1. OBJETIVO

Gestionar los incidentes de seguridad de la información que se materialicen al interior de la Entidad, a través de la identificación, atención y respuesta a los mismos con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la Caja de la Vivienda Popular.

2. ALCANCE

Cualquier evento de seguridad que involucre la afectación de la confidencialidad, integridad y disponibilidad de la información de la Caja de la Vivienda Popular de los diferentes activos de información en la entidad y datos personales según la ley 1581 de 2012.

Para aquellos servicios de TI alojados en un tercero contratado, se realizará gestión y seguimiento de los eventos y/o incidentes de seguridad presentados siguiendo los procedimientos definidos por el tercero contratado junto con los ANS acordados.

3. RESPONSABLES

La responsabilidad en la gestión que se realice de los reportes de posibles incidentes de seguridad de la información que se materialicen en la Entidad, se encuentra liderado por el jefe de la Oficina TIC y a su vez del Especialista de seguridad de la información o el que haga de sus veces. Adicional, se deberá involucrar los demás grupos internos de la Oficina TIC que sean necesarios para la atención del incidente que se identifique.

Así mismo, la responsabilidad de la modificación o actualización de este procedimiento está en cabeza del jefe de la Oficina de Tecnología de la Información y las Comunicaciones - TIC.

Responsables adicionales en cumplimiento del procedimiento:

- La Oficina TIC y el Especialista de Seguridad de la Información: Como encargados de velar por el cumplimiento de las actividades y normativas del procedimiento.
- Administradores de los sistemas de información de la Caja de la Vivienda Popular.
- Mesa de Servicios: Como encargado de direccionar los eventos y/o incidentes en seguridad de la información reportados en la herramienta de mesa de servicios y registro completo del incidente reportado en la herramienta para generar la documentación necesaria.
- Proveedor de servicio contratado por la entidad para el hosting de servicios en la nube.
- Responsable de la información: Dado el caso de presentarse incidentes con información institucional, el responsable y/o propietario del activo de información afectado, deberá realizar acompañamiento durante las actividades de gestión y solución del incidente.

4. GENERALIDADES O POLÍTICAS OPERACIONALES

I. Identificación de un incidente de seguridad de la información:

Es todo evento que tienen probabilidad significativa de comprometer la operación normal y/o los servicios misionales prestados por la Caja de la Vivienda Popular, amenazando la triada de la información (confidencialidad y/o integridad y/o disponibilidad), por ejemplo:

- Ocurrió daño o pérdida y robo de información.
- Se presenta exposición, adulteración, pérdida, consulta, uso o acceso no autorizado a los datos personales y/o documentación entregada a la entidad en calidad de custodio de esta información.
- Ocurrió hurto de credenciales o información mediante Phishing.
- Se presentó modificación no autorizada de la información.
- Se presenta un comportamiento anormal de un equipo de cómputo y/o sistema de información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.

- Se presentó pérdida o alteración de registros de base de datos.
- Se presentó una pérdida de un activo de información.
- Hubo presencia de código malicioso “malware, ransomware entre otros”.
- Se presentó una denegación de servicio.
- Se presentó algún ciber-ataque.

II. Responsabilidades:

- ✓ Es responsabilidad de todos los servidores y demás partes interesadas que tengan acceso a los activos de información de la Caja de la Vivienda Popular y evidencien un posible incidente de seguridad de la información, y/o es conocedor de que alguna persona que está violando las políticas de seguridad de la información y/o conoce de riesgos asociados a la información, deberá reportar esta situación a través de la herramienta de mesa de servicios dispuesta en la entidad.

- ✓ Todo reporte de un posible incidente de seguridad de la información debe contener como mínimo los siguientes datos:

  - Nombre del servidor público o tercero que reporta.
  - Teléfono de contacto.
  - Correo electrónico institucional.
  - Descripción del posible incidente de seguridad, esta descripción debe reunir la información que llevó a determinar que es un posible incidente.
  - Indicar datos adicionales para el diagnóstico del incidente como: capturas de pantalla, correos electrónicos, fotografías, videos, archivos entre otros.
  - Fecha y hora del evento reportado.

- ✓ Todo reporte de un posible incidente de seguridad de la información será valorado por la mesa de ayuda, teniendo en cuenta las siguientes consideraciones al momento de realizar la asignación del caso:

  - Relacionar el posible incidente con una afectación en la confidencialidad, integridad y disponibilidad de la información.
  - Reunir información básica (lugar, tipo de información, datos de contacto de la persona que reporta) que llevó a determinar que es un posible incidente de seguridad de la información. Esta Información recopilada podrá ser

utilizada en la investigación y/o para empezar a contener los daños y minimizar el riesgo.
- Esta información se usará para documentar el evento reportado en la herramienta de mesa de servicio.

✓ Todos los incidentes de seguridad de la información deben estar registrados y clasificados en la herramienta de mesa de servicios y asi mismo registrarlos en el formato **208-TIC-FT-34 REGISTRO DE INCIDENTES V1**.

✓ El Especialista de Seguridad de la Información o quien haga sus veces, documentará las acciones adelantadas para tratar el incidente. Se debe diligenciar el formato de registro de incidentes de seguridad de la información que se encuentra en la carpeta de calidad, en el cual se realiza una descripción del incidente, y detalles de cada acción tomada (quién llevó a cabo la acción, cuándo lo hizo y por qué).

✓ El jefe de la Oficina TIC notificará a la Dirección Jurídica los incidentes de seguridad de la información que tengan consecuencias mayores o catastróficas y que requieran trámites jurídicos.

✓ Para los incidentes que se presenten con documentos de archivo físico, se debe tener en cuenta las condiciones de operación y gestión definidas por la Subdirección Administrativa en los documentos: (208-SADM-Mn-05 PROGRAMA DE GESTIÓN DOCUMENTAL -PGD V6, 208-SADM-Pr-19 CONSULTA DE DOCUMENTOS V5 y 208-SADM-Pr-33 RECONSTRUCCION EXPEDIENTES V1).

✓ Es responsabilidad de todos los servidores y demás partes interesadas que tengan acceso a los activos de información de la Caja de la Vivienda Popular reportar cualquier posible incidente de seguridad de la información que se relacione también en materia de **datos personales** de cualquier fuente en donde se cuente con acceso, manejo o uso de esta información.

III. Clasificación de los incidentes de seguridad de la información:

Los incidentes de seguridad de la información en la Caja de la Vivienda Popular serán clasificados así:

Clases de incidentes de seguridad de la información	Descripción de la causa raíz	Ejemplo
Incidente de desastre natural	Por desastres naturales fuera del control humano.	Terremotos, erupciones volcánicas, inundaciones, huracanes, tormentas eléctricas, incendio forestal, tsunamis, derrumbes, etc.
Incidente de daño físico	Debido a acciones físicas accidentadas o intencionales en las instalacionesde la CVP.	Incendio, agua, ambiente nefasto (contaminación, polvo, corrosión, congelamiento), destrucción de equipos, destrucción de medios, robo de equipos, robo de medios, etc.
Incidente de fallas de infraestructura tecnológica	Generado por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información y servicios de TI en la CVP.	Fallas en la alimentación eléctrica, en las redes, en el aire acondicionado, fallas de hardware, etc.
Incidente de código malicioso	Causas asociadas de programas maliciosos creados y/o divulgados en forma intencional.	Virus informáticos, gusanos de red, troyanos, malware, botnet (red de robots), ataques combinados, páginas web con códigos maliciosos, sitio hosting con códigos maliciosos, etc.

Incidente de ataque técnico	Resultado de ataques a sistemas de información, a través de redes u otros medios técnicos, mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, que genera un estado anormal de los sistemas de información.	Aprovechamiento de puertas traseras, aprovechamiento de vulnerabilidades informáticas, denegación de servicios, escaneo de redes, intentos de ingreso, interferencia, etc.
Incidente relacionado con contenidos peligrosos	Por causas asociadas de propagación de contenido indeseable a través de redes de información, lo que pone en peligro la seguridad nacional, la estabilidad social y/o la seguridad y beneficios públicos.	Contenido ilegal, contenido que provoca pánico, contenido malicioso, contenido abusivo, etc.
Incidente de puesta en riesgo de la información	La pérdida de seguridad de la información es causada al poner en riesgo en forma accidental o intencional la confidencialidad, integridad y disponibilidad de la información.	Interceptación, espionaje, interceptación ilegal de llamadas telefónicas, divulgación, enmascaramiento, ingeniería social, phishing de redes (Suplantación de identidad), robo de datos, alteración de datos, errores de datos, etc.
Incidente por uso indebido de recursos de TI	Debido al uso no autorizado de recursos y violación de derechos de autor.	Uso de recursos de acceso para propósito no autorizado, por ejemplo, el uso del correo para participar en cadenas ilegales, pirámides, etc. Causada por la venta e instalación de copias de software sin licencia, u otros materiales protegidos por derechos de autor.

IV. Evaluación de niveles de criticidad del incidente:

Se definen niveles de criticidad de acuerdo con niveles de afectación de activos de información y posibles interrupciones en la normal operación de la entidad así:

Nivel	Descripción
Alto	Afecta diferentes activos de información que son considerados de impacto catastrófico que contribuyen directamente sobre los objetivos misionales de la entidad. Adicional son incluidos aquellos incidentes que afecten la reputación y buen nombre de la entidad y que a su vez involucren aspectos legales.
Medio	Afecta por poco tiempo los procesos generales de la entidad, el incidente/evento compromete un activo importante o activos que influyen en los objetivos de los procesos de la entidad.
Bajo	No afecta el normal funcionamiento de la entidad; el incidente/evento se detecta y puede ser controlado con recursos existentes en la entidad que impida el cambio del impacto que genere el incidente.

En caso de que el incidente de seguridad de la información se considere de prioridad alto, el Especialista de Seguridad de la Información o quien haga sus veces de la CVP deberá proponer el equipo que participará en el tratamiento del incidente y este será aprobado por el jefe de la Oficina TIC.

Los incidentes de seguridad de la información que no se consideren prioridad alto estarán liderados por el Profesional de Seguridad de la Información o quien haga sus veces en apoyo con los demás grupos internos de la oficina TIC que sean requeridos por la mitigación del incidente materializado.

V. Niveles de escalamiento:

De acuerdo con el análisis, evaluación y valoración del incidente reportado, su criticidad o afectación, se prevén niveles de escalamiento tanto internos como externos.

Prioridad	Escalamiento
Alto	Autoridades competentes (CSIRT Gobierno, CSIRT policía nacional, Alta Consejería Distrital de las TIC, COLCERT) y proveedores de servicio pertinentes.
Medio	Se escala al equipo de la Oficina TIC y/o a las dependencias involucradas.
Bajo	Se documenta el incidente/evento en la herramienta de mesa de ayuda y se escala al administrador del servicio Tic correspondiente. En caso de ser necesario, se contacta al propietario del activo de información involucrado.

5. DEFINICIONES Y SIGLAS

Activo de información: Elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. En su sentido más amplio, éstos hacen referencia a la información que se recibe, transforma y produce en la entidad u organismo distrital en el cumplimiento de sus funciones.

Clasificación: es la identificación y agrupamiento de características que presentan los incidentes de seguridad de la información para determinar el tratamiento de este.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por una persona, área o entidad autorizada. Un documento disponible es aquel que puede ser localizado, recuperado, presentado e interpretado. Su presentación debe mostrar la

actividad u operación que lo produjo.

Evento de seguridad de la información: presencia identificada de una condición en un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Información: Conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos. La integridad de un documento hace referencia a su carácter completo e inalterado. Es necesario que un documento este protegido contra modificaciones no autorizadas

Incidente de seguridad de la información: evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y afectar la seguridad de la información.

Registro: Documento que presenta resultados obtenidos o proporciona evidencia de actividades ejecutadas.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad.

6. DESCRIPCIÓN DE ACTIVIDADES

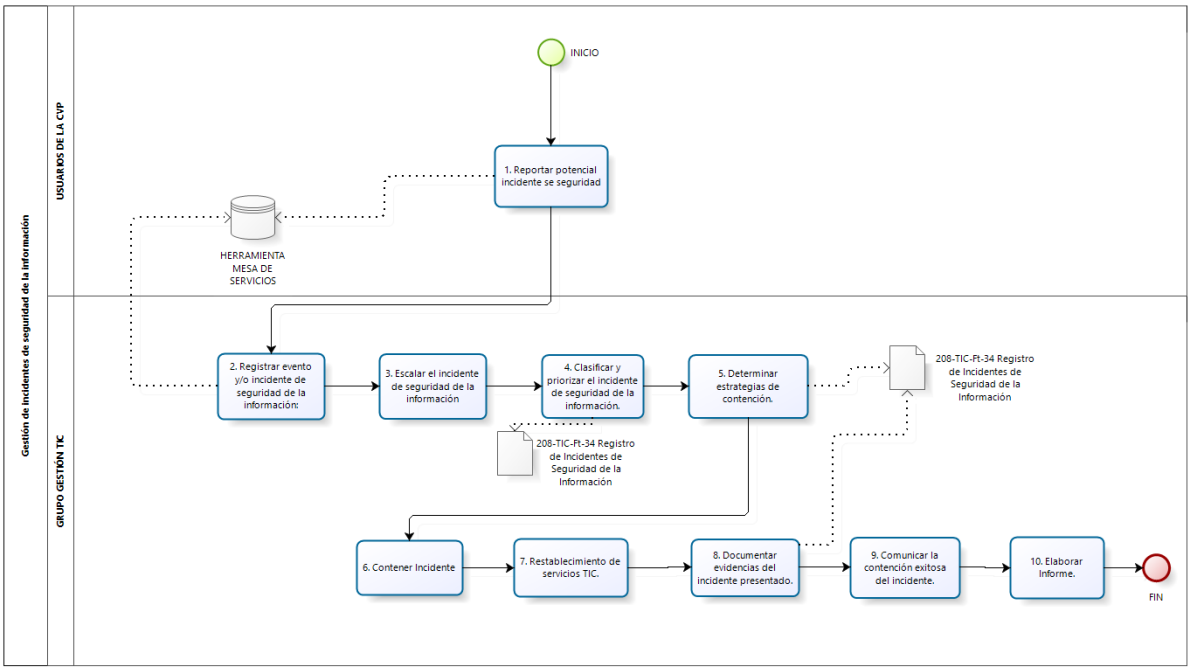
N°	Actividad y Descripción	Responsable	Registros
1	**Reportar potencial incidente se seguridad:** Los funcionarios, contratistas y demás partes interesadas, que tengan acceso a información de la entidad y evidencien un ataque a los activos de información de la entidad, y/o es conocedor de que alguna persona está violando las políticas de seguridad de la información y/o conoce de riesgos asociados a la información, deberá reportar esta situación como un evento o incidente de seguridad de la información a través de la herramienta de mesa de servicios o mediante el correo institucional soporte@cajaviviendapopular.gov.co.	Usuarios de la CVP	Correo institucional Herramienta mesa de servicios
2	**Registrar evento y/o incidente de seguridad de la información:** La mesa de ayuda registrará en la herramienta de mesa de ayuda el evento y/o incidente de acuerdo con la información suministrada.	Agente mesa de servicios y/o Profesional oficina TIC	Herramienta mesa de servicios y/o Correo institucional
3	**Escalar el incidente de seguridad de la información:** Asignar requerimiento de servicio al profesional de seguridad de la información o el que haga de sus veces para la evaluación del evento y/o incidente reportado; determinando así, la afectación de activos de información, alcance de afectación, probabilidad de expansión e impactos potenciales a la entidad para	Agente mesa de servicios y/o profesional de la oficina TIC	Herramienta mesa de servicios y/o Correo institucional

	determinar su mitigación. Así mismo, el profesional de la oficina TIC encargado de administrar el correo soporte@cajaviviendapopular.gov.co, escalara el evento reportado al especialista en seguridad de la información para su respectiva atención de ser requerido.		
4	**Clasificar y priorizar del incidente de seguridad de la información:** Evaluar el incidente de acuerdo con las políticas operacionales del procedimiento y demás documentos que de apoyo en el inicio de la evaluación y categorización del nivel de criticidad del incidente haciendo uso del formato 208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información.	Especialista en seguridad de la información	Correo institucional 208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información
5	**Determinar estrategias de contención:** Establecer las estrategias para la contención del incidente de seguridad de información presentado, su erradicación y recuperación de los servicios afectados o que requieran reanudación de actividades. Con base en la clasificación del incidente realizada en la actividad anterior. Nota: De requerirse efectuar cambios en la plataforma tecnológica de la entidad en pro a la mitigación del incidente, se hará llamado al procedimiento *208-TIC-Pr-14 GESTIÓN DE CAMBIOS DE LA PLATAFORMA TECNOLÓGICA* y ejecutar las actividades correspondientes.	Jefe Oficina TIC Especialista en seguridad de la información	Correo institucional 208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información
6	**Contener Incidente:**	Jefe Oficina TIC	Correo institucional.

	Contener el incidente con el fin de mitigar el impacto de la afectación y disminuir los daños en la plataforma tecnológica. Adicional se deben efectuar las siguientes actividades: • Aislar el activo o elemento afectado. • Realizar el apagado de ser requerido el sistema afectado. • Bloquear servicios afectados incluyendo las diferentes segmentaciones de red • Evaluar la posibilidad de implementar controles adicionales mientras está en curso el incidente. • Solicitar apoyo de terceros especializados, proveedores de servicio. • Reportar ante las entidades competentes (CSIRT Gobierno, CSIRT policía nacional, Alta Consejería Distrital de las TIC, COLCERT) • Reportar a la alta gerencia de la Caja de la Vivienda Popular el incidente materializado y funcionarios de la entidad. Nota: De ser requerido, se hará llamado al procedimiento de copias de seguridad y restauración del proceso GTIC de la CVP.	Administrador de sistemas de información DBA Administrador de red institucionales Especialista en seguridad de la información	Herramienta mesa de servicios
7	**Restablecimiento de servicios TIC:** Realizar la erradicación y eliminación de cualquier rastro dejado por el elemento que generó el incidente de seguridad donde se realicen las siguientes actividades: • Restauración del servicio caído. • Corrección de efectos producidos. • Restauración de backups.	Administrador de sistemas de información DBA	Herramienta de mesa de servicios Formato TIC Incidente

	• Reparar el sitio web. • Re-instalación del equipo (PC, servidor o equipo activo de red) y recuperación de datos.	Administrador de red institucionales Especialista en seguridad de la información	
8	**Documentar evidencias del incidente presentado:** Recopilar y documentar las evidencias producto de la investigación del incidente, las cuales son registradas en el formato de registro de incidentes de seguridad de la información.	Especialista en seguridad de la información	Herramienta mesa de servicios 208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información
9	**Comunicar la contención exitosa del incidente:** Comunicar a los funcionarios de la entidad la mitigación exitosa del incidente de seguridad de información presentado y la reanudación de los servicios TIC.	Jefe Oficina TIC Especialista en seguridad de la información	Correo institucional
10	**Elaborar Informe:** Generar informe del incidente de seguridad materializado en la entidad para presentarse al jefe de la oficina TIC y posterior comunicarlo a las áreas interesadas que se vieron involucradas en el incidente acontecido.	Especialista en seguridad de la información	Informe Incidente de seguridad
Fin del procedimiento			

7. DIAGRAMA DE FLUJO



8. PUNTOS DE CONTROL

Se deben identificar las actividades sujetas de control indicando qué se controla, con qué frecuencia, quién lo controla, entre otros. Los puntos de control son los momentos en el desarrollo del procedimiento, en los que se realiza validación, revisión, verificación, supervisar, entre otros; de lo actuado hasta ese momento.

N° Actividad	Actividad	¿Qué y cómo se controla?	¿Con qué frecuencia?	¿Quién lo controla?
1	Reportar potencial incidente se seguridad.	Atención oportuna de posibles incidentes de información en la CVP.	Por cada solicitud recibida	Especialista en seguridad de la información

3	Escalar el incidente de seguridad de la información.	Identificar el impacto del posible incidente de seguridad en los activos de TI.		Agente mesa de servicios y/o profesional de la oficina TIC
4	Clasificar y priorizar el incidente de seguridad de la información.	Prevenir la afectación total de los servicios de TI junto con los activos de información de la CVP.		Especialista en seguridad de la información
6	Contener el incidente.	Afectación de servicios TI y los activos mediante el plan de acción definido para el incidente materializado	Por cada materialización de un incidente de seguridad de información	
7	Restablecimiento de servicios TIC.	Integridad, seguridad y disponibilidad de los activos de información de la CVP junto con los servicios de TI		Especialista en seguridad de la información grupo de gestión TIC (según lo defindio en el item 3 responsables)
9	Comunicar la contención exitosa del incidente		Por cada mitigación realizada en materia de incidentes de seguridad de la información	Jefe Oficina TIC – Especialista seguridad de la información

9. DOCUMENTOS RELACIONADOS

9.1 Normograma

- Ver Normograma de la oficina TIC publicado en \\10.216.160.201\calidad\SGC\14. PROCESO GESTIÓN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES\1. CARACTERIZACION\1.2 NORMATIVIDAD

9.2 Documentos Internos

- Ver Listado Maestro de Información Documentada o Listado Maestro de Documentos

9.3 Formatos Asociados

- 208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información.

9.4 Documentos Externos

Nombre del Documento	Fecha de publicación o versión del documento	Entidad que lo emite	Ubicación
N/A.	N/A.	N/A.	N/A.

10. CONTROL DE CAMBIOS

Versión	Fecha Aprobación (dd-mm-aaaa)	Cambios	Revisó Nombre y Cargo Líder del Proceso
01	23-12-2019	Creación del procedimiento	Andrés Orlando Briceño Díaz- Jefe Oficina TIC
02	21-11-2022	Se realizan los siguientes ajustes al procedimiento: • Objetivo. • Alcance. • Responsables. • Políticas o generalidades operacionales. • Definiciones. • Descripción de actividades del procedimiento: En este punto, se realiza la separación de las actividades de copias de seguridad y restauración de copias de seguridad. Generando subprocesos de acuerdo con las actividades de restauración que lo ameritan para identificar la aplicabilidad de actividades durante el procedimiento. • Modelado de las actividades de los procedimientos y subprocesos en la herramienta Bizagi. • Puntos de Control según el caso. • Control de cambios. • Actualización de la plantilla vigente para procedimientos del SGC en la entidad aprobado por la OAP.	Luz Yamile Reyes Bonilla – Jefe Oficina TIC

11. APROBACIÓN

ELABORADO	REVISADO	APROBADO
Nombre: Fabian David Rojas Castiblanco **Cargo:** Contratista Oficina TIC **Fecha: 28-06-2022**	**Nombre:** Miguel Angel Cepeda Duarte **Cargo:** Contratista Oficina TIC **Fecha: 28-06-2022** **Nombre:** Gustavo Adolfo Beltrán **Cargo:** Contratista Oficina TIC **Fecha: 25-11-2022**	**Nombre:** Luz Yamile Reyes Bonilla **Cargo:** Jefe Oficina TIC **Fecha: 28-11-2022**

Este documento fue revisado por parte de la Oficina Asesora de Planeación frente a la estructura del documento y cumplimiento de los lineamientos del SIG conforme a lo establecido en el numeral 4 del procedimiento control de la información documentada: 02/12/2022