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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.*

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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

COPIA CONTROLADA

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.*

COPIA CONTROLADA

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)	✓ **Sí 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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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	

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.*

COPIA CONTROLADA

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.

COPIA CONTROLADA

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:

COPIA CONTROLADA

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:***

COPIA CONTROLADA

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:

COPIA CONTROLADA

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.

COPIA CONTROLADA

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

COPIA CONTROLADA

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

COPIA CONTROLADA

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.

COPIA CONTROLADA

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

COPIA CONTROLADA

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.

COPIA CONTROLADA

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						

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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).

COPIA CONTROLADA

- 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.

COPIA CONTROLADA

- ✓ **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.

COPIA CONTROLADA

Reglas de Generación de prefijos:

Determinar el prefijo según las siguientes condiciones:

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

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

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

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

COPIA CONTROLADA

• 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

COPIA CONTROLADA

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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

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

COPIA CONTROLADA

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**	

COPIA CONTROLADA