Firmado Electronicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 1 de 10

SECRETARÍA DE INTEGRACIÓN SOCIAL

FOR-GD-005

CIRCULAR Nº 030 29 JUN 2021

PARA: Subsecretario, Jefe Oficina Asesora de Comunicaciones, Jefe Oficina Asesora Jurídica, Jefe de Control Interno y Jefe Oficina de Asuntos Disciplinarios, Directora de Gestión Corporativa, Directora de Análisis y Diseño Estratégico, Director Territorial, Directora Poblacional, Director de Nutrición y Abastecimiento.

DE: Secretaria Distrital de Integración Social

ASUNTO: Actualización del Sistema de Gestión

A continuación, se describen las nuevas directrices que deben ser conocidas e implementadas a partir de la fecha por sus equipos de trabajo, en aquellas acciones que involucren a su dependencia como instancia responsable:

a) Procedimiento del proceso Gestión de talento humano:

	Justificación	**Aprobó**
1. PCD-TH-020 Procedimiento Expedición de certificados laborales, versión 0.	Se requiere la creación del procedimiento en cumplimiento de lo establecido en el mapa de riesgos de corrupción del Proceso Gestión de Talento Humano.	Subdirectora de Gestión y Desarrollo del Talento Humano en condición de líder del proceso Gestión de Talento Humano, mediante memorando I2021018191 del 21/06/2021.

Firmado Electrónicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 2 de 10

b) Procedimientos del proceso Gestión de soporte y mantenimiento tecnológico:

	Justificación	Aprobó
2. PCD-SMT-006 Procedimiento Gestión de incidentes de tecnologías de la información, versión 0. 3. PCD-SMT-008 Procedimiento Gestión de requerimientos de tecnologías de la información, versión 0. 4. PCD-SMT-012 Procedimiento Gestión incidentes de seguridad de la información, versión 0.	Actualización de los documentos por cambios en el mapa de procesos de la Entidad.	Subdirector de Investigación e Información en condición de líder del proceso Gestión de soporte y mantenimiento tecnológico, mediante memorando I2021017399 del 11/06/2021.

c) Riesgo del proceso Gestión de soporte y mantenimiento tecnológico:

Riesgo de corrupción	Justificación	Aprobó
5. RC-SMT-001 Posibilidad de un mal uso de las credenciales asignadas para la administración de los recursos tecnológicos de la Entidad con el fin de obtener un beneficio propio o para terceros (actualización).	En el Riesgo de Corrupción del proceso SMT, se realiza un cambio en el indicador de la primera actividad de control. Quedando así de la siguiente manera: (Número de cambios realizados en los ambientes de producción / Total de cambios solicitados en los sistemas de información) * 100	Subdirector de Investigación e Información en condición de líder del proceso Gestión de soporte y mantenimiento tecnológico, mediante memorando I2021018615 del 24/06/2021.

Firmado Electrónicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 3 de 10

Riesgos de seguridad digital. 6. RS-SMT-001 Pérdida de Confidencialidad, Integridad y Disponibilidad de los activos de información (creación). 7. RS-SMT-002 Pérdida de Integridad y Disponibilidad de los activos de información (creación). 8. RS-SMT-003 Pérdida de Integridad de los activos de información (creación).	Como una mejora continua, se identifica la necesidad de crear los riesgos de Seguridad Digital con base en los activos de información críticos de la entidad	Subdirector de Investigación e Información en condición de líder del proceso Gestión de soporte y mantenimiento tecnológico, mediante memorando I2021018615 del 24/06/2021.

d) Riesgos del proceso Gestión contractual:

Riesgos de corrupción:	**Justificación**	**Aprobó**
9. RC-GEC-001 Posibilidad de direccionar la contratación y/o vinculación a favor de un tercero no presentando claridad tanto en los anexos técnicos como en los estudios previos que posibilitan que la selección de proveedores no se realice de forma eficiente y transparente (actualización).	La actividad de control se decidió modificar a la siguiente: El líder del proceso de Gestión Contractual cita y lidera los comités de contratación cuando requiera de ello, con el objetivo de asesorar a las diferentes dependencias en las etapas precontractual, contractual y post contractual para satisfacer las necesidades misionales y transversales de la entidad, así como en materia de políticas y de buenas prácticas en la contratación pública.	Subdirectora de Contratación en condición de líder del proceso Gestión contractual, mediante memorando I2021017626 del 15/06/2021.

Firmado Electrónicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 4 de 10

10. RC-GEC-002 Posibilidad de que se realice una supervisión e interventoría inadecuada por un interés ilícito en su ejercicio a través de la manipulación u omisión de funciones en beneficio del contratista o de un tercero (actualización).	La actividad de control se decidió modificar a la siguiente: El líder del proceso de Gestión Contractual socializa semestralmente con los diferentes supervisores o apoyos a las supervisiones, las directrices y lineamientos oficiales y vigentes referente a la contratación institucional, así como los posibles incumplimientos cuando a ello hubiere lugar, según lo evidenciado en la supervisión.	Subdirectora de Contratación en condición de líder del proceso Gestión contractual, mediante memorando I2021017626 del 15/06/2021.
Riesgos de gestión: 11. R-GEC-002 Pérdida de información en los expedientes que soportan la ejecución del proceso contractual (actualización).	El riesgo se cambia de la siguiente manera: Pérdida de información en los expedientes que soportan la ejecución del proceso contractual. También se cambia una de las actividades de este riesgo.	
12. R-GEC-003 Posible retraso en la actualización de las directrices oficiales para la modernización del proceso de contratación (creación).	Se crea un tercer riesgo: Posible retraso en la actualización de las directrices oficiales para la modernización del proceso de contratación.	

Firmado Electronicamente con AZSign
Acuerdo: 20210702-110403-c38430-758707 47
2021-07-07T10:18:42-05:00 - Pagina 5 de 10

e) Riesgo del proceso Gestión de infraestructura física:

Riesgo de corrupción:	Justificación	Aprobó
13. RC-GIF-001 Probabilidad de emitir la viabilidad de equipamientos para ser tomados en arriendo en predios que no cumplen las condiciones técnicas mínimas exigidas por la SDIS, con el fin de beneficiar intereses particulares (actualización).	Se hace necesario ajustar la redacción del control del riesgo en cuanto al propósito del mismo, de acuerdo a las recomendaciones emitidas por la OCI en el marco del primer seguimiento.	Subdirector de Plantas Físicas (E) en condición de líder del proceso Gestión de infraestructura física, mediante memorando I2021018298 del 22/06/2021.

Así mismo, se informa que las siguientes directrices quedan sin efecto, razón por la cual deben dejarse de aplicar y retirarse de todos los puestos de trabajo de sus dependencias, por haber sido declaradas obsoletas por las instancias competentes:

f) Procedimientos del proceso Mantenimiento y Soporte TIC:

	Justificación	Derogó
13. PCD-MS-002 Procedimiento Gestión de Incidentes de Seguridad de la Información, versión 1. 14. PCD- MS-003 Procedimiento Gestión de incidentes de TI, versión 0.	Derogación de los documentos en el proceso Mantenimiento y Soporte TIC y creación en el proceso Gestión del Soporte y Mantenimiento Tecnológico.	Subdirector de Investigación e Información en condición de líder del proceso Mantenimiento y Soporte TIC, mediante memorando I2021017399 del 11/06/2021.

Firmado Electronicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 6 de 10

g) Riesgos del proceso Tecnologías de la información:

16. Mapa de riesgos de seguridad digital: 16.1 Daños o pérdida de la información. 16.2 Fuga o daño de información por acceso de usuarios no autorizados. 16.3 Fuga o daños de la información. 16.4 Fuga o robo de información. 16.5 Mal uso de los servicios tecnológicos. 16.6 Incumplimiento a la política de propiedad intelectual. 16.7 Indisponibilidad de la información.	**Justificación**	**Derogó**
	Se deroga el presente riesgo de seguridad Digital dado que el mismo se mitiga al no ser materializado por una acción en el pasado. Por otro lado, como una mejora continua, se identifica la necesidad de actualizar los riesgos de Seguridad Digital con base en los activos de información críticos de la entidad.	Subdirector de Investigación e Información en condición de líder del proceso Tecnologías de la información, mediante memorando I2021018615 del 24/06/2021.

Firmado Electronicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 7 de 10

Las directrices expedidas mediante la presente circular harán parte del manual del SG y deben tenerse en cuenta en los ejercicios de inducción y reinducción ordenados por el instructivo I-TH-PR-006 del proceso Gestión de Talento Humano, dado que podrían ser aplicables al puesto de trabajo de las personas vinculadas a sus dependencias.

Xinia Rocío Navarro Prada
Secretaria Distrital de Integración Social

Aprobó: Julian Torres Jimenez, Director de Análisis y Diseño Estratégico.

Revisó: Diana Larisa Caruso Lopez, Subdirectora de Diseño, Evaluación y Sistematización.
Nidia Carolina Parra Osorio, Contratista apoyo.

Elaboró: Viviana Lucia Mendoza Hortua, Contratista Subdirección de Diseño, Evaluación y Sistematización.
Andres Camilo Gómez Cardoso, Contratista Subdirección de Diseño, Evaluación y Sistematización.
Sofy Lorena Arenas Vera, Contratista Subdirección de Diseño, Evaluación y Sistematización.
David Andres Moncayo Nastar, Contratista Subdirección de Diseño, Evaluación y Sistematización.

Anexos: Cuatro (4) procedimientos, tres (3) matrices de riesgos de corrupción, una (1) matriz de riesgos de gestión y una (1) matriz de riesgos de seguridad digital.

Firmado Electronicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 8 de 10

REGISTRO DE FIRMAS ELECTRONICAS

20210629_Circular_SG_030_jun_extra

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20210702-110403-c38430-75870747 Creación: 2021-07-02 11:04:03

Estado: Finalizado Finalización: 2021-07-07 10:18:40

Escanee el código para verificación

Elaboración: Elaboró:

Viviana Lucia Mendoza Hortua

vmendoza@sdis.gov.co
Contratista Subdirección de Diseño, Evaluación y Sistematización

Elaboración: Elaboró:

Andrés Camilo Gómez Cardoso
1022348378
acgomezc@sdis.gov.co
Contratista
Subdirección de Diseño, Evaluación y Sistematización

Elaboración: Elaboró:

Sofy Lorena Arenas Vera
52919133
sarenasv@sdis.gov.co
Contratista Subdirección de Diseño, Evaluación y Sistematización
Secretaria Distrital de Integración Social

Elaboración: Elaboró:

David Andres Moncayo Nastar

dmoncayo@sdis.gov.co
Contratista Subdirección de Diseño, Evaluación y Sistematización

Firmado Electronicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 9 de 10

REGISTRO DE FIRMAS ELECTRONICAS

20210629_Circular_SG_030_jun_extra

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20210702-110403-c38430-75870747 Creación: 2021-07-02 11:04:03

Estado: Finalizado Finalización: 2021-07-07 10:18:40

Escanee el código para verificación

Firma: Firmante:

XINIA ROCIO NAVARRO PRADA

XNavarro@sdis.gov.co
Secretaria Distrital de Integración Social

Aprobación: Aprobó:

JULIAN TORRES JIMENEZ
79751506
jtorresj@sdis.gov.co
DIRECTOR DE ANALISIS Y DISEÑO ESTRATÉGICO
SECRETARIA DISTRITAL DE INTEGRACION SOCIAL

Revisión: Revisó:

Diana Larisa Caruso López

dcaruso@sdis.gov.co
Subdirectora Diseño, Evaluación y Sistematización
SDIS

Revisión: Revisó:

Nidia Carolina Parra Osorio
1019006751
nparrao@sdis.gov.co
Contratista Apoyo
SDIS

Firmado Electrónicamente con AZSign
Acuerdo: 20210702-110403-c38430-75870747
2021-07-07T10:18:42-05:00 - Pagina 10 de 10

REPORTE DE TRAZABILIDAD

20210629_Circular_SG_030_jun_extra

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20210702-110403-c38430-75870747 Creación: 2021-07-02 11:04:03

Estado: Finalizado Finalización: 2021-07-07 10:18:40

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	David Andres Moncayo Nastar dmoncayo@sdis.gov.co Contratista Subdirección de Diseño, Evaluación y Sis	Aprobado	Env.: 2021-07-02 11:04:04 Lec.: 2021-07-02 11:05:11 Res.: 2021-07-02 11:06:30 IP Res.: 181.54.241.185
Elaboración	Sofy Lorena Arenas Vera sarenasv@sdis.gov.co Contratista Subdirección de Diseño, Evaluación y Sis Secretaria Distrital de Integración Social	Aprobado	Env.: 2021-07-02 11:06:30 Lec.: 2021-07-02 12:12:01 Res.: 2021-07-02 12:12:07 IP Res.: 191.156.136.246
Elaboración	Andrés Camilo Gómez Cardoso acgomezc@sdis.gov.co Contratista Subdirección de Diseño, Evaluación y Sistematización	Aprobado	Env.: 2021-07-02 12:12:07 Lec.: 2021-07-02 12:29:01 Res.: 2021-07-02 12:29:52 IP Res.: 191.95.60.219
Elaboración	Viviana Lucía Mendoza Hortua vmendoza@sdis.gov.co Contratista Subdirección de Diseño, Evaluación y Sis	Aprobado	Env.: 2021-07-02 12:29:52 Lec.: 2021-07-02 12:53:13 Res.: 2021-07-02 12:55:56 IP Res.: 186.87.38.250
Revisión	Nidia Carolina Parra Osorio nparrao@sdis.gov.co Contratista Apoyo SDIS	Aprobado	Env.: 2021-07-02 12:55:56 Lec.: 2021-07-02 13:13:15 Res.: 2021-07-02 13:14:08 IP Res.: 190.130.74.26
Revisión	Diana Larisa Caruso López dcaruso@sdis.gov.co Subdirectora Diseño, Evaluación y Sistematización SDIS	Aprobado	Env.: 2021-07-02 13:14:08 Lec.: 2021-07-02 17:27:00 Res.: 2021-07-02 17:27:09 IP Res.: 186.31.222.63
Aprobación	JULIAN TORRES JIMENEZ jtorresj@sdis.gov.co DIRECTOR DE ANALISIS Y DISEÑO ESTRATÉGICO SECRETARIA DISTRITAL DE INTEGRACION SOCIAL	Aprobado	Env.: 2021-07-02 17:27:09 Lec.: 2021-07-02 17:28:32 Res.: 2021-07-02 17:28:49 IP Res.: 186.31.222.187
Firma	XINIA ROCIO NAVARRO PRADA XNavarro@sdis.gov.co Secretaria Distrital de Integración Social	Aprobado	Env.: 2021-07-02 17:28:49 Lec.: 2021-07-07 10:17:18 Res.: 2021-07-07 10:18:40 IP Res.: 190.130.78.23

Firmado Electronicamente con AZSign
Acuerdo: 20210621-143910-c5e496-91400715
2021-06-21T15:40:05-05:00 - Pagina 1 de 3

1. Objetivo

Establecer el procedimiento a seguir para el trámite, elaboración y respuesta oportuna de las solicitudes de expedición de certificaciones laborales allegadas a la Subdirección de Gestión y Desarrollo del Talento Humano.

2. Glosario

- Certificación[1]: son actos administrativos por medio de los cuales el director de una oficina pública da fe sobre la existencia o estado de actuaciones o procesos administrativos que se hayan surtido.

- Certificación laboral: es un documento en el cual una entidad ya sea pública o privada certifica la fecha de ingreso de un empleado, el cargo que desempeña, las funciones que ejerce y el salario que devenga (según sea solicitado), debidamente firmada por el funcionario designado para tal fin.

- Certificación de funciones: es un documento en el cual se certifica la fecha de ingreso y/o retiro del funcionario o exfuncionario, según sea el caso, el cargo en el que se encuentra posesionado y la situación administrativa en la que se encuentra, el grupo al cual se encuentra adscrito, las reubicaciones efectuadas, las situaciones administrativas y las funciones que desempeñó en cada caso, de conformidad con el manual de funciones vigente para cada época.

- Certificación salarial: es un documento en el cual se certifica la fecha de ingreso y/o retiro del funcionario o exfuncionario, según sea el caso, el cargo en el que se encuentra posesionado y la situación administrativa en que se encuentra, el grupo al cual se encuentra adscrito y el salario que devenga o devengó.

- Certificación de permanencia: en un documento mediante el cual se indica nombres y apellidos del funcionario, numero de documento de identidad, tipo de vinculación, cargo que se encuentra desempeñando, fecha de ingreso a la entidad, en caso de que sea exfuncionario se nombra fecha de terminación de su vínculo laboral y acto administrativo que lo soporta. Al finalizar se indica la fecha de expedición y se firma para posteriormente ser entregada

- Certificación plan 25 Compensar: es un documento exclusivo para exfuncionarios pensionados, mediante la cual Compensar da un alivio al funcionario pensionado en la Caja de Compensación. En ella se indica nombres y apellidos, numero de documento de identidad, fecha de ingreso a la entidad, fecha de retiro de la entidad, acto administrativo que soporta el retiro, último cargo del cual fue titular. Al finalizar se indica la fecha de expedición y se firma para posteriormente ser entregada.

- Funciones[2]: objeto y marco general de competencias de un empleo al interior de la entidad.

[1] Función Pública - Glosario
[2] Ibíd

Firmado Electronicamente con AZSign
Acuerdo: 20210621-143910-c5e496-91400715
2021-06-21T15:40:05-05:00 - Pagina 2 de 3

- Manual de Funciones y Competencias[3]: instrumento de gestión del talento humano que rige las condiciones del empleo público al interior de las entidades, en él se identifican los cargos de la planta de personal de la entidad, enmarcando sus funciones, competencias y los requisitos exigidos para su desempeño.

3. Condiciones generales

3.1. Las solicitudes de expedición de certificaciones laborales se pueden realizar a través de los siguientes canales:

- Radicando una solicitud escrita en el Grupo de Correspondencia (Carrera 7 No. 32 - 12 Pisos 6 al 25 - Atención a la Ciudadanía Local 101 - Correspondencia Local 103, Bogotá), adjuntado el formato Solicitud certificaciones laborales (FOR-TH-041) o indicando cada una de las características que debe tener el certificado laboral requerido.
- A través de la línea de atención al ciudadano +57 (1) 3808330 o línea administrativa +57 (1) 3279797. En este caso quien atienda la llamada la direcciona a la persona encargada en la Subdirección de Gestión Humana o remite a servicio al ciudadano. Si este es el caso, quien tome la llamada deberá indicar al solicitante el correo electrónico al cual debe enviar la solicitud, adjuntando el formato Solicitud certificaciones laborales (FOR-TH-041) o indicando cada una de las características que debe tener el certificado laboral requerido.
- A través del Aplicativo PQRSD de la página Web de la Secretaria Distrital de Integración Social https://www.integracionsocial.gov.co/index.php/noticias/2489 indicando cada una de las características que debe tener el certificado laboral requerido.
- Por medio de correo electrónico dirigido a certificacioneslaboralesth@sdis.gov.co, subdireccion.talentohumano@sdis.gov.co mediante el diligenciamiento del formato Solicitud certificaciones laborales (FOR-TH-041), el cual está dispuesto en la documentación SIG, en el link: https://sig.sdis.gov.co/index.php/es/gestion-de-talento-humano-documentos-asociados.

3.2. Las solicitudes internas de expedición de certificaciones laborales se pueden realizar a través de los siguientes canales:

- Radicando el formato Solicitud certificaciones laborales (FOR-TH-041) ante el despacho de la Subdirección de Gestión y Talento Humano.
- Enviando correo electrónico al responsable de la elaboración o expedición de estos.

3.3. Para efectos de control y organización administrativa la Subdirección de Gestión de Talento Humano determina lo siguiente:

- Las solicitudes pueden ser de origen interno (funcionarios activos) o de origen externo (exfuncionarios).
- Las certificaciones requeridas por entes de control interno o externo se realizarán siguiendo lo establecido en el presente procedimiento.

[3] Función Pública - Glosario

Firmado Electronicamente con AZSign
Acuerdo: 20210621-143910-c5e496-91400715
2021-06-21T15:40:05-05:00 - Pagina 3 de 3

- Los tipos de certificaciones laborales que se emiten por parte de la Secretaría Distrital de Integración Social son:

  - Certificación de funciones
  - Certificación salarial
  - Certificación de permanencia
  - Certificación Plan 25 Compensar

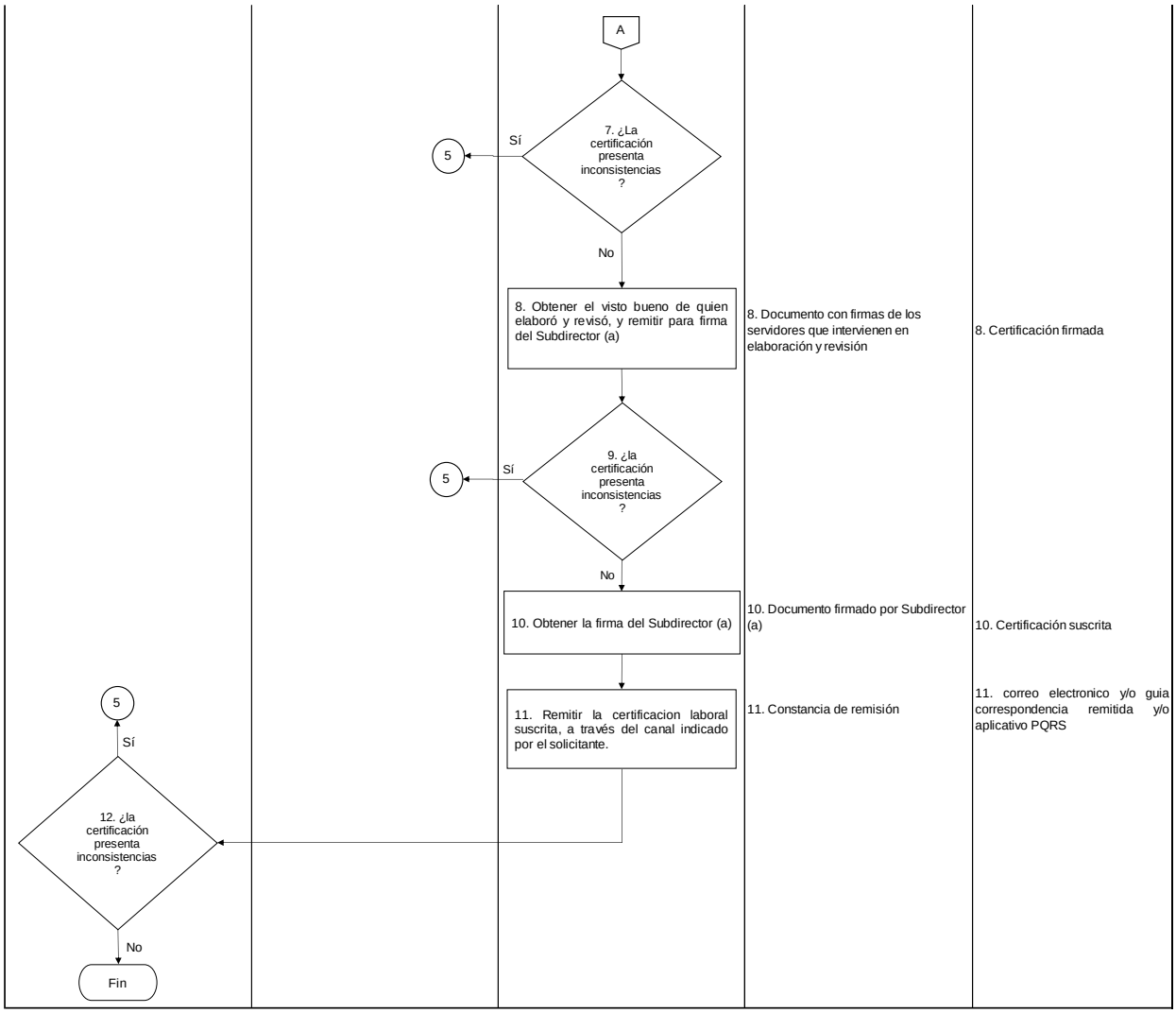
  Para la expedición de las certificaciones laborales la Subdirección de Gestión y Desarrollo de Talento Humano consulta la información que reposa en las historias laborales y/o manuales de funciones y/o liquidación de nomina

- Las certificaciones laborales emitidas, deben incluir el visto bueno de las personas que las elaboraron y revisaron; adicionalmente, deben ser firmadas por el/la subdirector (a) de Gestión de Talento Humano

4. Descripción de actividades

Funcionarios, Exfuncionarios, Entes de Control	Funcionario y/o área que recibe la solicitud	Subdirección de Gestión y Desarrollo del Talento Humano - Administración de personal	Punto de Control	Activo de Información
Inicio				
1. Presentar la solicitud a través de los canales habilitados, con el diligenciamiento del formato solicitud de certificación laboral o indicando cada una de las características que debe tener el certificado laboral requerido.			1. Documento que soporta la solicitud	1. Formato Solicitud Certificación Laboral FOR-TH-041 y/o correo electrónico y/o solicitud escrita
	2. Remitir solicitud a la Subdirección de Gestión y Desarrollo de Talento Humano - Administración de personal.			2. Formato Solicitud Certificación Laboral FOR-TH-041 y/o correo electrónico y/o solicitud escrita
		3. Determinar el tipo de certificación solicitada y asignar al responsable para la elaboración y gestión de acuerdo con el tipo de solicitud.		
		4. Solicitar las Historias Laborales y/o Manual de Funciones y/o Información liquidación de nóminas.	4. Documento de solicitud de la información	4.Formato Préstamo y Consulta Documental – Historias Laborales. FOR-GD-012 y/o Correo Electronico
		5. Identificar la información requerida y elaborar la certificación.	5. Servidor encargado elabora borrador de la certificación	5. Certificación elaborada
		6. Revisar la certificación elaborada	6. El líder funcional de administración de personal revisa el borrador de la certificación	6. Certificación revisada
		A		

Firmado Electronicamente con AZSign
Acuerdo: 20210621-143910-c5e496-91400715
2021-06-21T15:40:05-05:00 - Pagina 3 de 3



4.1 Aclaración de actividades

No aplica.

5. Disposiciones de almacenamiento y archivo

Las disposiciones de almacenamiento y archivo de la documentación del Sistema Integrado de Gestión, se realizará de conformidad con lo dispuesto en el Subsistema de Gestión Documental y Archivo (SIGA).

6. Dependencia encargada de administrar este procedimiento

Dirección de Gestión Corporativa, Subdirección de Gestión y Desarrollo del Talento Humano-Administración de Personal.

Firmado Electronicamente con AZSign
Acuerdo: 20210621-143910-c5e496-91400715
2021-06-21T15:40:05-05:00 - Pagina 3 de 3

7. Documentos asociados

- FOR-TH-041 Formato Solicitud Certificación Laboral.
- FOR-GD-012 Formato Préstamo y Consulta Documental – Historias Laborales.

8. Aprobación del documento

	Elaboró	Revisó	Aprobó
Nombre	María Camila Jiménez C.	Fabián Andrés Mafla Díaz John Jairo Zúñiga Serna Ruby Elena Blanco Galindo	María Mercedes Rodríguez Escobar
Cargo/Rol	Contratista Subdirección de Gestión y Desarrollo del Talento Humano	Contratista – Subdirección de Gestión y Desarrollo de Talento Humano Contratista - Gestor SG Subdirección de Gestión y Desarrollo del Talento Humano Contratista - Gestora SG Proceso Gestión de Talento Humano	Subdirectora de Gestión y Desarrollo de Talento Humano

Firmado Electronicamente con AZSign
Acuerdo: 20210621-143910-c5e496-91400715
2021-06-21T15:40:05-05:00 - Pagina 3 de 3

REGISTRO DE FIRMAS ELECTRONICAS

21-06-2021 Procedimiento Certificación Laboral (versión final)

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20210621-143910-c5e496-91400715 Creación: 2021-06-21 14:39:10

Estado: Finalizado Finalización: 2021-06-21 15:40:04

Escanee el código para verificación

Revisión: revisa

Ruby Elena Blanco Galindo

Rblanco@sdis.gov.co
Profesional Especializado - Contratista
Subdirección de Gestión y Desarrollo del Talento Humano

Revisión: revisa

jzunigas@sdis.gov.co

Revisión: revisa

fmaflad@sdis.gov.co

Elaboración: Elabora

Maria Camila Jiménez C.

mcjimenezc@sdis.gov.co
Profesional contratista

Firmado Electronicamente con AZSign
Acuerdo: 20210621-143910-c5e496-91400715
2021-06-21T15:40:05-05:00 - Pagina 3 de 3

REGISTRO DE FIRMAS ELECTRONICAS

21-06-2021 Procedimiento Certificación Laboral (versión final)

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo:	20210621-143910-c5e496-91400715	Creación:	2021-06-21 14:39:10
Estado:	Finalizado	Finalización:	2021-06-21 15:40:04

Escanee el código para verificación

Firma: firmante

MARIA MERCEDES RODRIGUEZ ESCOBAR

mmrodrigueze@sdis.gov.co
Subdirectora de Gestión y Desarrollo del Talento Humano

Firmado Electronicamente con AZSign
Acuerdo: 20210621-143910-c5e496-91400715
2021-06-21T15:40:05-05:00 - Pagina 3 de 3

REPORTE DE TRAZABILIDAD

21-06-2021 Procedimiento Certificación Laboral (versión final)

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20210621-143910-c5e496-91400715 Creación: 2021-06-21 14:39:10

Estado: Finalizado Finalización: 2021-06-21 15:40:04

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	Maria Camila Jiménez C. mcjimenezc@sdis.gov.co Profesional contratista	Aprobado	Env.: 2021-06-21 14:39:11 Lec.: 2021-06-21 14:39:59 Res.: 2021-06-21 14:40:38 IP Res.: 186.80.0.180
Revisión	FABIAN ANDRES MAFLA DIAZ fmaflad@sdis.gov.co	Aprobado	Env.: 2021-06-21 14:40:38 Lec.: 2021-06-21 14:55:17 Res.: 2021-06-21 14:55:30 IP Res.: 191.95.59.45
Revisión	JOHN JAIRO ZUÑIGA SERNA jzunigas@sdis.gov.co	Aprobado	Env.: 2021-06-21 14:55:30 Lec.: 2021-06-21 14:55:38 Res.: 2021-06-21 14:55:59 IP Res.: 191.156.152.234
Revisión	Ruby Elena Blanco Galindo Rblanco@sdis.gov.co Profesional Especializado - Contratista Subdirección de Gestión y Desarrollo del Talento Hum	Aprobado	Env.: 2021-06-21 14:55:59 Lec.: 2021-06-21 15:11:54 Res.: 2021-06-21 15:15:13 IP Res.: 200.118.62.108
Firma	MARIA MERCEDES RODRIGUEZ ESCOBAR mmrodrigueze@sdis.gov.co Subdirectora de Gestión y Desarrollo del Talento Hum	Aprobado	Env.: 2021-06-21 15:15:13 Lec.: 2021-06-21 15:39:48 Res.: 2021-06-21 15:40:04 IP Res.: 181.61.205.234

1. Objetivo

Describir las actividades a ejecutar para la gestión de Incidentes de Tecnología de la Información (TI), con el fin de restaurar la operación normal de los servicios de TI, minimizando el impacto negativo sobre las actividades misionales desarrolladas por la Secretaría Distrital de Integración Social - SDIS que dependan de las Tecnologías de la Información.

2. Glosario

Cambio de emergencia: es un cambio que se debe introducir tan pronto como sea posible - por ejemplo, para resolver un incidente grave o aplicar un parche de seguridad. Normalmente, el proceso de gestión de cambios tendrá un procedimiento específico para el manejo de cambios de emergencia[1].

Caso: es el número definitivo de la solicitud, este número es generado cuando ya la solicitud ha sido definida, clasificada y asignada a uno de los especialistas de nivel 1 o 2 el cual brindará la gestión oportuna.

Catálogo de servicios de tecnologías de la información: es una base de datos o un documento estructurado con información sobre todos los servicios de Tecnología de la Información (TI) en producción, incluye a los servicios que están disponibles para su implementación[2].

Elemento de configuración (CI): es cualquier componente u activo de servicio que debe ser gestionado con el fin de entregar un servicio de Tecnología de la Información (TI). Los elementos de configuración están bajo el control de la gestión del cambio; por lo general incluyen servicios de Tecnología de la Información (TI), hardware, software, edificios, personas y documentación formal como documentación del proceso y los acuerdos de niveles de servicio[3].

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[4].

Herramienta de gestión: son todos los sistemas, aplicaciones, controles, soluciones de cálculo, metodología, etc., que ayudan a la gestión de una empresa; para el caso de Tecnología de la Información (TI), se utilizan para el manejo y control de servicios es el software en donde se documentan los servicios de gestión tecnológica como incidentes, requerimientos, problemas, controles de cambios, etc., todas estas correspondientes a Tecnología de la Información (TI).

ITIL (Information Technology Infrastructure Library) / (Biblioteca de Infraestructura de Tecnologías de Información): es un conjunto de publicaciones de mejores prácticas para la gestión de servicios de TI. Es propiedad de la Oficina del Gabinete (parte del Gobierno de Su Majestad), ITIL

[1] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0
[2] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0
[3] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0
[4] Guía Técnica Colombiana NTC-ISO-IEC 27035.

proporciona guías de calidad para la prestación de servicios de Tecnología de la Información (TI) y los procesos, las funciones y otras competencias necesarios para sustentarlas. El marco de trabajo ITIL se basa en el ciclo de vida de servicio y dicho ciclo consta de cinco etapas (estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio), cada una de ellas tiene su propia publicación de apoyo[5].

Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información[6].

Incidente de tecnologías de la información: es una interrupción no planificada de un servicio de TI o la reducción en la calidad de un servicio de Tecnología de la Información (TI). La falla de un elemento de configuración que no ha afectado aún el servicio es también un incidente - por ejemplo, la falla en un disco de un conjunto de discos[7].

Incidente mayor de tecnologías de la información: es un Incidente de Tecnología de la Información (TI) grave que produce una importante interrupción de los servicios de tecnología afectando los procesos claves de la entidad. La identificación de un incidente mayor se define de acuerdo a los criterios establecidos.

Mesa de servicio: es el único punto de contacto entre el proveedor de servicios y los usuarios. La mesa de servicios maneja incidentes, requerimientos de servicio y la comunicación con los usuarios.

Precaso: Es el número generado por la herramienta de gestión una vez el usuario ingresa su solicitud a través de este canal de comunicación, posteriormente el analista define, clasifica y categoriza de forma correcta la solicitud, este procedimiento genera el número definitivo de ticket.

Problema de tecnologías de la información: es la causa raíz de uno o más incidentes. Usualmente no se conoce dicha causa raíz al momento de crear el registro del problema, y el proceso de gestión de problemas es responsable de la investigación posterior[8].

Requerimiento de tecnologías de la información: es una petición formal de tecnologías de la información por parte de un usuario, para que algo sea provisto, por ejemplo, una solicitud de información o asesoría; restablecer una contraseña, o instalar una estación de trabajo para un nuevo usuario.

Solicitud de tecnologías de la información: es una petición de información o asesoramiento, acceso a un servicio por parte del usuario.

[5] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0
[6] Ibíd
[7] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0
[8] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0

Solución temporal: es la reducción o eliminación del impacto de una incidencia o problema para la que aún no existe una solución completa.

Ticket / Número de servicio: número consecutivo suministrado por la herramienta de gestión durante el reporte de una solicitud de un servicio, para facilitar a través del mismo, el seguimiento y control de los grupos de soporte que participan en la solución.

Tecnologías de la Información (TI): las Tecnologías de la información y las comunicaciones, son un conjunto de elementos (servicios, redes, software y aparatos) que tienen como objeto el avance y el bienestar de las personas en un entorno principalmente de informática, internet y telecomunicaciones, integrado a un sistema de información relacionado y complementario

3. Condiciones generales

3.1 Reporte del incidente de Tecnologías de la Información

Todos los incidentes de TI deben registrarse a través de la mesa de servicio de acuerdo con los canales de comunicación que se tienen dispuestos para tal fin, como son:

- Canal Telefónico.
- Correo Electrónico.
- Herramienta de gestión.

3.1.1 Tratamiento del incidente de acuerdo con el canal de comunicación:

- Herramientas de gestión: el sistema genera el número de precaso, posteriormente el analista define, clasifica y categoriza de forma correcta la solicitud, este procedimiento genera el número definitivo de ticket.

- Correo electrónico y canal telefónico: el analista define, clasifica y categoriza de forma correcta la solicitud, este procedimiento genera el número definitivo de ticket.

3.2 Gestión dentro de la mesa de servicio

Recibe las solicitudes remitidas por parte del usuario y realiza un análisis que permita determinar si hace referencia a un requerimiento o incidente de Tecnología de la Información (TI), posteriormente clasifica y categoriza el requerimiento, Asignado un número de ticket definitivo.

Si el requerimiento cuenta con la información y documentos requeridos, procede con el escalamiento o solución de la solicitud. En caso contrario se solicita por parte del Analista de Mesa, la información o documentos necesarios para tramitar el requerimiento.

3.3 Procedimientos asociados

En el caso de que la solicitud no corresponda a un incidente Tecnología de la Información (TI), la mesa de servicio remitirá el pre-caso a los procedimientos asociados así:

- Procedimiento Gestión de requerimientos de Tecnologías de la Información (PCD-SMT-008): corresponde a la gestión de solicitudes de acceso a nuevos servicios de TI, solicitudes de gestión IMAC (Instalaciones, Movimientos, Adiciones y Cambios) para elementos de configuración, que se encuentren dentro del catálogo de servicios de TI de la Subdirección de Investigación e Información y solicitudes de información de TI.
- Procedimiento Gestión de Incidentes de Seguridad de la Información (PCD-SMT-012): se gestionan eventos e incidentes de seguridad de la información que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Procedimiento Gestión de cambios de Tecnologías de la Información (PCD-SMT-001): en este procedimiento se gestionan los cambios de tecnologías de la información con el fin de minimizar el impacto negativo que estos puedan generar a la operación, ejemplo: actualización de aplicativos, lanzamiento de nuevos servicios, instalación de elementos de configuración de infraestructura de servicios, etc.
- Procedimiento Gestión de quejas, reclamos y felicitaciones de la mesa de servicios (PCD-SMT-009): se encarga de recibir y gestionar las quejas, reclamos y felicitaciones expresadas por los usuarios internos de la Secretaría Distrital de Integración Social frente a los servicios de tecnologías de la información y comunicaciones brindados por el soporte técnico de la Subdirección de Investigación e Información.

3.4 Diagnóstico de primer nivel del incidente

Todos los incidentes deben diagnosticarse en primer nivel de atención según el siguiente flujo:

1. La mesa de servicio clasifica el incidente de acuerdo con el servicio o aplicativo afectado.
2. La Mesa de Servicio debe gestionar el incidente de acuerdo con el diagnóstico de primer nivel realizado. Si es necesario debe realiza las validaciones de primer nivel bajo los criterios de verificación suministrados y/o establecidos por el segundo o el tercer nivel de soporte (si aplica), las cuales deben ser documentadas en el ticket con el fin de asegurar que se realizó el diagnóstico de primer nivel.
3. Si el incidente no es resuelto se debe escalar el incidente al Segundo Nivel según el grupo encargado para su gestión, por medio de la herramienta de gestión establecida por la Subdirección de Investigación e Información.

3.5 Información básica para la atención de incidentes

Para la atención de incidentes es necesario que el usuario informe a través de los canales de atención los siguientes datos básicos con el fin de atender el incidente en el menor tiempo posible.

Nombre del usuario:
Usuario de Red:
Contacto Telefónico (Fijo o celular):
Ubicación:

- Localidad:
- Unidad Operativa:

- Dirección:
- Piso:
- Número de contacto:

Elemento Afectado:
Placa:
Serial:
Descripción de la solicitud o falla:
Evidencias/captura de pantalla en donde se logre identificar la inconsistencia o error generado:

3.6 Estados de la solicitud:

Un estado es la etapa o fase en la que se puede encontrar un caso a lo largo de su ciclo de vida el cual inició cuando se registra y finaliza con su respectivo cierre.

- Sin clasificar: cuando el usuario radica la solicitud a través de la herramienta de gestión se asigna un número temporal que se denomina pre-caso, posteriormente la solicitud pasa a ser clasificada por los analistas de la Mesa de Servicio.
- Registrado: la solicitud ya ha sido definida, clasificada y asignada a uno de los especialistas de nivel 1 o 2 el cual brindará la gestión oportuna, en este estado se genera el número de caso definitivo, con el cual el usuario puede hacer seguimiento en cualquiera de sus etapas.
- En proceso: el especialista inicia la validación de la solicitud y los soportes para brindar atención.
- Suspendido: el caso se suspende por falta de evidencias, claridad de la solicitud y/o documentación de soporte. En este estado el analista de Mesa de Servicio realizará seguimiento durante los 3 días hábiles siguientes, si a partir de la notificación el usuario no suministra la información faltante, se procederá a dar cierre al ticket y será necesario que el usuario radique una nueva solicitud cuando cuente con la información solicitada para la atención de este.
- Solucionado: el caso fue solucionado a satisfacción del usuario por el especialista encargado.
- Desaprobado: el usuario puede desaprobar el caso siempre y cuando la solución brindada por parte del especialista no responde a la necesidad inicial de la solicitud.
- Anulado: este estado se presenta en diferentes casos por duplicidad de la solicitud, falta información, por visitas fallidas.

3.7 Incidente mayor

La mesa de servicio debe identificar y clasificar si el incidente corresponde a un incidente mayor de acuerdo con los siguientes criterios:

- Incidente en donde se evidencie caída completa de un servicio de Tecnología de la Información (TI) o aplicación.

- Incidentes repetitivos en donde se registren comportamientos inesperados o degradación en los servicios y/o aplicativos institucionales al alcance de la Subdirección de Investigación e Información.
- Incidentes con la misma sintomatología de diferentes unidades operativas, Subdirección Local de Integración Social (SLIS) o Comisarias.

La mesa de servicio debe informar al Gestor de Incidentes acerca de la existencia del incidente mayor y a su vez el gestor es el encargado de realizar las validaciones del ticket con las personas o dependencias que están encargadas de dar la solución al incidente. El gestor de incidentes notifica el número del incidente mayor generado en la herramienta de gestión al responsable del servicio de TI que presenta la falla e informa a las dependencias afectadas en caso de requerirlo.

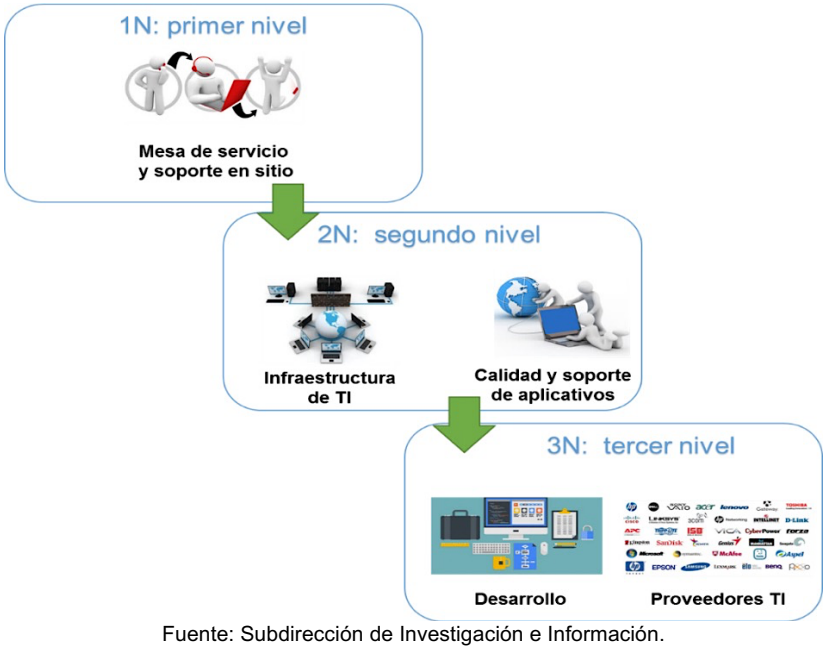
El gestor de incidentes participa como mínimo en la creación, actualización y cierre del incidente mayor. El Incidente mayor también puede ser tratado, gestionado y solucionado desde la gestión de problemas si es postulado desde la gestión de incidentes.

Los incidentes relacionados al incidente mayor corresponden a los tickets que se generen a causa del incidente mayor y son tratados por la Mesa de Servicio de acuerdo con la solución temporal dada por el nivel 2 o 3. Si no es posible brindar una solución temporal escalar el ticket al especialista de nivel 2 o 3 encargado.

3.8 Niveles de atención

Existen para Tecnología de la Información (TI) 3 niveles de atención o grupos de solución como lo muestra la siguiente gráfica:

Grafica 1. Niveles de atención



Fuente: Subdirección de Investigación e Información.

Primer nivel (1N): en la entidad el primer nivel está compuesto por la mesa de servicio y soporte en sitio, quienes validan los casos directamente con los usuarios finales y están a cargo de hacer el diagnóstico bajo las premisas consignadas por los grupos de soporte de nivel 2 o 3 (si aplica) y brindan solución al incidente. Si el incidente no puede ser solucionado se debe escalar al segundo nivel.

Segundo nivel (2N): son los grupos de infraestructura de TI, de calidad y soporte de aplicativos de la entidad los cuales validan los incidentes de acuerdo con su especialidad y deben trabajar en conjunto con el primer nivel con el fin de dar solución al incidente escalado. Si el incidente no puede ser solucionado se debe escalar al tercer nivel.

Tercer nivel (3N): son los grupos de desarrollo y proveedores de servicios de TI, los cuales deben tener acceso a los códigos fuentes de las aplicaciones o a las consolas de administración e información privilegiada de los dispositivos de la entidad con el fin de realizar las validaciones que consideren necesarias y dar solución a los incidentes.

3.9 Actividades Gestor de Incidentes:

- Realizar las validaciones del ticket mayor con las personas o dependencias que estén encargadas de dar la solución al incidente.
- Definir roles específicos dentro del ciclo de vida del incidente que permitan definir responsabilidades en la gestión de las fases de solución y atención de este, y faciliten su control y gestión.

- Notificar el número del incidente mayor generado en la herramienta de gestión al responsable del servicio de Tecnología de la Información (TI) que presenta la falla e informa a las dependencias afectadas en caso de requerirlo.
- En caso de que el incidente mayor sea reiterativo y no sea solucionado efectivamente, se deberá postular como problema.
- Validar periódicamente la eficiencia del proceso de gestión de incidentes a partir de la creación de reportes e informes desde las diversas plataformas de gestión de la entidad que permitan construir planes de mejora, que faciliten la elaboración de procesos mecanismos e instrumentos que optimicen los procesos de atención de incidentes.

3.7 No aplica como incidentes cuando se evidencie de que no se cumplen los siguientes lineamientos:

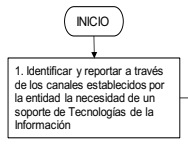
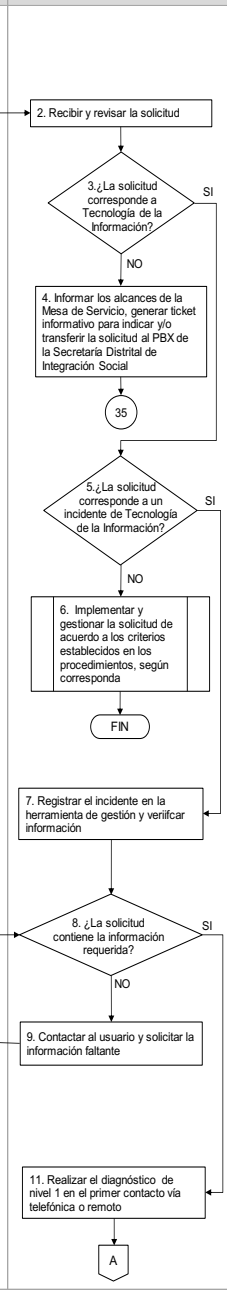
- Los funcionarios no deben mover o reubicar las herramientas tecnológicas asignadas, instalar o desinstalar dispositivos, ni retirar sellos de estos, sin la autorización de la Subdirección de Investigación de la Información, en caso de requerir este servicio deberá solicitarlo a través de los canales autorizados.
- Las herramientas tecnológicas asignadas, deberán ser para uso exclusivo del ejercicio de las funciones asignadas a los funcionarios o contratistas de la SDIS.
- No se deberán consumir alimentos o ingerir líquidos mientras se operan las herramientas tecnológicas asignadas por la Entidad.
- El funcionario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos. En caso de que no se cumpla, solicitar el ordenamiento de cables con el equipo de la mesa de servicio.
- Se prohíbe que un funcionario distinto al personal Subdirección de Investigación e Información abra, destape o manipule las herramientas tecnológicas que sufran daños.
- Todos los funcionarios que hagan uso de equipos de cómputo deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.
- Los suministros serán instalados sobre la base de canje (se retira el elemento dañado y se reemplaza por otro en perfectas condiciones). Por ningún motivo puede retirarse un equipo o parte de él sin que se deje su respectivo reemplazo. Manejando un soporte sistematizado de control de las partes o equipos cambiados donde quede registrado el historial de los ajustes realizados a la máquina.

3.10 Encuesta de satisfacción

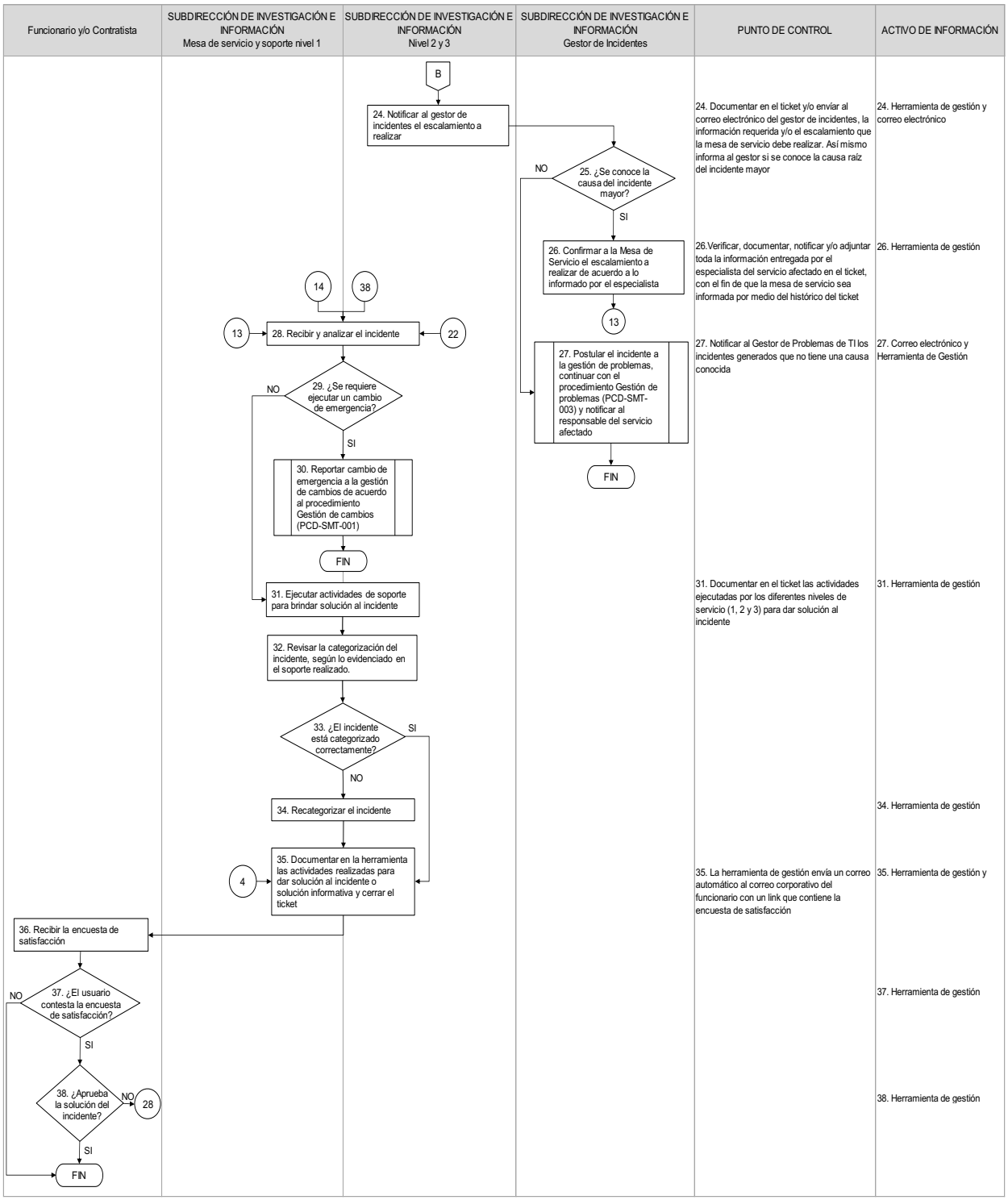
La encuesta de satisfacción es generada por la herramienta de gestión cuando el ticket es solucionado y es enviada al correo del usuario de forma automática, el usuario solicitante califica y aprueba o desaprueba la solución del ticket. Si el usuario no contesta la encuesta de satisfacción, no puede aprobar o desaprobar la solución de este, al igual, si el usuario no contesta la encuesta, la herramienta de gestión realiza el cierre del ticket de forma automática pasados dos (2) días hábiles después de haberse solucionado el ticket.

Si el caso es desaprobado se realizará reapertura de este y se iniciará una nueva atención prioritaria.

4. Descripción de actividades

Funcionario y/o Contratista	SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Mesa de servicio y soporte nivel 1	SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Nivel 2 y 3	SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Gestor de Incidentes	PUNTO DE CONTROL	ACTIVO DE INFORMACIÓN
				2. Verificar que la solicitud corresponda a solicitudes de Tecnologías de la Información mediante la verificación en el Catálogo de Servicios de la Subdirección de Investigación e Información. 5. La mesa de servicio identifica si la solicitud corresponde a un incidente de TI de acuerdo a las definiciones de ITIL establecidas en las consideraciones generales. 6. Verificar los tipos de solicitudes y procedimientos asociados en las condicines generales. 7. El analista de la Mesa de Servicio registra, prioriza y categoriza el incidente de TI de acuerdo a los lineamientos establecidos por la Subdirección de Investigación e Información. Se debe verificar los datos de contacto, ubicación del usuario y descripción del incidente. 9. La mesa de servicio contacta al usuario por los medios que se tengan disponibles para tal fin. Todo contacto o intento de contacto se documenta en histórico del ticket 10. El usuario debe enviar la información dentro de los tres (3) días hábiles siguientes, a través de los canales de comunicación disponibles. Al no recibir la información solicitada en el tiempo establecido la mesa de servicio realiza el cierre del ticket 11. Describir las actividades realizadas por medio de anotación en el ticket	1. Grabación de llamada, correo electrónico institucional y/o 7. Herramienta de gestión y correo electrónico 9. Herramienta de gestión 10. Herramienta de gestión y correo electrónico 11. Herramienta de gestión

Funcionario y/o Contratista	SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Mesa de servicio y soporte nivel 1	SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Nivel 2 y 3	SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Gestor de Incidentes	PUNTO DE CONTROL	ACTIVO DE INFORMACIÓN
	A 12.¿Es posible solucionar el incidente en el primer nivel? SI NO 13. Documentar y escalar el ticket al grupo de nivel que corresponda 26 28 14.¿El incidente es un incidente mayor? NO SI 15. Notificar al Gestor de Incidentes de TI la información relacionada con el ticket			13. La mesa de servicio realiza el escalamiento del ticket de acuerdo a las información del Catálogo de Servicios de TI, dejando la respectiva anotación en el ticket. 15. Documentar las actividades de diagnóstico y pruebas realizadas, así como los errores adjuntos en imágenes y otra información especifica relevante para identificar el incidente mayor	13. Herramienta de gestión 15. Herramienta de gestión
			16. Analizar e identificar el impacto generado por el incidente 17. Informar al líder y responsable del servicio afectado por medio de los canales disponibles 18. Registrar el incidente mayor, notificar y escalar al especialista encargado	16. Definir el impacto generado revisando la documentación de los incidentes reportados 17. Informar a través de correo electrónico o extensión telefónica la existencia del incidente mayor. El correo y/o contacto se adjunta y documenta en el ticket 18. Indicar el número del ticket al especialista por medio de los canales disponibles y herramienta de gestión, para la posterior documentación y solución	16. Herramienta de gestión 17. Herramienta de gestión y correo electrónico 18. Herramienta de gestión
		19. Recibir y analizar el incidente el mayor 20. ¿Se puede aplicar una solución temporal a los incidentes relacionados? NO SI 21. Documentar en el incidente mayor las soluciones temporales 22. Notificar a la Mesa de Servicio las soluciones temporales dadas desde nivel 2 o 3 28 23. Generar pieza comunicativa a los usuarios de la entidad informando la indisponibilidad del servicio B		21. Documentar las actividades a realizar o adjuntar manuales en el ticket 22. Adjuntar al ticket el correo electronico donde el especialista de nivel 2 o 3 notifica a la mesa de servicio las soluciones temporales dadas. 23. Adjuntar al ticket el comunicado remitido a los usuarios.	19. Herramienta de gestión 32. Herramienta de gestión 22. Correo electrónico y herramienta de gestión 23. Herramienta de gestión y correo electrónico


Funcionario y/o Contratista
SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Mesa de servicio y soporte nivel 1
SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Nivel 2 y 3
SUBDIRECCIÓN DE INVESTIGACIÓN E INFORMACIÓN Gestor de Incidentes
PUNTO DE CONTROL
ACTIVO DE INFORMACIÓN
B
24. Notificar al gestor de incidentes el escalamiento a realizar
24. Documentar en el ticket y/o envíar al correo electrónico del gestor de incidentes, la información requerida y/o el escalamiento que la mesa de servicio debe realizar. Así mismo informa al gestor si se conoce la causa raíz del incidente mayor
24. Herramienta de gestión y correo electrónico
25. ¿Se conoce la causa del incidente mayor?
NO
SI
26. Confirmar a la Mesa de Servicio el escalamiento a realizar de acuerdo a lo informado por el especialista
26.Verificar, documentar, notificar y/o adjuntar toda la información entregada por el especialista del servicio afectado en el ticket, con el fin de que la mesa de servicio sea informada por medio del histórico del ticket
26. Herramienta de gestión
13
27. Postular el incidente a la gestión de problemas, continuar con el procedimiento Gestión de problemas (PCD-SMT-003) y notificar al responsable del servicio afectado
27. Notificar al Gestor de Problemas de TI los incidentes generados que no tiene una causa conocida
27. Correo electrónico y Herramienta de Gestión
FIN
14
38
13
28. Recibir y analizar el incidente
22
29. ¿Se requiere ejecutar un cambio de emergencia?
NO
SI
30. Reportar cambio de emergencia a la gestión de cambios de acuerdo al procedimiento Gestión de cambios (PCD-SMT-001)
FIN
31. Ejecutar actividades de soporte para brindar solución al incidente
31. Documentar en el ticket las actividades ejecutadas por los diferentes niveles de servicio (1, 2 y 3) para dar solución al incidente
31. Herramienta de gestión
32. Revisar la categorización del incidente, según lo evidenciado en el soporte realizado.
33. ¿El incidente está categorizado correctamente?
SI
NO
34. Recategorizar el incidente
34. Herramienta de gestión
4
35. Documentar en la herramienta las actividades realizadas para dar solución al incidente o solución informativa y cerrar el ticket
35. La herramienta de gestión envía un correo automático al correo corporativo del funcionario con un link que contiene la encuesta de satisfacción
35. Herramienta de gestión y
36. Recibir la encuesta de satisfacción
37. ¿El usuario contesta la encuesta de satisfacción?
NO
SI
37. Herramienta de gestión
38. ¿Aprueba la solución del incidente?
NO
28
SI
38. Herramienta de gestión
FIN

5. Disposiciones de almacenamiento y archivo

Las disposiciones de almacenamiento y archivo de la documentación del Sistema Integrado de Gestión, se realizará de conformidad con lo dispuesto en el Subsistema de Gestión Documental y Archivo (SIGA).

6. Dependencia encargada de administrar este procedimiento

Subdirección de Investigación e Información.

7. Documentos asociados

El presente procedimiento no cuenta con documentos asociados.

8. Aprobación del documento

	Elaboró	Revisó	Aprobó
Nombre	Jelly Suleyma Cubillos Gomez	Santiago Sandoval Bautista Mayra Andrea Ruiz Abello	Luis Armando Solarte Solarte
Cargo/ Rol	Contratista – Subdirección de Investigación e Información	Contratista - Subdirección de Investigación e Información Contratista - Gestora SG del proceso Gestión de soporte y mantenimiento tecnológico	Subdirector de Investigación e Información

1. Objetivo

Gestionar los Requerimientos de TI (asociados a los servicios de tecnología de la información) generados por los funcionarios o contratistas internos de la Secretaria Distrital de Integración Social - SDIS, que ingresan a través de la Mesa de Servicio.

2. Glosario

Cambio programado: son cambios previamente acordados, planificados, y validados cuya ejecución es única siguiendo un plan de actividades programado, los evalúa el comité de cambios.

Caso: es el número definitivo de la solicitud, este número es generado cuando ya la solicitud ha sido definida, clasificada y asignada a uno de los especialistas de nivel 1 o 2 el cual brindará la gestión oportuna.

Catálogo de servicios de tecnologías de la información: es una base de datos o un documento estructurado con información sobre todos los servicios de Tecnologías de la Información (TI) en producción, incluye a los servicios que están disponibles para su implementación[1].

Elemento de configuración (CI): es cualquier componente u activo de servicio que debe ser gestionado con el fin de entregar un servicio de Tecnologías de la Información (TI). Los elementos de configuración están bajo el control de la gestión del cambio; por lo general incluyen servicios de TI, hardware, software, edificios, personas y documentación formal como documentación del proceso y los acuerdos de niveles de servicio[2].

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 [3].

Herramienta de gestión: son todos los sistemas, aplicaciones, controles, soluciones de cálculo, metodología, etc., que ayudan a la gestión de una empresa; para el caso de Tecnologías de la Información (TI), se utilizan para el manejo y control de servicios es el software en donde se documentan los servicios de gestión tecnológica como incidentes, requerimientos, problemas, controles de cambios, etc., todas estas correspondientes a Tecnologías de la Información (TI)

ITIL (Information Technology Infrastructure Library) / (Biblioteca de Infraestructura de Tecnologías de Información): es un conjunto de publicaciones de mejores prácticas para la gestión de servicios de TI. Es propiedad de la Oficina del Gabinete (parte del Gobierno de Su Majestad), ITIL proporciona guías de calidad para la prestación de servicios de Tecnologías de la Información (TI) y los procesos, las funciones y otras competencias necesarios para sustentarlas. El marco de trabajo ITIL se basa en el ciclo de vida de servicio y dicho ciclo consta de cinco etapas (estrategia

[1] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0
[2] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0
[3] Guía Técnica Colombiana NTC-ISO-IEC 27035.

del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio), cada una de ellas tiene su propia publicación de apoyo[4].

Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información[5].

Incidente de tecnologías de la información: es una interrupción no planificada de un servicio de Tecnologías de la Información (TI) o la reducción en la calidad de un servicio de Tecnologías de la Información (TI). La falla de un elemento de configuración que no ha afectado aún el servicio es también un incidente - por ejemplo, la falla en un disco de un conjunto de discos[6].

Mesa de servicio: es el único punto de contacto entre el proveedor de servicios y los usuarios. La Mesa de Servicio es el grupo de gestión de personas especializadas que maneja incidentes, requerimientos de servicio y la comunicación con los usuarios.

Precaso: Es el número generado por la herramienta de gestión una vez el usuario ingresa su solicitud a través de este canal de comunicación, posteriormente el analista define, clasifica y categoriza de forma correcta la solicitud, este procedimiento genera el número definitivo de ticket.

Requerimiento de tecnologías de la información: es una petición formal de servicios de tecnologías de la información por parte de un usuario, para que algo sea provisto, por ejemplo, una solicitud de información o asesoría; restablecer una contraseña, o instalar una estación de trabajo para un nuevo usuario.

Gestión de IMAC: Gestión de Instalaciones, Movimientos, Adiciones y Cambios de los elementos de configuración (CIs).

Requerimiento informativo: son catalogados como requerimientos informativos todos aquellos registros (tickets) en los cuales no se gestione ningún tipo de soporte a los usuarios o no cumplen con los requisitos para ser gestionados, pero se entregue información de Tecnologías de la Información (TI). Por ejemplo: Un usuario llama para solicitar el seguimiento de ticket o solicita información de cómo llenar el formato de solicitud de suministros de impresión.

Solicitud de tecnologías de la información: es una petición de información o asesoramiento, acceso a un servicio por parte del usuario.

Ticket / Número de servicio: número consecutivo suministrado por la herramienta de gestión durante el reporte de una solicitud de un servicio, para facilitar a través del mismo, el seguimiento y control de los grupos de soporte que participan en la solución.

Tecnologías de la Información (TI): las Tecnologías de la información y las comunicaciones, son un conjunto de elementos (servicios, redes, software y aparatos) que tienen como objeto el

[4] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0
[5] Ibíd
[6] ITIL® Glossary of Terms English - Spanish (Latin America) v.1.0

avance y el bienestar de las personas en un entorno principalmente de informática, internet y telecomunicaciones, integrado a un sistema de información relacionado y complementario.

3. Condiciones generales

3.1 Reporte del requerimiento Tecnologías de la Información

Todos los requerimientos de Tecnologías de la Información (TI)deben reportarse a través de la Mesa de Servicio de acuerdo con los canales de comunicación que se tienen dispuestos para tal fin, como son:

- Herramienta de gestión.
- Correo electrónico.
- Canal Telefónico.

3.1.1 Tratamiento del requerimiento de acuerdo con el canal de comunicación:

- Herramientas de gestión: el sistema genera el número de precaso, posteriormente el analista define, clasifica y categoriza de forma correcta la solicitud, este procedimiento genera el número definitivo de ticket.

- Correo electrónico y canal telefónico: el analista define, clasifica y categoriza de forma correcta la solicitud, este procedimiento genera el número definitivo de ticket.

3.2 Requisitos de los requerimientos de Tecnologías de la Información (TI).

Todos los requerimientos de Tecnologías de la Información (TI) que realicen los usuarios internos deben cumplir con los requisitos mínimos para ser validados:

- ✓ Usar los formatos que están establecidos, de acuerdo al tipo de solicitud (si aplica).
- ✓ Los formatos deben venir en la última versión que se encuentre en la página web institucional Entidad, en el Sistema Integrado de Gestión, en el módulo de Gestión de soporte y mantenimiento tecnológico, documentos asociados.
- ✓ Incluir el detalle de contacto del usuario que requiere el que contenga como mínimo:
    - Información relevante y detallada en la descripción de la solicitud.
    - Datos del contacto del usuario solicitante, es decir, del usuario que requiere el servicio
    - Relacionar datos de ubicación: Localidad, unidad operativa, o sede, nombre de la unidad operativa o dependencia, dirección, piso (si aplica).

3.3 Gestión dentro de la mesa de servicio

Recibe las solicitudes remitidas por parte del usuario y realiza un análisis que permita determinar si hace referencia a un requerimiento o incidente de Tecnologías de la Información

(TI), posteriormente clasifica y categoriza el requerimiento, Asignado un número de ticket definitivo.

Si el requerimiento cuenta con la información y documentos requeridos, procede con el escalamiento o solución de la solicitud. En caso contrario se solicita por parte del Analista de Mesa, la información o documentos necesarios para tramitar el requerimiento.

Así mismo, notifica al usuario cualquier eventualidad que se presente frente al requerimiento para optimizar y garantizar una solución satisfactoria.

Escalamiento a Nivel 2

En caso de que el requerimiento implique gestiones, configuraciones o intervenciones especializadas que no puedan ser solventadas en el primer contacto o en la gestión inicial de los analistas de la mesa de servicio, se procederá a realizar el análisis y escalamiento necesario a los equipos especializados de nivel 2 quienes brindaran solución al caso. El nivel 2 se encarga de analizar la solicitud enviada como requerimiento para establecer un Plan de Acción, que permita resolver la solicitud, o cerrar el caso si se requiere.

Dentro de los servicios especializados de segundo nivel se encuentran los siguientes grupos:

- Calidad y Soporte: en este grupo se atenderán casos relacionados con los aplicativos Azdigital, Carnetización, Comisarias, Directorio Activo, Invict – Oralidad, Iops, Seven, Sirbe.

- Desarrollo: en este grupo se atenderán casos relacionados con los aplicativos Iops, Kactus, Kactus Web, Sirbe.

- Infraestructura Tecnologías de la Información (TI): en este grupo se atenderán casos relacionados con Cable de Red, Canal de Comunicaciones, Celu-Fijos, Correo, CPU, Directorio Activo, Dispositivos Inalámbricos Localidades, Equipo Completo, Intranet, Laser, Líneas telefónicas, Máquina Virtual – Vmware, Otro, Punto De Red, Routers, Sistema Operativo Pcs, Switch Localidades, Telefonos IP, Violación Política Seguridad Información, VPN

- SDIS Soporte Segundo Nivel: en este grupo se atenderán casos relacionados con los canales de comunicaciones, Equipo Completo, Laser, Microsoft Office, Perifericos, Sistema Operativo PCS

3.4 Estados de la solicitud:

Un estado es la etapa o fase en la que se puede encontrar un caso a lo largo de su ciclo de vida el cual inició cuando se registra y finaliza con su respectivo cierre.

- Sin clasificar: cuando el usuario radica la solicitud a través de la herramienta de gestión se asigna un número temporal que se denomina pre-caso, posteriormente la solicitud pasa a ser clasificada por los analistas de la Mesa de Servicio.

- Registrado: La solicitud ya ha sido definida, clasificada y asignada a uno de los especialistas de nivel 1 o 2 el cual brindará la gestión oportuna, en este estado se genera el número de caso definitivo, con el cual el usuario puede hacer seguimiento en cualquiera de sus etapas.
- En proceso: el especialista inicia la validación de la solicitud y los soportes para brindar atención.
- Suspendido: el caso se suspende por falta de evidencias, claridad de la solicitud y/o documentación de soporte. En este estado el analista de Mesa de Servicio realizará seguimiento durante los 3 días hábiles siguientes, si a partir de la notificación el usuario no suministra la información faltante, se procederá a dar cierre al ticket y será necesario que el usuario radique una nueva solicitud cuando cuente con la información solicitada para la atención de este.
- Solucionado: el caso fue solucionado a satisfacción del usuario por el especialista encargado.
- Desaprobado: el usuario puede desaprobar el caso siempre y cuando la solución brindada por parte del especialista no responde a la necesidad inicial de la solicitud.
- Anulado: este estado se presenta en diferentes casos por duplicidad de la solicitud, falta información, por visitas fallidas.

3.5 Actividades mínimas para realizar por parte del Gestor de requerimientos:

- Verificar que desde la mesa de servicio se estén clasificando y gestionando de forma correcta las diferentes solicitudes.
- Realizar seguimiento constante a la documentación de los casos gestionados desde la Mesa de Servicio y especialistas de soporte en sitio.
- Verificar el cumplimiento de los ANS.
- Identificación de actividades masivas que puedan ocasionar incidentes.
- Verificar que cada solicitud cuente con los números de casos de acuerdo con los requerimientos y sus casos relacionados cuando aplique.

3.6 Gestión de Instalaciones, Movimientos, Adiciones y Cambios (IMAC) masivo

Los requerimientos tipo IMAC están catalogados como cambios estándar dentro de las buenas prácticas de ITIL de la Subdirección de Investigación e Información, involucran como su nombre lo indica, nuevas instalaciones, movimientos, adiciones y cambios, realizados en sitio como soporte. Estos se realizan de manera programada en conjunto con el usuario solicitante siempre y cuando sean superiores a 10 elementos de configuración en un día.

3.7 Procedimientos asociados

Si la solicitud corresponde a una solicitud de tecnologías de la información, pero no corresponde a un Requerimiento de Tecnologías de la Información (TI), se remite a los procedimientos asociados así:

- Procedimiento Gestión de Incidentes de Tecnologías de la Información (PCD-SMT-006): corresponde a la gestión de solicitudes de soporte derivadas de fallas e interrupciones no

planificadas de un servicio de Tecnologías de la Información (TI), ejemplo: intermitencia en el servicio de navegación, falla de encendido de un PC, caída total del servicio de telefonía IP, etc.

- Procedimiento Gestión de incidentes de Seguridad de la Información (PCD-SMT-012): se gestionan eventos e incidentes de seguridad de la información que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Procedimiento Gestión de cambios de Tecnologías de la Información (PCD-SMT-001): en este procedimiento se gestionan los cambios de tecnologías de la información con el fin de minimizar el impacto negativo que estos puedan generar a la operación, ejemplo: actualización de aplicativos, lanzamiento de nuevos servicios, instalación de elementos de configuración de infraestructura de servicios, etc.
- Procedimiento Gestión de quejas, reclamos y felicitaciones de la mesa de servicios (PCD-SMT-009): se encarga de recibir y gestionar las quejas, reclamos y felicitaciones expresadas por los usuarios internos de la Secretaría Distrital de Integración Social frente a los servicios de tecnologías de la información y comunicaciones brindados por el soporte técnico de la Subdirección de Investigación e Información.

3.8 Procedimientos específicos de requerimientos de Tecnologías de la Información (TI)

Este procedimiento no aplica para la creación de usuarios y/o asignación de perfiles; o solicitud de suministro para impresoras o plotter, en estos casos es necesario remitirse a los siguientes procedimientos según corresponda:

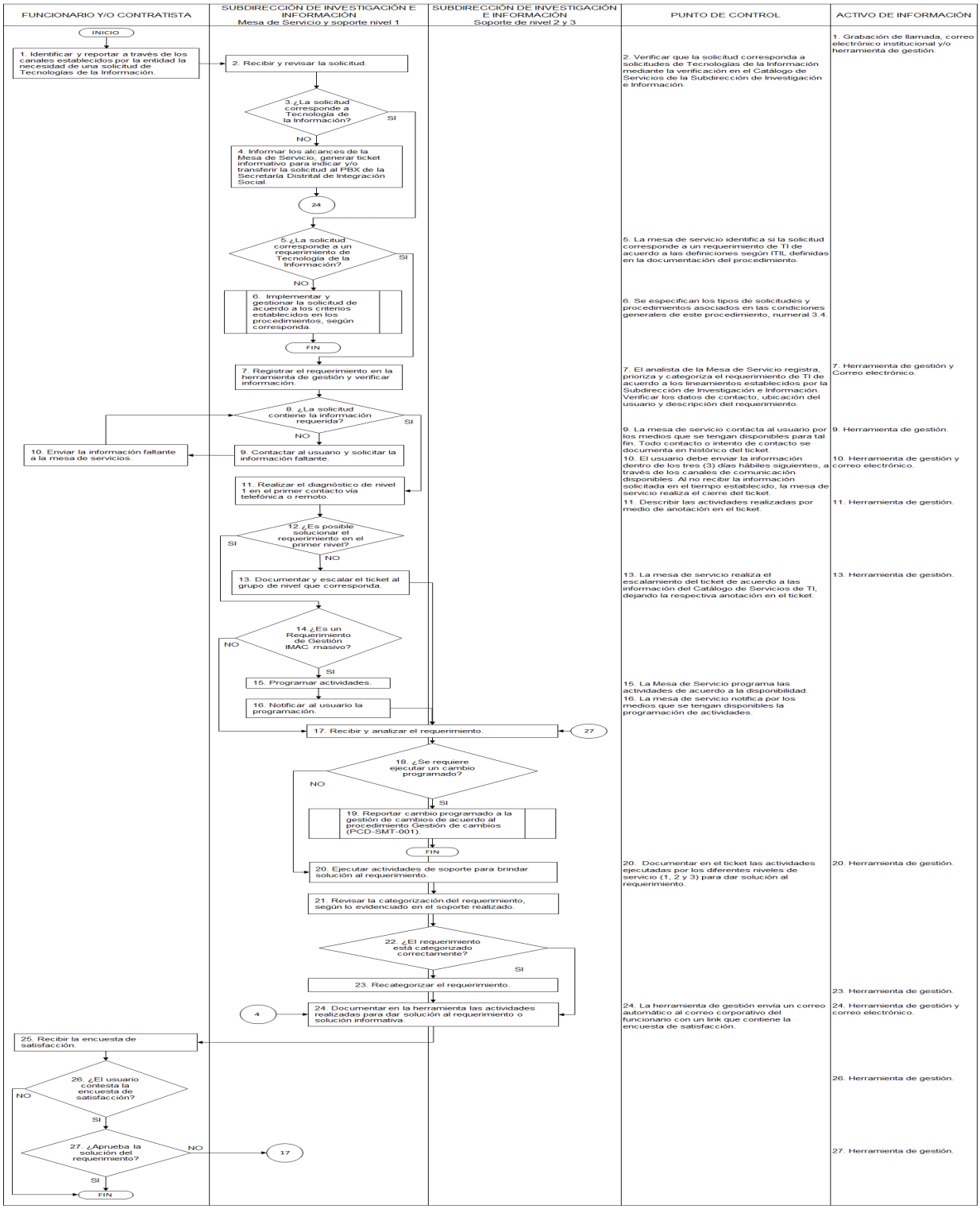
- Procedimiento Creación de usuarios y asignación de perfiles (PCD-SMT-007): se gestionan los requerimientos de Tecnologías de la Información (TI) que corresponden a solicitudes de administración de usuarios en los sistemas, aplicativos y/o servicios dentro Catálogo de Servicios de la Subdirección de Investigación e Información.
- Procedimiento Solicitud de suministro para impresora o plotter (PCD-SMT-002): en este procedimiento se gestionan los requerimientos de Tecnologías de la Información (TI) que corresponden a solicitudes de suministros (tóner, cartuchos de tinta, cintas, unidades de imagen y kit de mantenimiento) para las impresoras y plotter de la Secretaria Distrital de Integración Social.

3.9 Encuesta de satisfacción

La encuesta de satisfacción es generada por la herramienta de gestión cuando el ticket es solucionado y es enviada al correo del usuario de forma automática, el usuario solicitante califica y aprueba o desaprueba la solución del ticket. Si el usuario no contesta la encuesta de satisfacción, no puede aprobar o desaprobar la solución de este, al igual, si el usuario no contesta la encuesta, la herramienta de gestión realiza el cierre del ticket de forma automática pasados dos (2) días hábiles después de haberse solucionado.

Si el caso es desaprobado se realizará reapertura del mismo y se iniciará una nueva atención prioritaria.

4. Descripción de actividades



5. Disposiciones de almacenamiento y archivo

Las disposiciones de almacenamiento y archivo de la documentación del Sistema Integrado de Gestión, se realizará de conformidad con lo dispuesto en el Subsistema de Gestión Documental y Archivo (SIGA).

6. Dependencia encargada de administrar este procedimiento

Subdirección de Investigación e Información.

7. Documentos asociados

- PCD-SMT-007 Procedimiento Creación de usuarios y asignación de perfiles.
- FOR-MS-006 Formato Solicitud de creación, modificación o desactivación de usuarios y asignación de perfiles
- PCD-SMT-006 Procedimiento Gestión de Incidentes de Tecnologías de la Información
- PCD-SMT-012 Procedimiento Gestión de incidentes de Seguridad de la Información
- PCD-SMT-001 Procedimiento Gestión de cambios de Tecnologías de la Información
- PCD-SMT-009 Procedimiento Gestión de quejas, reclamos y felicitaciones de la mesa de servicios
- PCD-SMT-002 Procedimiento Solicitud de suministro para impresora o plotter

8. Aprobación del documento

	Elaboró	Revisó	Aprobó
Nombre	Jelly Suleyma Cubillos Gomez	Santiago Sandoval Bautista Mayra Andrea Ruiz Abello	Luis Armando Solarte Solarte
Cargo/ Rol	Contratista – Subdirección de Investigación e Información	Contratista - Subdirección de Investigación e Información Contratista - Gestora SG del proceso Gestión de soporte y mantenimiento tecnológico	Subdirector de Investigación e Información

1. Objetivo

Definir parámetros de detección, reporte y evaluación de los eventos de incidentes de seguridad de la información, con el fin de realizar su gestión y lograr la mejora continua de la seguridad de la información de la Secretaría Distrital de Integración Social-SDIS.

2. Glosario

Activo: cualquier cosa que tiene valor para la entidad, bienes, derechos, información y otros recursos con los que se dispone.

Activo de información: hace referencia a la información que se recibe, transforma y produce en la entidad u organismo distrital en el cumplimiento de sus funciones, estos pueden ser 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[1].

Cambio: adición, modificación o eliminación de algo que podría afectar los servicios de las Tecnologías de la Información-TI. El alcance debería incluir todos los servicios de TI, elementos de configuración, procesos, documentación entre otros, los cuales pueden generar indisponibilidad por lo que deben ser evaluados por el comité de control de cambios. Entre ellos están los que solucionan fallos conocidos, mejoramiento referente a soluciones, productos nuevos (Hardware/Software), eliminación de recursos y productos, exigencias legales y obligaciones contractuales[2].

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

Comité de Control de Cambios -CCC: grupo interno interdisciplinar encargado de revisar y aprobar los requerimientos de cambio de forma periódica[3].

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados[4].

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada[5].

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[6].

---

[1] Décimo primer lineamiento, inventario de activos de información-Sistema Integrado de Gestión Distrital
[2] Fundamentos de ITIL® - Volumen3 2008
[3] PCD-MS-001 Procedimiento Gestión de Cambios de Tecnologías de la Información.
[4] Norma Técnica Colombiana NTC-ISO-IEC 27001
[5] Ibíd.
[6] Guía Técnica Colombiana NTC-ISO-IEC 27035.

Herramienta de gestión: medio por el cual los usuarios internos registran las novedades, incidentes, requerimientos y demás solicitudes relacionadas con las TI. Este es el punto de contacto de los usuarios internos con la Subdirección de Investigación e Información.

Incidente mayor: es todo incidente de seguridad de la información que genera afectación considerable en la confidencialidad, integridad o disponibilidad de la información.

Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información[7].

Incidente de tecnología: es la interrupción no planificada de un servicio tecnológico que afecta la operación normal. Estos no afectan ni exponen la información de la entidad.

Información: se entiende por información todo aquel 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 entidad o de fuentes externas) o de la fecha de elaboración[8].

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos[9].

Seguridad de la información (SI): preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad[10].

Spam: correo basura o mensaje basura a los mensajes no solicitados, son tipo publicitario, enviados de forma masiva, que perjudican de alguna o varias maneras al receptor.

3. Condiciones generales

En el marco de este procedimiento, un incidente de seguridad de la información se puede identificar como todo evento o serie de eventos que tienen probabilidad significativa de comprometer la operación interna y/o los servicios sociales, amenazando la confidencialidad, integridad y/o disponibilidad de la información.

Los demás eventos que se presenten a nivel tecnológico y no afectan o exponen la información de la entidad serán tratados como incidentes de tecnologías de la información, de acuerdo al procedimiento Gestión de incidentes de Tecnologías de la Información (PCD-SMT-006).

[7] Ibíd.
[8] Norma Técnica Colombiana NTC-ISO-IEC 27001.
[9] Ibíd.
[10] Norma Técnica Colombiana NTC-ISO-IEC 27001.

3.1. Responsabilidades

Es responsabilidad de los funcionarios y contratistas reportar todos los posibles incidentes de seguridad de la información a la mesa de servicio, a través de:

- Mensaje de correo electrónico con la solicitud a mesadeservicio1035@sdis.gov.co.
- Llamada a la mesa de servicio a la extensión 1035.
- Reporte en la herramienta de gestión.

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

- Nombre de funcionario o contratista que reporta el incidente.
- Teléfono y/o extensión de contacto.
- Correo electrónico.
- Descripción completa del posible incidente.

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

- Relacionar el posible incidente con una afectación en la integridad, disponibilidad y confidencialidad 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, datos que podrán ser utilizados en la investigación y/o para empezar a contener los daños y minimizar el riesgo.

Para identificar si el incidente es real o potencial, se requiere de la información o consideraciones emitidas en el ítem anterior.

Una vez se reciba la notificación de un incidente de seguridad de información, la mesa de servicio debe realizar la primera categorización del mismo (de acuerdo con el árbol de categorías de la herramienta de gestión que utiliza la mesa de servicios) para iniciar con la atención del mismo.

El grupo de seguridad de la información hará la tipificación del incidente y documentará las acciones adelantadas para tratar el incidente.

Se deben conservar las pruebas recopiladas, las cuales serán custodiadas por el líder de Seguridad de la información, con el fin de reducir la probabilidad de que las evidencias se modifiquen o se consideren no aceptables en el caso de una investigación.

El líder de Seguridad de la Información notificará a la Oficina de Asuntos Disciplinarios[11], a la Oficina Asesora Jurídica[12], y a la Alta Consejería Distrital de Tecnologías de Información y Comunicaciones los incidentes de seguridad de la información con consecuencias mayores o

[11] Resolución 607 de 2007, Articulo 8, literal d
[12] Resolución 607 de 2007, Articulo 5, literal f

catastróficas (De acuerdo a las definiciones de la tabla 4 Consecuencias de los incidentes de seguridad de la información) para el trámite correspondiente, según sea el caso.

3.2. Clasificación de los incidentes de seguridad de la información

Los incidentes de seguridad de la información se clasifican, así:

Tabla 1 Clases de incidentes de seguridad de la información

Clases de incidentes de SI	Descripción de la causa raíz	Ejemplo
Daño físico	Debido a acciones físicas accidentadas en las instalaciones de la Entidad.	Incendio, agua, ambiente nefasto (contaminación, polvo, corrosión, congelamiento), destrucción de equipos, destrucción de medios, robo de equipos, robo de medios, etc.
Malware	Causas asociadas de programas maliciosos creados y divulgados en forma intencional.	Virus informáticos, gusanos de red, troyanos, botnet (red de robots), ataques combinados, páginas web con códigos maliciosos, sitio hosting con códigos maliciosos, etc.
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.
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, “chuzada” de teléfonos, divulgación, enmascaramiento, ingeniería social, phishing de redes (Suplantación de identidad), robo de datos, alteración de datos, errores de datos, etc.
Violación de reglas	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.

Fuente:*Basado en la Guía Técnica Colombiana 27035:2012.

Un incidente de seguridad de la información que se identifique en varias de las clases citadas debe ser clasificado por la solicitud padre, de acuerdo con la tabla 1.

3.3. Tipificación en prioridad de los incidentes de seguridad de la información

Para la correcta gestión, todos los incidentes de seguridad de la información deberán tipificarse en prioridad de acuerdo con su impacto y urgencia por el gestor de Incidentes de Seguridad de la Información:

Tabla 2 Nivel de prioridad de los incidentes de seguridad de la información

Nivel de prioridad			
Impacto/Urgencia	Alta	Media	Baja
Alto	Alta	Alta	Media
Medio	Alta	Media	Baja
Bajo	Media	Baja	Baja

Tabla 3 Descripción del nivel de prioridad de los incidentes de seguridad de la información

Prioridad	Alcance	Descripción
ALTO	El incidente de seguridad puede afectar la continuidad de la prestación de los servicios sociales de la Entidad.	El incidente alto tiene un impacto considerable (afectación total a la confidencialidad, disponibilidad o integridad) en la información y se considera crítica para la misión de la Entidad, esto incluye información en diferentes medios y/o sistemas críticos. Estos incidentes implican una grave violación de seguridad o pueden dañar la confianza en la administración pública (pérdida de imagen institucional), o podrían afectar la seguridad física de las personas, causar una pérdida importante de recursos de la SDIS.
MEDIO	El incidente de seguridad afecta a una o más dependencias, (por ejemplo, nivel central, subdirecciones locales, etc.).	Se clasifican con este nivel aquellos eventos que puedan afectar o está afectando a los activos de información de la Entidad, con una valoración considerable en la triada de la información (confidencialidad, disponibilidad o integridad), lo cual puede resultar en la pérdida directa de información para la SDIS.
BAJO	El incidente afecta a un colaborador o varios colaboradores de una dependencia.	Se clasifican con este nivel aquellos eventos que puedan ser una amenaza que afecta o está afectando a activos de información de la SDIS con una valoración de impacto limitado en la triada de la información (confidencialidad, disponibilidad o integridad). Su impacto debe ser nulo o insignificante para la Entidad.

En caso de que el incidente de seguridad de la información se considere de prioridad alta, el grupo de seguridad de la información de la Entidad deberá proponer el equipo que participará en el tratamiento del incidente.

Los incidentes de seguridad de la información que no se consideren prioridad alta estarán liderados por el líder de seguridad de la información de la SDIS.

3.4. Prioridades de tratamiento de incidentes de seguridad de la información

Se debe actuar para reducir los efectos reales y potenciales de un incidente, ya que esto puede marcar la diferencia entre un impacto menor o uno de mayor importancia, ver tabla 3. La respuesta exacta dependerá de la naturaleza del incidente al que se enfrente. No obstante, se sugieren las siguientes prioridades como punto de partida:

- ✓ Proteger la vida humana y la seguridad de las personas.
- ✓ Proteger la información reservada y confidencial.
- ✓ Proteger otra información relevante (por ejemplo, propiedad intelectual o del ámbito directivo).
- ✓ Proteger el hardware y software de la SDIS.
- ✓ Minimizar la interrupción de los servicios tecnológicos.

Existen varias medidas que se pueden tomar para contener el daño y minimizar el riesgo en el entorno. Como mínimo debe llevar a cabo las siguientes acciones:

- ✓ Realizar análisis de vulnerabilidades a las aplicaciones y la infraestructura tecnológica de manera periódica con el fin de minimizar el riesgo de ataques,
- ✓ Asegurar el cambio periódico de las contraseñas: locales, de las cuentas de servicio y administrativas en todo el entorno.
- ✓ Documentar cada cambio realizado en los sistemas en producción.

3.5. Posibles acciones a los incidentes de seguridad de la información

- ✓ Una solución efectiva: la gestión del incidente logró remediar los servicios o activos afectados por el incidente.
- ✓ Una solución provisional: la gestión del incidente logró remediar los servicios o activos afectados por el incidente, sin embargo, no se puede identificar la totalidad de la remediación a primera mano.
- ✓ Una solución que relaciona un cambio: la gestión del incidente logró remediar los servicios o activos afectados por el incidente, sin embargo, el incidente puede replicarse, siendo necesario ejecutar un cambio para evitar reincidencia.

Cualquier incidente que implique interrupción de algún servicio social o afectación a un proceso de manera crítica, ya sea por el número de usuarios afectados o porque se han visto involucrados sistemas o servicios sociales para la SDIS, se debe dar una respuesta, que puede incluir la generación de un control de cambios para lo cual se deberá tener en cuenta las actividades del procedimiento de Gestión de Cambios de Tecnologías de la Información (PCD-SMT-001).

La valoración del incidente de seguridad de la información se realizará por el líder de seguridad de la información de la SDIS para determinar las consecuencias, las cuales constituirán una prueba importante y necesaria si se decide emprender acciones legales. Entre ellos, se pueden contar con los siguientes:

- Consecuencias asociadas a la pérdida de información confidencial.
- Consecuencias legales.
- Consecuencias laborales por el análisis de los incidentes, la reinstalación del software y la recuperación de datos.
- Consecuencias en el tiempo de inactividad de los sistemas (por ejemplo, pérdida de productividad de los funcionarios y/o contratistas, sustitución del hardware, del software y de otras propiedades).
- Consecuencias relacionadas con la reparación y posible actualización de las medidas de seguridad físicas dañadas o ineficaces (cierres, paredes, cajas, etc.).
- Consecuencias relacionadas con la imagen del proceso afectado por un incidente.
- Otros daños derivados, como la pérdida de la reputación o de la confianza de los beneficiarios de la SDIS.

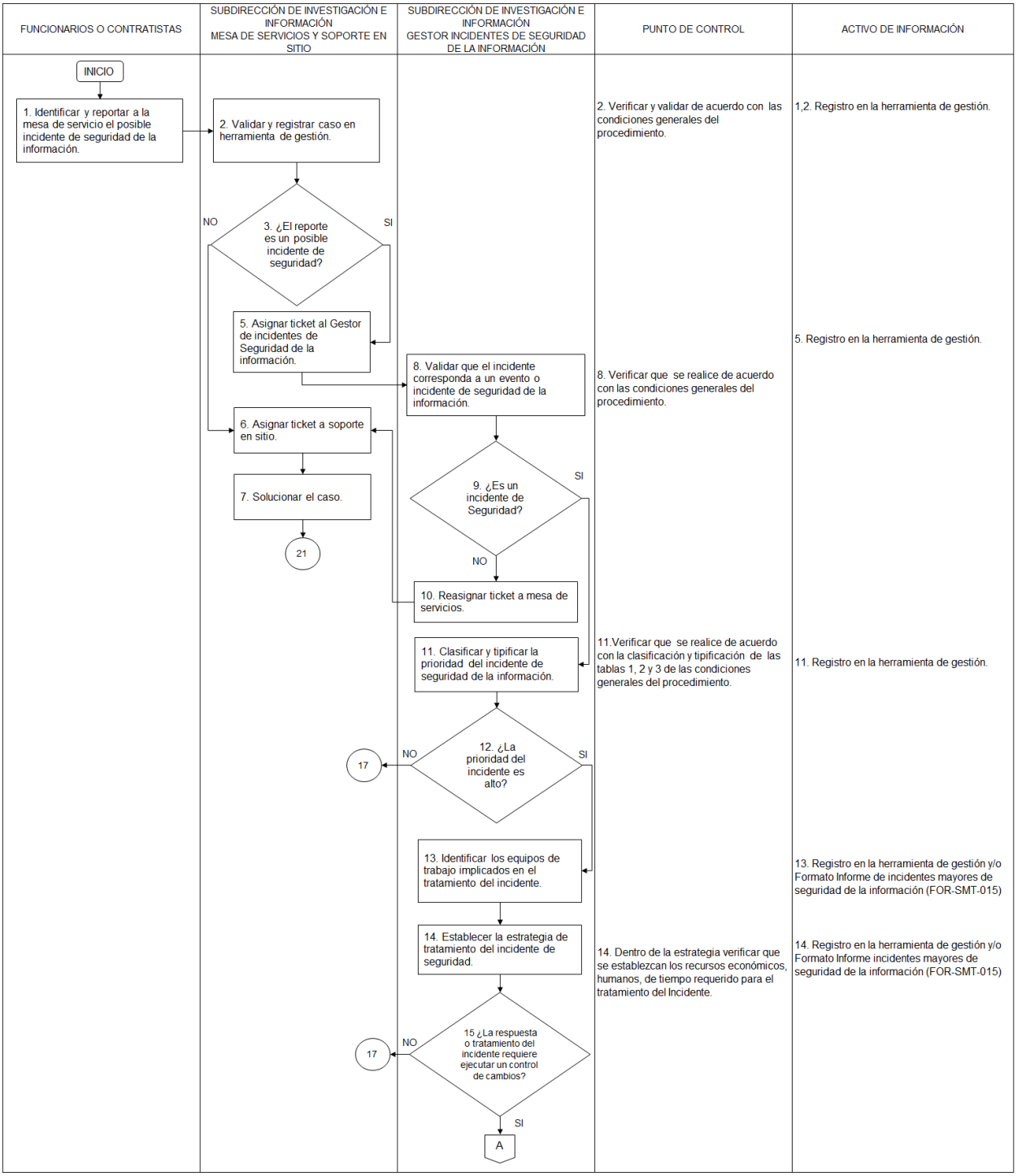
Se utilizará la siguiente tabla para valorar las consecuencias de los incidentes de seguridad de la información en la SDIS:

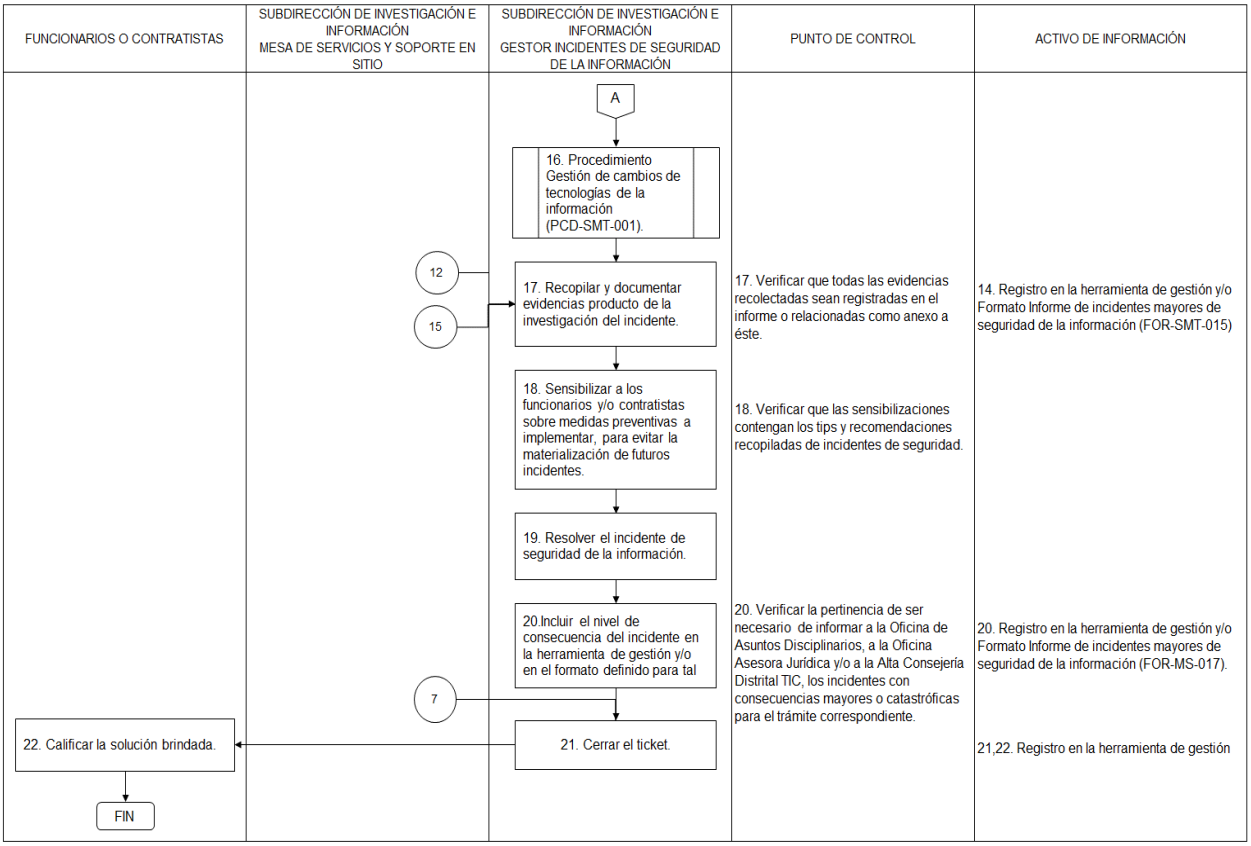
Tabla 4 Consecuencias de los incidentes de seguridad de la información

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderada	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Catastrófica	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Debe tenerse en cuenta que los incidentes deben clasificarse únicamente en un descriptor de consecuencia y puede tener incumplimiento legal, sanciones, costos, pérdida de imagen o afectación de la operación de la SDIS.

4. Descripción de actividades





5. Disposiciones de almacenamiento y archivo

Las disposiciones de almacenamiento y archivo de la documentación del Sistema Integrado de Gestión, se realizará de conformidad con lo dispuesto en el Subsistema Interno de Gestión Documental y Archivo (SIGA)

6. Dependencia encargada de administrar este procedimiento

Subdirección de Investigación e Información.

7. Documentos asociados

FOR-SMT-007 Formato informe de incidentes de seguridad de la información

8. Aprobación del documento

	Elaboró	Revisó	Aprobó
Nombre	Isis Johana Gomez Peralta	Mauricio Tellez Saavedra Mayra Andrea Ruiz Abello	Luis Armando Solarte Solarte
Cargo/ Rol	Contratista Subdirección de Investigación e Información	Oficial de Seguridad de la Información Contratista Gestora SG del proceso Gestión de soporte y mantenimiento tecnológico	Subdirector de Investigación e Información

SECCIÓN A. Identificación y análisis											SECCIÓN B. Valoración y tratamiento											
Proceso	Objetivo del proceso	Circular y fecha de oficialización	Código	Causas	Riesgo	Consecuencias	Clasificación	Riesgo Inherente			Actividad de control	Tipo de actividad de control	¿Debe establecer acciones para fortalecer las actividades de control?	Riesgo Residual			Decisión del líder de proceso	Plan de tratamiento					
								Probabilidad	Impacto	Nivel				Probabilidad	Impacto	Nivel		Actividades a desarrollar	Responsable	Indicador o criterio de medición	Meta	Fecha de inicio	Fecha de terminación
Gestión de soporte y Mantenimiento tecnológico.	El proceso de gestión de soporte y mantenimiento tecnológico busca gestionar la continuidad del negocio mediante el soporte y mantenimiento de las Tecnologías de la Información y las Comunicaciones, acogiendo las mejores prácticas de TIC, los lineamientos y directrices internos y la normativa vigente para coadyuvar el cumplimiento de los objetivos institucionales.		RC-SMT-001	1. Carencia de controles en la administración de la infraestructura tecnológica.	**Posibilidad de un mal uso de las credenciales asignadas para la administración de los recursos tecnológicos de la Entidad con el fin de obtener un beneficio propio o para terceros.**	* Parálisis en los procesos. *Demandas y demás acciones jurídicas. * Detrimento de la imagen de la entidad ante sus grupos de valor. * Investigaciones disciplinarias.	Tecnológico	2 - Improbable	5 - Catastrófico	Extremo	El líder de servicios realiza cambios permanentemente en los ambientes de producción bajo lo establecido en el procedimiento Gestión de cambios de tecnologías de la información, específicamente en la revisión del cambio de emergencia, vota por la aprobación o no del cambio y realiza el Comité de control de cambios CAB; en caso de que sea requerido realizar un control de cambios de emergencia y en su momento no se cuente con el líder de servicio, la Subdirectora de Investigación e Información dará la aprobación. Evidencia: formatos Requerimiento de cambio.	Preventiva	NO	1 - Raro	5 - Catastrófico	Extremo	Reducir	El líder de servicios realiza cambios permanentemente en los ambientes de producción bajo lo establecido en el procedimiento Gestión de cambios de tecnologías de la información, específicamente en la revisión del cambio de emergencia, vota por la aprobación o no del cambio y realiza el Comité de control de cambios CAB; en caso de que sea requerido realizar un control de cambios de emergencia y en su momento no se cuente con el líder de servicio, la Subdirectora de Investigación e Información dará la aprobación. Evidencia: formatos Requerimiento de cambio.	Líder de servicios.	(Número de cambios realizados en los ambientes de producción / Total de cambios solicitados en los sistemas de información)*100	100%	########	30/11/2021
				2. Insuficiente capacitación del personal frente al buen uso del rol para la administración de los recursos tecnológicos de la Entidad.							El líder de infraestructura trimestralmente gestiona la ejecución de jornadas y/o piezas comunicativas de sensibilización a los colaboradores sobre el correcto uso de las credenciales asignadas para la administración de los recursos tecnológicos de la Entidad, en caso de no realizar dicha gestión, el Oficial de seguridad lo incluirá en las sensibilizaciones de seguridad de la información. Evidencia: listados de asistencia a las sensibilizaciones y/o piezas comunicativas.	Preventiva	NO					El líder de infraestructura trimestralmente gestiona la ejecución de jornadas y/o piezas comunicativas de sensibilización a los colaboradores sobre el correcto uso de las credenciales asignadas para la administración de los recursos tecnológicos de la Entidad, en caso de no realizar dicha gestión, el Oficial de seguridad lo incluirá en las sensibilizaciones de seguridad de la información. Evidencia: listados de asistencia a las sensibilizaciones y/o piezas comunicativas.	Líder de infraestructura.	(Número de sensibilizaciones realizadas al correcto uso de las credenciales asignadas para la administración de los recursos tecnológicos de la Entidad / Número de sensibilizaciones programadas al correcto uso de las credenciales asignadas para la administración de los recursos tecnológicos de la Entidad) * 100 Nota: 4 sensibilizaciones.	100%	########	30/11/2021

SECCIÓN A. Identificación y análisis											SECCIÓN B. Valoración y tratamiento											
Proceso	Objetivo del proceso	Circular y fecha de oficialización		Activo de Información	Amenazas / Vulnerabilidades	Riesgo	Consecuencias	Riesgo Inherente			Actividad de control	Tipo de actividad de control	¿Debe establecer acciones para fortalecer las actividades de control?	Riesgo Residual			Plan de tratamiento					
			Código					Probabilidad	Impacto	Nivel				Probabilidad	Impacto	Nivel	Actividades a desarrollar	Responsable	Indicador o criterio de medición	Meta	Fecha de inicio	Fecha de terminación
Gestión de soporte y mantenimiento tecnológico	El proceso de gestión de soporte y mantenimiento tecnológico busca gestionar la continuidad del negocio mediante el soporte y mantenimiento de las Tecnologías de la Información y las Comunicaciones, acogiendo las mejores prácticas de TIC, los lineamientos y directrices internos y la normativa vigente para coadyuvar el cumplimiento de los objetivos institucionales.		RS-SMT-001	SIRBE - Comisarias - Nóminas/Hojas De Vida (Recursos Humanos) - Web - Nómina RRHDAT – Bd - Nómina Web - Siap – Bd - Nómina Sistema Información de Administración de Personal - Siap – Bd - IOPS - (Nuevo) - The Gnu Crypto Project - Nómina Delfi - Kactus - Seven Erp - Software De Enrolamiento - Biometría - Invict - Oralidad - Centros Forjar - Ciudad Bolívar - Centros Forjar Suba - Centros Forjar Rafael Uribe - Radicaciones	* Fallas técnicas. * Mal funcionamiento del software. * Compromiso de las funciones. * Error en el uso o abuso de derechos *Software. * Asignación errada de los derechos de acceso. * Ausencia de terminación de sesión. * Interfaz de usuario compleja. * Ausencia de documentación.	Pérdida de Confidencialidad, Integridad y Disponibilidad de los activos de información	* No prestar soporte sobre las aplicaciones que están en producción. * Procesos Disciplinarios por la pérdida de confidencialidad, integridad y/o disponibilidad del sistema de información. * Reprocesos internos y elevación de costos sobre la información levantada previamente. * Insatisfacción del cliente interno y externo.	4 - Probable	4 - Mayor	Extremo	El funcionario o contratista encargado de ejecutar las actividades de líder de soluciones tecnológicas verificará cada vez que se genere una nueva versión o se implemente un nuevo desarrollo de los sistemas de información o se adquiera un nuevo sistema de información, se le socialice a los usuarios el manual del sistema de información, procedimiento de creación, activación y desactivación de usuarios, la responsabilidad en el uso de los usuarios y las contraseñas y la trazabilidad que dejan. En caso que la socialización no sea efectiva, se revisarán las incidencias y requerimientos presentados por los usuarios en mesa de ayuda y se realizará refuerzo en los temas más recurrentes. La evidencia será la planilla o listado de asistencia de la socialización realizada. En caso de que la socialización no sea efectiva, se revisarán.	Preventiva	Si	3 - Posible	2 - Menor	Moderado	1.Socializar el procedimiento de creación, activación y desactivación de usuarios, con el propósito de que los usuarios conozcan como crear, activar y desactivar usuarios en un sistema de información.	El funcionario o contratista encargado de ejecutar las actividades de líder de soluciones tecnológicas.	N° de socializaciones ejecutadas /Socializaciones planeadas * 100	3 Socializaciones realizadas.	abr-21	ene-22
																	2.Realizar campañas de socialización y educación en seguridad de la información, haciendo énfasis en la confidencialidad y los controles de acceso para salvaguardar esta propiedad.	El funcionario o contratista encargado de ejecutar las actividades de líder de soluciones tecnológicas.	Actividades ejecutadas /Actividades planeadas * 100	100% del Cumplimiento de las actividades definidas en el Plan de sensibilización, capacitación y comunicación de seguridad y privacidad de la información.	abr-21	ene-22
																	3.Realizar socializaciones a los usuarios en temas uso y apropiación de los sistemas de información.	El funcionario o contratista encargado de ejecutar las actividades de líder de soluciones tecnológicas.	No. De socializaciones ejecutadas / Socializaciones planeadas * 100	100% del Cumplimiento de las actividades definidas en la estrategia de Uso y Apropiación.	abr-21	ene-22
																	4.Mantener actualizados los manuales de los sistemas de información.	El funcionario o contratista encargado de ejecutar las actividades de líder de soluciones tecnológicas o quien este designe.	No. Manuales actualizados / No. Total de sistemas de Información identificados como activos de información críticos* 100	100% de manuales de usuario de los sistemas de Información identificados como activos de información críticos.	abr-21	ene-22
Gestión de soporte y mantenimiento tecnológico	El proceso de gestión de soporte y mantenimiento tecnológico busca gestionar la continuidad del negocio mediante el soporte y mantenimiento de las Tecnologías de la Información y las Comunicaciones, acogiendo las mejores prácticas de TIC, los lineamientos y directrices internos y la normativa vigente para coadyuvar el cumplimiento de los objetivos institucionales.		RS-SMT-002	RAD - (REGISTRO DE ASISTENCIA DIARIA) - COMEDORES - SICO -CORRESPONDENCIA WEB - DATASIX _CONTABILIDAD - "HEFI - HERRAMIENTA FINANCIERA - SISPAGOS" - HERRAMIENTA CONTRATACION - LOGIN SDIS - Nómina SIAP Antiguo - Nómina HSIAP - Informes SDIS - Historias laborales - Kactus Self-services - AZDigital	* Fallas técnicas. * Mal funcionamiento del software. * Red. * Líneas de comunicación sin protección. * Punto único de falla.	Pérdida de Integridad y Disponibilidad de los activos de información	* Reprocesos internos y elevación de costos sobre la información levantada previamente. * Insatisfacción del cliente.	3 - Posible	3 - Moderado	Alto	El funcionario o contratista encargado de ejecutar las actividades de líder de infraestructura debe monitorear los servicios de tecnología que soportan los sistemas de información con el fin de evitar la indisponibilidad de un sistema de información o actuar de manera oportuna cuando un servicio falle, este monitoreo se debe evidenciar en un informe. El funcionario o contratista encargado de ejecutar las actividades de oficial de seguridad realizará la verificación mensual de este informe. En caso de que un servicio falle causando que el sistema de información no esté disponible, se debe verificar la causa de su fallo y generar un plan de acción para que no vuelva a ocurrir. La Evidencia es el informe de monitoreo junto con la revisión mensual del oficial de seguridad.	Preventiva	Si	3 - Posible	2 - Menor	Moderado	Monitorear los servicios de tecnología que soportan los sistemas de información diariamente (días hábiles) con el fin de detectar la caída de un sistema de información o actuar de manera oportuna cuando un servicio falle, este monitoreo se debe evidenciar en un informe.	El funcionario o contratista encargado de ejecutar las actividades de líder de infraestructura o quien este designe	Porcentaje de disponibilidad de los servicios monitoreados	99,95% de disponibilidad de los servicios monitoreos	abr-21	ene-22
																	Configurar certificados seguros en todas las aplicaciones con el fin de garantizar el cifrado de la información.	El funcionario o contratista encargado de ejecutar las actividades de líder de infraestructura o quien este designe	No. de sistemas de información con certificados seguros monitoreados / No. Total de sistemas de información catalogados como activos críticos *100	100% de sistemas de información catalogados como críticos.	abr-21	ene-22
Gestión de soporte y mantenimiento tecnológico	El proceso de gestión de soporte y mantenimiento tecnológico busca gestionar la continuidad del negocio mediante el soporte y mantenimiento de las Tecnologías de la Información y las Comunicaciones, acogiendo las mejores prácticas de TIC, los lineamientos y directrices internos y la normativa		RC-SMT-003	Acciones de mejora -Asistencias	* Acciones de mejora. * Asistencias. * Red. * Tráfico sensible sin protección.	Pérdida de Integridad de los activos de información	* Reporte de información fuera del tiempo requerido en el área funcional. * Aumento de solicitudes de soporte técnico. * Reprocesos internos y elevación de costos sobre la información levantada previamente. * Insatisfacción del cliente.	3 - Posible	3 - Moderado	Alto	El funcionario o contratista encargado de ejecutar las actividades de líder de soluciones tecnológicas realizará pruebas no funcionales para verificar la integridad de la información cada vez que se genere una nueva versión o se implemente un nuevo desarrollo de los sistemas de información, con el fin de evitar la alteración de los datos. En caso que los datos se corrompan se revisara en el área de desarrollo para validar la causa, remediarla e iniciar nuevamente la prueba. La evidencia será el plan de pruebas.	Preventiva	Si	3 - Posible	2 - Menor	Moderado	Realizar las pruebas no funcionales cada vez que se genere una nueva versión o se implemente un nuevo desarrollo de los sistemas de información.	El funcionario o contratista encargado de ejecutar las actividades de líder de soluciones tecnológicas o quien este designe	No. de pruebas no funcionales exitosas / No. Total de pruebas realizadas sobre los sistemas de información catalogados como activos críticos *100	100% de pruebas no funcionales realizadas.	abr-21	ene-22

SECCIÓN A. Identificación y análisis											SECCIÓN B. Valoración y tratamiento												
Proceso	Objetivo del proceso	Circular y fecha de oficialización	Código	Causas	Riesgo	Consecuencias	Clasificación	Riesgo Inherente			Actividad de control	Tipo de actividad de control	¿Debe establecer acciones para fortalecer las actividades de control?	Riesgo Residual			Decisión del lider de proceso	Plan de tratamiento					
								Probabilidad	Impacto	Nivel				Probabilidad	Impacto	Nivel		Actividades a desarrollar	Responsable	Indicador o criterio de medición	Meta	Fecha de inicio	Fecha de terminación
Gestión Contractual	El proceso de Gestión contractual consiste en adelantar las actividades de contratación requeridas por la entidad, previstas en el plan de adquisiciones que permitan contar con bienes, servicios y obras de manera efectiva, oportuna y cumpliendo la normatividad vigente (para cada modalidad contractual) para el desarrollo en el cumplimiento de la misión de la entidad.		RC-GEC-001	1. Inadecuada elaboración de los documentos previos, tales como estudios previos, pliegos de condiciones, análisis del sector y estudio de mercado	**Posibilidad de direccionar la contratación y/o vinculación a favor de un tercero no presentando claridad tanto en los anexos técnicos como en los estudios previos que posibilitan que la selección de proveedores no se realice de forma eficiente y transparente**	*Incredulidad en la ética, transparencia e imparcialidad del personal directivo para otorgar la contratación con el debido proceso. *Pérdida de la imagen, la credibilidad, la transparencia y la probidad de la Entidad.	Estratégico	4 - Probable	3 - Moderado	Alto	El líder del proceso de Gestión Contractual cita y lidera los comités de contratación cuando requiera de ello, con el objetivo de asesorar a las diferentes dependencias en las etapas precontractual, contractual y post contractual para satisfacer las necesidades misionales y transversales de la Entidad, así como en materia de políticas y de buenas prácticas en la contratación pública. Como evidencia se cuenta con la citación del comité y actas de las mismas. En caso de que no se pueda llevar a cabo el comité se enviará memorando a las diferentes áreas técnicas.	Preventiva	NO	3 - Posible	3 - Moderado	Alto	Reducir	El líder del proceso de Gestión Contractual cita y lidera los comités de contratación cuando requiera de ello, con el objetivo de asesorar a las diferentes dependencias en las etapas precontractual, contractual y post contractual para satisfacer las necesidades misionales y transversales de la Entidad, así como en materia de políticas y de buenas prácticas en la contratación pública. Como evidencia se cuenta con la citación del comité y actas de las mismas. En caso de que no se pueda llevar a cabo el comité se enviará memorando a las diferentes áreas técnicas.	Líder del proceso Gestión Contractual	(Número de actas de Comité de contratación / Número de Comités de contratación realizados) * 100	100%		30/11/2021
				2. Tráfico de influencias							El líder del proceso de Gestión Contractual cita y lidera los comités de contratación cuando requiera de ello, con el objetivo de asesorar a las diferentes dependencias en las etapas precontractual, contractual y post contractual para satisfacer las necesidades misionales y transversales de la Entidad, así como en materia de políticas y de buenas prácticas en la contratación pública. Como evidencia se cuenta con la citación del comité y actas de las mismas. En caso de que no se pueda llevar a cabo el comité se enviará memorando a las diferentes áreas técnicas.	Preventiva	NO					El líder del proceso de Gestión Contractual cita y lidera los comités de contratación cuando requiera de ello, con el objetivo de asesorar a las diferentes dependencias en las etapas precontractual, contractual y post contractual para satisfacer las necesidades misionales y transversales de la Entidad, así como en materia de políticas y de buenas prácticas en la contratación pública. Como evidencia se cuenta con la citación del comité y actas de las mismas. En caso de que no se pueda llevar a cabo el comité se enviará memorando a las diferentes áreas técnicas.	Líder del proceso Gestión Contractual	(Número de actas de Comité de contratación / Número de Comités de contratación realizados) * 100	100%		30/11/2021
			RC-GEC-002	1. Designación de supervisor que no cuenta con los conocimientos requeridos para ejercer la función	**Posibilidad de que se realice una supervisión e interventoría inadecuada por un interés ilícito en su ejercicio a través de la manipulación u omisión de funciones en beneficio del contratista o de un tercero**	* Adquisición de bienes, productos o servicios no acordes a las necesidades reales de la entidad o sin el cumplimiento de requisitos. * Detrimento patrimonial. * Investigaciones disciplinarias, penales, fiscales y civiles. * Incumplimiento clausulas del contrato (parcial o total).	Estratégico	4 - Probable	3 - Moderado	Alto	El líder del proceso de Gestión Contractual socializa semestralmente con los diferentes supervisores o apoyos a la supervisiones, las directrices y lineamientos oficiales y vigentes referente a la contratación institucional, así como los posibles incumplimientos cuando a ello hubiere lugar, según lo evidenciado en la supervisión. Como evidencia se cuenta con registro de las socializaciones realizadas (presentaciones, actas, listados de asistencias, entre otras). En caso de no poder hacer la socialización en el día definido se reprogramará y realizará a la mayor brevedad posible, acorde con la disponibilidad del líder.	Preventiva	NO	3 - Posible	3 - Moderado	Alto	Reducir	El líder del proceso de Gestión Contractual socializa semestralmente con los diferentes supervisores o apoyos a la supervisiones, las directrices y lineamientos oficiales y vigentes referente a la contratación institucional, así como los posibles incumplimientos cuando a ello hubiere lugar, según lo evidenciado en la supervisión. Como evidencia se cuenta con registro de las socializaciones realizadas (presentaciones, actas, listados de asistencias, entre otras). En caso de no poder hacer la socialización en el día definido se reprogramará y realizará a la mayor brevedad posible, acorde con la disponibilidad del líder.	Líder del proceso Gestión Contractual	(Número de socializaciones ejecutadas / Número de socializaciones programadas)* 100	100%		30/11/2021
				2. Mal ejercicio de la supervisión y/o interventoría							El líder del proceso de Gestión Contractual socializa semestralmente con los diferentes supervisores o apoyos a la supervisiones, las directrices y lineamientos oficiales y vigentes referente a la contratación institucional, así como los posibles incumplimientos cuando a ello hubiere lugar, según lo evidenciado en la supervisión. Como evidencia se cuenta con registro de las socializaciones realizadas (presentaciones, actas, listados de asistencias, entre otras). En caso de no poder hacer la socialización en el día definido se reprogramará y realizará a la mayor brevedad posible, acorde con la disponibilidad del líder.	Preventiva	NO					El líder del proceso de Gestión Contractual socializa semestralmente con los diferentes supervisores o apoyos a la supervisiones, las directrices y lineamientos oficiales y vigentes referente a la contratación institucional, así como los posibles incumplimientos cuando a ello hubiere lugar, según lo evidenciado en la supervisión. Como evidencia se cuenta con registro de las socializaciones realizadas (presentaciones, actas, listados de asistencias, entre otras). En caso de no poder hacer la socialización en el día definido se reprogramará y realizará a la mayor brevedad posible, acorde con la disponibilidad del líder.	Líder del proceso Gestión Contractual	(Número de socializaciones ejecutadas / Número de socializaciones programadas)* 100	100%		30/11/2021

PROCESO GESTIÓN DEL SISTEMA INTEGRADO - SIG

FORMATO MAPA Y PLAN DE TRATAMIENTO DE RIESGOS

Mapa de riesgos de: Gestión

SECCIÓN A. Identificación y análisis											SECCIÓN B. Valoración y tratamiento												
Proceso	Objetivo del proceso	Circular y fecha de oficialización	Código	Causas	Riesgo	Consecuencias	Clasificación	Riesgo Inherente			Actividad de control	Tipo de actividad de control	¿Debe establecer acciones para fortalecer las actividades de control?	Riesgo Residual			Decisión del líder de proceso	Plan de tratamiento					
								Probabilidad	Impacto	Nivel				Probabilidad	Impacto	Nivel		Actividades a desarrollar	Responsable	Indicador o criterio de medición	Meta	Fecha de inicio	Fecha de terminación
Gestión Contractual	Adelantar las actividades de contratación requeridas por la entidad, previstas en el proceso de gestión contractual que permitan contar con bienes, servicios y obras de manera efectiva, oportuna y cumpliendo la normatividad vigente (para cada modalidad contractual) para el desarrollo en el cumplimiento de la misión de la Entidad.		R-GEC-002	Deficiencia en el ejercicio de la supervisión y/o interventoría	Pérdida de información en los expedientes que soportan la ejecución del proceso contractual	* Investigaciones disciplinarias, fiscales y penales * Demandas	Operativo	4 - Probable	3 - Moderado	Alto	1. El líder del proceso de Gestión Contractual socializa semestralmente con los diferentes supervisores o apoyos a la supervisiones, las directrices y lineamientos oficiales y vigentes referente a la contratación institucional, documentación de los expedientes, así como los posibles incumplimientos cuando a ello hubiere lugar, según lo evidenciado en la supervisión. Como evidencia se cuenta con registro de las socializaciones realizadas (presentaciones, actas, listados de asistencias, entre otras). En caso de no poder hacer la socialización en el día definido se reprogramará y realizará a la mayor brevedad posible, acorde con la disponibilidad del líder.	Preventiva	NO	3 - Posible	3 - Moderado	Alto	Reducir	1. El líder del proceso de Gestión Contractual socializa semestralmente con los diferentes supervisores o apoyos a la supervisiones, las directrices y lineamientos oficiales y vigentes referente a la contratación institucional, documentación de los expedientes, así como los posibles incumplimientos cuando a ello hubiere lugar, según lo evidenciado en la supervisión. Como evidencia se cuenta con registro de las socializaciones realizadas (presentaciones, actas, listados de asistencias, entre otras), En caso de no poder hacer la socialización en el día definido se reprogramará y realizará a la mayor brevedad posible, acorde con la disponibilidad del líder.	Líder del proceso	(Número de socializaciones ejecutadas / Número de socializaciones programadas)*100	100%		31/12/2021
											2. El Subdirector de Contratación envía memorandos de manera trimestral a los supervisores de contrato, con el fin de recordar la obligación de gestionar la documentación que se genera en la ejecución contractual, de acuerdo a como se produce en la plataforma transaccional del SECOP II. En caso de no emitir el memorando se envían correos trimestrales por el/la Subdirector de Contratación. Como evidencia de esta actividad, quedan os memorandos o los correos.	Preventiva	NO					2. El Subdirector de Contratación envía memorandos de manera trimestral a los supervisores de contrato, con el fin de recordar la obligación de gestionar la documentación que se genera en la ejecución contractual, de acuerdo a como se produce en la plataforma transaccional del SECOP II. En caso de no emitir el memorando se envían correos trimestrales por el/la Subdirector de Contratación. Como evidencia de esta actividad, quedan los memorandos o los correos.	Líder del proceso	(N° de memorando enviados en el periodo / N° de memorandos programadas para el periodo) *100%	100%		31/12/2021
			R-GEC-003	Desconocimiento o por parte de las dependencias de los procedimientos establecidos para el control de riesgos asociados a la contratación	Posible retraso en la actualización de las directrices oficiales para la modernización del proceso de contratación	* Detrimento patrimonial * Desconocimiento institucional de hechos que puedan afectar los procesos contractuales. * Incumplimiento con los objetivos estratégicos de la Entidad	Estratégico	3 - Posible	3 - Moderado	Alto	Cada vez que las dependencias inician un proceso de contratación, remiten la solicitud del aval de la respectiva matriz de riesgos previsibles inherentes a la compra o contratación de bienes y/o servicios, a los profesionales designados en la Subdirección de Contratación de acuerdo con lo definido en el *"Procedimiento Administración de riesgos previsibles inherentes a la compra o contratación de bienes o servicios"* , quienes revisan y avalan que los ordenadores de gasto hayan realizado un análisis de los posibles eventos que se puedan presentar en desarrollo de las actividades contratadas. En caso que las áreas radiquen un proceso sin la matriz de riesgos avalada, se procede con la devolución de la misma para que se surta con este trámite. Como evidencia se cuenta con los correos electrónicos de aval y una matriz de consolidado trimestral con la relación de solicitudes y avales generados.	Preventiva	NO	2 - Improbable	2 - Menor	Bajo	Reducir	Cada vez que las dependencias inician una solicitud de contratación, remiten la solicitud del aval de la respectiva matriz de riesgos previsibles inherentes a la compra o contratación de bienes o servicios, a los profesionales designados en la Subdirección de Contratación de acuerdo con lo definido en el *Procedimiento Administración de riesgos previsibles inherentes a la compra o contratación de bienes o servicios* , quienes revisan y avalan que los ordenadores de gasto hayan realizado un análisis de los posibles eventos que se puedan presentar en desarrollo de las actividades contratadas. En caso que las áreas radiquen un proceso sin la matriz de riesgos avalada, se procede con la devolución de la misma para que se surta con este trámite. Como evidencia se cuenta con los correos electrónicos de aval y una matriz de consolidado trimestral con la relación de solicitudes y avales generados.	Profesionales designados para al revisión de matrices en la Subdirección de Contratación	(N° de matrices avaladas en el periodo / N° de solicitudes de matrices en el periodo) *100%	100%		31/12/2021

SECCIÓN A. Identificación y análisis											SECCIÓN B. Valoración y tratamiento												
Proceso	Objetivo del proceso	Circular y fecha de oficialización	Código	Causas	Riesgo	Consecuencias	Clasificación	Riesgo Inherente			Actividad de control	Tipo de actividad de control	¿Debe establecer acciones para fortalecer las actividades de control?	Riesgo Residual			Decisión del líder de proceso	Plan de tratamiento					
								Probabilidad	Impacto	Nivel				Probabilidad	Impacto	Nivel		Actividades a desarrollar	Responsable	Indicador o criterio de medición	Meta	Fecha de inicio	Fecha de terminación
Gestión de Infraestructura Física	Definir los lineamientos y atender las necesidades de intervención de infraestructura a través de las modalidades de construcción, modificación, ampliación, reforzamiento estructural y/o mantenimiento de los equipamientos o predios administrados por la Secretaría Distrital de Integración Social, para la prestación de los servicios sociales.		RC-GIF-001	1. Posibles intereses en la viabilidad de un equipamiento para ser tomado en arriendo, por quien propone el equipamiento .	**Probabilidad de emitir la viabilidad de equipamientos para ser tomados en arriendo en predios que no cumplen las condiciones técnicas mínimas exigidas por la SDIS, con el fin de beneficiar intereses particulares.**	* Predios que por no cumplir las condiciones técnicas o de gestión predial exigidas, presenten alguna afectación del predio o deterioro en la infraestructura que impida la adecuada prestación del servicio.	Estratégico	2 - Improbable	4 - Mayor	Alto	La coordinación del área de Gestión Predial y Mantenimiento de la Subdirección de Plantas Físicas, realiza la correcta aplicación del procedimiento de Emisión de Conceptos Técnicos, a través de la implementación de los formatos establecidos, cada vez que se recepciona la solicitud de emisión de conceptos técnicos, con el fin de verificar las condiciones técnicas de infraestructura y de gestión predial de los equipamientos. En caso de no realizarse, la Coordinación de Mantenimiento /o del Área Predial realiza las alertas correspondientes en reunión de seguimiento de coordinadores para la toma de decisiones según sea el caso. Como registros quedan el memorando remisorio de los conceptos técnicos y sus anexos, o acta con las alertas identificadas y decisiones tomadas.	Preventiva	NO	1 - Raro	3 - Moderado	Moderado	Reducir	La coordinación del área de Gestión Predial y Mantenimiento de la Subdirección de Plantas Físicas, realiza la correcta aplicación del procedimiento de Emisión de Conceptos Técnicos, a través de la implementación de los formatos establecidos, cada vez que se recepciona la solicitud de emisión de conceptos técnicos, con el fin de verificar las condiciones técnicas de infraestructura y de gestión predial de los equipamientos. En caso de no realizarse, la Coordinación de Mantenimiento /o del Área Predial realiza las alertas correspondientes en reunión de seguimiento de coordinadores para la toma de decisiones según sea el caso. Como registros quedan el memorando remisorio de los conceptos técnicos y sus anexos, o acta con las alertas identificadas y decisiones tomadas.	Coordinador (a) área de gestión predial y Coordinador (a) área de Mantenimiento	(Número de conceptos técnicos emitidos en el periodo / Número de solicitudes de conceptos técnicos recibidas en el periodo)*100	100%	29/01/2021	30/11/2021