades descritas en la sección 5.3 – Gestión de Controles Criptográficos de este procedimiento en caso que aplique. En caso de ser por medio extraíble (USB, DISCO EXTERNO u OTRO) realiza las actividades del procedimiento Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos – PGTI-04, que apliquen de acuerdo a la naturaleza de la	Registro en el Sistema de Mesa de Servicios	**Punto de Control:** Informa a Director y Subdirectores de Tecnologías de la Información y las comunicaciones que los servicios abiertos para atender la solicitud fueron cerrados.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		solicitud. Finaliza la atención como se indica en el procedimiento Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos – PGTI-04 y cierra o desactiva los servicios autorizados temporalmente para la atención del requerimiento.		

5.3. Procedimiento de Criptografía

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, Asesor, Gerente, Profesional, Técnico, Secretario o Auxiliar.	Revisa la clasificación del activo en el registro de activos de información contenido en los Instrumentos de Gestión de Información Pública, sí el activo de información no se encuentra registrado se activa Procedimiento PGD-08 – "Actualización de los Instrumentos de Gestión de Información Pública". Numeral 5.1 Actualización, aprobación y		**Observación:** Resultado de la clasificación de los activos de información, surge la necesidad de aplicación de controles criptográficos para la gestión de la información.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		divulgación de Instrumentos: Registro de Activos de Información, Índice de Información Clasificada y Reservada o Esquema de Publicación de Información. Identifica si el activo de información se encuentra calificado como público clasificado o publico reservado.		
2	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, asesor, gerente, profesional, técnico, secretaria, auxiliar, (Funcionario perteneciente a la dependencia propietario del activo de información).	Registra el requerimiento de aplicación de controles criptográficos al activo a través de la mesa de servicio, se activa procedimiento PGTI-04 - "Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos".	Registro en el Sistema de Mesa de Servicios	**Observación**: Informa el nombre del funcionario y tiempo de utilización del control criptográfico.
3	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información.	Revisa los riesgos de seguridad digital del activo de información establecidos en el mapa de riegos, en caso no existir registro éste y según evaluación		**Punto de Control:** Valida la clasificación según el nivel de confidencialidad y privilegios de acceso a la información y

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		solicita a dueño de proceso su incorporación en el mapa de riesgos de seguridad digital.		define si continua con la ejecución del procedimiento o si la información no requiere controles criptográficos termina el procedimiento y se registra en el Sistema de Mesa de Servicios.
4	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información.	Determina los mecanismos criptográficos a implementar, basado en lo descrito en el Anexo 1 "Mecanismos Criptográficos".		Observación: Se utilizarán controles criptográficos en los siguientes casos: 1. En la protección de claves de acceso a sistemas, datos y/o servicios. 2. Para la transmisión de información Reservada o Clasificada, fuera de la Entidad. 3. En la protección de la información a custodiar, cuando así lo establezca el dueño de la información o Oficial de Seguridad de la Información.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
5	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, asesor, gerente, profesional, técnico, secretaria, auxiliar, (Funcionario perteneciente a la dependencia propietario del activo de información).	Asigna la clave para el cifrado de la información, debe ser establecida por el usuario que administra dicha información utilizando para ello protocolos para generar llaves seguras y teniendo siempre presente que en caso de olvidar la clave, la información cifrada no es recuperable.		**Observación**: Para la generación de llaves y/o claves seguras, tener presente lo descrito en el Anexo 5. "Instructivo para la gestión de contraseñas seguras", del PGTI-07 **–**Procedimiento De control de acceso a usuarios
6	Asesor, Profesional Especializado con funciones de Oficial de Seguridad de la Información.	Realiza el aprovisionamiento o alistamiento de hardware, software, y demás recursos necesarios para poner en marcha los controles criptográficos que serán utilizados.		**Observación**: Teniendo presente los controles que se implementaran se da inicio al procedimiento PGTI-08 "Procedimiento para la Gestión de cambios y capacidad tecnológica"

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
7	Asesor, Profesional Especializado con funciones de Oficial de Seguridad de la Información.	Actualiza el inventario de los mecanismos criptográficos controlando, fechas de expiración, asignaciones realizadas, activo custodiado y así poder renovar oportunamente y/o revocar los controles que ya no son requeridos.	Inventario de mecanismos criptográficos	**Observación:** Para gestionar el ciclo de vida de las llaves criptográficas debe tener presente lo descrito en el Anexo 2. "Lineamiento Gestión de llaves criptográfica".

6. ANEXOS

Anexo 1. Mecanismos Criptográficos

Dentro de los mecanismos criptográficos que la Contraloría de Bogotá puede implementar se encuentran:

- **Certificado Digital:** o certificado electrónico es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital.
- **Certificados SSL**: Sirve para brindar seguridad al visitante de un sitio web, es una manera de indicarle a los usuarios que el sitio es auténtico, real y confiable para ingresar datos personales. Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que los datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada.
- **Certifirma:** Aplicativo desarrollado por Certicámara S.A., en donde el usuario interactúa para realizar los procesos de firma de documentos en diferentes formatos ej. (Doc, jpeg, PDF). este aplicativo tiene un tipo de licencia freeware.
- **Cifrado de archivos y carpetas**: Es un procedimiento que vuelve completamente ilegibles los datos de un documento o de cualquier archivo. De esta manera, el

archivo se vuelve prácticamente inservible para un usuario no autorizado a leerlo, ya que incluso si lo ha interceptado o lo ha copiado, si no cuenta con la clave correspondiente, no podrá leerlo o visualizarlo.

- **Clave:** conjunto finito de caracteres alfanuméricos necesarios para el uso del certificado digital, el cual debe ser conocido únicamente por el titular del certificado.
- **Correo Electrónico Certificado**: Permite a los suscriptores tener las notificaciones electrónicas de los correos electrónicos demostrando que reproduce con exactitud la información generada, enviada o recibida, a su vez es posible determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje aportando validez jurídica y probatoria.
- **Dispositivos Criptográficos**: Hace referencia a mecanismos por ejemplo para doble autenticación como es el uso del Token.
- **Estampado Cronológico**: Estampar cronológicamente, consiste en certificar que un conjunto de datos o documentos ha existido e incorpora la fecha y la hora en que ocurre dicho evento, específicamente cuando fue creado, modificado, recibido, etc., en un sistema de cómputo.
- **Firma Digital**: Es un método criptográfico que asocia una identidad ya sea de una persona en particular o de un equipo a un mensaje enviado a través de transmisión por la red. Su uso puede ser diferente dependiendo de lo que se requiera hacer con la firma como por ejemplo, expresar conformidad con algún documento de tipo legal como podría ser la firma de un contrato laboral e incluso asegurar que no podrá modificarse el contenido del mensaje. La firma digital es el resultado de aplicar a un documento, en línea, un procedimiento matemático que requiere datos que exclusivamente conoce la persona que firma, encontrándose ésta bajo su absoluto control.
- **Generación de Firmas Digitales**: Es un servicio que integra la firma digital a una plataforma de acceso seguro en la cual se puede firmar y enviar documentos a usuarios internos o externos de la entidad a través de circuitos de firma y flujos de trabajo.
- **Token de seguridad** (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Anexo 2. Lineamientos Gestión de Llaves Criptográfica

Dentro de la gestión de los controles criptográficos, se debe administrar el ciclo de vida de los mecanismos utilizados donde se deben contemplar mínimamente las siguientes fases:

- **Generación de contraseñas:** Aplicar 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. Anexo 5. "Instructivo para la gestión de contraseñas seguras", del PGTI-07 –Procedimiento De control de acceso a usuarios.

- **Distribución**: Disponer adecuadamente de mecanismo criptográfico: Comprende la forma como llega y se autentica el mecanismo criptográfico en el banco o base de datos que autoriza el acceso a la plataforma.
- **Políticas de Uso:** Aplicar políticas para generar, emplear, recuperar, reemplazar y disponer de las claves y contraseñas. Determinar los límites de uso, y esto incluye tipo de caracteres; longitud de la contraseña; políticas de almacenamiento en la base de datos; políticas de recuperación de clave o contraseña olvidada; y caducidad u obsolescencia ("vencimiento") de las claves.
- **Almacenamiento en Base de datos: D**ebe almacenar o alojar la información de las claves o contraseñas en una Base de Datos; y restringir el acceso a ella, la cual se basa en los siguientes controles de seguridad:
  - Encripción de los archivos que contienen las claves y contraseñas.
  - Activación del control de acceso al sistema operativo de la Base de Datos.
  - Almacenamiento de hashes criptográficos para claves y contraseñas.
  - Verificación del dispositivo (capacidades de seguridad, amenazas y/o requerimientos de autenticación).
- **Obsolescencia:** En esta etapa final del ciclo de vida de claves y contraseñas, se debe dar disposición final adecuada a las claves o contraseñas cuando caen en desuso, no deben usarse por tiempo indefinido. Existen dos tipos de disposición de las claves y contraseñas una vez se hacen obsoletas:
  - Disposición por Expiración: Establecer el tiempo máximo de vida útil de claves y contraseñas. Esto da una ventana de tiempo predeterminada para que las mismas caigan en desuso, y sea necesario crear una nueva clave o contraseña para el acceso seguro.
  - Disposición por Revocación: Ocurre cuando se detecta compromiso en las claves y contraseñas, y para asegurar la integridad de las mismas, procede a su descontinuación inmediata. También se revoca una clave o contraseña por fuerza mayor (despido, deceso o redefinición de privilegios de usuario; actualizaciones; restructuraciones, entre otros).

    Cuando las claves y contraseñas se hacen obsoletas, se deberá determinar los parámetros de su destrucción y disposición final. Generalmente, los controles más comunes para adelantar esta destrucción son los siguientes:
    - Borrado seguro.
    - Destrucción física por desmagnetización o trituración de medios magnéticos.

7. CONTROL DE CAMBIOS

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

Aprobación		Revisión Técnica	
Firma:		Firma:	
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 Diciembre 28 de 2018**	

1. OBJETIVO:

Estandarizar las actividades para dar soporte técnico a las incidencias, solicitudes o eventos que afecten el funcionamiento de los sistemas de información y/o equipos informáticos de la Contraloría de Bogotá D.C., para garantizar el normal funcionamiento de los mismos, asegurando la continuidad en su operación y de los servicios informáticos.

2. ALCANCE:

El procedimiento inicia con el ingreso de la solicitud de soporte por parte del funcionario, encargado y/o el reporte de los problemas detectados en los elementos computacionales de la entidad y finaliza con la elaboración y presentación del Informe mensual y consolidado Trimestral y Estadístico.

3. BASE LEGAL:

NORMA	FECHA	DESCRIPCIÓN
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 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 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información

NORMA	FECHA	DESCRIPCIÓN
		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 20000-1:2011	abr-2011	Norma Técnica Colombiana NTC-ISO/IEC 27001 Colombiana. Tecnología de la Información. Gestión de Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio.
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.
Lineamientos MINTIC LI.ST.08, LI.ST.09	26-May-2015	Implementación del procedimiento para atender los requerimientos de soporte de primer, segundo y tercer nivel, para sus servicios de TI, a través de una Mesa de Servicio.

NORMA	FECHA	DESCRIPCIÓN
Guía No 3	25-abr-2016	Procedimientos de Seguridad de la Información, MINTIC.

4. DEFINICIONES:

ANS o SLA (Service Level Agreement): acuerdos de nivel de servicio, con relación a la cantidad de equipos y al tiempo de respuesta para cada uno de ellos.

Asistencia: Apoyo técnico en sitio.

Caso: Número consecutivo asignado al Requerimiento o Incidente.

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

Desarrollo nuevas funcionalidades: Actividades referentes a los sistemas de información existentes (campos nuevos, reportes, modificaciones y/o nuevos formularios, plantillas).

Escalamiento: Se refiere al movimiento de casos entre agentes con el fin de brindar solución a los requerimientos en el nivel de soporte técnico especializado. En el escalamiento se documentará los avances de la gestión realizada.

Falla: Es un error en hardware o software que genera discontinuidad en la actividad realizada o mal funcionamiento de la infraestructura tecnológica.

Hardware: Son todos aquellos componentes físicos de una computadora, todo lo visible y tangible. Algunos componentes del hardware son: Teclado, Mouse, CPU, entre otros. También hacen parte las impresoras, los escáneres.

Herramientas ofimáticas: Programas que facilitan las labores propias de la oficina. Ejemplo: Procesadores de palabra, hojas electrónicas, mensajería y colaboración, diagramación entre otros.

Infraestructura Tecnológica: Es el conjunto de hardware y software sobre el cual funcionan los diferentes servicios que presta la Contraloría de Bogotá: equipos de cómputo, equipos de comunicaciones, sistemas de información, equipos de fotocopiado, equipos de digitalización, equipos de telefonía.

Mantenimiento de equipos: Conjunto de tareas tendientes a mantener en perfecto funcionamiento las estaciones de trabajo e impresoras de la Entidad.

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.

Repuesto: Es una pieza o parte que se utiliza para reemplazar las originales en equipos que debido a su uso diario han sufrido deterioro o un daño.

Requerimiento técnico: Aviso o manifestación de una situación problema a nivel técnico

Sistemas de Información: conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control en una institución.

Software: Programa o grupo de ellos que indica al equipo como operar y reaccionar ante diferentes eventos. El término incluye sistemas operativos, programas y aplicaciones.

Solicitud: Son peticiones de atención a daños o fallos en la infraestructura de software y/o hardware que pueden ser de soporte, de mantenimiento, de nuevos desarrollos o de capacitación.

El soporte se categorizará en los siguientes niveles:

Soporte primer nivel (N1): Soporte inicial, responsable de las incidencias básicas del usuario. Es el encargado de hacer el diagnóstico inicial en sitio, hacer las configuraciones e instalaciones básicas de Sistemas Operativos, drivers, y utilitarios o de sistemas de información. La principal labor es reunir toda la información del usuario y determinar la solución inmediata.

Soporte segundo nivel (N2): Es el soporte que deben realizar los especialistas en un tema específico como redes, conectividad sistemas de información, sistemas de seguridad, bases de datos, administración técnica de los sistemas de información y actividades relacionadas con el aplicativo para rendición de cuentas por parte de los sujetos de control.

Soporte tercer nivel (N3): Lo pueden efectuar los administradores funcionales y técnicos de los servicios o aquellos servicios de los cuales existe un administrador o super-usuario con el conocimiento de la actividad especializada, y están encargados de realizar actividades como, investigación y desarrollo de soluciones a los problemas nuevos o desconocidos, es decir ajustes a los sistemas en funcionamiento y/o nuevos desarrollos.

Soporte cuarto nivel (N4): Corresponde al soporte directo del fabricante, Contratista o Proveedor de un equipo, aplicación informática, sistema de información o equipo asociado a la prestación de los servicios informáticos de la Entidad.

Soporte técnico: Es un rango de servicios por medio del cual se proporciona asistencia a los usuarios que tengan algún problema al utilizar un producto o servicio, bien sea, relacionado con hardware, software o cualquier otro equipo o dispositivo informático.

Usuario: Funcionario de la Contraloría de Bogotá o del sujeto de control fiscal que solicita asistencia técnica sobre los sistemas de información e infraestructura tecnológica implementada en la entidad.

Usuario interno: Funcionario de la Contraloría de Bogotá D.C.

Usuario externo: Sujeto de Vigilancia y Control Fiscal.

5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 ATENCIÓN DE REQUERIMIENTOS DE SOPORTE TIC

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Auxiliar Administrativo Secretario Técnico Operativo Profesional Universitario, Especializado Gerente Subdirector Técnico, Financiero, Administrativo Jefe Oficina Director Técnico Asesor Contralor Auxiliar Contralor (Funcionarios de la Contraloría de Bogotá)|	**Ingresa la solicitud** **Solicitud usuario Interno** Reporta a través del Sistema de Mesa de Servicios, la solicitud, requerimiento u oficio con la descripción de la necesidad, error, falla o problema de Software, de los aplicativos o sistemas de información Institucionales. Continúa en la **actividad 3**	Registro en el Sistema de Mesa de Servicios	**Punto de Control:** La Dirección de Tecnologías de la Información y las Comunicaciones la única autorizada para realizar la instalación y desinstalación de sistemas de información, aplicativos y configuración de equipos. **Observación:** En caso de contingencia por ausencia del sistema automático de Mesa de Servicios, se deberá diligenciar el formato Registro de Soporte Anexo 1 PGTI-04-01.
2	Profesional Especializado,	**Solicitud de usuario Externo**	Registro en el Sistema de Mesa	**Punto de Control:** El Sistema de

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Profesional Universitario, Técnico responsable del Sistema de Mesa de Servicios.	Recepciona solicitud a través de medio telefónico, correo electrónico, o por comunicación escrita recibida directamente o a través de la dependencia competente. Registra en el Sistema de Mesa de Servicios. Informa el número de caso para atención de este. Continúa en la **actividad 3**	de Servicios	Mesa de Servicios asigna número de caso para la atención de este y almacena información básica de la solicitud en la base de datos. **Observación:** En caso de contingencia por ausencia de un sistema de Mesa de Servicios, se deberá diligenciar el formato Registro de Soporte Anexo 1 PGTI-04-01, cuando pase la contingencia la información de este formato se ingresará al Sistema de Mesa de Servicios. Actualizar de acuerdo con la información de cada actividad y según sea el caso.
3	Profesional Especializado, Profesional Universitario, Técnico responsable del Sistema de Mesa de Servicios.	Evalúa sí la información brindada por el usuario es suficiente para atender la solicitud, si se requiere información adicional se continua con la **actividad 4**; de lo contrario se continua con la **actividad 5**.		
4	Profesional Especializado, Profesional Universitario, Técnico responsable del Sistema de Mesa de Servicios.	**Solicitud Usuario Interno** Solicita información adicional a través del Sistema de Mesa de Servicios. **Solicitud Usuario**	Sistema de Mesa de Servicios por número de caso.	**Punto de Control:** Documenta en el Sistema de Mesa de Servicios por el número de caso, la información solicitada.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Externo Solicita información adicional por el mismo medio en que se recibió la solicitud (correo electrónico, comunicación escrita y/o teléfono).		
5	Profesional Especializado, Profesional Universitario, Técnico responsable del Sistema de Mesa de Servicios.	**Analizar la solicitud de soporte** Realiza análisis técnico clasificándola por tipo de solicitud y categorización del caso en atención de primer nivel (N1), segundo nivel (N2), tercer nivel (N3) o cuarto nivel (N4); nivel acorde a su criticidad, complejidad o alcance necesario para la solución. Cada nivel de atención tendrá diferentes ANS o SLA (tiempo estimado de solución). Asigna el caso al profesional especializado, Profesional Universitario o Técnico de la Dirección TIC. Sí la solicitud es de: • **Adquisición, desarrollo soporte y/o mantenimiento a Sistemas de Información**, se activa procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información PGTI-09, en caso que sea para adquisición y/o desarrollo nuevo sistema de	Sistema de Mesa de Servicios por número de caso.	**Punto de Control:** Documenta en el Sistema de Mesa de Servicios por el número de caso, la información relacionada con la asignación o especificidad para el tratamiento del caso.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		información: realiza categorización del caso en atención tercer nivel (N3) y asigna el caso al Subdirector de Gestión de Sistemas de Información. • **Instalación de aplicativos:** Se activa procedimiento gestión de recursos y servicios tecnológicos numeral de Administración de licencias de software. • **Capacitación**: Continúa con el numeral 5.2. Solicitud Capacitaciones Sistemas de información. • **Soporte a equipos informáticos:** Continúa con el numeral 5.3. Soporte a Equipos Informáticos. • **Reporte de incidentes de seguridad**: Se activa procedimiento de Gestión de Incidentes de Seguridad PGTI-10 **Otro tipo de solicitud:** No contemplado en los anteriores, continua con la **actividad 6**		
6	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – responsable de	Inicia proceso de solución en sitio o remotamente o en el aplicativo que sea requerido. Ejecuta Solución.	Sistema de Mesa de Servicios por número de caso.	**Punto de control:** Ejecuta la solución dentro de los tiempos establecidos (ANS) para el requerimiento

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	atención del caso	Si la información registrada en el requerimiento no es suficiente para brindar una solución, se comunica con el solicitante a través de los canales establecidos por la entidad, para dar continuidad a la solución. Actualiza en el Sistema de Mesa de Servicios las acciones realizadas que dieron solución a la solicitud y asigna estado solucionado al número de caso.		asignado. Si requiere apoyo de otro nivel de servicio reasigna el caso al nivel correspondiente para dar solución definitiva, dejando registro de lo requerido. No se autoriza la instalación de aplicativos no licenciados. Se prohíbe la instalación 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.
7	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – responsable de atención del caso	**Solución del caso** Sí la solución es satisfactoria para el usuario el requerimiento se cierra. Sí la solución no es satisfactoria para el usuario, el caso se asigna nuevamente al responsable de atender la solicitud y se continua con la **actividad 6.**	Sistema de Mesa de Servicios por número de caso.	**Punto de control** Director de TIC, y/o Subdirector de Gestión de la Información realizaran monitoreo con el fin de establecer si hay casos sin atender en el tiempo asignado y tomar correctivos, según corresponda. La satisfacción del

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				usuario se realiza a través de la encuesta del servicio.
8	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – responsable del Sistema de Mesa de Servicios.	**Informes consolidados y Estadístico.** Elaborar informe trimestral que indique casos atendidos, categoría, nombre usuarios que generaron las solicitudes, tiempos de atención, entre otros.	Informe en formato Word, Excel o PDF, generado por el Sistema de Mesa de Servicios.	**Observación:** El informe debe otorgar información del nivel de satisfacción del servicio de soporte.

5.2 SOLICITUD CAPACITACIÓNES SISTEMAS DE INFORMACIÓN

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – responsable de atención del caso.	Realiza actividades de la 1 a la 5 del **numeral 5.1 Atención de Requerimientos de Soporte TIC.**	Sistema de Mesa de Servicios por número de caso.	
2	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – responsable de atención del caso.	Proyecta solicitud de gestión de capacitación a la Subdirección de Capacitación y Cooperación Técnica en el caso de que aplique, de lo contrario realiza las gestiones para su programación. Activa el procedimiento para la Planificación, Ejecución, Modificación y Evaluación de la Capacitación PGTH-11.	Comunicación Oficial Interna Sistema de Mesa de Servicios por número de caso.	**Punto de control:** Director de TIC y/o Subdirector de Gestión de la Información revisaran la pertinencia de la solicitud y la solución y aprobaran la misma para su trámite.
3	Profesional Especializado,	Informa al usuario lugar, fecha y hora de	Sistema de Mesa de Servicios por	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Profesional Universitario, Técnico de la Dirección TIC – responsable de atención del caso y/o Subdirección de Capacitación	capacitación a través del sistema de requerimientos y/o comunicación oficial interna.	número de caso. Comunicación Oficial Interna	
4	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – responsable de atención del caso	**Desarrollo de capacitación** Ejecuta las actividades correspondientes a la capacitación. Entrega listado de asistencia a Escuela de Capacitación y a funcionario de la Dirección de TIC que administra la gestión documental. Cambia a estado solucionado en Sistema de Mesa de Servicios.	Registro de Asistencia PGTH-11-02 del Procedimiento para la Planificación, Ejecución, Modificación y Evaluación de la Capacitación, Inducción, Reinducción y Programa de Formadores Internos PGTH-11. Comunicación Oficial Interna	

5.3 SOPORTE A EQUIPOS INFORMÀTICOS

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – responsable de atención del caso	Realiza actividades de la 1 a la 5 del numeral 5.1 Atención de Requerimientos de Soporte TIC.	Sistema de Mesa de Servicios por número de caso	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
2	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	**Atender caso Nivel 1** Verifica en sitio o en forma remota falla y/o requerimiento del usuario, realiza diagnóstico de las causas que originaron la solicitud; dependiendo de la magnitud del problema, proyecta la solución y determina qué tipo de Intervención se requiere. Subsana la falla de acuerdo con los tiempos de respuesta asignados (ANS o SLA). Si la falla es corregida realiza las pruebas necesarias para determinar un correcto funcionamiento. En los casos, en que se dé una solución satisfactoria a la solicitud se debe continuar con la actividad 10. (Documentar la solución). Si las pruebas realizadas no son satisfactorias y se diagnostica que es necesaria una reparación mayor que implica trasladar el equipo de cómputo, ejecuta la **actividad 3 de éste numeral**. Si las pruebas realizadas NO son satisfactorias y se diagnostica que es necesario el apoyo de personal especializado, se debe escalar a Nivel 2, y continuar con la **actividad 8 de éste numeral.**		**Punto de control:** Con el número de caso registra y documenta las acciones ejecutadas, a través del Sistema de Mesa de Servicios. **Punto de control**: El Director de TIC o Subdirector de Recursos Tecnológicos, verifican el cambio de Nivel de servicio en el Sistema de Mesa de Servicios.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		(Atender caso Nivel 2). Si el equipo se encuentra en garantía se continua con la **actividad 5 de éste numeral (Atender caso Nivel 4).**		
3	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	**Reparar fallas que impliquen traslado de equipos** Se realiza cuando la solución a la falla no es inmediata y demanda un proceso riguroso de pruebas técnicas que requieren un tiempo considerable y se deben realizar en un lugar determinado para tal fin. Solicita autorización del funcionario que tiene a su cargo el equipo y del delegado de inventarios de la dependencia correspondiente, para realizar el traslado. Si es un equipo de cómputo se debe salvaguardar la información que en él reposa. Si la solución implica riesgo de pérdida de la información, realiza un backup, antes de efectuar cualquier intervención, en coordinación con el usuario funcional del equipo. Una vez corregida la anomalía del equipo de cómputo de ser necesario, se debe configurar con el		**Punto de control:** Con el número de caso registra y documenta las acciones ejecutadas, a través del Sistema de Mesa de Servicios, así como vía Comunicado oficial.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		usuario a cargo del mismo y restablecer el backup realizado. Posteriormente, trasladarlo al puesto de trabajo del funcionario que lo tiene a su cargo. Realiza las pruebas necesarias para determinar un correcto funcionamiento. En los casos que se dé una solución satisfactoria a la solicitud se debe continuar con la **actividad 10 de éste numeral. (Documentar la solución)** Si la falla es por Hardware que implica cambio o sustitución de partes para la puesta en funcionamiento. Ejecute la **Actividad 4.**		
4	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	**Fallas de hardware que implican sustitución de partes** Verifica si el periférico, parte o equipo de cómputo que requiere cambio, se encuentra en garantía o tiene contrato vigente de mantenimiento correctivo. Si es así, se escalará el caso, debidamente documentado, al Proveedor del equipo o Servicio y se informará a la Subdirección de Recursos Materiales sobre el estado de inactividad del equipo por garantía o cambio de parte para reclasificación	Comunicación Oficial	**Punto de control:** Con el número de caso registra y documenta las acciones ejecutadas, a través del Sistema de Mesa de Servicios, así como vía Comunicado oficial. Director de TIC y/o Subdirector de Recursos Tecnológicos revisaran la pertinencia de la solicitud y la solución y

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		de cuentas. Ejecuta la **Actividad 5 de éste numeral (atender caso Nivel 4).** Si no existe garantía o Contrato de Mantenimiento vigente, ejecutar **actividad 7 de éste numeral**.		aprobaran la misma para su trámite.
5	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	**Atender caso Nivel 4** Según el trámite de requerimiento por garantía, solicita al Proveedor o Contratista realizar el diagnostico correspondiente y cambio de partes que se requiera (Hardware), ajustes, correcciones o modificaciones (Software) y puesta en funcionamiento para la reparación de la falla, de acuerdo a las condiciones estipuladas en el Contrato de Compra o Prestación del Servicio de Mantenimiento y dentro de los plazos establecidos para tal fin. Realizan pruebas de funcionamiento y entrega a satisfacción al Profesional Especializado, Profesional Universitario o Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos, con la debida documentación de la labor realizada. Ejecuta **Actividad 6 de este numeral.**	Comunicado oficial o a través del sistema de solicitud de garantías o servicio de Proveedores que tenga dispuesta la entidad. Documento del Proveedor o Contratista	**Punto de control:** Se deben realizar las actividades de requerimiento de garantías y mantenimientos de conformidad con los procedimientos vigentes del Proceso Gestión Administrativa y Financiera para tal fin.
6	Profesional Especializado, Profesional	**Recibir del Proveedor o Contratista de equipos garantías o servicios de**		**Punto de control:** Con el **n**úmero de caso registra y

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	**mantenimiento.** Recibe del Proveedor o Contratista, el equipo ya reparado para ser entregado al funcionario que lo tiene a cargo. Para equipos de cómputo o periféricos, corregida la anomalía, de ser necesario se debe configurar con el usuario a cargo del mismo y restablecer el backup realizado. Posteriormente trasladarlo al puesto de trabajo del funcionario que lo tiene a su cargo. Realiza las pruebas necesarias para determinar un correcto funcionamiento. En los casos que SI se dé una solución satisfactoria a la solicitud se debe continuar con la **actividad 10 de éste numeral. (Documentar la solución)** e informar a la Subdirección de Recursos Materiales el ingreso del equipo para activarlo en el inventario y reclasificación de cuentas En los casos que NO se dé una solución satisfactoria a la solicitud **se debe escalar nuevamente a Nivel 4. Actividad 5 de éste numeral.**		documenta las acciones ejecutadas, a través de la Mesa de Servicios.
7	Profesional Especializado, Profesional	**Solicitud y cambio de partes (repuestos) para equipos informáticos.**		**Punto de control:** Verificar el

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	Determina con precisión la causa de la falla, revisa el Sistema de Información de Control de Elementos Informáticos SICEINFO por placa. Si no es posible repararlo, emitir concepto técnico para solicitar dar de baja el equipo de acuerdo al procedimiento establecido, Si es posible repararlo, toma el número de parte o serial del repuesto directamente del equipo o manual para realizar la solicitud de la misma. Realiza el trámite correspondiente para solicitar repuestos, de acuerdo a los procedimientos establecidos en la entidad para tal fin. Si la entidad no cuenta con los repuestos disponibles se informa a la Subdirección de Recursos Materiales para la inactivación del equipo en el inventario general de la entidad y reclasificación de cuentas. Así mismo se adquirirán siguiendo el procedimiento establecido en el proceso Gestión Administrativa y Financiera. Una vez recibidos, realiza el cambio de partes necesarios para corregir la falla y dejar en perfecto funcionamiento el equipo.	Sistema de Mesa de Servicios con el número de caso.	Sistema de Información de Control de Elementos Informáticos SICEINFO por placa donde se haya registrado el cambio de parte.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Realiza las pruebas necesarias para determinar un correcto funcionamiento. Hace entrega del equipo al funcionario que lo tiene a cargo. En los casos que SI se dé una solución satisfactoria a la solicitud se debe continuar con **la actividad 10 de éste numeral. (Documentar la solución).**		
8	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	**Atender caso Nivel 2** Verifica falla y/o requerimiento del usuario, dependiendo de la magnitud del problema proyecta la solución y determina qué tipo de intervención se requiere. Realiza un diagnóstico de la causa que originó la solicitud. Subsana la falla de acuerdo con los tiempos de respuesta asignados. Si la falla es corregida realiza las pruebas necesarias para determinar un correcto funcionamiento. En caso de requerir apoyo para la solución definitiva del caso deberá escalarlo al nivel correspondiente: **Nivel 1 (actividad 2 de éste numeral), Nivel 3 (actividad 9 de éste numeral).**	Comunicado Oficial Sistema de Mesa de Servicios por número de caso	**Punto de control:** Verificar el cambio de nivel en el Sistema de Mesa de Servicios.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		En los casos que se dé una solución satisfactoria a la solicitud se debe continuar con la **actividad 10 de éste numeral. (Documentar la solución).** Si las pruebas realizadas no son satisfactorias y se diagnostica que es necesaria una reparación mayor que implica intervención del especialista o del fabricante o Proveedor, escala el caso al **Nivel 3** (**actividad 9 de éste numeral)** o al **Nivel 4 (actividad 5 de éste numeral)**, según corresponda para brindar la solución requerida.		
9	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	**Atender caso Nivel 3** Verifica falla y/o requerimiento del usuario, dependiendo de la magnitud del problema proyecta la solución y determina qué tipo de Intervención se requiere. Realiza un diagnóstico de las causas que originaron la solicitud. Subsana la falla de acuerdo con los tiempos de respuesta asignados. Si la falla es corregida realiza las pruebas necesarias para determinar un correcto funcionamiento. En caso de requerir apoyo	Comunicado Oficial Sistema de Mesa de Servicios por número de caso	**Punto de control:** Verificar el cambio de nivel en el Sistema de Mesa de Servicios.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		para la solución definitiva del caso deberá escalarlo al nivel correspondiente: **Nivel 1 (actividad 2 de éste numeral), Nivel 2 (actividad 8 de éste numeral).** En los casos que se dé una solución satisfactoria a la solicitud **se debe continuar con la actividad 10 de éste numeral. (Documentar la solución)** Si las pruebas realizadas no son satisfactorias y se diagnostica que es necesaria una reparación mayor que implica intervención del fabricante o Proveedor del Servicio o aplicativo informático, escala el caso al **Nivel 4 (actividad 5 de éste numeral)**.		
10	Profesional Especializado, Profesional Universitario, Técnico de la Dirección TIC – encargado del Soporte Técnico a equipos Informáticos	**Documentar la solución** Documenta los pasos que realizó para la solución a través del Sistema de Mesa de Servicios, con el objetivo de alimentar la base de conocimientos y Sistema de Información de Control de Elementos Informáticos, registrando los cambios y/o ajustes realizados. El caso deberá actualizarse como **"Solucionado".** Cuando se haya solicitado inactivación de un equipo en el inventario general de	Sistema de Mesa de Servicios por número de caso Sistema de Información de Control de Elementos Informáticos SICEINFO por número de placa	**Punto de control**: Verificar el cambio de estado del caso a "*Solucionado*" en el Sistema de Mesa de Servicios. Verifica el registro de los cambios, reparaciones y/o ajustes realizados en el Sistema de Información de Control de Elementos Informáticos SICEINFO

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		la entidad se solicitará la activación del mismo en el inventario.		

6. ANEXOS

ANEXO 1. Formato Registro de Soporte

CONTRALORÍA DE BOGOTÁ, D.C.	Formato Registro de Soporte	Código formato: PGTI-04-01 Versión: 1.0 Código documento: PGTI-04 Versión 1.0 Página x de y

BITACORA DE CASOS													
Fecha de Solicitud	Hora de Solicitud	Tipo de solicitud	No de servicio	Dependencia / Entidad que solicita el servicio	Funcionario que solicita servicio Tipo de Solicitud	Detalle de solicitud	Categorización del servicio	Profesional asignado para atención de servicio	Escalar servicio	Profesional asignado para atención (escala)	Descripción de la solución	Fecha de la solución	Estado

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCION DEL CAMPO
Fecha de Solicitud	Día, mes, año de la solicitud.
Hora de Solicitud	Hora de Solicitud.
Tipo de solicitud	Incidente, cambio y/o requerimiento
No de servicio	Número asignado por la Dirección de Tecnologías de la Información.
Dependencia / Entidad que	Dependencia o entidad que solicita el servicio.

solicita el servicio	
Funcionario que solicita servicio	Nombres y apellidos del funcionario que solicita el servicio.
Detalle de solicitud	Describa en detalle la solicitud.
Categorización del servicio	Recursos Audiovisuales, Servicios Gestión Documental y/o Soporte Técnico.
Profesional asignado para atención de servicio	Nombres y apellidos del profesional que fue asignado al caso.
Escalar servicio	Nivel 1, 2 o 3
Profesional asignado para atención (escala)	Nombres y apellidos del profesional que fue escalado el caso.
Descripción de la solución	Describa la solución.
Fecha de la solución	Día, mes, año de la solución.
Estado	Asignado, cerrado, solucionado

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	R.R. No. 007 16 Febrero 2018	Ajuste a la normatividad. Se Modifica el numeral 5.1 Soporte a Sistemas de Información a Procedimiento para las siguientes actividades: Se agrupan las actividades 4 y 5, 6 y 7. Se eliminan las actividades de la 9 a la 15. Se crea el numeral 5.2 Solicitud Capacitaciones Sistemas de información Cambia el numeral 5.2 a numeral 5.3 Soporte a Equipos Informáticos. Se adiciona actividad No 1 Se eliminan actividades 2, 3,13. PGTI-04-01 Formato Pruebas de Sistemas de Información se traslada a PGTI-09 Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información con código PGTI-09-04. PGTI-04-02 Formato Control de Cambios Software se traslada a PGTI-09 Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información con código PGTI-09-06 y cambia de nombre a Formato Registro de Aplicación y Sistema de Información. PGTI-04-03 Formato Pruebas de Sistemas de Información cambia a código PGTI-04-01.

		PGTI-04-04 Formato de solicitud para desarrollo de nuevas funcionalidades se traslada a PGTI-09 Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, con código PGTI-09-02. Cambia en registro Anexo 1 Formato Hoja de Vida de Equipos de Cómputo y de Comunicaciones del PGTI-05-01 del Procedimiento Gestión de Recursos y Servicios Tecnológicos por registro o actualización en Sistema de Información de Control de Elementos Informáticos SICEINFO por número de placa.
2.0	R.R. No. 047 28 Diciembre 2018	

Aprobación		Revisión Técnica	
Firma:		Firma:	
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 Diciembre 28 de 2018**	

1. OBJETIVO:

Determinar las actividades para la administración y gestión de los Sistemas de Información, aplicativos, licencias y equipos informáticos de la Contraloría de Bogotá D.C.

2. ALCANCE:

El procedimiento inicia con la recepción y verificación de la legalidad del aplicativo, sistema de información o licencia de software de propósito general y equipos tecnológicos en medio digital (DVD, CD o WEB, o en servidor de la entidad) y termina con la calificación del servicio por parte del usuario.

3. BASE LEGAL:

NORMA	FECHA	DESCRIPCIÓN
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 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.
Ley 1915	12-jul-2018	Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

NORMA	FECHA	DESCRIPCIÓN
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único 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.
Lineamientos MINTIC LI.ST.08,	26-May-2015	Implementación del procedimiento para atender los requerimientos de soporte de primer, segundo y tercer nivel, para sus servicios de TI, a través de una Mesa de

NORMA	FECHA	DESCRIPCIÓN
LI.ST.09		Servicio.
Guía No 3	25-abr-2016	Procedimientos de Seguridad de la Información, MINTIC.

4. DEFINICIONES:

Activos de Información[1] : Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Características Técnicas: Es la descripción de los componentes de una herramienta tecnológica como pueden ser modelo, velocidad, capacidad de almacenamiento, entre otras.

Caso: Número consecutivo asignado al Requerimiento o Incidente.

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

Fecha de Adquisición: Fecha en la que se compró la herramienta tecnológica.

Fecha de Caducidad: Fecha en la cual la licencia deja de funcionar por vencimiento ante el proveedor

Hardware - HW: es la parte física de cualquier dispositivo electrónico o informático, es usual que sea utilizado en una forma más amplia, generalmente para describir componentes físicos de una tecnología, incluyendo equipos de cómputo, periféricos, redes, cableado y cualquier otro elemento físico involucrado.

Herramientas Ofimáticas: Programas que facilitan las labores propias de la oficina. Ejemplo: Procesadores de palabra, hojas electrónicas, mensajería y colaboración, diagramación, entre otros.

Infraestructura Tecnológica: Es el conjunto de hardware y software sobre el cual funcionan los diferentes servicios que presta la Contraloría de Bogotá: equipos de cómputo, equipos de comunicaciones, sistemas de información, equipos de fotocopiado, equipos de digitalización, equipos de telefonía.

[1] Resolución 305 de 2008, Comisión Distrital de Sistemas – Secretaría General de la Alcaldía Mayor

Inventarios: Es la relación ordenada, completa y detallada de toda clase de bienes que integran el patrimonio de la entidad. El inventario permite verificar, clasificar, analizar, valorar y controlar los bienes, lo cual posibilita efectuar un control razonable de las existencias reales, para evitar errores, pérdidas, deterioro y desperdicio de elementos.

Licencia: Un acuerdo legal en el que una parte otorga a otra ciertos derechos y privilegios. En el campo de la informática, un editor de software generalmente otorgará un derecho no exclusivo (licencia) a un usuario para que utilice una copia de su programa informático, y prohibirá la realización de otras copias y la distribución de dicho programa a otro usuario. Las licencias dependiendo de la herramienta tienen diferentes niveles y términos.

Mantenimiento de Equipos: Conjunto de tareas tendientes a mantener en perfecto funcionamiento las estaciones de trabajo e impresoras de la Entidad.

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.

Nivel de Satisfacción: Calificación dada por el usuario al servicio recibido por soporte técnico o por capacitación recibida. El rango es de 1 a 5, donde uno (1) corresponde a la calificación más baja y cinco (5) a la calificación más alta.

Obsolescencia Tecnológica: Se considera obsoleto un equipo cuando en el mercado tecnológico legal, no existen partes o repuestos de soporte por tener demasiado tiempo de haber sido adquirido o porque el mismo fabricante ha dejado de producir el producto del modelo específico.

Plataforma Tecnológica: Es el conjunto de hardware y software sobre el cual funcionan los diferentes servicios tecnológicos y operativos que presta la Contraloría de Bogotá: equipos de cómputo, equipos de comunicaciones, sistemas de información, equipos de fotocopiado, equipos de digitalización, equipos de telefonía, impresoras, switches, routers, firewall, escáneres, cableado estructurado, cpu`s, servidores, software informático, equipos de comunicación, internet, red Lan, etc.

Placa: Etiqueta con un Código de barras y numero consecutivo para marcar todos los activos fijos de propiedad de la entidad, y que sirve de guía para realizar los inventarios. REPUESTO: Es una pieza o parte que se utiliza para reemplazar las originales en equipos que debido a su uso diario han sufrido deterioro o un daño.

Requerimiento Técnico: Aviso o manifestación de una situación problema a nivel técnico

Serie - S: Una de las características específicas (número de serie, marca, modelo), que identifican individualmente cada uno de los elementos o herramientas tecnológicas.

Software - SW se refiere al equipamiento lógico de un computador, está compuesto por todos los aplicativos y licencias que están instalados en cada uno de los equipos de cómputo del ente departamental.

Solicitud: Son peticiones de atención a daños o fallos en la infraestructura de software y/o hardware que pueden ser de soporte, de mantenimiento, de nuevos desarrollos o de capacitación.

Soporte Técnico: Es un rango de servicios por medio del cual se proporciona asistencia a los usuarios que tengan algún problema al utilizar un producto o servicio, bien sea, relacionado con hardware, software o cualquier otro equipo o dispositivo informático.

Traslado de bienes devolutivos entre funcionarios: Inicia con la solicitud en el aplicativo de radicación por la dependencia que requiere el elemento a la Subdirección de Recursos Materiales y termina con la actualización del inventario individual y por dependencia en la base de datos del área de inventarios y el archivo del cuadro de traspaso de elementos entre funcionarios.

Usuario: Funcionario de la Contraloría de Bogotá o del sujeto de control fiscal que solicita asistencia técnica sobre los sistemas de información.

5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Administración de Sistemas de Información o Aplicativos.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1.	Profesional Especializado, Profesional Universitario, Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	**Recibir aplicativo o sistema de información.** Recibe el aplicativo o sistema de información o licencia de software de propósito general en el medio digital (DVD, CD o web, o en servidor de la entidad) y verifica su legalidad y conformidad de acuerdo con las especificaciones técnicas establecidas en el contrato, orden de compra, prestación del servicio o convenio.	Comunicación Oficial o Sistema de Mesa de Servicios	**Punto de control:** Los autorizados para realizar la instalación y desinstalación de sistemas de información, aplicativos es la Dirección de Tecnologías de la Información y las Comunicaciones. Verifica la

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Solicita vía comunicación oficial, el nombre de los usuarios a los cuales se les asignó el acceso al aplicativo, sistemas de información o licencia de software de propósito general, así como los perfiles de acceso definidos por el Administrador funcional según las parametrizaciones y permisos establecidos en cada caso.		legalidad de la licencia, las especificaciones técnicas pactadas y definidas en las obligaciones contractuales teniendo en cuenta los aspectos relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. El Director de TIC y/o Subdirectores deberán verificar el cumplimiento de estas obligaciones en caso de ser supervisores según los procedimientos del Proceso Gestión Administrativa y Financiera para tal fin, en caso contrario si encuentra incumplimientos comunicarlo a los supervisores delegados.
2	Profesional	**Actualizar hoja de vida**	Formato	**Puntos de**

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Especializado, Profesional Universitario, Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	**del aplicativo, sistema de información.** Actualiza el Formato Registro de Aplicación y Sistema de Información, sí es una nueva versión de un sistema de información, software, aplicativo o herramienta informática, diligenciando los campos requeridos. Si es adquisición nueva crea el Formato Registro de Aplicación y Sistema de Información correspondiente. Registra las características y términos del licenciamiento adquirido.	Registro de Aplicación y Sistema de Información PGTI-09-06 del Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	**control:** Verifique el registro de los datos de creación y registro del sistema de información o aplicativo y las características de licenciamiento adquiridas.
3	Profesional Especializado, Profesional Universitario, Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	**Instalar sistema de información o aplicativo** Realiza la instalación del sistema, software o aplicativo en los equipos o usuarios que se le informen a través del Sistema de Mesa de Servicios o comunicación oficial y realiza las respectivas pruebas de funcionamiento registrándolo en el Formato de Pruebas de Sistemas de Información.	Formato Pruebas de Sistemas de Información PGTI-09-04 del Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. Formato Registro de Aplicación y Sistema de Información PGTI-09-06 del	**Puntos de control:** La finalización del proceso de instalación, debe otorgar información del recibo a satisfacción de los usuarios funcionales a través del cumplido en el Sistema de Mesa de Servicios de servicio de soporte o solicitudes.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Actualiza el Formato Registro de Aplicación y Sistema de Información con los usuarios a los cuales se les instaló el sistema de información, software o aplicativos.	Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	

5.2 Administración de licencias de software

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de TIC, Subdirector de Gestión de la Información y Profesional, Técnico Asignado	**Ingreso de Licencias:** Recibe las licencias y determina su distribución; asigna a un funcionario de la Dirección de TIC para que actualice la herramienta respectiva con la información básica requerida para su administración. Registra en el Formato Registro de Aplicación y Sistema de Información, los datos correspondientes al licenciamiento.	Inventario interno de Licencias. Formato Registro de Aplicación y Sistema de Información PGTI-09-06 del Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	**Punto de control** Verifica la legalidad de la licencia, las especificaciones técnicas pactadas y definidas en las obligaciones contractuales teniendo en cuenta los aspectos relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. **Observación**: El archivo *Inventario de licencias* es de

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				uso interno de la Dirección de TIC, para el control técnico de la Infraestructura Tecnológica.
2	Contralor Auxiliar Directores Subdirectores Jefes De Oficina	Envían los requerimientos sobre necesidades de Licencias de software para las diferentes áreas de la entidad a través de la Mesa de Servicios que tenga dispuesto la entidad, siguiendo el procedimiento Registro y Atención de Requerimientos de Soporte a los Sistemas de Información y Equipos Informáticos - PGTI-04.	Registro en el Sistema de Mesa de Servicios.	
3	Subdirector de Gestión de Información	Verifica la disponibilidad y el estado de las licencias: fechas de caducidad de las licencias, cantidad de licencias usadas y cantidad de licencias disponibles en el inventario interno de licencias. En caso de existir disponibilidad aprueba la solicitud y asigna al profesional de la Dirección de TIC, la instalación de las respectivas Licencias en	Formato Registro de Aplicación y Sistema de Información PGTI-09-06 del Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. Sistema de Mesa de Servicios por	**Observación:** Se actualiza el inventario interno de licencias de la Dirección de TIC.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		las áreas solicitadas. Actualiza el Formato Registro de Aplicación y Sistema de Información. Si no hay licencias disponibles, se evalúa la pertinencia de su adquisición; si es pertinente se activa el trámite en el procedimiento de adquisición correspondiente del Proceso de Gestión Administrativa y Financiera; luego de adquirida volverá a ejecutar la **actividad 1 y** luego la **actividad 4** de este numeral. Si no es pertinente, se rechaza la solicitud informando al usuario a través del Sistema de Mesa de Servicios, con las debidas justificaciones.	número de caso.	
4	Profesional Especializado, Profesional Universitario o Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	Confronta con el inventario general de la Entidad, el listado de Licencias, si hay inconsistencias comunica a la dependencia correspondiente del Proceso Gestión Administrativa y Financiera, para su corrección o	Inventario Interno de Licencias Formato Registro de Aplicación y Sistema de Información PGTI-09-06 del Procedimiento	**Puntos de control:** Verifique el registro de los datos de creación y registro del sistema de información o aplicativo y las características de licenciamiento

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		actualización. Verifica el registro de la licencia en el portal del fabricante o proveedor y guarda pantallazo de verificación. Si la licencia es nueva crea Formato Registro de Aplicación y Sistema de Información. Realiza la instalación de las respectivas Licencias en las áreas solicitadas e indica al usuario final las condiciones y políticas de uso del licenciamiento.	para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	adquiridas.
5	Profesional Especializado, Profesional Universitario o Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	**Monitoreo del estado de licencias.** Analiza el estado de las licencias: fecha de caducidad y/o nivel de obsolescencia. En caso de presentarse caducidad u obsolescencia, emite concepto técnico para dar de baja. Actualiza el estado de la licencia en Formato Registro de Aplicación y Sistema de Información e informa a Director y Subdirectores de TIC para el trámite correspondiente.	Formato Registro de Aplicación y Sistema de Información PGTI-09-06 del Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. Anexo No 1 Equipos Tecnológicos para dar de Baja PGTI-05-01	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
6	Director de TIC, Subdirector de Gestión de la Información, Subdirector de Recursos Tecnológicos	**Aprobar concepto técnico.** Revisa el concepto emitido por el profesional de TIC. Si el concepto es aprobado, informa a la Subdirección administrativa y Financiera para que se realicen las actividades que permitan dar de baja las licencias reportadas.	Comunicación Oficial	**Puntos de control:** Tramitar según lo indicado en el PGAF-10-Procedimiento para el manejo y control de almacén e inventarios del Proceso Gestión Administrativa y Financiera.
7	Profesional Especializado, Profesional Universitario o Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones.	Actualiza el inventario interno de licencias de la Dirección de TIC.	Inventario interno de Licencias actualizado.	

5.3. Administración de Nuevos Elementos Informáticos

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de TIC, Subdirector de Recursos Tecnológicos, Subdirector de Gestión de la información	**Recibir elementos informáticos** Recibe los elementos informáticos. Determina su distribución y solicita a la	Comunicación Oficial	**Punto de control:** Inicia con PGAF-10 procedimiento para el manejo y control de almacén e

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Subdirección de Recursos materiales el traspaso de elemento, activa procedimiento PGAF-10 procedimiento para el manejo y control de almacén e inventarios – Traslado de bienes devolutivos entre funcionarios. Informa a funcionario que recibirá el elemento informático a través de comunicación oficial Asigna a un funcionario de la Dirección de TIC para que haga entrega del equipo.		inventarios, en el recibo de los elementos se verifica legalidad del equipo informático de conformidad con las especificaciones técnicas pactadas y definidas en las obligaciones contractuales teniendo en cuenta los aspectos relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. Deben verificar el cumplimiento de las obligaciones contractuales en caso de ser supervisores según los procedimientos del Proceso Gestión Administrativa y Financiera para tal fin, en caso contrario si encuentra incumplimientos comunicarlo a los supervisores

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				delegados.
2	Profesional Especializado, Profesional Universitario o Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	**Realizar la instalación** Alista el elemento tecnológico (configura e instala software necesario) con los datos del usuario a quien se le entregará el equipo. Para el caso de servidores, equipos de comunicación y otros tipos de equipos tecnológicos que requieren una instalación y configuración técnica especializada, se almacenan en los lugares pertinentes a su instalación y se disponen para su instalación de acuerdo con las obligaciones pactadas en los contratos de adquisición de los mismos. Registra elemento informático en el Sistema de Información de Control de Elementos Informáticos SICEINFO Entrega el elemento a usuario correspondiente, diligencia formato Formato Recibo a Satisfacción Elemento Informático.	Registro en Sistema de Información de Control de Elementos Informáticos SICEINFO Anexo 2. Formato Recibo a Satisfacción Elemento Informático PGTI-05-02.	**Punto de control:** Verifica datos de control de placa, serie y demás pertinentes frente al elemento físico recibido.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
3	Auxiliar Administrativo Secretario Técnico Operativo Profesional Universitario y/o Especializado Gerente Subdirector Técnico, Financiero o Administrativo Jefe Oficina Director Técnico Asesor Contralor Auxiliar Contralor (Funcionarios Contraloría de Bogotá) o Contratista	**Recibido a satisfacción del equipo informático** Verifica el estado del equipo informático de acuerdo a los registros y/o requerimientos. Si considera que está conforme a la solicitud, recibe el equipo firmando el Formato de Recibo a Satisfacción. En caso contrario, lo devuelve a la Dirección de TIC, indicando la inconformidad.	Anexo 2. Formato Recibo a Satisfacción Elemento Informático PGTI-05-02.	

5.4. Traslado de Elementos Informáticos de Usuario Final

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor, Contralor Auxiliar, Director, Subdirector, Jefe de Oficina.	**Registrar solicitud** Ingresa al Sistema de Mesa de Servicios y presenta la solicitud, siguiendo el procedimiento Registro de Atención de Requerimientos de Soporte a Sistemas de Información y Equipos Informáticos - PGTI-04. Garantiza que la información sensible,	Registro Sistema de Mesa de Servicios.	**Punto de control** Inicia con procedimiento PGAF-10 Procedimiento para el manejo y control de almacén e inventarios numeral Traslados. Es

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		reservada, clasificada del usuario contenida en el elemento informático a trasladar fue salvaguardada adecuadamente. La solicitud debe contener ubicación inicial, ubicación final y características del equipo.		responsabilidad del funcionario que utiliza el elemento informático a trasladar de realizar copia de la información y salvaguardarla adecuadamente.
2	Profesional Especializado, Profesional Universitario o Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	**Atender solicitud** Realiza atención de la solicitud. Actualiza la información la ubicación y usuario del elemento informático en el Sistema de Información de Control de Elementos Informáticos SICEINFO. Realiza borrado de la información de los usuarios contenida en los elementos informáticos antes de dar nueva disposición al elemento.	Sistema de Mesa de Servicios por número de caso. Sistema de Información de Control de Elementos Informáticos SICEINFO por número de placa	**Punto de control:** Solicita el formato de traslado de elementos - PGAF-10-08 diligenciado y firmado por las partes, para la atención del requerimiento.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
3	Profesional Especializado, Profesional Universitario o Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	**Solución de la solicitud** Actualiza el estado del caso a solucionado en el Sistema de Mesa de Servicio e informa al usuario.	Sistema de Mesa de Servicios por número de caso.	

5.5. Mantenimientos Preventivos de Elementos Informáticos y Comunicaciones.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de TIC, Subdirector de Recursos Tecnológicos	**Programar ejecución de mantenimientos preventivos a Infraestructura Tecnológica Instalada** Elabora Cronograma de Mantenimientos Preventivos para los Equipos Tecnológicos que cuenten con él, de acuerdo con las obligaciones pactadas en los contratos y convenios suscritos. De acuerdo con la programación de	Cronograma Anual de Mantenimientos Preventivos Comunicación Oficial	**Punto de Control:** Verifica que las condiciones de los mantenimientos preventivos considerados son coherentes con los registros de la Hoja de Vida de Equipos de Cómputo y Comunicaciones en el Sistema de Información de Control de Elementos Informáticos.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		mantenimientos preventivos comunique a los usuarios de los equipos la realización del mantenimiento a través de una comunicación oficial.		
2	Profesional Especializado, Profesional Universitario o Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	**Ejecución de mantenimientos preventivos** Ejecuta o acompaña a los contratistas o proveedores en la ejecución del mantenimiento. Actualiza información del mantenimiento del elemento informático en el Sistema de Información de Control de Elementos Informáticos SICEINFO. Diligencia el formato Recibo a Satisfacción Elemento Informático	Sistema de Información de Control de Elementos Informáticos SICEINFO por número de placa Anexo 2. Formato Recibo a Satisfacción Elemento Informático PGTI-05-02.	**Punto de Control:** Verifica que las condiciones de los mantenimientos preventivos se efectúen de conformidad a lo pactado, si se presentan no conformidades informe al Director de TIC y Subdirector de Recursos Tecnológicos Si en ejecución del mantenimiento preventivo se encuentran anomalías, active las actividades

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				que apliquen del numeral 5.3. Soporte a Equipos Informáticos del PGTI-04 Procedimiento registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos.
3	Auxiliar Administrativo Secretario Técnico Operativo Profesional Universitario y/o Especializado Gerente Subdirector Técnico, Financiero o Administrativo Jefe Oficina Director Técnico Asesor Contralor Auxiliar Contralor (Funcionarios Contraloría de Bogotá) o Contratista	**Recibir el mantenimiento preventivo del equipo informático** Verifica el estado del equipo informático. Firma el Formato de Recibo a Satisfacción, Si considera que está conforme con el mantenimiento realizado, en caso contrario, lo devuelve a la Dirección de TIC, indicando la inconformidad.		

5.6. Baja de Elementos Informáticos y Comunicaciones

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Almacenista General	Solicita concepto técnico a la Subdirección de Recursos Tecnológicos de los elementos informáticos a postular en el comité técnico de bajas. Activa procedimiento Registro y Atención de Requerimientos de Soporte a los Sistemas de Información y Equipos Informáticos - PGTI-04.	Registro Sistema de Mesa de Servicios o Comunicación oficial	**Punto de control:** La actividad inicia con el PGAF-10 procedimiento para el manejo y control de almacén e inventarios (Baja de bienes (Devolutivos y de consumo controlado)
2	Subdirector de Recursos Tecnológicos, Profesional Especializado, Profesional Universitario o Técnico de la Dirección de Tecnologías de la Información y las Comunicaciones	Revisa el estado del equipo, sus partes y licenciamiento e identifica sí el equipo presenta daño total u obsolescencia tecnológica. En caso que el equipo informático sea para dar de baja: • Realiza borrado seguro de la información de usuarios, sistemas operativos, software y aplicativos con licencia, utilitarios, sistemas de información de la Entidad. • Diligencia Formato Equipo Tecnológico para dar de Baja y actualiza información del elemento informático en el Sistema de Información de Control de Elementos Informáticos SICEINFO. • Informa a encargado TIC de la administración de	Anexo 1. Formato Equipo Tecnológico para dar de Baja PGTI-05-01 Sistema de Información de Control de Elementos Informáticos SICEINFO por número de placa Comunicación oficial Sistema de Mesa de Servicios por número de caso.	

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		licencias de Software a través de un comunicado oficial, para que actualice el inventario interno de licencias. Genera respuesta a la solicitud informando concepto técnico mediante una comunicación oficial, en caso que se determine que el elemento informático se da de baja se adjunta Formato Equipo Tecnológico para dar de Baja. Si la solicitud se realizó por el Sistema de Mesa de Servicio, actualiza el estado del caso a solucionado.		

5.7. Gestión de Medios Removibles

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor Auxiliar, Director, Jefe de Oficina.	Solicita activación de puerto USB justificando la necesidad a través del Sistema Mesa de Servicios e indicando usuario, identificación y ubicación de la estación PC o portátil. Activa procedimiento de Registro y Atención de Requerimientos de Soporte a los Sistemas de Información y Equipos Informáticos –	Registro Sistema de Mesa de Servicios	**Observación** Existirá mínimo un equipo por dependencia que tenga habilitados los puertos USB.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		PGTI-04.		
2	Subdirector de Recursos Tecnológicos, Profesional Especializado, Profesional Universitario	Aprueba o deniega la solicitud. En caso de aprobación asigna la solicitud a funcionario TIC para realizar la gestión de habilitación de los puertos USB de la estación de trabajo del usuario solicitante	Sistema de Mesa de Servicios por número de caso.	
3	Profesional Especializado, Profesional Universitario o Técnico de la Dirección TIC	Atender solicitud Realiza atención de la solicitud y actualiza su estado e informa al usuario en el Sistema de Mesa de Servicios.		
4	Profesional de la Subdirección de Recursos Tecnológicos - Dirección de TIC	Solución de la solicitud Actualiza el estado del caso a solucionado en el Sistema de Mesa de Servicio e informa al usuario.	Sistema de Mesa de Servicios por número de caso.	

6. ANEXOS

ANEXO 1. Formato Equipo Tecnológico para dar de Baja

CONTRALORÍA DE BOGOTÁ, D.C.	Equipo Tecnológico para dar de Baja	Código formato: PGTI-05-01 Versión: 1.0 Código documento: PGTI-05 Versión 1.0 Página 1de 1

REVISION DEL EQUIPO	
Fecha de la revisión	
Dependencia y/o Ubicación del equipo	
Nombre del responsable actual	

Profesional de TIC que revisa	

Información básica del activo fijo							
Tipo de Equipo		_____ (Computador, portátil, impresora, escaner, mouse, switch, router, etc)				**Fecha de dar de baja**	
	Marca		**Modelo**			**Placa**	
	Descripción del estado en que se encuentra el equipo						
	Faltan partes:	***SI***		***NO***			
	Detalle las partes faltantes:						
1							
	Fecha de Adquisición		***Se considera Obsoleto?***		***SI***	***NO***	

Observaciones

Firma del profesional de TIC **Firma de quien recibe por recursos Materiales**

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Fecha de la revisión	Fecha en la cual se realiza la revisión
Dependencia	Ubicación del equipo
Nombre del responsable actual	Responsable del equipo
Profesional de TIC que revisa	Nombre del profesional de la Dirección de TIC que realiza la revisión
Tipo de Activo	Indique si es computador, portátil, escáner, impresora, SWITCH, firewall, servidor, etc.

Fecha de dar de baja	Indique la fecha en la cual se da de baja el equipo
Marca	Nombre de la marca o fabricante del equipo informático
Modelo	Número o referencia del equipo
Placa	Número de identificación del equipo en el inventario de la Contraloría de Bogotá
Descripción del estado en que se encuentra el equipo	Realice una descripción del estado del equipo por la cual se considera debe darse de baja
Faltan partes:	Según lo que observe diligencia SI cuando el equipo le hace falta alguno de sus componentes para funcionar o NO si está completo
Detalle de las partes faltantes:	En caso de que falten partes relacione en forma detallada las características de las partes
Fecha de Adquisición	Fecha en la cual se adquirió el equipo, corresponde a la fecha de ingreso a almacén
Se considera obsoleto	Marca SI en el caso de que el análisis determinó que la tecnología del equipo ya está fuera del mercado, o descontinuado por el fabricante. Marca NO si el análisis determinó que no es obsoleto
Observaciones	Cualquier información adicional que considere debe informarse
Firma del profesional de TIC	Firma del profesional que realizó la revisión y dio concepto técnico de baja de activo
Firma de quien recibe por Recursos Materiales	Firma del funcionario de Recursos Materiales que recibe el equipo para dar de baja del inventario de la entidad

ANEXO 2. Formato Recibo a Satisfacción Elemento Informático

CONTRALORÍA DE BOGOTÁ, D.C.	**Recibo a Satisfacción Elemento Informático**	Código formato: PGTI-05-02 Versión: 1.0 Código documento: PGTI-05 Versión 1.0 Página 1de 1

Bogotá D.C.,

Señores

DIRECCION DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Contraloría de Bogotá
Ciudad

Por medio del presente documento certifico que se me realizó la entrega de los equipos informáticos identificados con las siguientes placas de inventario:

No.	EQUIPO INFORMÁTICO	PLACA
1		
2		
3		
4		
6		

OBSERVACIONES

Cordialmente,

Quien recibe a Satisfacción:
Firma:
Nombre:
Cargo:

Quien entrega:
Firma:
Nombre:
Cargo:

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Equipo informático	Tipo del equipo informático que recibe, puede ser computador, portátil, escáner, impresora, etc.
Placa	Número de identificación del equipo informático en el inventario de la Contraloría de Bogotá
Observaciones	Cualquier información adicional que considere debe informar
Quien recibe a satisfacción	Firma del funcionario que recibe el equipo informático

Quien entrega	Firma del funcionario que hace entrega del equipo al funcionario

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	R. R. No.007 16 Febrero 2018	Ajuste a la normatividad. Numeral 5.3. Administración de Elementos informáticos cambia de nombre a 5.3. Administración de Nuevos Elementos Informáticos. Numeral 5.4. Instalación, Retiros o Cambios de Equipos de Usuario Final cambia de nombre a Traslado de Elementos Informáticos de Usuario Final. Elimina actividad No 4 de numeral 5.3. Administración de Elementos Informáticos. Elimina actividad No 2 del numeral 5.4. Instalación, Retiros o Cambios de Equipos de Usuario Final y se cambia redacción de las actividades 1,3,4. Cambia redacción de actividades 5.5. Mantenimientos Preventivos de Elementos Informáticos y Comunicaciones. Cambia en registro Anexo 1 Formato Hoja de Vida de Equipos de Cómputo y de Comunicaciones por registro o actualización en Sistema de Información de Control de Elementos Informáticos SICEINFO por número de placa. Cambia de nombre Anexo No 2 Formato Equipos Tecnológicos para dar de Baja por Formato Equipo Tecnológico para dar de Baja y cambia a ser anexo No 1. Cambia nombre de anexo No 3 Formato Recibo a Satisfacción por Formato Recibo a Satisfacción Elemento Informático. Elimina Anexo No 4 - Lista de Chequeo

		Mantenimiento Preventivo Equipos de Cómputo y Comunicaciones. Agrega procedimiento el numeral 5.6. Baja de Elementos Informáticos y Comunicaciones. Agrega procedimiento el numeral 5.7. Gestión de Medios Removibles.
2.0	R.R. 047 28 Diciembre 2018	

Aprobación		Revisión Técnica	
Firma:		Firma:	
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 Diciembre 28 de 2018**	

1. OBJETIVO:

Implementar actividades que permitan gestionar los riesgos inherentes para garantizar la seguridad de la plataforma tecnológica y servicios informáticos de la Contraloría de Bogotá D.C., para salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad.

2. ALCANCE:

El procedimiento inicia con la asignación de roles y responsabilidades para administración de estrategias y acciones entorno a la seguridad física y lógica aplicada a activos de información de la Contraloría de Bogotá D.C. y termina con el análisis de los informes y comunicación a la Dirección de TIC de los informes.

3. BASE LEGAL:

TIPO DE NORMA	FECHA	DESCRIPCIÓN
Ley 1273	5-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 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.
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la

TIPO DE NORMA	FECHA	DESCRIPCIÓN
		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 Reglamentario Unico 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.
CONPES 3701-2011	14 - jul - 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa Estrategia Nacional de Ciberseguridad y Ciberdefensa
CONPES 3854 - 2016	11-Abr-2016	Política Nacional de Seguridad Digital.
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.

TIPO DE NORMA	FECHA	DESCRIPCIÓN
Lineamientos MINTIC LI.ST.08, LI.ST.09, LI.ST.10	26-May-2015	Implementación del procedimiento para atender los requerimientos de soporte de primer, segundo y tercer nivel, para sus servicios de TI, a través de una Mesa de Servicio.
Guía No 3	25-abr-2016	Procedimientos de Seguridad de la Información, MINTIC.

4. DEFINICIONES:

Activo de Información: Es una pieza de información definible e identificable, almacenada en cualquier medio. Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Características de los activos de la información: Un activo de información puede tener las siguientes características, independiente del tipo de activo:

- El activo de información es reconocido como valioso
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o combinación de los mismos.
- Forma parte de la identidad de la entidad y sin la cual la Contraloría de Bogotá puede estar en algún nivel de riesgo.

Antivirus: Programas cuyo objetivo es detectar o eliminar virus informáticos.

Amenaza: Potencial violación de la seguridad.

Características técnicas: Es la descripción de los componentes de una herramienta tecnológica como pueden ser modelo, velocidad, capacidad de almacenamiento, entre otras.

Caso: Número consecutivo asignado al Requerimiento o Incidente.

Central de servicios de TI: Sistema por medio del cual se gestiona el portafolio de servicios de TI, asesoría en Proyectos de TI, desarrollo de Sistemas de Información, adquisiciones tecnológicas, soporte técnico, Administración de servicios de TI. (Abreviado CSTI).

Centro de datos: Espacio físico ubicado en el 7 piso de la entidad en el cual se encuentran los equipos servidores, equipos de comunicaciones que alojan los servicios de red como aplicativos, bases de datos, servicio de Internet, servicio de Directorio Activo y seguridad perimetral de la Contraloría de Bogotá.

Centros de cableado: Espacio físico ubicados en diferentes sedes y pisos de la entidad en el cual se encuentran los diferentes equipos de comunicaciones que permite la comunicación entre los diferentes sedes y pisos de la Contraloría de Bogotá.

CSIRT: (Computer Security Incident Response Team) Equipo de Respuesta a Incidentes de Seguridad cibernética, por su sigla en inglés.

Denegar: Responder negativamente a una petición o solicitud.

Hardware – HW: Es la parte física de cualquier dispositivo electrónico o informático, es usual que sea utilizado en una forma más amplia, generalmente para describir componentes físicos de una tecnología, incluyendo equipos de cómputo, periféricos, redes, cableado y cualquier otro elemento físico involucrado.

Herramientas Ofimáticas: Programas que facilitan las labores propias de la oficina. Ejemplo: Procesadores de palabra, hojas electrónicas, mensajería y colaboración, diagramación, entre otros.

Información: Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.

Inventarios: Es la relación ordenada, completa y detallada de toda clase de bienes que integran el patrimonio de la entidad. El inventario permite verificar, clasificar, analizar, valorar y controlar los bienes, lo cual posibilita efectuar un control razonable de las existencias reales, para evitar errores, pérdidas, deterioro y desperdicio de elementos.

Infraestructura tecnológica: Es el conjunto de hardware y software sobre el cual funcionan los diferentes servicios que presta la Contraloría de Bogotá: equipos de cómputo, equipos de comunicaciones, sistemas de información, equipos de fotocopiado, equipos de digitalización, equipos de telefonía.

Licencia: Un acuerdo legal en el que una parte otorga a otra ciertos derechos y privilegios. En el campo de la informática, un editor de software generalmente otorgará un derecho no exclusivo (licencia) a un usuario para que utilice una copia de su programa informático, y prohibirá la realización de otras copias y la distribución de dicho programa a otro usuario. Las licencias dependiendo de la herramienta tienen diferentes niveles y términos.

Obsolescencia tecnológica: Se considera obsoleto un equipo cuando en el mercado tecnológico legal, no existen partes o repuestos de soporte por tener demasiado tiempo

de haber sido adquirido o porque el mismo fabricante ha dejado de producir el producto del modelo específico.

Plataforma tecnológica: Es el conjunto de hardware y software sobre el cual funcionan los diferentes servicios tecnológicos y operativos que presta la Contraloría de Bogotá: equipos de cómputo, equipos de comunicaciones, sistemas de información, equipos de fotocopiado, equipos de digitalización, equipos de telefonía, impresoras, switches, routers, firewall, escáneres, cableado estructurado, cpu`s, servidores, software informático, equipos de comunicación, internet, red Lan, etc.

Requerimiento técnico: Aviso o manifestación de una situación problema a nivel técnico.

Software - SW: se refiere al equipamiento lógico de un computador, está compuesto por todos los aplicativos y licencias que están instalados en cada uno de los equipos de cómputo del ente departamental.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Roles: Conjunto de responsabilidades y actividades asignadas a una persona o grupo de personas para apoyar la adopción y aplicación del Marco de Referencia de Arquitectura Empresarial para la gestión de TI.

Seguridad perimetral informática (FIREWALL): Corresponde a hardware o software o la integración de ambos para la protección de perímetros lógicos y físicos, detección de tentativas de intrusión y/o disuasión de intrusos en la red de la Entidad.

WSUS: o Windows Server Update Services es una función dentro del catálogo disponible en Windows, permite la distribución de los parches y actualizaciones publicadas por Microsoft de forma centralizada para todos los PC, portátiles, servidores que tengan sistemas operativos Microsoft, de forma programada permitiendo una gestión correcta del ancho de banda disponible en la red de comunicaciones de la Entidad.

5. DESCRIPCIÓN DEL PROCEDIMIENTO:

5.1 Gestión de Acceso al Centro de Datos y Centros de Cableado

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de Tecnologías de la Información y las	Asigna a funcionarios roles de: • Administrador de Centro de Datos.		**Punto de Control:** Segregación de funciones de acuerdo a perfiles

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Comunicaciones, Subdirector de Recursos Tecnológicos	• Administrador de Centros de Cableado. Operador de Centro de datos y de centros de cableado	Comunicación oficial interna.	y competencias. Se debe realizar una descripción específica del alcance de cada uno de los roles
2	Director de Tecnologías de la Información y las Comunicaciones, Subdirector de Recursos Tecnológicos	Asigna permisos en dispositivos de control de acceso biométrico a centro de datos y los centros de cableado a los funcionarios con roles: • Administrador de Centro de Datos • Administrador de Centros de Cableado. • Operador de Centro de datos y de centros de cableado	Comunicación Oficial Interna. Anexo 1. Formato de Acceso Permanente al Centro de Datos y Centros de Cableado. PGTI-06-01	**Punto de Control:** Asignación de privilegios según las funciones. Monitoreo periódico a control de accesos, determinar pertinencia y continuidad.
3	Director de Tecnologías de la información y las Comunicaciones, Subdirector de Recursos Tecnológicos	Informa a Subdirección de Servicios Generales la autorización de ingreso en horario extra laboral en casos de emergencia a centro de datos piso 7 y centros de cableado ubicados en los diferentes pisos, a funcionarios con roles de • Administrador de Centro de Datos. • Administrador de Centros de Cableado. Operador de Centro de Datos y operador de Centros de Cableado.	Comunicación oficial interna.	**Observación:** En caso de presentarse una emergencia en horarios no laborales, la Dirección Administrativa debe tener conocimiento de funcionarios de contacto y acción de la Dirección de Tecnologías de la Información y las Comunicaciones
4	Profesional Especializado, Profesional Universitario, Técnico	Realiza actividades de administración, monitoreo y/o mantenimiento en centro de datos y/o centros de cableado de acuerdo a		**Punto de Control:** El Director Tecnologías de la información y las Comunicaciones

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	con roles de: Administrador del centro de datos Administrador de centros de cableado Operador de Centro de datos y de centros de cableado	las responsabilidades definidas al rol y de acuerdo con las planificaciones de la actividad. En caso de requerir acceso a centro de datos y/o centros de cableado a personal no autorizado, se debe realizar las actividades 5, 6 y 7	Anexo 2. Bitácora de Acceso a centro de datos y/o centros de cableado. PGTI-06-02	y/o Subdirector de Recursos Tecnológicos deben verificar periódicamente el diligenciamiento de la Bitácora de Acceso y los fines de los accesos
5	Profesional Especializado, Profesional Universitario con roles de: Administrador del centro de datos Administrador de centros de cableado	Solicita autorización de acceso a centro de datos y/o centros de cableado a personal no autorizado (funcionario, tercero, y/o contratista) a través de diligenciamiento de formato, en caso de requerirse el acceso, indicando claramente la identificación del personal, las actividades a realizar, el tiempo programado de las actividades y las fechas y horarios de acceso y permanencia.	Anexo 3. Formato de Autorización Acceso a centro de datos y/o centros de cableado. PGTI-06-03	
6	Subdirector de Recursos Tecnológicos	Autoriza o deniega el ingreso de personal dependiendo de la pertinencia de las labores y los accesos. Informa a la Subdirección de Servicios Generales la autorización de ingreso del personal en caso de ser autorizado indicando el horario de acceso y tiempo de permanencia.	Anexo 3. Formato de Autorización Acceso a centro de datos y/o centros de cableado. PGTI-06-03 Comunicación Oficial Interna.	**Punto de Control:** Restringir el acceso a áreas seguras, de almacenamiento, procesamiento y transmisión de datos, permitiendo el acceso solo al personal autorizado y en los casos necesarios.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
7	Profesional Especializado, Profesional Universitario con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado	Acompaña y monitorea al personal autorizado temporalmente para ejecutar actividades en centro de datos y/o centros de cablead	Anexo 2. Bitácora de Acceso a centro de datos y/o centros de cableado. PGTI-06-02	**Punto de Control** Registro de las actividades realizadas en centro de datos y / o centros de cableado, en la Bitácora y de ser necesaria según la complejidad de la actividad entregar informe detallado de actividades y/o intervenciones.
8	Profesional Especializado, Profesional Universitario con roles de: Administrador del centro de datos Administrador de centros de cableado	Elabora informe mensual de actividades de administración de centro de datos y centros de cableado	Informe mensual de administración de centro de datos y centros de cableado	
9	Subdirector de Recursos Tecnológicos.	Analiza los informes y comunica los aspectos relevantes a la Dirección para la toma de decisiones.		**Punto de Control** Se debe analizar periódicamente la generación de nuevos riesgos, el nivel de vulnerabilidad de la plataforma tecnológica y la efectividad de los controles implementados

5.2 Gestión de Ingreso y/o Salida de Equipos y Elementos del Centro de Datos y/o Centros de Cableado

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional Especializado, Profesional Universitario con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado.	Solicita autorización para ingreso y/o salida de equipos o elementos al centro de datos o los centros de cableado.	Anexo 3. Formato de Autorización Acceso a centro de datos y/o centros de cableado. PGTI-06-03	
2	Subdirector de Recursos Tecnológicos	Autoriza o deniega ingreso y/o salida de equipos o elementos al centro de datos o centros de cableado teniendo en cuenta la pertinencia y necesidad de la acción.	Anexo 3. Formato de Autorización Acceso a centro de datos y/o centros de cableado. PGTI-06-03	**Punto de Control:** Restringir el ingreso de equipos y/o elementos a áreas seguras, de almacenamiento, procesamiento y transmisión de datos, permitiendo el acceso solo a los equipos y/o elementos autorizados y debidamente verificados y controlados.
3	Profesional Especializado, Profesional Universitario con roles de: Administrador de Centro de Datos.	Ingresa y/o retira equipos o elementos al centro de datos o los centros de cableado. En caso que el ingreso o retiro del equipo o elemento tenga afectación en el inventario.	Anexo 4. Formato de Ingreso y Salida de Equipos y/o Elementos del Centro de Datos y/o Centros de Cableado	**Punto de Control:** Verifica y registra identificación del elemento, características técnicas y estado del elemento a ingresar o retirar.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Administrador de Centros de Cableado.		PGTI-06-04	
4	Director de Tecnologías de la información y las Comunicaciones, Subdirector de Recursos Tecnológicos	Solicita a la Subdirección de Recursos Materiales con los soportes requeridos, el ingreso/salida del (los) elementos registrado(s) como nuevo o cambio o baja en inventario de la Dirección de Tecnologías de la Información y las Comunicaciones, según corresponda.	Comunicación Oficial Interna.	**Punto de control:** Se activa el Procedimiento de Gestión de Recursos y Servicios Tecnológicos. Se activa el Procedimiento para el Manejo y Control de Almacén e Inventarios vigente del Proceso Gestión Administrativa y Financiera.

5.3. Gestión de Cambios en el Centro de Datos y los Centros de Cableado

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional Especializado, Profesional Universitario con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado.	Solicita autorización para ejecutar actividades técnicas soporte y/o mantenimiento (instalación, configuración y/o desinstalación) de equipos o elementos de centro de datos o centros de cableado.	Anexo 3. Formato de Autorización Acceso a centro de datos y/o centros de cableado. PGTI-06-03	**Observación:** Se debe informar fecha, horario de acceso y tiempo de permanencia e indicar la afectación en la disponibilidad de los servicios informáticos /plataforma tecnológica a funcionarios y/o ciudadanos, indicando el alcance de la afectación y el

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				tiempo de la misma. **Punto de control:** El Director de Tecnologías de la información y las Comunicaciones y Subdirector de Recursos Tecnológicos deben evaluar con anterioridad el impacto de las intervenciones en la infraestructura tecnológica instalada, para activar los planes de contingencia, respaldo, y comunicación en caso de ser necesario.
2	Subdirector de Recursos Tecnológicos	Autoriza o deniega ejecución de actividades técnicas. En caso que la actividad tenga afectación de servicios informáticos de la Contraloría de Bogotá D.C. ejecuta la actividad 3.	Anexo 3. Formato de Autorización Acceso a centro de datos y/o centros de cableado. PGTI-06-03	
3	Subdirector de Recursos Tecnológicos	Remite a Oficina Asesora de Comunicaciones, información para su publicación a funcionarios y/o ciudadanía acerca de la actividad a realizar y los horarios de indisponibilidad de servicios informáticos de la Contraloría de Bogotá.	Correo electrónico institucional	**Punto de control:** El Director de Tecnologías de la información y las Comunicaciones y Subdirector de Recursos Tecnológicos deben evaluar con anterioridad el

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				impacto de las intervenciones en la infraestructura tecnológica instalada, para activar los planes de contingencia, respaldo, y comunicación en caso de ser necesario.
4	Profesional Especializado, Profesional Universitario con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado.	Ejecutar actividades técnicas de instalación, configuración, soporte y/o mantenimiento de equipos y/o elementos de centro de datos y/o centros de cableado. Efectúa trámite para la Actualización de planos de RACK en centro de datos y centros de cableado según los cambios aplicados.	Anexo 5. Formato Registros de Cambios. PGTI-06-05 Sistema de Información de Control de Elementos Informáticos SICEINFO Actualización de planos de RACK en centro de datos y centros de cableado	**Punto de Control:** Las actividades realizadas deben estar acompañadas y supervisadas por el responsable de esta actividad.
5	Profesional Especializado, Profesional Universitario con roles de: Administrador de Centro de Datos. Administrador	Registra actividades en el Sistema de Información de Control de Elementos Informáticos SICEINFO	Sistema de Información de Control de Elementos Informáticos SICEINFO	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	de Centros de Cableado.			
6	Profesional Especializado, Profesional Universitario con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado.	Verifica el correcto funcionamiento de equipos y/o elementos de centro de datos y/o centros de cableado y disponibilidad de los servicios informáticos afectados con la actividad de soporte y/o mantenimiento	Anexo 5. Formato Registro de Cambios en el Centro de Datos y/o Centros de Cableado. PGTI-06-05	
7	Profesional Especializado, Profesional Universitario con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado.	Elabora el informe de gestión de cambios en centro de datos y centros de cableado.	Informe mensual de gestión de cambios de centro de datos y centros de cableado	**Punto de Control:** Informe a Subdirector de Recursos Tecnológicos el resultado de la actividad de instalación, configuración, soporte y/o mantenimiento realizados.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
8	Subdirector de Recursos Tecnológicos.	Analiza los informes y comunica los aspectos relevantes a la Dirección para la toma de decisiones.		**Punto de Control:** Se debe analizar periódicamente la generación de nuevos riesgos, el nivel de vulnerabilidad de la plataforma tecnológica y la efectividad de los controles implementados

5.4 Seguridad Perimetral Informática – Antivirus - WSUS

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de Tecnologías de la Información y las Comunicaciones, Subdirector de Recursos Tecnológicos	Asigna a funcionarios los roles de: Administrador de Seguridad Perimetral Administrador de Plataforma Antivirus. Administrator Windows Server Update Services – WSUS Conformar Equipo de Respuesta ante Incidentes de Seguridad de la Información- CSIRT.	Comunicación oficial interna	**Punto de Control:** Segregación de funciones de acuerdo a perfiles y competencias. Se debe realizar una descripción específica del alcance de cada uno de los roles. La conformación de Equipos y Roles asignados debe ser coherente con las establecidas en

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				el Plan de Contingencias, en caso de requerir ajustes se deben tramitar los mismos de acuerdo con su pertinencia.
2	Director de Tecnologías de la Información y las Comunicaciones, Subdirector de Recursos Tecnológicos	Otorga permisos de acceso al portal del fabricante de las plataformas de seguridad perimetral, antivirus, WSUS, según se requiera, a los funcionarios con los roles de : Otorga permisos de acceso al portal del fabricante de las plataformas de seguridad perimetral, antivirus, WSUS, según se requiera, a los funcionarios con los roles de : Administrador de Seguridad Perimetral, Administrador de Plataforma WSUS, Administrador de plataforma antivirus.	Comunicación oficial interna	**Punto de Control:** Asignación de privilegios según las funciones y perfiles requeridos. Aplicar protocolos de seguridad en el suministro de las claves y usuarios de acceso, según corresponda
3	Profesional Especializado, Profesional Universitario, Técnico con rol de: Administrador de Seguridad Perimetral	Revisa, administra, monitorea, la aplicación de políticas de seguridad en equipos de seguridad perimetral informática y guarda evidencia del ingreso a la plataforma correspondiente. En caso de presentar alerta de riesgo, debe realizar actividades 6, 7,8.		**Observación:** Las actividades de revisar, administrar, monitorear se realizan diariamente. **Punto de Control:** Validar el correcto funcionamiento de las políticas de seguridad

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				implementadas en los equipos de seguridad perimetral Realice documentación técnica de las actividades realizadas
4	Profesional Especializado, Profesional Universitario, Técnico con rol de: Administrador de Plataforma Antivirus	Revisa, administra, monitorea, la aplicación de políticas de seguridad en plataforma antivirus y guarda evidencia del ingreso a la plataforma correspondiente. En caso de presentar alerta de riesgo, debe realizar actividades 6, 7,8.		**Observación:** Las actividades de revisar, administrar, monitorear se realizan Diariamente. **Punto de Control:** Validar el correcto funcionamiento de las políticas de seguridad en plataforma antivirus. Realice documentación técnica de las actividades realizadas.
5	Profesional Especializado, Profesional Universitario, Técnico con rol de: Administrador de Plataforma WSUS	Revisa, administra, monitorea, la aplicación centralizada de actualizaciones y parches publicados por Microsoft o plataforma implementada en los PC y servidores de la Contraloría de Bogotá y guarda evidencia del ingreso a la plataforma correspondiente. En caso de presentar alerta		**Observación:** Las actividades de revisar, administrar, monitorear se realizan diariamente. **Punto de Control:** Validar la correcta aplicación de actualizaciones y

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		de riesgo, debe realizar actividades 6, 7,8.		parches de Microsoft o plataforma implementada en los equipos de computación con productos Microsoft u otras plataformas según corresponda. Realice documentación técnica de las actividades realizadas.
6	Profesional Especializado, Profesional Universitario, Técnico con rol de: Administrador de Seguridad Perimetral Administrador de Plataforma Antivirus Administrador de Plataforma WSUS	En caso de presentar alerta de riesgo, comunica inmediatamente al Director de Tecnologías de la Información y las Comunicaciones y Subdirector de Recursos Tecnológicos.	Informe de alerta de seguridad. Correo Electrónico	**Observación:** Realice documentación técnica de la alerta presentada
7	Director de Tecnologías de la Información y las Comunicaciones, Subdirector de Recursos Tecnológicos, Subdirector de Gestión de la	Analizan y toman decisión de acciones de mitigación de riesgos	Acta de reunión de seguridad	**Punto de Control:** Si son riesgos ya identificados y que se encuentran en el mapa de riesgos, se debe analizar la eficacia y efectividad de las acciones implementadas y

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	Información, Profesional Especializado, Profesional Universitario, Técnico con rol de: Administrador de Seguridad Perimetral, Administrador de Plataforma Antivirus, Administrador de Plataforma WSUS, CSIRT.			tomar decisiones sobre su actualización o modificación. Si se trata de nuevos riesgos identificados deben ser adicionados en el mapa de riesgos y gestionar su tratamiento e implementación activando el procedimiento correspondiente del Proceso de Direccionamiento Estratégico.
8	Profesional Especializado, Profesional Universitario, Técnico con rol de: Administrador de Seguridad Perimetral Administrador de Plataforma Antivirus Administrador de Plataforma WSUS	Ejecución de acciones de mitigación de riesgos	Informe de evento de seguridad (causa, consecuencia, acciones de mitigación)	
9	Profesional Especializado, Profesional Universitario, Técnico con rol de: Administrador	Elabora el informe sobre la administración perimetral, antivirus, WSUS según corresponda al rol	Informe mensual de seguridad perimetral. Informe mensual de plataforma	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	de Seguridad Perimetral Administrador de Plataforma Antivirus Administrador de Plataforma WSUS		antivirus. Informe mensual de plataforma WSUS	
10	Subdirector de Recursos Tecnológicos.	Analiza los informes y comunica los aspectos relevantes al Director para la toma de decisiones.		**Punto de Control:** Se debe analizar periódicamente la generación de nuevos riesgos, el nivel de vulnerabilidad de la plataforma tecnológica y la efectividad de los controles implementados.

6. ANEXOS

ANEXO 1. Formato de Acceso Permanente al Centro de Datos y Centros de Cableado

CONTRALORÍA DE BOGOTÁ, D.C.	Formato de acceso permanente al centro de datos y centros de cableado	Código formato: PGTI-06-01 Versión: 1.0
		Código documento: PGTI-06 Versión 1.0
		Página x de y

FECHA AUTORIZACIÓN:			
	DD	MM	YYYY
FIRMA:	FIRMA:		
NOMBRE:	NOMBRE:		
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES	SUBDIRECCIÓN DE RECURSOS TECNOLÓGICOS		

No. ORDEN	DATOS FUNCIONARIO AUTORIZADO
1	NOMBRE COMPLETO: _____ CEDULA: _____ CARGO: _____ ADMINISTRADOR DE: _____ TELEFONO FIJO: _____ TELEFONO MOVIL: _____
2	NOMBRE COMPLETO: _____ CEDULA: _____ CARGO: _____ ADMINISTRADOR DE: _____ TELEFONO FIJO: _____ TELEFONO MOVIL: _____
3	NOMBRE COMPLETO: _____ CEDULA: _____ CARGO: _____ ADMINISTRADOR DE: _____ TELEFONO FIJO: _____ TELEFONO MOVIL: _____
4	NOMBRE COMPLETO: _____ CEDULA: _____ CARGO: _____ ADMINISTRADOR DE: _____ TELEFONO FIJO: _____ TELEFONO MOVIL: _____

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Fecha autorización	Fecha en la cual se diligencia el formato, se conceden los permisos y se firma autorización.
Firmas	Corresponde a las firmas que autorizan los accesos y la validez del documento.
Nombre	Nombre de las personas que autorizan los accesos y la validez del documento.
N° Orden	Hace referencia al orden ascendente de los funcionarios a los cuales se les concede la autorización de acceso permanente.
Datos funcionario autorizado	En este campo se debe diligenciar el nombre completo, numero de documento de identidad, cargo del funcionario, así como si es administrador de lista y por último los teléfonos de contacto fijo - móvil.

ANEXO 2. Bitácora de Acceso a Centro de Datos y/o Centros de Cableado

CONTRALORÍA DE BOGOTÁ, D.C.	**Bitácora de acceso a centro de datos y/o centros de cableado**	Código formato: PGTI-06-02 Versión: 1.0
		Código documento: PGTI-06 Versión 1.0
		Página x de y

FECHA	NUMERO DE IDENTIFICACIÓN	NOMBRES Y APELLIDOS	EMPRESA/DEPENDENCIA	LABOR A REALIZAR	H. INGRESO	H. SALIDA	AUTORIZA	FIRMA

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Fecha	Hace referencia a la fecha de acceso al centro de datos o centros de cableado.
Nombres y Apellidos	Hace referencia al funcionario, contratista o terceros que ingresan al centro de datos o centros de cableado.
Número de identificación	Corresponde al NIT o CEDULA DE CIUDADANÍA según corresponde a persona Jurídica o natural
Empresa/Dependencia	Hace referencia a la empresa o dependencia interna de donde procede el funcionario, contratista o tercero que ingresa al centro de datos o los centros de cableado.
Labor a realizar	Hace referencia a las labores que se desarrollarán en el centro de datos o centros de cableado. P. Ej.: Mantenimiento Preventivo.
H. Ingreso	En este campo se debe indicar la hora de ingreso al centro de datos o centros de cableado, esta debe ser expresada en formato 24H.
H. Salida	En este campo de debe indicar la hora de salida del centro de datos o centros de cableado, esta debe expresarse en

	formato 24H.
Autoriza	Nombre del funcionario que autoriza el ingreso.
Firma	Firma del funcionario, tercero o contratista que ingresa al centro de datos o los centros de cableado.

ANEXO 3. Formato de Autorización Acceso a Centro de Datos y/o Centros de Cableado.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato de autorización acceso Centro de datos y/o centros de cableado**	Código formato: PGTI-06-03 Versión: 1.0
		Código documento: PGTI-06 Versión 1.0
		Página x de y

Fecha de solicitud			**Funcionario que solicita (Responsable)**				
DD	MM	AA	**Rol/ Cargo**				
	Autorización de acceso de personal Autorización para ejecución de actividades soporte y/o mantenimiento Autorización de ingreso o retiro de equipos y/o elementos						
Fecha de ingreso:			**Hora de ingreso:**			**Tiempo estimado de permanencia**	
						Horas	
DD	**MM**	**AA**	**HH**	**MM**	**AM/PM**	**Minutos**	

Datos de personal a autorizar					
Nombres y apellidos	**Cedula**	**Empresa/ dependencia**	**ARL**	**Teléfono de contacto**	**Acceso a: CD: Centro de datos CC: Centros de cableado (piso)**

Descripción de la actividad a realizar

¿La actividad requiere de inactividad/ suspensión /apagado de servicio informático o dispositivos de plataforma tecnológica? SI: ☐ NO: ☐

Áreas de servicio y/o aplicaciones afectadas:

Ingreso/ retiro de equipos y/o elementos

Fecha del movimiento	DD	MM	AA

Equipo y/o elemento	**Placa / serial**	**Ubicación inicial**	**Ubicación final**	**Ingreso/salida**

Observaciones: _____

☐ **Autorizado**
☐ **Denegado**

_____

Firma Director(a) y/o Subdirector(a) de Recursos Tecnológicos
Dirección Tecnologías de la Información y las Comunicaciones

Este formato no debe contener remarcados, tachones o enmendaduras

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Fecha de solicitud	Fecha de solicitud de la autorización, formato día, mes, año
Funcionario que solicita (Responsable)	Nombres y apellidos de Funcionario con rol administrador responsable de la actividad, que realiza la solicitud de la autorización
Rol	Indicar el nombre del rol del funcionario. Ejemplo : Administrador de centro de datos, administrador de centros de cableado
Tipos de solicitud	Opciones de tipos de solicitud
Autorización de acceso de personal	Seleccionar con una "X" sí la solicitud de autorización es de acceso
Autorización para ejecución de actividades soporte y/o mantenimiento	Seleccionar con una "X" sí la solicitud de autorización para realizar actividades de soporte y/o mantenimiento
Autorización de ingreso o retiro de equipos y/o elementos	Seleccionar con una "X" sí la solicitud de autorización para realizar el ingreso o retiro de elementos en centro de datos y/o centros de cableado

Fecha de ingreso	Fecha programada para ingreso a centro de datos y/o centros de cableado, formato día, mes, año
Hora de ingreso	Hora programada para ingreso a centro de datos y/o centros de cableado
Tiempo estimado de permanencia	Tiempo estimado de permanencia en centros de datos y/o centros de cableado
Datos de personal a autorizar	Esta información aplica para solicitudes de acceso a personal
Nombres y apellidos	Nombres y Apellidos de la persona a la cual se está solicitando la autorización
Cedula	Número de cédula de la persona a la cual se está solicitando la autorización
Empresa/ dependencia	Empresa o dependencia a la que pertenece la persona que se está solicitando la autorización
ARL	ARL a la que pertenece la persona que se está solicitando la autorización
Teléfono de contacto	Teléfono de la persona que se está solicitando la autorización
Acceso a:CD Centro de datos/CC: Centros de cableado (Piso)	Indicar CD o CC, sí es centros de cableado indicar el piso de ubicación
Descripción de la actividad a realizar	Describir la actividad a realizar en centros de datos y/o centros de cableado, éste campo aplica para el caso de las 3 opciones de solicitud
¿La actividad requiere de inactividad/ suspensión /apagado de servicio informático o dispositivos de plataforma tecnológica? SI: NO:	Indicar si la actividad a realizar va a tener afectación en la presentación de los servicios informáticos de la Entidad, Sí se requiere de apagado, suspensión, inactividad o situación que afecte el funcionamiento temporal o permanente de un servicio informático (Sistema de información, plataforma tecnológica).
Áreas de servicio y/o aplicaciones afectadas:	Indicar las áreas de servicio, aplicaciones, plataforma tecnológica que van a tener afectación con la actividad.
Ingreso/ retiro de equipos y/o elementos	Estos campos de información aplican para la solicitud de autorización para el ingreso o retiro de equipos y/o elementos.
Fecha del movimiento	Fecha de ingreso o retiro de equipos y/o elementos del centro de datos y/o centros de cableado.
Equipo y/o elemento	Nombre de equipo y/o elemento que ingresa o retira de centro de datos y/o centros de cableado.
Placa / serial	Placa /serial de equipo y/o elemento que ingresa o retira de centro de datos y/o centros de cableado.
Ubicación inicial	Sitio de donde proviene el equipo y/o elemento que ingresa o retira de centro de datos y/o centros de cableado.
Ubicación final	Sitio de donde queda ubicado el equipo y/o elemento que ingresa o retira de centro de datos y/o centros de cableado.
Ingreso/salida	Indicar sí es un ingreso o salida de equipo y/o elemento.
Observaciones	Indicar observaciones de la solicitud.

Autorizado	Indicar con una "X" sí es autorizada la solicitud.
Denegado	Indicar con una "X" sí es denegada la solicitud.
Firma Director(a) y/o Subdirector(a) de Recursos Tecnológicos Dirección Tecnologías de la Información y las Comunicaciones	Firma de Director(a) de Dirección TIC y /o Subdirector de Recursos Tecnológicos que autoriza la solicitud.

ANEXO 4. Formato de Ingreso y Salida de Equipos y/o Elementos del Centro de Datos y/o Centros de Cableado.

CONTRALORÍA DE BOGOTÁ, D.C.	Formato de ingreso y salida de equipos y/o elementos del centro de datos y/o centros de cableado	Código formato: PGTI-06-04 Versión: 1.0
		Código documento: PGTI-06 Versión 1.0
		Página x de y

Fecha de solicitud			Fecha de ejecución			Lugar del movimiento		Tipo de solicitud	
						Centro de Datos		Ingreso	
DD	MM	AA	DD	MM	AA	Centros cableado	Edificio: Piso:	Salida	

Ejecutante		Empresa:	
Responsable		Equipo propiedad de:	
Afecta Inventario TIC	Sí ☐ No ☐	Guía de mensajería	

Ubicación			Características												
Área (DC/CC)	RACK**	POSICIÓN**	NOMBRE EQUIPO	MARCA MODELO	SERIAL	PROCESADOR*	DISCOS*	MEMORIA*	S.O T SOFTWARE	FUENTES	ALIMENTACION	CONSUMO AMPERIOS	CONSUMO WATTS	Ou's Requeridas	Ingresa/Salida

Nombre de quien Ingresa/retira		**Nombre Administrador**		**Director(a) / subdirector(a) que autoriza**	
Firma		**Firma**		**Firma**	
Observaciones: Los equipos ingresados deben estar debidamente etiquetados para facilitar su identificación | Si los equipos no son de rack, estos deben venir con su respectiva bandeja | Los campos marcados con (*) si aplica. (**) Campos exclusivos para uso del administrador del centro de datos y/o centros de cableado. Este formato no debe contener remarcados, tachones o enmendaduras.					

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Tipo de solicitud	Tipo: Ingreso / Salida.
Centro de datos	Lugar donde ingresará o del que saldrá el equipo o elemento.
Centros de cableado	Lugar donde ingresará o del que saldrá el equipo o elemento.
Fecha de ejecución	Fecha en que ingresará o saldrá el equipo o elemento al centro de datos o centros de cableado.
Solicitante	Funcionario, contratista o tercero que requiere ingresar o retirar equipos o elementos del centro de datos o centros de cableado.
Responsable	Funcionario que ejerce responsabilidad sobre el ingreso o retiro de equipos o elementos del centro de datos o centros de cableado.
Empresa	(Si aplica) Empresa que retira o ingresa equipos o elementos al centro de datos o centros de cableado.
Equipo propiedad de	Referencia a la propiedad del equipo o elemento que ingresa o sale del centro de datos o centros de cableado.
Guía de mensajería	Documento de control para envío de equipos o elementos que ingresan o salen del centro de datos o centros de cableado.
Ubicación	Lugar donde ingresará o desde donde saldrá el equipo o elemento, este puede ser DC (Centro de datos) o CC (Centros de cableado).
Rack	Número de gabinete donde residirá el equipo que ingresa o desde donde saldrá el equipo en retiro.
Posición	Posición espacial dentro del Rack, esta medida se expresa en OU.
Nombre de Equipo	Especificar el nombre del equipo que ingresa o se retira del centro de datos o los centros de cableado.
Marca Modelo	Marca y modelo del equipo que ingresa o se retira del centro de datos o los centros de cableado
Serial	Información con característica única con la que se

	referencian los equipos.
Procesador (Si aplica)	Indicar la cantidad de procesadores de los equipos que ingresan o salen del centro de datos o centros de cableado.
Discos (Si aplica)	Indicar la cantidad de discos de los equipos que ingresan o salen del centro de datos o centros de cableado.
Memoria (Si aplica)	Indicar la cantidad de memoria de los equipos que ingresan o salen del centro de datos o centros de cableado.
S.O y Software (Si aplica)	Indicar tipo de S.O y software de los equipos que
Fuentes	Indicar el número de fuentes y el voltaje y tensión a la cual trabajan.
Alimentación	Indicar el tipo de alimentación AC / DC.
Consumo	Especificar el consumo en potencia y amperaje de los equipos que ingresan o salen del centro de datos o los centros de cableado
OU's Requerida	Indicar el número de unidades de Rack que se requieren para el ingreso de los equipos o los que quedan disponible con el retiro.
Nombre y firma de quien ingresa o retira y de quien autoriza	Funcionarios, contratistas o terceros que ingresan o retiran el equipo o componente del centro de datos o centros de cableado y el funcionario que autoriza esta acción.
Nombre y firma Administrador responsable	Administrador responsable de la actividad
Nombre y firma de Director(a) / Subdirector(a) de Recursos Tecnológicos que autoriza	Director(a) / Subdirector(a) de Recursos Tecnológicos que autoriza

ANEXO 5. Formato Registros de cambios de centro de datos y centro de cableado.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato registro de cambios en el centro de datos y/o centros de cableado**	Código formato: PGTI-06-05 Versión: 1.0
		Código documento: PGTI-06 Versión 1.0
		Página x de y

Ticket: ND ---------- Espacio reservado para ser diligenciado por Mesa de Servicio	**Fecha Cambio:** DD MM AAAA

Identificación del responsable del Cambio			
Nombre	**Cargo**	**Teléfono/ Ext**	**Correo Electrónico**

Fecha estimada del cambio			**Hora estimada del Cambio**			**Tiempo estimado para realizar el cambio**	
						Horas	
DD	**MM**	**AA**	**HH**	**MM**	**PM**	**Minutos**	

Áreas de servicio y/o aplicaciones afectadas:
Antecedentes del Cambio (Por qué se requiere?):

Nombre del Cambio	**Prioridad del cambio:**
	Urgente ( )
Alcance del Cambio:	Alto ( )
	Medio ( )
	Bajo ( )

Análisis de Impacto
Qué procesos de negocio del Cliente afecta el cambio?
Qué áreas de servicio o elementos de TI afecta el cambio? (Hardware, Software, Aplicaciones, servicios de TI)
Cantidad de usuarios afectados?
Cómo impacta el cambio el cumplimiento de los Acuerdos de Niveles de Servicio?
Beneficios del cambio

Consecuencias de no realizar el cambio solicitado:

Plan Actividades Previas del Cambio

TAREA	FECHA/HORA INICIO	FECHA/HORA FINALIZACIÓN	RESPONSABLE	NUMERO CELULAR

Plan de ejecución

TAREA	FECHA/HORA INICIO	FECHA/HORA FINALIZACIÓN	RESPONSABLE	NUMERO CELULAR

Plan de Reversión y Control de Riesgos (roll-back)

TAREA	FECHA/HORA INICIO	FECHA/HORA FINALIZACIÓN	RESPONSABLE	NUMERO CELULAR

Plan de Pruebas

TAREA	FECHA/HORA INICIO	FECHA/HORA FINALIZACIÓN	RESPONSABLE	NUMERO CELULAR

Entregables y Criterios de Aceptación
Mensaje para los usuarios o dependencias afectadas por el cambio:
Antes de realizarlo:
Después de realizarlo:
Fecha y frecuencia estimada para envío de mensajes a usuarios:
Antes de realizar el cambio:
Después de realizar el cambio:
Documentos anexos (si existen)
LOS SIGUIENTES ÍTEMS DEBEN SER DILIGENCIADOS POR EL ADMINISTRADOR DEL CAMBIO
Aprobaciones respectivas

Funcionario administrador /rol	**Subdirector de Recursos Tecnológicos**

Fecha Aprobación:			**Observaciones:**

Día	Mes	Año	

INSTRUCTIVO DE DILIGENCIAMIENTO

Nombre del campo	Descripción del campo
Ticket: ND	Espacio reservado para ser diligenciado por Mesa de Servicio
Fecha de cambio	Indica la fecha en la que se solicita el cambio
Nombre	Nombre del responsable del cambio, es la persona que lo solicita
Cargo	Cargo del responsable del cambio o de la persona que lo solicita
Teléfono/Ext	Número telefónico de contacto con el responsable del cambio
Correo electrónico	Dirección de correo electrónico del responsable del cambio (Debe incluir el signo arroba)
Fecha estimada del cambio	Fecha en la cual se proyecta realizar el cambio
Hora estimada del cambio	Expresar la hora en HH, los minutos MM y el tipo de horario que puede ser PM ó AM
Tiempo estimado para realizar el cambio	Expresa las horas y los minutos que se requiere para implementar el cambio
Áreas de servicio y/o aplicaciones afectadas	Relaciona los procesos y /o los servicios que se puedan afectar
Antecedentes del cambio	Describe el por qué se realiza el cambio
Nombre del cambio	En forma corta describe el cambio sin detalles
Alcance del cambio	Describe el objetivo del cambio: para qué ?
Prioridad del cambio	Selecciona una de las cuatro opciones: Urgente, Alto, Medio, Bajo
Qué procesos de negocio del cliente afecta el cambio	relaciona las áreas o los procesos que se van a ver afectados con el cambio
Que áreas de servicio o elementos de TI afecta el cambio (Hardware, software, aplicaciones, servicios de TI.	Relaciona los elementos que se ven afectados con el cambio
Cantidad de usuarios afectados	Número de usuarios del servicio que se ve afectado.
Cómo impacta el cambio el cumplimiento de los Acuerdos de Niveles de Servicio.	Si el cambio afecta los SLA´s describa como se afecta
Beneficios del cambio	Describe las ventajas del cambio sobre los servicios o plataforma tecnológica
Consecuencias de no realizar el cambio solicitado	Describe que pasaría si no se implementa el cambio
Plan de actividades previas al cambio	Relaciona en cada fila una actividad o tarea a realizar antes del cambio indicando fecha/hora de inicio, fecha /hora de

	finalización, Nombre del responsable de realizar la actividad y el número celular o fijo de contacto
Plan de ejecución	Relaciona las actividades a desarrollar cuando se va a ejecutar el cambio indicando fecha y hora de inicio, fecha y hora de finalización, nombre del responsable de ejecutar la tarea y el número de contacto celular o fijo
Plan de Reversión y Control de Riesgos (roll-bacj)	Relaciona las actividades a desarrollar cuando se va a realizar la reversión y Control de riesgos indicando fecha y hora de inicio, fecha y hora de finalización, nombre del responsable de ejecutar la tarea y el número de contacto celular o fijo
Plan de Pruebas	Relaciona las actividades a desarrollar como pruebas del cambio indicando fecha y hora de inicio, fecha y hora de finalización, nombre del responsable de ejecutar la tarea y el número de contacto celular o fijo
Entregables y Criterios de Aceptación	Detalle los documentos, manuales, equipos, configuraciones, informes y cualquier documento o elementos físico que debe ser entregado como producto del cambio
Mensaje para los usuarios o dependencias afectadas por el cambio	Elabore un mensaje que el responsable del cambio considera debe ser informado a los usuarios o dependencias afectadas por el cambio antes y después de haberlo implementado.
Fecha y frecuencia estimada para envío de mensajes a usuarios	Indica la fecha y la frecuencia con la cual debe ser informado el mensaje antes y después del cambio
Aprobaciones respectivas	Es exclusivo del administrador del cambio. Relaciona las acciones o cambios que fueron aprobados
Funcionario administrador/ rol	Firma del administrador que aprueba el cambio e indica el rol que tiene como administrador, puede ser administrador de centro de datos o administrador de centro de cableado
Fecha de aprobación	Corresponde al día, mes y año de aprobación del cambio
Observaciones	Registra cualquier información adicional que considera debe registrarse como producto de la solicitud de cambio

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	R.R No. 007 16 Febrero de 2018	Ajuste a la normatividad Cambia el registro "*Formato Hoja de Vida de Equipos de Cómputo y de Comunicaciones PGTI-05-01*"en la actividad No 4 del numeral 5.3 *Gestión de cambios en el centro de datos y centros de cableado* por Sistema de Información de Control de Elementos

		Informáticos SICEINFO.
2.0	R.R. No. 047 28 Diciembre de 2018	