CONTRALORÍA DE BOGOTÁ D.C.

Resolución Reglamentaria Número 016

(Agosto 10 de 2020)

"Por medio de la cual se modifican y adopta nuevas versiones de procedimientos del Proceso Gestión de Tecnologías de la Información de la Contraloría de Bogotá, D.C."

LA CONTRALORA DE BOGOTÁ, D.C. (E)
En ejercicio de sus atribuciones constitucionales y legales, en especial las conferidas en el Acuerdo 658 de 2016, modificado parcialmente por el Acuerdo 664 de 2017, expedidos por el Concejo de Bogotá D.C. y

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 de conformidad con 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, la definición de políticas como guías de acción y procedimientos para la ejecución de procesos, así como, la simplificación y actualización de normas y procedimientos.

Que el Acuerdo Distrital 658 de 2016 expedido por el Concejo de Bogotá, D.C., modificado por el Acuerdo 664 de 2017, regula en el artículo 6°, la autonomía administrativa, en virtud de la cual 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 los respectivos Acuerdos.

Que el artículo 40 del precitado Acuerdo, establece las funciones de la Dirección de Tecnologías de la Información y las Comunicaciones, entre otras, correspondiéndole diseñar y proponer la política de uso y aplicación de tecnologías, estrategias y herramientas, para el mejoramiento continuo de los procesos de la Contraloría de Bogotá D.C.; coordinar la aplicación a todo nivel de la organización de los estándares, buenas prácticas y principios para el manejo de la información y desarrollar estrategias para el flujo eficiente de la información en todos los procesos de la entidad.

Que mediante Resolución Reglamentaria No.038 del 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 de 2015 - Decreto Único Reglamentario del Sector de la Función Pública-, con el fin de incorporar la estructura definida en la Dimensión No. 7ª - Control Interno del Manual Operativo del Modelo Integrado de Planeación y Gestión - MIPG.

Que el Decreto 1008 del 14 de junio de 2018, estableció los lineamientos generales de la Política de Gobierno Digital y subrogó el Capítulo 1 del Título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, estableciendo a la Seguridad de la Información como un habilitador transversal de la Política de Gobierno Digital.

Que mediante Resolución Reglamentaria No. 047 del 28 de diciembre de 2018, se adoptó la versión 2.0 del Procedimiento Gestión de Seguridad Informática – PGTI-06 y las versiones 1.0 de los procedimientos: Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información – PGTI-09; Procedimiento Gestión de Incidentes de Seguridad PGTI-10 y del Procedimiento Gestión de Seguridad en las Comunicaciones y Criptografía - PGTI-11.

Que teniendo en cuenta el concepto de mejora, se consideró necesario: i) actualizar las definiciones, base legal, actividades, puntos de control y los formatos de los citados procedimientos; 2) fusionar el Procedimiento Gestión de Seguridad Informática – PGTI-06 con el Procedimiento Gestión de Seguridad en las Comunicaciones y Criptografía - PGTI-11, el cual queda identificado con el nombre de Procedimiento Gestión de Seguridad Informática, las Comunicaciones y Criptografía – PGTI – 06 y 3) eliminar el Procedimiento Gestión de Seguridad en las Comunicaciones y Criptografía - PGTI-11.

RESUELVE:

ARTÍCULO PRIMERO. Adoptar la nueva versión de los siguientes procedimientos del Proceso Gestión de Tecnologías de la Información – PGTI:

No.	Documento	Código	Versión
1	Procedimiento Gestión de Seguridad Informática, las Comunicaciones y Criptografía.	PGTI-06	3.0
2	Procedimiento para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	PGTI-09	2.0
3	Procedimiento Gestión de Incidentes de Seguridad.	PGTI-10	2.0

ARTÍCULO SEGUNDO. Eliminar la versión 1.0 del Procedimiento Gestión de Seguridad en las Comunicaciones y Criptografía - PGTI-11 del Proceso Gestión de Tecnologías de la Información – PGTI.

ARTÍCULO TERCERO. Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina y Gerentes, velar por la administración y divulgación del procedimiento adoptado.

ARTÍCULO CUARTO. La presente Resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias, en especial los numerales 3, 4 y 5 del artículo primero y el numeral 3 del artículo segundo de la Resolución Reglamentaria No. 047 del 28 de diciembre de 2018.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los diez (10) días del mes de agosto del año dos mil veinte (2020).

MARIA ANAYME BARÓN DURÁN
Contralora de Bogotá, D.C. (E)

Aprobación		**Revisión Técnica**
Firma:		
Nombre:	CARMEN ROSA MENDOZA SÚAREZ	ROBER ENRIQUE PALACIOS SIERRA
Cargo:	Directora Técnica	Director Técnico (EF)
Dependencia	Dirección de Tecnologías de la Información y las Comunicaciones.	Dirección de Planeación.
R.R. No.	**Nº. 016**	**FECHA: 10 DE AGOSTO DE 2020**

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 de sistemas de información.

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.

NORMA	FECHA	DESCRIPCIÓN
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 2012.
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014.
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.
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.
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.
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 la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización[3].

Administrador funcional: funcionario con rol administrador que realiza las labores administrativas para el funcionamiento del sistema, se encargará de velar por la oportunidad, consistencia y confiabilidad de los datos, hará el seguimiento al funcionamiento y operación del Sistema y presentará los proyectos de mejoramiento que considere necesarios; entre sus responsabilidades están las siguientes:

- Parametrizar tablas y datos del sistema.
- Monitorear el funcionamiento del sistema.
- Es el responsable de que el sistema se esté utilizando y en operación por todas las áreas que lo deben manejar.
- Garantizar que la información del sistema sea coherente con los procesos y funcionalidades definidas.
- Administrar los usuarios y perfiles del sistema de información.
- Coordinar en los casos que sea necesario con los demás administradores funcionales de los otros sistemas de información, la ejecución de las actividades que puedan tener incidencia en los distintos aplicativos y concerta los correctivos para minimizar su impacto.
- Generar los reportes y crear las estadísticas que permitan evaluar la gestión del sistema de información.

Ambiente de desarrollo: corresponde a la infraestructura de hardware y software necesaria para realizar la implementación del sistema y la ejecución de pruebas unitarias por parte de cada desarrollador, responsable de seguridad y líder funcional.

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.

---

[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.

Entregables: los entregables corresponden a documentos y/o archivos que hacen parte del desarrollo como: Modelo de Datos, Diseños, Pantallas, códigos fuente, scripts, ejecutables, manuales (técnico, usuario, entre otros), reportes e informes, de acuerdo al avance de la implementación.

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: ss 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:
- Validar 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.
- Liderar 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.
- Participar activamente en las etapas y actividades que hacen parte del desarrollo de software en su 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 el 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.
- Garantizar la generación, revisión y aprobación de la documentación técnica requerida para el desarrollo y/o mantenimiento de los sistemas de información.
- Validar que se cumpla con toda la documentación requerida para la entrega a producción de los sistemas de información/aplicaciones nuevas y/o actualizadas.

Manual de administración: documento que presenta una guía de gestión para el rol del administrador del 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 y/o Actualización de sistema de información: conjunto de actividades que implican realizar una modificación al código fuente del sistema de información, se utiliza para:

- Corregir posibles fallas del sistema de información.
- Adicionar nuevas funcionalidades requeridas por un usuario.
- Mejorar el rendimiento y propiedades del sistema de información.
- Comprende los update y upgrade.

Mesa de servicios: es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar requerimientos y/o incidentes relacionados con 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 el 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, Qué, Cuándo y Cómo se debe hacer. La Dirección de Tecnologías de la Información y las Comunicaciones adopta algunos aspectos de la Metodología de Programación Extrema XP para el desarrollo de software de acuerdo con los elementos contentivos en el presente procedimiento para desarrollos internos o los contratados a la medida (llave en mano).

Pruebas: son las que revisan el comportamiento del sistema, subsistema o componente de software.

Requerimiento funcional: describe cualquier actividad que un sistema o software deba realizar, en otras palabras, el comportamiento o función particular necesario 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.

Soporte a sistemas de información: conjunto de actividades que se realizan para:

- Corregir o solucionar gestión de configuración del sistema.
- Cargue y generación de información.
- Corrección de información.
- Actividades de administración del sistema.
- Procesos de documentación del sistema.
- Fallas en la operación del sistema.
- Procesos de recuperación de datos.
- Asistencia a los usuarios sobre las funcionalidades del sistema.
- Conceptos técnicos sobre la operación del sistema.

Viabilidad técnica: hace referencia a aquello que atiende a las características tecnológicas involucradas en un proyecto y el contexto en que se pretenda implementar.

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.	**Fase de exploración** Identifica y registra el requerimiento de la necesidad de un nuevo sistema de información en el aplicativo Mesa de Servicios, adjuntando el formato diligenciado "Solicitud para nuevos Sistemas de	Registro en el sistema de Mesa de Servicios. Solicitud para Nuevos Sistemas de Información PGTI-09-01.	**Observación:** La identificación de la necesidad del nuevo software debe ser conocida por el responsable del proceso relacionado. El solicitante puede, si así lo requiere, solicitar apoyo o explicación a la Dirección de Tecnologías de la

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Información – PGTI-09-01 (anexo 1). Activa Procedimiento Registro y Atención de Requerimientos de Soporte a los Sistemas de Información y Equipos Informáticos PGTI-04.		Información sobre el diligenciamiento del formato. Se deberá seguir lo establecido en el Procedimiento PGTI-04, en lo referente a las actividades de los responsables de Atender Caso Nivel 1, 2, 3 o 4 según corresponda y aplique, hasta el cierre del caso.
2	Subdirector de Gestión de Información.	Analiza la solicitud 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 D.C., existe alguno que cumpla de forma parcial o total con los requerimientos planteados, para lo cual: ✓ **Si existe** Pasa a numeral 5.2 soporte y mantenimiento de sistemas de información, e informa a usuario solicitante.	Registro en el Sistema de Mesa de Servicios identificado mediante el número de caso de Servicio.	**Punto de Control:** Verificar que se incluya 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. **Observación:** Si se adquiere el sistema de información, se activa el Procedimiento Gestión de Recursos y Servicios Tecnológicos PGTI -05 numeral 5.1 Administración de Sistemas de Información o Aplicativos.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		✓ **No existe:** Realiza análisis de viabilidad e informa al usuario solicitante, lo correspondiente a: • **Si se requiere adquisición:** Se activa Procedimiento de Gestión Contractual-PAGF-08, para lo cual la Subdirección de Gestión de Información apoyará la elaboración de las especificaciones o requisitos técnicos de los estudios previos en el proceso precontractual. • **Si se desarrolla Internamente** Asigna Líder Técnico a cargo de la solicitud. Cuando se trate de una encuesta, formulario o desarrollos de similar complejidad continua actividad 11 y 12 solamente.		
3	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina.	Designa Líder funcional a cargo de la solicitud	Comunicación Oficial Interna.	**Punto de Control:** El responsable del proceso según la(s) dependencia(s) que lo requiere(n) debe(n) evaluar el perfil requerido para designar el líder funcional.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
4	Profesional Dirección TIC (Líder Técnico) Profesional Dependencia Solicitante (Líder Funcional) Profesional Dirección TIC (Seguridad de la Información)	**Fase de planificación** Documentan los requerimientos funcionales, técnicos y de seguridad de la información relacionados con la solicitud, diligenciando el formato "*Definición de Requerimientos de Sistema de Información*" - PGTI-09-03 (anexo 3). Presentan definición de requerimientos para ser aprobados.	Acta de Reunión.	**Punto de Control:** Definir las fechas de las reuniones para el desarrollo de las actividades, para la definición de los requerimientos de sistemas de información. **Observación:** Si la solicitud hace parte de un proyecto o una iniciativa en el PETI vigente (Plan Estratégico de Tecnologías de la Información), se documentará de acuerdo a lo establecido en los lineamientos para la Gestión de Proyectos de TI.
5	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.	Definición de Requerimientos de Sistemas de Información PGTI-09-03.	**Observación:** El Jefe de la dependencia solicitante aprueba los requerimientos funcionales. El Subdirector de Gestión de la Información y el Subdirector de Gestión de Recursos Tecnológicos: aprueban los requerimientos técnicos y de seguridad de la información.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
6	Profesional Dirección TIC (Líder Técnico) Técnico Dirección TIC Profesional Dependencia solicitante (Líder Funcional)	Generan y presentan alternativas de solución, respecto a los requerimientos aprobados. Diseñan y construyen modelos, prototipos, diagramas para desarrollo de la aplicación (para los que aplique). Presentan definición de diseño para ser aprobados.	Entregables	**Punto de control:** Analizar 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), licenciamiento, costo, presupuesto, adaptabilidad, escalabilidad y portabilidad, riesgos, modelo de base de datos e interacción con otros sistemas e impacto según se determine.
7	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.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
8	Subdirector de Gestión de Información Subdirector de Gestión de Recursos Tecnológicos Profesional Dirección TIC (Líder Técnico)	Gestionan la creación de ambientes de desarrollo, pruebas y producción para el sistema de información (aplicación, base de datos y recursos necesarios), asigna permisos de acceso a estos e informe. Creación de ambientes de desarrollo, pruebas y producción.	Registro Mesa de Servicios.	**Punto de control:** Aplicar los controles relacionados con desarrollo seguro contemplados en las Políticas de Seguridad de la Información de la entidad. 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.
9	Profesional Dirección TIC (Líder Técnico) Técnico, Profesional Dirección TIC (Desarrollador) Profesional Dependencia solicitante (Líder Funcional)	Establecen cronograma que incluya plan de entregas de la solución, 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)	Cronograma	**Observación:** En caso de que el desarrollo haga parte de una iniciativa establecida en el PETI vigente se deberán ajustar los aspectos que se requieran y apliquen.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
10	Técnico, Profesional Dirección TIC - Desarrollador	**Fase Desarrollo y Producción** Desarrolla acorde al diseño, cronograma y herramientas disponibles en la entidad. 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.	Acta de seguimiento. Entregables.	**Observación:** Considerar las especificaciones establecidas en el Anexo *PGTI-09-07 - "Buenas prácticas de Desarrollo y Estándar de Codificación de Software", si son aplicables.*

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
11	Técnico, Profesional Dirección TIC (Desarrollador, funcionario(s) designado(s) para pruebas de seguridad) Profesional Dirección TIC (Líder Técnico) Profesional Dependencia solicitante (Líder Funcional)	Ejecutan las pruebas. Diligencia el formato "*Pruebas de Sistemas de Información*" (Anexo 4).	Pruebas de Sistemas de Información PGTI-09-04	**Punto de Control:** Ejecutar actividades en ambiente de pruebas. Seleccionar, proteger y controlar cuidadosamente los datos de prueba. 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. **Observación:** Las pruebas se realizan respecto a las especificaciones funcionales aprobadas. En caso de no superar las pruebas el Líder Técnico devuelve resultado de las pruebas al profesional de TIC, que realizó el desarrollo para los ajustes pertinentes.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
12	Director TIC y/o Subdirector de Gestión de Información	Autoriza liberación de paso a producción. Para lo cual dilgencian el formato "*Paso a Producción*" (Anexo 5).	Paso a Producción PGTI-09-05	**Punto de Control:** Verificar que todas las pruebas hayan sido exitosas para autorizar paso a producción. **Observación:** Bajo ninguna circunstancia se autorizará paso a producción sin haber pasado por los ambientes de desarrollo y pruebas.
13	Técnico, Profesional Dirección TIC - Desarrollador	Entrega aplicaciones, reportes, ejecutables, base de datos, parametrización, manuales técnicos y de usuario y/o elementos necesarios para la puesta en producción.	Acta de remisión de entregables.	**Observación:** En la reunión participan los roles de Administrador de Centro de Datos, Profesional que realizará el despliegue y los roles técnicos que participaron en el desarrollo.
14	Profesional Dirección TIC (Administrador de centro de datos y desarrollador) 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*" (anexo 6).	Registro de Aplicación y Sistema de Información (actualizado) PGTI-09-06.	**Punto de control:** Garantizar el almacenamiento seguro y backup de elementos puestos en ambiente de producción.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Informa a Subdirector de Gestión de Información. Almacena copia del sistema en una unidad destinada para este fin. Activa Procedimiento para la Realización y Control de Copias de Respaldo (Backups) PGTI-03.		
15	Director TIC y Subdirector de Gestión de Información	Informa al jefe de la dependencia solicitante, la puesta en producción de la solución. Realiza solicitud para que la solución sea registrada en los inventarios de la entidad.	Comunicación Oficial Interna.	**Punto de control:** Verificar que la solución se registre en los inventarios de la entidad. **Observación:** El responsable del proceso al cual pertenece la dependencia solicitante designa el Administrador Funcional del sistema de información; a partir de ese momento será el responsable del activo de información.

5.2 Mantenimiento y/o Actualización de Sistema de Información

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, Asesor, Profesional, Técnico de la Dependencia solicitante.	Registra requerimiento o necesidad de mantenimiento y/o actualización en el Sistema de Mesa de Servicios. Adjunta a el formato diligenciado "Solicitud para Desarrollo Nuevas Funcionalidades – PGTI-09-02 (anexo 2). Define y documenta con usuario solicitante requerimientos funcionales, técnicos y de seguridad de la información de la solicitud. Activa 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. Solicitud Desarrollo Nuevas Funcionalidades PGTI-09-02.	**Punto de control:** El registro en la Mesa de Servicio lo debe realizar el jefe de la dependencia. **Observación:** Se deberá seguir lo establecido en el Procedimiento PGTI-04, en lo referente a las actividades de los responsables de Atender Caso Nivel 1, 2, 3 o 4 según corresponda y aplique, hasta el cierre del caso.
2	Técnico, Profesional Dirección TIC - Desarrollador	Recibe solicitud de servicio asignada a través de Sistema de Mesa de Servicios. Analizan viabilidad de la solicitud y	Registro en el Sistema de Mesa de Servicios.	**Observación:** El Subdirector de Gestión de la Información solicita al proveedor o contratista

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	(Responsable de atención de la solicitud) Subdirector de Gestión de la Información	determina si se atenderá por la Dirección TIC o requiere ser escalada a proveedor o contratista. Aprueban el desarrollo, en caso de tener requerimientos de infraestructura tecnológica se requiere aprobación de Subdirector de Gestión de Recursos Tecnológicos.		propuesta 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.
3	Técnico, Profesional Dirección TIC - Desarrollador (Responsable de atención de la solicitud)	✓ **Sí es solucionada por funcionario TIC** Evalúa(n) 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. Diseña la solución y la valida con usuario solicitante. Desarrolla la solución. Documenta la solución y genera y/o actualiza– manuales técnicos, administración y de	Entregables.	**Observación:** Considerar las especificaciones establecidas en el Anexo PGTI-09-07 – "*Buenas Prácticas de Desarrollo y Estándar de Codificación de Software", sin son aplicables.*

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		usuario, según aplique. Entrega solución para ejecución de pruebas, actividad 7 del numeral 5.2.		
4	Técnico, Profesional Dirección TIC (pruebas) Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, Asesor, Profesional, Técnico de la Dependencia solicitante.	Utiliza el Formato de Pruebas Sistemas de Información PGTI-09-04. 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 continúa con actividad 6.	Pruebas Sistemas de Información PGTI-09-04	
5	Profesional Dirección TIC - Desarrollador (Responsable de atención de la solicitud)	✓ **Si es escalada a proveedor o contratista:** a. Informa a proveedor o contratista las especificaciones técnicas y/o requerimientos de la solicitud. b. Recibe de Proveedor o Contratista la solución y la documentación.	Registro en la Mesa de Servicios (a. b. d.). c. Pruebas Sistemas de Información PGTI-09-04. Entregables.	**Punto de control:** Informar al Supervisor del Contrato, en el caso de incumplimiento del proveedor o contratista. Aplicar los controles relacionados con desarrollo seguro contemplados en las Políticas de Seguridad de la Información de la entidad.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		c. Ejecuta pruebas y diligencia el formato "*Pruebas de Sistemas de Información*" (Anexo 4). d. En caso de no superar alguna de las pruebas se devuelve a proveedor o contratista para su ajuste.		
6	Profesional 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. Diligencia el formato "*Paso a Producción*" (Anexo 5).	Paso a Producción PGTI-09-05. Entregables.	**Punto de Control:** Verificar que todas las pruebas hayan sido exitosas, para autorizar el paso a producción. El Subdirector de Gestión de Información verificará que bajo ninguna circunstancia se autorice el paso a producción sin haber pasado por los ambientes de desarrollo y pruebas.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
7	Profesional Dirección TIC (Administrador de Centro de Datos y Desarrollador)	Instala en ambiente de producción las aplicaciones para la ejecución de la solución. Informa a Subdirector de Gestión de Información. Actualiza el Sistema de Información en el formato "*Registro de Aplicación y Sistema de Información*" - PGTI-09-06 (anexo 6). Almacena copia de las versiones generadas en un repositorio destinado para este fin. Activa Procedimiento para la Realización y Control de Copias de Respaldo (Backup) PGTI-03.	Registro de Aplicación y Sistema de Información PGTI-09-06.	**Punto de control:** Garantizar el almacenamiento seguro y backup de elementos puestos en ambiente de producción.

5.3 Soporte de Sistema de Información.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, Asesor, Profesional, Técnico de la Dependencia solicitante.	Registra requerimiento o necesidad de soporte en el Sistema de Mesa de Servicios. Activa 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.	**Observación:** Se deberá seguir lo establecido en el Procedimiento PGTI-04, en lo referente a las actividades de los responsables de Atender Caso Nivel 1, 2, 3 o 4 según corresponda y aplique, hasta el cierre del caso.
2	Profesional, Técnico Dirección TIC	Analiza la solicitud. Si la solución implica modificación o corrección del código fuente se debe atender por el numeral 5.2 Mantenimiento del Sistema de Información. Atiende y documenta la solución.	Registro en Mesa de Servicios	**Observación:** En el caso de requerir soporte especializado por parte del proveedor o contratista, éste se documentará en la Mesa de Servicios.

6. ANEXOS

ANEXO 1. Formato de Solicitud para Nuevo Sistema de Información.

	Formato Solicitud para Nuevo Sistema de Información	Código formato: PGTI-09-01 Versión: 2.0 Código documento: PGTI-09 Versión 2.0 Página x de y

Fecha de solicitud		
DD	**MM**	**AA**

Número solicitud **(Corresponde al número de caso en la mesa de servicio – Diligencia TIC)**

INFORMACIÓN 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*
Responsable del proceso	*Nombre responsable del proceso*

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 documentos que consideren necesarios para a mayor claridad de la solicitud*
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 que corresponde al número de caso de la mesa de servicios.
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.
Responsable del proceso	Nombre del responsable del proceso del Sistema Integrado de Gestión (SIG).
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	Adjuntar documentos que consideren necesarios para a mayor claridad de la solicitud.
Observaciones	Indique observaciones del requerimiento.

ANEXO 2. Formato de Solicitud para Desarrollo Nuevas Funcionalidades.

	Formato de Solicitud para Desarrollo Nuevas Funcionalidades	Código formato: PGTI-09-02 Versión: 2.0 Código documento: PGTI-09 Versión 2.0 Página x de y

Fecha de solicitud		
DD	**MM**	**AA**

Número solicitud **(Corresponde al número de caso en la mesa de servicio – Diligencia TIC)**

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...*
Anexos	*Inserte imagen de las pantallas y o reportes de la nueva funcionalidad*
Propuesta a la solución requerida	*Explique el funcionamiento que desea obtener de los campos, botones, columnas, reportes etc.*
¿Se integra con otro aplicativo?, cuál? o afecta algún procedimiento	*¿Diligencie sí la nueva funcionalidad consulta, inserta, elimina o modifica información de otro(s) aplicativo(s), indique en cual(es)?* *Si la funcionalidad afecta algún procedimiento*
Definición de usuarios	*Descripción del perfil y responsabilidades de los usuarios que tendrán interacción con la nueva funcionalidad. Indique roles y perfiles.*

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCION DEL CAMPO
Fecha solicitud	Día, mes, año de la solicitud.
Número solicitud	Corresponde al número de caso en la mesa de servicio – Diligencia TIC.
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.
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.
Anexos	Inserte imagen de las pantallas y o reportes de la nueva funcionalidad.
Propuesta a la solución requerida	Explique el funcionamiento que desea obtener de los campos, botones, columnas, reportes, etc.
¿Se integra con otro aplicativo?, cuál? o afecta algún procedimiento	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.

ANEXO 3. Formato de Definición de Requerimientos de Sistema de Información.

	Formato para la Definición de Requerimientos de Sistema de Información	Código formato: PGTI-09-03 Versión: 2.0 Código documento: PGTI-09 Versión 2.0 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)

Número historia	*No*	**Prioridad**	*Alta/Media/Baja*	**Iteración asignada**	
Fechas proyectadas	**Inicial**		**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 (Mesa de servicios).
DESCRIPCIÓN DE LA SOLICITUD (Historia de usuario)	
Número historia	Número consecutivo que identifica una funcionalidad del sistema de información desarrollar.
Prioridad	Que tan importante es: Alta o Media o Baja.
Iteración asignada	Número consecutivo de cambios o modificaciones que se han realizado a la funcionalidad.
Fecha proyectada inicial	Indique fecha proyectada de inicio de desarrollo.
Fecha proyectada final	Indique fecha proyectada de final de desarrollo.
Título	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:

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
	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 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.

	Formato de Pruebas Sistemas de Información	Código formato: PGTI-09-04 Versión 2.0 Código documento: PGTI-09 Versión 2.0 Página 1 de 1

Fecha de diligenciamiento		Número de solicitud	
Sistema de Información y/o aplicativo		Número historia (en el caso que aplique)	
Nombre Servidor de Pruebas		IP Servidor de Pruebas	

EJECUCIÓN DE PRUEBAS

No	Fecha de la prueba	Número de iteración	Módulo, funcionalidad o componente a probar	Descripción de la prueba	Tipo de prueba	Resultado obtenido	Estado de la prueba	Funcionario que realiza la prueba	Dependencia del funcionario que realiza la prueba	Observaciones y/o Anexos

INSTRUCTIVO DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Fecha de diligenciamiento	Fecha en que apertura el formato
Número solicitud	Corresponde al número de caso de la mesa de servicios de la solicitud asignada en el formato de solicitud de un nuevo desarrollo o funcionalidad.
Sistema de Información y/o aplicativo	Nombre del sistema de información y/o aplicativo
Número de historia (en el caso que aplique)	Número de historia del Formato para la Definición de Requerimientos de Sistema de Información en el caso que aplique.
Nombre Servidor de Pruebas	Nombre del servidor en donde se prueba la aplicación.
IP Servidor de Pruebas	IP del servidor en donde se prueba la aplicación.
Fecha de la prueba	Fecha en que se ejecuta la prueba
Número de Iteración	Número de la iteración del Formato para la Definición de Requerimientos de Sistema de Información en el caso que aplique.
Módulo, funcionalidad o componente a probar	Nombre del módulo, funcionalidad o componente a probar

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Descripción de la prueba	Descripción detallada de la prueba.
Tipo de prueba	Escoja de la lista de opciones el tipo de prueba según corresponda • 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. • 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). • 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. • 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. • 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. • Regresión: Se definen el conjunto de pruebas necesarias para validar qué 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 la manera correcta. • Rendimiento: Se definen el conjunto de pruebas asociadas al rendimiento del software y los mecanismos por los cuales se realizarán estas pruebas. • Seguridad: Se definen el conjunto de pruebas asociadas a la seguridad del software y los mecanismos por los cuales se realizarán estas pruebas. • Unitaria: 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.
Resultado obtenido	Describa que resultado obtuvo de la prueba
Estado de la prueba	Escoja de la lista de opciones el resultado obtenido

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
	• Exitosa • Fallida
Funcionario que realiza la prueba	Nombres y apellidos de funcionario que realiza de la prueba
Dependencia del funcionario que realiza la prueba	Nombre de la dependencia del funcionario que realiza la prueba
Observaciones y/o Anexos	Observaciones de la prueba realizada y definición de los anexos que hacen parte de la prueba.

ANEXO 5. Formato de Paso a Producción.

	Formato de Paso a Producción	Código formato: : PGTI-09-05 Versión 2.0 Código documento: PGTI-09 Versión 2.0 Página X de Y

Número solicitud		**Número historia (en el caso que aplique)**	
Nombres y apellidos Subdirector de Gestión de la Información			
Funcionario responsable puesta en producción			
Sistema de Información o aplicativo		**Módulo**	
Componente/Funcionalidad			

APROBACIÓN PASO A PRODUCCIÓN

Aceptación de pruebas - Funcionarios que realizaron y aprobaron pruebas

Fecha formato pruebas	Número prueba realizada	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 DE DILIGENCIAMIENTO

NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO
Número solicitud	Corresponde al número de caso de la mesa de servicios de la solicitud asignada en el formato de solicitud de un nuevo desarrollo o funcionalidad
Número historia	Número de historia del Formato para la Definición de Requerimientos de Sistema de Información en el caso que aplique
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)
Fecha formato pruebas	Corresponde a la fecha del formato de PGTI-09-04
Número prueba realizada	Corresponde al número asignado en el formato de PGTI-09-04 a la prueba
Nombres y apellidos	Corresponde al nombre y apellidos del funcionario que realizó la prueba
Dependencia	Corresponde a la Dependencia del funcionario que realizó las pruebas
Firma	Firma del funcionario que realizó 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 servidor de alojamiento del componente.
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.

	Formato Registro de Aplicación y Sistema de Información	Código formato: PGTI-09-06 Versión 2.0 Código documento: PGTI-09 Versión 2.0 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		**VERSIÓN ACTUAL**			
SERVIDOR	**Nombre**		**IP**		
MOTOR BASE DE DATOS		**INSTANCIA DE BASE DATOS**			
MÓDULOS					
SISTEMA DE INFORMACIÓN	**Adquirido:**				
	Mantenimiento por:				
	Desarrollado por				

CONTROL DE CAMBIOS Y/O VERSIONAMIENTO						
No.	**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	DESCRIPCIÓN 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	Reléase 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.
Módulos	Nombre del módulo de software o sistema de información (si aplica).
Sistema de Información	Especifique en cada casilla dependiendo si el sistema fue adquirido, si se le realiza mantenimiento, por quien fue desarrollado.
Control de cambios	Especifique por cada cambio que se realice en el sistema, la información de: Número de cambio: Numero consecutivo, enumeración. Módulo: Nombre del módulo al que se le realizo el cambio. Componente: Nombre del componente del sistema. Fecha de implementación: fecha en que se realizó el cambio. Motivación del cambio: Diga porque se realiza el cambio. Versión: Reléase 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. Metodología de Desarrollo, Buenas Prácticas de Desarrollo, Estándar de Codificación de Software y Seguridad de la Información.

	Buenas Prácticas de Desarrollo, Estándar de Codificación de Software y Seguridad de la Información	Código formato: PGTI-09-07 Versión: 2.0 Código documento: PGTI-09 Versión 2.0 Página 1 de 9

1. METODOLOGÍA DE DESARROLLO

Metodología de Programación Extrema XP: Es el 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, Qué, Cuándo y Cómo se debe hacer. La Dirección de Tecnologías de la Información y las Comunicaciones adopta algunos aspectos de la Metodología de Programación Extrema XP para el desarrollo de software de acuerdo con los elementos contentivos en el presente procedimiento para desarrollos internos o los contratados a la medida (llave en mano).

Contempla las siguientes fases:

- **Fase de exploración:** El 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.

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.

2. 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.

2.1 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.

3. ESTÁNDAR DE CODIFICACIÓN DE SOFTWARE

3.1 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 **U**p**d**ateProgress: Ud, esto se debe documentar en comentario.

3.2 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.

3.2.1 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”.

3.2.2 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.

3.3 Nomenclatura de programación

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.

3.3.1 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

3.3.2. 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

3.3.3. Definición de Procedimientos

Nomenclatura: Pascal Case**.**
Nombre: Describe la acción

3.3.4. 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

3.3.5. 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 la 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.

4. 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.

5. PRÁCTICAS DE SEGURIDAD [4]

PRÁCTICAS DE SEGURIDAD A TENER ENCUENTA EN EL DESARROLLO DE SISTEMAS DE INFORMACIÓN
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.

[4] 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.

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 debe 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

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	R.R. No. 047 28-12- 2018	Se ajusta base legal y definiciones. Se unificaron y optimizaron las actividades del procedimiento, ajustando los responsables, observaciones y puntos de control, para dar mayor claridad al procedimiento. Se modificó numeral 5.2 se denomina Mantenimiento y/o Actualización del Sistema de Información. Se adicionó el numeral 5.3 Soporte de Sistemas de Información. Se restructuró los anexos: PGTI-09-01, PGTI-09-02 PGTI-09-03, PGTI-09-04, PGTI-09-05 y PGTI-09-06 con sus respectivos instructivos, para dar mayor claridad a los formatos.
2.0	**R.R. No. 016** **10 – 08 - 2020**	

	PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD	Código formato: PGD-02-05 Versión:11.0 Código documento: PGTI-10 Versión: 2.0 Página 1 de 13

Aprobación		**Revisión Técnica**
Firma:		
Nombre:	CARMEN ROSA MENDOZA SÚAREZ	ROBER ENRIQUE PALACIOS SIERRA
Cargo:	Directora Técnica.	Director Técnico (EF)
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones.	Dirección de Planeación.
R.R. No. 016	**Fecha 10-08-2020**	

1. OBJETIVO

Establecer las actividades para 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), recolección de evidencias y termina con la documentación y solución 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.

NORMA	FECHA	DESCRIPCIÓN
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 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
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.
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 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.

NORMA	FECHA	DESCRIPCIÓN
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 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.
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 la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización[3].

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.

[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.

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.

Evidencia: información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

Incidente de Seguridad[4]: 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.

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.

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

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

5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Gestión de incidentes de seguridad la información.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de Tecnologías de la Información y las 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, Oficial de Seguridad de la Información, 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 responsable 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 D.C. Partes interesadas.	Reporta el evento a través del sistema de mesa de servicio; se activa el Procedimiento de registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos - PGTI-04. En caso que no se tenga acceso a la mesa de servicios, puede realizar el reporte a través de	Sistema de Mesa de Servicios por número de caso	**Observación:** Se deberá seguir lo establecido en el procedimiento PGTI-04, en lo referente a las actividades de los responsables de Atender Caso Nivel 1, 2, 3 o 4 según corresponda y aplique, hasta el cierre del caso.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		cualquier medio de comunicación (telefónico, escrito, correo electrónico, verbal) para que la Dirección de TIC lo registre en el sistema correspondiente.		
3	Profesional o Técnico responsable del Sistema de Mesa de Servicios.	Asigna la solicitud al Líder Seguridad de la Información para atender requerimiento.	Registro en el Sistema de Mesa de Servicios	
4	Profesional Líder Seguridad de la Información.	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. Si el caso no es catalogado como incidente de seguridad de la información, puede recategorizarlo para darle solución definitiva o reasignarlo y finaliza este procedimiento. De lo contrario informa al Oficial de Seguridad de la Información.	Sistema de Mesa de Servicios por número de caso	
5	Profesional Líder Seguridad de la Información y Oficial de Seguridad.	Recolectan la información del incidente e identifica las causas y consecuencias. Clasifican el Incidente tomando como referencia la tabla de clasificación de los incidentes y/o eventos de seguridad (Anexo No. 1).	Sistema de Mesa de Servicios por número de caso Correo electrónico institucional convocatoria sesión equipo CSIRT	**Punto de control:** Verifica los activos de información que puedan ser afectados por el incidente de seguridad. Si el incidente es originado en la ejecución de un contrato, el supervisor del mismo,

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Documentan el Incidente y como resultado de la verificación convoca sesión de Equipo de Respuestas ante Incidentes de Seguridad de la Información (CSIRT) y les remite información documentada del caso.		debe diligenciar la información requerida en el incidente, incluyendo el plan de actividades que va a ejecutar el proveedor.
6	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT).	Realizan análisis del incidente para lo cual: • Revisan la información presentada del incidente. • Determinan las acciones que se deben ejecutar para la gestión y atención del Incidente de Seguridad. • Definen si el incidente puede ser gestionado internamente o se hace necesario el apoyo de un proveedor o Entidad externa y determinan sí es necesario recurrir a una recolección de evidencias, se activa procedimiento 5.2 Recolección de evidencias en incidente de seguridad.	Acta CSIRT	**Observación:** Si es necesario el apoyo de un proveedor para el manejo, se activa del procedimiento PGAF08 - Gestión Contractual. **Punto de Control:** El Director de TIC, junto con los Subdirectores de acuerdo a la clasificación del Incidente, .evalúa y aprueban la realización de las actividades propuestas en la estrategia de atención al incidente.
7	Profesional Líder Seguridad de la Información.	Asigna las tareas en la mesa de servicio a responsables de atención del incidente de seguridad.	Sistema de Mesa de Servicios por número de caso	

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
8	Profesional(es) responsable(s) de la ejecución de actividades para la atención del incidente de seguridad.	Ejecuta acciones y/o actividades necesarias para la: • Contención y mitigación inmediata, buscando minimizar su impacto y salvaguardar la información principal que está siendo afectada. • Erradicación de la causa raíz detectada del incidente de seguridad con el fin de controlar la vulnerabilidad explotada y la amenaza materializada. • Solución y remediación del incidente. • Recuperación o restauración según aplique. En caso de afectación de activo de información TI y de requerirse, activa el numeral 5.2 Restauración de copias de respaldo del Procedimiento para la Realización y Control de Copias de Respaldo (backups) – PGTI-03. Documentación en el sistema de mesa de servicio las acciones ejecutadas.	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: o Proteger la vida y la seguridad de las personas. o Proteger la información confidencial o del ámbito directivo. o Proteger el hardware y software contra el ataque. o Minimizar la interrupción de los procesos y/o sistemas de información.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
9	Profesional Especializado Líder Seguridad de la Información y Oficial de Seguridad.	Comprueban sí el incidente fue solucionado con las acciones ejecutadas. Documentan el caso en la mesa de servicio y en acta CSIRT. Informan a CSIRT que el incidente fue solucionado e indican recomendaciones. Sí la solución no es satisfactoria devuelve a la actividad 8.	Sistema de Mesa de Servicios por número de caso Acta CSIRT	**Observación:** Define la necesidad de convocar a sesión extraordinaria CSIRT según la complejidad de las acciones de atención y solución del incidente. El aprendizaje adquirido en el análisis y solución del incidente se gestionará de acuerdo a los lineamientos definidos por la Dirección de TIC con respecto a la gestión del conocimiento.

5.2 Recolección de evidencias en incidente de seguridad.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director y/o Subdirector TIC	Comunica a Contralor y/o Contralor Auxiliar la necesidad de reportar el incidente de seguridad a entidad externa o autoridad competente.		

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
2	Oficial de Seguridad	Restringe acceso físico /lógico para evitar el acceso al área donde ocurrió el incidente y/o alteración de la posible evidencia. Acompaña a funcionario de entidad externa o autoridad competente en las actividades de recolección y entrega de evidencia. Documenta las acciones ejecutadas. Continúa con los protocolos y/o recomendaciones establecidos por entidad externa o autoridad competente para el trámite de la evidencia.	Acta	**Punto de control:** Las actividades ejecutadas se deben realizar en coordinación y acompañamiento de funcionario(s) responsable(s) de área(s) donde ocurrió el incidente y partes interesadas. **Observación:** Documenta los datos relacionados con la evidencia, entre otros aspectos la siguiente información: • ¿Dónde?, ¿cuándo? y ¿quién? descubrió, recolectó y manejó la evidencia. • ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo?
3	Oficial de Seguridad	Entrega documentación o resultados de la actividad realizada a Comité CSIRT para continuar con procedimiento de gestión de incidentes de seguridad.	Acta y/o documentos soportes entregados por entidad externa o autoridad competente	**Observación:** El Líder de seguridad es el encargado de documentar en la mesa de servicio las acciones realizadas para atender el incidente de seguridad.

6. ANEXOS

ANEXO 1. Clasificación de Incidentes de Seguridad.

La clasificación de los incidentes de seguridad se debe realizar teniendo en cuenta los siguientes aspectos:

- **Impacto**: Establece la afectación del incidente seguridad a los activos de información, procesos, servicios y la importancia de los mismos para la organización.
- **Urgencia**: Define la celeridad de la atención según el retraso o bloqueo que se presente con el incidente de seguridad.
- **Prioridad:** Determina la importancia y los tiempos de respuesta según el impacto y la urgencia del incidente de seguridad.

IMPACTO	
Critico	Se considera crítico, cuando el incidente de seguridad presenta una o más de las siguientes afectaciones: • Afecta la integridad o disponibilidad o confidencialidad de los activos de información para la prestación de servicios al interior de la entidad o hacia la ciudadanía, que impida el cumplimiento de la misionalidad de la Entidad. • Daños a la imagen institucional por esta circunstancia. • Riesgo de demandas penales, económicas. • Riesgo de seguridad de la información. • Afecta la integridad humana.
Alto	Se considera alto, cuando el incidente de seguridad presenta una o más de las siguientes afectaciones: • Afecta la integridad o disponibilidad o confidencialidad de los activos de información para la prestación de servicios al interior de la entidad, que impida el cumplimiento de los objetivos de los procesos institucionales. • Daños a la imagen institucional por esta circunstancia. • Explotación de una vulnerabilidad sin materializar un riesgo de seguridad de la información. • Afecta el cumplimiento de los objetivos de los procesos institucionales.
Medio	Se considera medio, cuando el incidente de seguridad presenta una o más de las siguientes afectaciones: • Afecta la integridad o disponibilidad o confidencialidad de los activos de información no misionales que apoyan a los procesos de la entidad. • De alguna manera afecta los objetivo de los procesos institucionales.
Bajo	Se considera bajo, cuando el incidente de seguridad no afecta o afecta en mínima medida uno o más de los siguientes aspectos: • La integridad o disponibilidad o confidencialidad de los activos de información. • Cumplimiento de los objetivos institucionales. • Daños de imagen institucional. • La integridad humana. • Riesgo de demandas penales o económicas. • Explotación de vulnerabilidades o amenazas. • No hay materialización de riesgo de seguridad de la información.

Tabla No 1: Impacto

URGENCIA	
Inmediato	Presenta bloqueo total
Alto	Presenta bloqueo parcial
Medio	Presenta retraso que no implica bloqueo
Bajo	Mínimo retraso o no hay retraso

Tabla No 2: Urgencia

URGENCIA	IMPACTO			
	Bajo (1)	**Medio (2)**	**Alto (3)**	**Critico (4)**
Inmediato (4)	M	A	C	C
Alta (3)	B	M	A	C
Medio (2)	B	M	M	A
Baja (1)	B	B	B	M

Tabla No 3: Matriz de Prioridad

Prioridad	Tiempo de respuesta (solución) *horas laborales
Bajo (B)	<= 96 horas*
Medio (M)	Entre 32 – 48 horas*
Alto (A)	Entre 17 - 32 horas*
Critico (C)	Entre 0 – 16 horas consecutivas

Tabla No 4: Tiempo de atención según la prioridad

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	RR No 047 28 Diciembre de 2018	Se ajustó el alcance incorporando la recolección de evidencias y se optimizaron las actividades del procedimiento, ajustando los responsables, observaciones y puntos de control, para dar mayor claridad al procedimiento. Se ajustaron las actividades para la evaluación, categorización y clasificación del incidente de seguridad y convocatoria de Equipo CSIRT. Unificación de actividades para atención del incidente. Se crea procedimiento 5.2 Recolección de evidencias en incidente de seguridad y se renumera el procedimiento de Gestión de Incidente de Seguridad. Se ajustó el Anexo No 1, determinando la clasificación del incidente de seguridad según el impacto y urgencia de atención.
2.0	**R.R. No. 016 Fecha 10-08-2020**	

	PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA, LAS COMUNICACIONES Y CRIPTOGRAFÍA	Código formato: PGD-02-05 Versión: 11.0
		Código documento: PGTI-06 Versión: 3.0
		Página 1 de 50

Aprobación		**Revisión Técnica**
Firma:		
Nombre:	CARMEN ROSA MENDOZA SÚAREZ	ROBER ENRIQUE PALACIOS SIERRA
Cargo:	Directora Técnica.	Director Técnico (E)
Dependencia	Dirección de Tecnologías de la Información y las Comunicaciones.	Dirección de Planeación.
R.R. No. 016	**Fecha 10-08-2020**	

1. OBJETIVO:

Establecer las actividades para gestionar los riesgos inherentes para la seguridad de la plataforma tecnológica, servicios informáticos, aseguramiento de los servicios de red y el uso de mecanismos criptográficos 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 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 finaliza con la gestión de las llaves criptográficas.

3. BASE LEGAL:

NORMA	FECHA	DESCRIPCION
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

NORMA	FECHA	DESCRIPCIÓN
		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 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.

NORMA	FECHA	DESCRIPCIÓN
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 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 la misma (sistemas, soportes, edificios, personas...) 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 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, haciendo 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

[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.

aplicativos, bases de datos, servicio de Internet, servicio de Directorio Activo y seguridad perimetral de la Contraloría de Bogotá.

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.

Criptografía: es la técnica de crear información codificada a través de procedimientos o llaves secretas con el objeto de proteger la información y que solo pueda ser descifrada por el destinatario o las personas que posean la clave.

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.

Destrucción de las llaves criptográficas: las llaves de cifrado que se encuentren obsoletas deben ser eliminadas a través de borrado seguro, impidiendo una posible recuperación futura de la misma.

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.

Expiración llaves criptográficas: se presenta cuando se cumple el tiempo máximo de vida útil las llaves de cifrado.

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.

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.

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.

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 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.

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 llaves de cifrado: es la etapa final del ciclo de vida de las llaves de cifrado, cuando caen en desuso sea por expiración o revocación de las llaves.

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.

Revocación de llaves criptográficas: ocurre cuando se detecta compromiso en las llaves de cifrado y para asegurar la integridad de las mismas, procede a su descontinuación inmediata. También se aplica por fuerza mayor (despido, deceso o redefinición de privilegios de usuario, actualizaciones, restructuraciones, entre otros).

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 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 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 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. 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 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 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, teniendo 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 y transmisión de datos, permitiendo 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.	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 y gestión de aseguramiento de los servicios de red, haciendo 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 mantenimiento 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 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 su seguridad, se inicia		

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		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.	

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
4	Profesional o Técnico I, 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 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 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, que traten temas o información clasificada como información pública reservada o información pública clasificada

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				(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 transferencia de información,	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.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		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:** • Valida que esté autorizado por el		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. La Entidad realizará transferencia de información con organizaciones gubernamentales y privadas, basada en la necesidad planteada por la Contraloría de Bogotá.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		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 5.7 – Gestión de Controles Criptográficos de este procedimiento. 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.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
5	Profesional o Técnico 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 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.	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.
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, se inicia las actividades descritas	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

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		en la sección 5.7 – 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 solicitud. Cierra o desactiva los servicios autorizados temporalmente para la atención del requerimiento.		herramientas institucionales autorizadas.

5.7 Procedimiento de criptografía.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, Gerente, (Propietario y/o custodio del activo de información).	Registra solicitud de asignación o revocación mecanismo criptográfico a través de la mesa de servicio, indicando el nombre del funcionario responsable, el (los) activo(s) de información a proteger	Registro en el Sistema de Mesa de Servicios	**Observaciones** Se utilizan los controles criptográficos de cifrado en los siguientes casos: 1. Para almacenamiento, transporte o la transmisión de información Reservada o Clasificada.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		y la justificación de la necesidad. En caso de revocación indicar nombre del responsable y la motivación.		2. En la protección de claves de acceso a sistemas, datos y/o servicios. 3. En la protección de la información a custodiar, cuando así lo establezca el dueño de la información u el Oficial de Seguridad de la Información. 4. El activo de información se encuentre en algún riesgo de seguridad de la información por perdida de confidencialidad. **Punto de control:** El activo de información a proteger debe estar registrado en los instrumentos de gestión de la información pública y categorizado como reservado o clasificado. En caso contrario, se debe anexar a la mesa de servicio la copia de la solicitud radicada ante la dependencia correspondiente de la creación o actualización del registro de activos de información, índice de información clasificada y reservada.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
2	Profesional o Técnico responsable del Sistema de Mesa de Servicios.	Asigna la 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 informáticos PGTI- 04.	Registro en el Sistema de Mesa de Servicios	
3	Profesional o Técnico de la Dirección TIC (Administrador servidor mecanismo criptográfico)	Asigna llaves de mecanismo criptográfico y realiza aprovisionamiento o alistamiento de hardware, software, y demás recursos necesarios. Registra en SICEINFO la instalación de la herramienta criptográfica. O Realiza revocación de llaves según sea la solicitud.	Sistema de Información de Control de Elementos Informáticos SICEINFO por número de placa.	**Punto de Control:** Verifica la disponibilidad de licencias con respecto a numeral 5.2 Administración de licencias de software del Procedimiento Gestión Recursos y Servicios Tecnológicos PGTI- 05. Valida la clasificación en confidencialidad de (los) activo(s) de información a proteger en los instrumentos de gestión de la información pública, en los riesgos de seguridad de la información, según sea el caso, en la copia radicado de creación o actualización del instrumento de información pública, adjunta a la mesa de servicio y define si continúa con la ejecución

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
				del procedimiento o lo finaliza. La vigencia máxima de las llaves de cifrado es de acuerdo a lo establecido en la política de controles criptográfico en las políticas de seguridad de la información.
4	Profesional o Técnico de la Dirección TIC (Administrador servidor mecanismo criptográfico)	Actualiza a estado solucionado en el Sistema de Mesa de Servicios las acciones realizadas que dieron solución o finalización a la solicitud.	Registro en el Sistema de Mesa de Servicios.	
5	Profesional o Técnico de la Dirección TIC (Administrador servidor mecanismo de criptográfico)	Gestiona las llaves criptográficas, según los lineamientos definidos por la Dirección TIC. Controla fechas de expiración, asignación y revocación de las llaves de criptográficas.	Servidor de mecanismo criptográfico.	**Observaciones:** Para la gestión de las llaves criptográficas, se debe tener en cuenta los lineamientos definidos por la Dirección TIC.

6. ANEXOS

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

	Formato de acceso permanente al centro de datos y los centros de cableado	Código formato: PGTI-06-01 Versión: 3.0
		Código documento: PGTI-06 Versión 3.0
		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 los centros de cableado.

	Bitácora de acceso a centro de datos y/o los centros de cableado	Código formato: PGTI-06-02 Versión: 3.0
		Código documento: PGTI-06 Versión 3.0
		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 los centros de cableado.

	Formato de autorización acceso Centro de datos y/o los centros de cableado.	Código formato: PGTI-06-03 Versión: 3.0
		Código documento: PGTI-06 Versión: 3.0
		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 los centros de cableado.

	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: 3.0 Código documento: PGTI-06 Versión 3.0 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**												
Area (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	DESCRIPCION 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.

	Formato registro de cambios en el centro de datos y en los centros de cableado	Código formato: PGTI-06-05 Versión: 3.0
		Código documento: PGTI-06 Versión 3.0
		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**	
Areas 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, serviciosde 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: Día Mes Año	Observaciones:

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	RR No 047 28 Diciembre de 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 Fecha 10-08-2020**	