	Responsable del Proceso	Dirección de Planeación
	Aprobación	**Revisión Técnica**
Firma:		
Nombre:	WISMAN YESID COTRINO GARCÍA	MICHAEL ANDRÉS RUIZ FALACH
Cargo:	Director Técnico	Director Técnico
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones	Dirección de Planeación
R.R. Nº 013		**Fecha: ABRIL 27 DE 2021**

1. OBJETIVO:

Establecer las actividades para gestionar los riesgos inherentes para la seguridad de la plataforma tecnológica, servicios informáticos y aseguramiento de los servicios de red, para salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Contraloría de Bogotá D.C.

2. ALCANCE:

El procedimiento inicia con la asignación de roles de administrador y operador para la gestión de acceso al centro de datos y los centros de cableado y termina con la validación del medio de transferencia de información digital y el cierre o desactivación de los servicios autorizados temporalmente

3. BASE LEGAL:

NORMA	FECHA	DESCRIPCIÓN
Ley 527	18-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.

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. Artículos 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 al 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 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.
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.

NORMA	FECHA	DESCRIPCIÓN
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 de la Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas - CDS	20-oct-2008	Por la cual se expiden las 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, la cual fue modificada por la Resolución 004 del 28 de noviembre de 2017.
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 - Requisitos del Sistema de Gestión de la Seguridad de la Información.
Norma GTC ISO/IECISO 27002	22-jul-2015	Guía Técnica Colombiana ISO - Tecnologías de la Información. Técnicas de Seguridad. Código de Práctica para Controles de Seguridad de la Información.
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 de MINTIC	25-abr-2016	Procedimientos de Seguridad de la Información.

4. DEFINICIONES:

Activo (inglés: Asset): cualquier cosa que tenga valor para un individuo, una organización o un gobierno[1] .

Activo de Información: conocimiento o datos que tienen valor para el individuo u organización[2]. En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización[3].

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 D.C puede estar en algún nivel de riesgo.

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

Amenaza: potencial violación de la seguridad.

Borrado seguro: método de borrado de archivos basado en software cuya función es sobrescribir los datos con el propósito de destruir completamente todos los datos electrónicos que residen en una unidad de disco duro u otros medios de almacenamiento, por lo que es imposible la recuperación posterior de los datos.

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 D.C.

---

[1] Tomado de la Norma ISO/IEC 27032:2012 (definición 4.6, traducida al español), disponible en Internet en: https://www.iso.org/obp/ui/#iso:std:isoiec:27032:ed-1:v1:en.
[2] Ibídem (definición 4.27, traducida español)
[3] Tomado del Portal de ISO 27001 en español, Gestión de Seguridad de la Información. En http://www.iso27000.es/glosario.html#section10a.

Centros de cableado: espacio físico ubicado en diferentes sedes y pisos de la entidad en el cual se encuentran los diferentes equipos de comunicaciones que permite la comunicación entre las diferentes sedes y pisos de la Contraloría de Bogotá D.C.

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.

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 al reducir sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuantas 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.

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.

Instrumentos de Gestión de la información Pública: está conformado por el Registro de Activos de Información, Índice de Información Clasificada y Reservada, Esquema de Publicación de Información, documentos que se encuentran publicados en el link de transparencia en la página web de la entidad.

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 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 la utilización de una copia de su programa informático, y prohibirá la realización de otras copias y la distribución de dicho programa a otro usuario. Según las herramientas, las licencias tienen diferentes niveles y términos.

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.

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 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 D.C.: 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.

Riesgos de seguridad de la información: registrados en los riesgos institucionales de la Contraloría de Bogotá D.C.

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.

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.

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.

Transferencia de información: proceso a través del cual se entrega información en formato digital que se encuentra en custodia de la Dirección de TIC a un proceso de la Contraloría de Bogotá D.C o a un tercero interesado de acuerdo con la solicitud presentada.

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. Lo anterior, permite 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 los Centros de Cableado.

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 roles de: • Administrador de Centro de Datos. • Administrador de Centros de Cableado. • Operador de centro de datos y de centros de cableado	Comunicación oficial interna.	**Punto de Control:** Se debe asegurar de definir las funciones de acuerdo a perfiles 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 Técnico de Recursos Tecnológicos.	Asigna permisos en dispositivos de control de acceso biométrico a centro de datos y los centros de cableado, a través de comunicación oficial 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. Registra el permiso diligenciado el formato "*Acceso Permanente al Centro de Datos y los Centros de Cableado*" - PGTI-06-01 (anexo 1).	Comunicación oficial interna. Formato de acceso permanente al centro de datos y los centros de cableado. PGTI-06-01	**Punto de Control:** Verifica que se asignen privilegios según las funciones. Se debe realizar monitoreo periódico a control de accesos, determinar pertinencia y continuidad.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
3	Director de Tecnologías de la Información y las Comunicaciones, Subdirector de Recursos Tecnológicos	Informa a la Subdirección de Servicios Generales, la autorización de ingreso en horario extra laboral en casos de emergencia al centro de datos ubicado en el piso 7 y a los centros de cableados, ubicados en los diferentes pisos, a los 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 la información de los funcionarios de contacto de la Dirección de Tecnologías de la Información y las Comunicaciones.
4	Profesional o Técnico con roles de: Administrador del Centro de Datos. Administrador de Centros de Cableado. Operador de Centro de Datos y de Centros de Cableado.	Realiza las actividades de administración, monitoreo y/o mantenimiento en el centro de datos y/o los centros de cableado de acuerdo a las responsabilidades definidas al rol y de acuerdo con las planificaciones de la actividad. Diligencia el formato "*Bitácora de Acceso a centro de datos y/o los centros de cableado -*	Bitácora de Acceso a centro de datos y/o los centros de cableado. PGTI-06-02.	**Punto de Control:** El Director Tecnologías de la información y las Comunicaciones y/o Subdirector de Recursos Tecnológicos deben verificar periódicamente el diligenciamiento de la Bitácora de Acceso y los fines de los accesos.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		PGTI-06-02 (Anexo 2). 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.		
5	Profesional con roles de: Administrador del Centro de Datos. Administrador de centros de cableado.	Solicita autorización de acceso al centro de datos y/o los centros de cableado a personal no autorizado, (funcionario, tercero, y/o contratista), en caso que sea requerido el acceso, para lo cual debe diligenciar el formato "*Autorización Acceso a centro de datos y/o los centros de cableado*" - PGTI-06-03 (Anexo 3).		**Observación:** Relacionar claramente la identificación del personal autorizado, la descripción de las actividades a realizar, el tiempo programado de las actividades y las fechas y horarios de acceso y permanencia.
6	Subdirector de Recursos Tecnológicos.	Autoriza o deniega el ingreso de personal dependiendo de la pertinencia de las labores y los accesos. En caso que el acceso sea en tiempos no laborales se informa a la Subdirección de Servicios Generales la autorización de ingreso de personal indicando el horario de acceso y tiempo de permanencia.	Autorización Acceso a centro de datos y/o los centros de cableado. PGTI-06-03 Comunicación Oficial Interna.	**Punto de Control:** Restringe el acceso a áreas seguras, de almacenamiento, procesamiento, transmisión de datos y permite el acceso solo al personal autorizado y en los casos necesarios.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
7	Profesional o Técnico con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado Operador de centro de datos y de centros de cableado.	Acompaña y monitorea al personal autorizado temporalmente para ejecutar actividades en centro de datos y/o centros de cableado. Diligencia el formato "*Bitácora de acceso a centro de datos y/o los centros de cableado"* - PGTI-06-02 (Anexo 2).	Bitácora de acceso a centro de datos y/o los centros de cableado. PGTI-06-02	**Punto de Control:** Registrar las actividades realizadas en centro de datos y / o los 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 con roles de: Administrador del Centro de Datos. Administrador de Centros de Cableado.	Elabora informe mensual de actividades de administración del centro de datos, los centros de cableado y gestión de aseguramiento de los servicios de red.	Informe mensual de administración de centro de datos, centros de cableado y gestión de aseguramiento de los servicios de red.	
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 los Centros de Cableado.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional o Técnico con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado. Operador de Centro de Datos y de Centros de Cableado.	Solicita autorización para ingreso y/o salida de equipos o elementos al centro de datos o los centros de cableado, para lo cual diligencia el formato "*Ingreso y Salida de Equipos y/o Elementos del Centro de Datos y/o los Centros de Cableado*" - PGTI-06-04 (Anexo 4).		**Punto de Control:** Verifica y registra la identificación del elemento, características técnicas y estado del elemento a ingresar o retirar.
2	Subdirector de Recursos Tecnológicos	Autoriza o deniega la solicitud de ingreso y/o salida de equipos o elementos del centro de datos o de los centros de cableado, para lo cual, debe tener en cuenta la pertinencia y necesidad de la acción, para lo cual firma en la casilla autoriza la solicitud.	Ingreso y Salida de Equipos y/o Elementos del Centro de Datos y/o los Centros de Cableado PGTI-06-04	**Punto de Control:** Verifica que la información del formato esté completa con los datos de los equipos o elementos que ingresan o se retiran. Restringir el ingreso de equipos y/o elementos a áreas seguras, de almacenamiento, procesamiento, transmisión de datos y permitir el acceso solo a los equipos y/o elementos autorizados y debidamente verificados y controlados.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
3	Profesional o Técnico con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado. Operador de centro de datos y de centros de cableado.	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, se informa al Director o Subdirector de Recursos Tecnológicos para que se informe la novedad de inventarios.	Ingreso y Salida de Equipos y/o Elementos del Centro de Datos y/o los 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, la actualización del inventario (ingreso, salida, baja del (los) elementos registrado(s), según corresponda) de la Dirección de Tecnologías de la Información y las Comunicaciones, mediante Comunicación oficial, anexando los soportes requeridos.	Comunicación Oficial Interna.	**Observación:** Activa el Procedimiento de Gestión de Recursos y Servicios Tecnológicos – PGTI-05 y el Procedimiento para la Gestión de Bienes, Propiedad, Planta y Equipo – PGAF-10 del Proceso Gestión Administrativa y Financiera.

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

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional 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, para lo cual diligencia el formato "*Registro de cambios en el centro de datos y/o en los centros de cableado*" - PGTI-06-05 (Anexo 5) y registra caso en la mesa de servicio.		**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 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 la ejecución de actividades técnicas, para lo cual firma en la casilla autoriza la solicitud.	Registro de cambios en el centro de datos y/o en los centros de cableado PGTI-06-05.	

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		En caso que la actividad tenga afectación de servicios informáticos de la Contraloría de Bogotá D.C. ejecuta la actividad 3.		
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 D.C.	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 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 o Técnico con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado.	Ejecuta actividades técnicas de instalación, configuración, soporte y/o mantenimiento de equipos y/o elementos de centro de datos y/o los centros de cableado. Efectúa trámite para la Actualización de planos de RACK en centro de datos y centros de cableado según los cambios aplicados.	Registro de cambios en el centro de datos y/o en los centros de cableado PGTI-06-05 Actualización de planos de RACK en centro de datos y centros de cableado.	**Punto de Control:** Verifica que las actividades se realicen de acuerdo a lo planeado.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
5	Profesional o Técnico con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado.	Registra actividades en el Sistema de Información de Control de Elementos Informáticos SICEINFO.	Sistema de Información de Control de Elementos Informáticos SICEINFO.	
6	Profesional o Técnico 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.	Registro de cambios en el centro de datos y/o en los centros de cableado PGTI-06-05	
7	Profesional o Técnico con roles de: Administrador de Centro de Datos. Administrador de Centros de Cableado.	Actualiza el Informe mensual de administración de centro de datos, centros de cableado, gestión de aseguramiento de los servicios de red y hace énfasis en los cambios realizados en el centro de datos y centros de cableado.	Informe mensual de administración de centro de datos, centros de cableado y gestión de aseguramiento de los servicios de red.	**Observación:** Remite el informe al Subdirector de Recursos Tecnológicos el resultado de la actividad de instalación, configuración, soporte y/o mantenimientos realizados.
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. • Administrador Windows Server Update Services – WSUS.	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 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: • 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.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
3	Profesional o 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 implementadas en los equipos de seguridad perimetral. Realice documentación técnica de las actividades realizadas.
4	Profesional o 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.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
5	Profesional o 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 D.C 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 la correcta aplicación de actualizaciones y 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 o 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 al Subdirector de Recursos Tecnológicos, vía correo electrónico o telefónicamente en caso de ser necesario.	Informe de alerta de seguridad: Correo Electrónico.	**Observación:** Elabora documentación técnica de la alerta presentada.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
7	Director de Tecnologías de la Información y las Comunicaciones, Subdirector de Recursos Tecnológicos, Subdirector de Gestión de la Información, Profesional o Técnico, con rol de: Administrador de Seguridad Perimetral, Administrador de Plataforma Antivirus, Administrador de Plataforma WSUS, CSIRT.	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 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 o 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).	

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
9	Profesional o Técnico, con rol de: Administrador de Seguridad Perimetral.	Elabora el informe sobre la administración perimetral, antivirus, WSUS según corresponda al rol.	Informe mensual de seguridad perimetral. Informe mensual de plataforma 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.

5.5 Aseguramiento de Servicios en la Red.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional o Técnico responsable de administrar algún elemento de la infraestructura de redes de TI.	Revisa los registros (logs) de auditoría y eventos de los elementos de red (switches, firewall, controladores inalámbricos, otros). En caso de encontrar alertas que comprometan la red o		

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		su seguridad, se inicia con las actividades del Procedimiento Gestión de Incidentes de Seguridad – PGTI-10.		
2	Profesional o Técnico 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 y/o sistemas de información de acuerdo a lo establecido en el Procedimiento Control de Acceso a Usuarios – PGTI-07 con el fin de verificar que se encuentren los usuarios correctos.		**Observación**: Se debe llevar relación de los usuarios habilitados en cada dispositivo como administradores y superusuarios de los sistemas de información.
3	Profesional o Técnico responsable de administrar algún elemento de la infraestructura de redes de TI.	Revisa necesidades y/o solicitudes de cambios de organización, segmentación, o nuevos accesos entre redes (Vlan, puertos y wifi). En caso de ser necesario activa el Procedimiento Gestión de Cambios y Capacidad Tecnológica – PGTI-08.	Diagramación y documentación de la segmentación de la red de la Contraloría de Bogotá D.C.	

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
4	Profesional o Técnico, responsable de administrar algún elemento de la infraestructura de redes de TI.	Revisa, monitorea y gestiona las conexiones VPN configuradas en el firewall.	Registro de VPN en el Firewall	**Punto de Control** Las VPN activas deben estar aprobadas por la Dirección TIC.
5	Profesional o Técnico, responsable de administrar Directorio Activo.	Revisa y actualiza el directorio activo de la entidad que permitan asegurar el acceso a los servicios de red a los funcionarios activos de la entidad.	Directorio activo actualizado Informe de administración y gestión de conexiones de red.	
6	Profesional o Técnico responsable de administrar algún elemento de la infraestructura de redes de TI.	Revisa las versiones del firmware de los equipos switchs, firewall y controladores de wifi, con el fin de mantener los equipos actualizados con las versiones estables y recientes del fabricante. Actualiza mensualmente el Informe de administración de centro de datos, centros de cableado y gestión de aseguramiento de los servicios de red. Registra los cambios en SICEINFO.	Sistema de Información de Control de Elementos Informáticos SICEINFO. Informe de administración de centro de datos, centros de cableado y gestión de aseguramiento de los servicios de red.	

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
7	Subdirector de Recursos Tecnológicos	Analiza informe de administración de centro de datos, centros de cableado y gestión de aseguramiento y comunica los aspectos relevantes a la Dirección para la toma de decisiones.		

5.6 Transferencia de Información digital.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Servidores públicos de la Contraloría de Bogotá D.C, propietario del activo de información.	Reporta la solicitud de transferencia o transmisión de información, con base en 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	**Observaciones**: Para solicitudes de transferencia de información con entidades externas debe ser solicitado por el jefe de la dependencia propietario de la información. Observaciones: Tener en cuenta los acuerdos de confidencialidad establecidos por la Entidad. Los servidores públicos de la Contraloría de Bogotá D.C, que traten temas o información clasificada como información pública

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				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 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, donde establecerá si 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.
3	Profesional o Técnico 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:** • Establece un acuerdo de transferencia de información con terceros, el cual deberá contener cláusulas donde se establezcan las herramientas a utilizar para asegurar la	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

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		transferencia de información, acuerdo 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. • Medio de envió y autenticación detallada para la transferencia de información. • Tiempo aproximado 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:**		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 detectar algún incidente de seguridad que ponga en riesgo la Información de la Contraloría de Bogotá D.C. La Entidad realizará transferencia de información con organizaciones gubernamentales y privadas, basada en la necesidad planteada por la Contraloría de Bogotá D.C.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		• Valida que esté 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. Pasa a la actividad No 5.		
4	Profesional o Técnico 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 medio 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 o Técnico de la Dirección TIC – responsable de atención de la	**Transferencia de información interna** Realiza las actividades de transferencia de	Registro en el Sistema de	**Observación:** La Dirección de Tecnologías de la Información y las comunicaciones,

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	solicitud (Asignada)	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 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.	Mesa de Servicios	implementará las herramientas, y controles para asegurar la transferencia de información al interior de la Entidad.
6	Profesional o Técnico de la Dirección TIC – responsable de atención de la solicitud (Asignada)	Valida el medio de transferencia. En caso de ser por el protocolo de transferencia de archivos FTP o almacenamiento en la nube o correo electrónico o que la información sea clasificada o reservada. En caso de ser por medio extraíble (USB, disco externo u otro) realiza las actividades del Procedimiento Registro y Atención de	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. El almacenamiento en la nube se debe realizar únicamente en las herramientas institucionales autorizadas.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Requerimientos de Soporte a los Sistemas de Información y Equipos Informáticos – PGTI-04, que apliquen de acuerdo a la naturaleza de la solicitud. Cierra o desactiva los servicios autorizados temporalmente para la atención del requerimiento.		

6. ANEXOS

ANEXO 1. Formato de acceso permanente al centro de datos y los centros de cableado.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato de acceso permanente al centro de datos y los centros de cableado**	Código formato: PGTI-06-01 Versión: 4.0
		Código documento: PGTI-06 Versión 4.0
		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: _____ CÉDULA: _____ CARGO: _____ ADMINISTRADOR DE: _____ TELÉFONO FIJO: _____ TELÉFONO MÓVIL: _____
2	NOMBRE COMPLETO: _____ CÉDULA: _____ CARGO: _____ ADMINISTRADOR DE: _____ TELÉFONO FIJO: _____ TELÉFONO MÓVIL: _____
3	NOMBRE COMPLETO: _____ CÉDULA: _____ CARGO: _____ ADMINISTRADOR DE: _____ TELÉFONO FIJO: _____ TELÉFONO MÓVIL: _____
4	NOMBRE COMPLETO: _____ CÉDULA: _____ CARGO: _____ ADMINISTRADOR DE: _____ TELÉFONO FIJO: _____ TELÉFONO MÓVIL: _____

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 los centros de cableado.

CONTRALORÍA DE BOGOTÁ, D.C.	**Bitácora de acceso a centro de datos y/o los centros de cableado**	Código formato: PGTI-06-02 Versión: 4.0
		Código documento: PGTI-06 Versión 4.0
		Página x de y

FECHA	NÚMERO 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 CÉDULA 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 los centros de cableado.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato de autorización acceso centro de datos y/o los centros de cableado.**	Código formato: PGTI-06-03 Versión: 4.0 Código documento: PGTI-06 Versión: 4.0 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	**Cédula**	**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.
Cédula	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, este 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 dónde 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 los centros de cableado.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato de ingreso y salida de equipos y/o elementos del centro de datos y/o los centros de cableado**	Código formato: PGTI-06-04 Versión: 4.0
		Código documento: PGTI-06 Versión 4.0
		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**		**Ou's Requeridas**	**Ingresa /Salida**
												AMPERIOS	**WATTS**		

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.

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
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 ingresan o salen del centro de datos o centros de cableado.
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 disponibles 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 en el centro de datos y en los centros de cableado.

CONTRALORÍA DE BOGOTÁ, D.C.	**Formato registro de cambios en el centro de datos y en los centros de cableado**	Código formato: PGTI-06-05 Versión: 4.0
		Código documento: PGTI-06 Versión 4.0
		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?

Análisis de Impacto

¿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.

Nombre del campo	Descripción del campo
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-back)	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 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	RR No 047 28 diciembre 2018	Se ajusta el nombre del procedimiento a: Procedimiento Gestión de Seguridad Informática, las Comunicaciones y Criptografía. Lo anterior, teniendo en cuenta que, el Procedimiento Gestión de Seguridad Informática - PGTI-06, se fusionó con el Procedimiento Gestión de Seguridad en las Comunicaciones y Criptografía - PGTI-11, en consideración a que ambos tienen el mismo objeto relacionado con la seguridad informática, por lo tanto, el citado procedimiento PGTI-11 se elimina del listado maestro de documentos, así como sus anexos. En este sentido, se ajusta el Procedimiento PGTI-06, incluyendo los siguientes numerales: 5.6 Aseguramiento de Servicios en la Red. 5.7 Transferencia de Información digital. 5.8 Procedimiento de criptografía. Adicionalmente, se unificaron y optimizaron las actividades del procedimiento, ajustando los responsables, observaciones y puntos de control, para dar mayor claridad al procedimiento y se ajustaron las definiciones.
3.0	R.R No. 016 10 agosto 2020	Se cambia el nombre del procedimiento a: Procedimiento Gestión de Seguridad Informática y las Comunicaciones. Se elimina el numeral 5.7 procedimiento de criptografía, en razón a que se identificó que estas actividades son gestionadas a través de las políticas de seguridad de la información descritas en el numeral 7.5 de las políticas de seguridad de la información dando cumplimento a los

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
		requisitos solicitados en la norma ISO/IEC 27001:2013 en el dominio A10 Criptografía. Se eliminan las definiciones de criptografía, destrucción de llaves criptográficas, expiración de llaves criptográficas, obsolescencia de llaves de cifrado y renovación de llaves criptográficas. En numeral 5.6 Transferencia de Información digital, se elimina en las actividades 3 y 6 los apartes donde hace llamado de actividades del numeral 5.7 Procedimiento de Criptografía.
4.0	R.R No. 013 27 Abril 2021	