SECRETARIA DISTRITAL DE SALUD

SUBSECRETARIA DE SALUD PÚBLICA

ACCIÓN O PROCESO INTEGRAL E INTEGRADO: PROCESO INTEGRAL E INTEGRADO DE VIGILANCIA EN SALUD PÚBLICA

LÍNEA OPERATIVA O SUBPROCESO: GESTIÓN ZONAL Y DE LA INFORMACIÓN PARA LA VIGILANCIA EN SALUD PUBLICA

VIGENCIA: OCTUBRE 1 DE 2025 A 30 DE JUNIO 2027

Bogotá D.C. 2025

Contenido

FICHA TÉCNICA GESTIÓN ZONAL Y DE LA INFORMACIÓN PARA LA VIGILANCIA EN SALUD PUBLICA 4
1. Conceptualización de la Gestión Zonal y de la información 4
1.1. Objetivo General 6
1.2. Objetivos Específicos 6
2. Descripción de la acción de bienestar o acción de gestión para el bienestar: 6
2.1. Línea Operativa: Gestión, análisis y divulgación de información de la vigilancia en salud pública 6
2.2. Marco metodológico y operativo 7
2.2.1. Funciones del Sistema de Gestión Zonal 12
2.2.2. Funciones del Sistema de Gestión de la Información 13
2.2.3. Políticas de protección y tratamiento de datos personales 14
2.2.4. Implementación de nuevas estrategias para el análisis de información 15
2.2.5. Características Generales para los equipos de cómputo para VSP: 17
2.2.5.1. Hardware 17
2.2.5.2. Software 18
2.2.5.3. Servicio de Internet 19
2.2.6. Gestión de Correos Electrónicos Institucionales por Proceso 20
3. Gestión Zonal para la vigilancia en salud pública: 25
3.1. Descripción de la actividad 25
3.1.1. A la primera categoría pertenecen: 34
3.1.2. A la segunda categoría pertenecen: 35
4. Gestión de la información para los subsistemas de la vigilancia en salud pública: . 38
4.1. Apoyo Técnico al Área 38
4.2. Coves distritales y Locales 38
4.3. Infraestructura Tecnológica 41

4.3.1. Hardware 41

4.3.2. Software 42

4.4. Protocolos de transferencia de información 43

4.5. Gestión Documental 45

4.6. Seguridad de la Información 48

4.7. Soporte Tecnológico 51

4.7.1. Capacitaciones y evaluación de procesos 51

4.7.2. Monitoreo y seguimiento de la calidad del dato de las fuentes de información de VSP (depuración, precrítica, critica, ajuste y realimentación dato, evaluación de indicadores) 53

4.7.3. Asistencia técnica remota 58

Entrega de Productos Mensuales 61

5. Indicadores 62

Monitoreo y seguimiento 62

Referencias Bibliográficas 63

Control de cambios 64

FICHA TÉCNICA GESTIÓN ZONAL Y DE LA INFORMACIÓN PARA LA VIGILANCIA EN SALUD PUBLICA

1. Conceptualización de la Gestión Zonal y de la información

La estructura general de la Vigilancia en Salud Pública de acuerdo con lo señalado en el Decreto 780 de 2016 consiste en un sistema organizado y continuo que recopila, analiza, interpreta y difunde información sobre los eventos de interés en salud pública, para apoyar la toma de decisiones en la prevención y control de enfermedades, factores de riesgo y determinantes sociales. Este proceso es esencial para la gestión del riesgo en salud y debe ser desarrollado en todos los niveles territoriales.

El Sistema de Vigilancia en Salud Pública es un conjunto de usuarios, normas, procedimientos, recursos técnicos, financieros y de talento humano, organizados entre sí para la recopilación, análisis, interpretación, actualización, divulgación y evaluación sistemática y oportuna de la información sobre eventos en salud.

La Gestión Zonal y de la Información constituyen sistemas de información complementarios y estratégicos dentro de la Vigilancia en Salud Pública, cuya finalidad es garantizar la detección temprana, el análisis oportuno y la respuesta eficaz frente a los eventos que afectan la salud de la población.

Esta se concibe como la estructura organizativa y operativa que articula los procesos de vigilancia en salud pública de los territorios delimitados (zonal(subredes), localidades, upz o áreas de influencia). Su importancia radica en que permite adaptar la vigilancia a las realidades locales, reconociendo los determinantes sociales, ambientales y epidemiológicos de cada contexto, y fortaleciendo la capacidad de respuesta mediante la coordinación interinstitucional y comunitaria.

Se fundamenta en: Gestión territorial de los determinantes sociales y epidemiológicos, articulación intersectorial y comunitaria para la vigilancia activa y descentralización operativa, permitiendo respuestas adaptadas al contexto local.

Esta gestión zonal y de la información de vigilancia en salud Pública se establece en el enfoque de gestión territorial, reconociendo que los determinantes sociales, ambientales y epidemiológicos varían según la región. De esta manera, busca fortalecer la capacidad instalada en cada zona, mejorar la calidad de los datos, optimizar el flujo de información y garantizar la articulación entre los niveles local, zonal, departamental y nacional del Sistema de Vigilancia en Salud Pública (SIVIGILA).

Por su parte, la Gestión de la Información asegura la recolección, validación, consolidación, análisis y difusión de los datos generados en los procesos de vigilancia. A

través de herramientas normativas y tecnológicas, garantiza que la información sea oportuna, confiable, íntegra e interoperable, convirtiéndose en un insumo estratégico para la gestión del riesgo y la toma de decisiones en salud pública.

Su importancia radica en que permite:

1. Estandarizar procesos de captura y flujo de datos entre las unidades notificadoras locales y los nodos zonales, evitando duplicidades, errores o pérdidas de información.
2. Favorecer el análisis contextualizado de la información teniendo en cuenta las particularidades sociales, culturales, ambientales y epidemiológicas de cada zona.
3. Fortalecer la capacidad de respuesta ante eventos de interés en salud pública, ya que la información organizada y validada permite identificar alertas tempranas y tomar decisiones oportunas.
4. Articular la vigilancia local con los niveles superiores (departamental y nacional) mediante sistemas interoperables, garantizando la continuidad en el ciclo de vigilancia.
5. Convertir los datos en conocimiento, facilitando la elaboración de informes zonales, la priorización de riesgos y la planeación de intervenciones en salud pública.
6. Apoyar la transparencia y la gobernanza sanitaria, al asegurar que la información sea accesible, confiable y pertinente para los diferentes actores institucionales y comunitarios.

En este sentido, la gestión de la información no solo se limita a un proceso técnico de consolidación de datos, sino que se convierte en un instrumento de gestión territorial, que potencia la vigilancia epidemiológica y fortalece la capacidad de anticipación, prevención y control de riesgos en salud pública en cada zona.

De manera conjunta, estos procesos fortalecen la gobernanza sanitaria, ya que la gestión zonal contextualiza la vigilancia en el territorio, mientras que la gestión de la información asegura la calidad y el flujo de datos a lo largo de todos los niveles del sistema. Su integración permite transformar los datos en conocimiento útil para la acción, optimizando la capacidad de prevención, control y respuesta frente a amenazas a la salud pública.

Ahora bien, la vigilancia en salud pública es transversal, continuo y sistemático a todos los procesos de la salud pública, permite identificar en tiempo real las situaciones que pueden ser potencialmente brotes o emergencias en salud pública, así como la implementación de las acciones de prevención y control, propicia la inteligencia epidemiológica a través de la activación de la salas de análisis del riesgo y se complementa con la información que proveen las estadísticas de los hechos vitales que son la base para la medición de los indicadores trazadores en salud pública. Su propósito es apoyar la planificación, ejecución y evaluación de acciones de control. En el contexto de Bogotá, se articula con el Plan de Desarrollo Distrital y el Plan Territorial de Salud, permitiendo identificar problemas de salud emergentes, priorizar recursos y orientar la toma de decisiones.

Para el desarrollo de este proceso estamos en la **línea operativas**:

Gestión, análisis y divulgación de información de la vigilancia en salud pública, que se enfoca en la Gestión, análisis y divulgación de información de la vigilancia en salud pública, la cual abarca la planificación, coordinación y ejecución de acciones orientadas a fortalecer la Vigilancia en Salud Pública a través de la gestión eficiente de la información, el análisis oportuno y la divulgación efectiva de los eventos de interés en salud pública, se desarrolla en la acciones de vigilancia para el bienestar:

- Gerencia de la Vigilancia en Salud Pública, la coordinación del proceso integral.
- Mantenimiento del sistema de información y red de operadores con el sistema de información de la VSP

1.1. Objetivo General

Garantizar la gestión integral de la vigilancia en salud pública zonal mediante la articulación efectiva de los actores institucionales, comunitarios e intersectoriales, garantizando la notificación oportuna y de calidad, el análisis riguroso de la información epidemiológica y la implementación de acciones coordinadas para la prevención y control de eventos de interés en salud pública.

1.2. Objetivos Específicos

1. Planificar y coordinar las acciones técnicas, operativas y estratégicas de vigilancia en salud pública, asegurando la articulación interinstitucional y territorial.
2. Evaluar la calidad y oportunidad de la información generada, promoviendo su análisis e interpretación para la toma de decisiones basada en evidencia.
3. Gestionar recursos humanos, técnicos y financieros necesarios para el funcionamiento eficiente y sostenible del sistema de vigilancia en todos los niveles.
4. Garantizar la calidad, oportunidad, integridad y confidencialidad de los datos recolectados en los procesos de vigilancia en salud pública.
5. Estandarizar y optimizar los procesos de recolección, procesamiento y almacenamiento de la información, conforme a las normativas vigentes.
6. Fortalecer las capacidades del personal en el uso de herramientas tecnológicas y en la gestión efectiva de la información para apoyar la toma de decisiones.

2. Descripción de la acción de bienestar o acción de gestión para el bienestar:

2.1. Línea Operativa: Gestión, análisis y divulgación de información de la vigilancia en salud pública

Acción de gestión para el bienestar: Gerencia de la vigilancia en la salud pública.

Esta acción de bienestar se centra en la promoción del uso adecuado de la información y la gestión zonal como herramientas para proteger la salud de la población. Esto incluye:

- Coordinar las acciones de vigilancia para el bienestar que brinden respuesta con calidad, oportunidad y pertinencia de acuerdo a las necesidades de los ciudadanos en los eventos de interés de salud pública.
- Generar procesos de seguimiento, monitoreo y evaluación acorde con los requerimientos territoriales
- Fortalecer la capacidad local para responder de manera ágil ante alertas epidemiológicas.
- Garantizar la equidad en el acceso a la información, de forma que cada zona disponga de datos claros y oportunos para la toma de decisiones.
- Promover la participación comunitaria, asegurando que la población se beneficie de la vigilancia como un mecanismo de prevención, control y bienestar colectivo.
- Cuidar el bienestar del talento humano, mediante estrategias de capacitación, acompañamiento y autocuidado para reducir la carga laboral y mejorar el clima organizacional.
- Establecer mecanismos eficaces y estandarizados para la recolección y almacenamiento de datos cuantitativos y cualitativos relevantes en salud pública, garantizando su calidad, integridad y accesibilidad.
- Aplicar técnicas estadísticas y analíticas que permitan transformar los datos en información útil para identificar problemas de salud, evaluar riesgos y orientar intervenciones sanitarias.
- Diseñar e implementar estrategias de comunicación y difusión de la información, dirigidas a tomadores de decisiones, equipos técnicos y comunidades, fomentando la acción intersectorial y la participación social.
- Asegurar el cumplimiento de principios éticos y normativos, como la confidencialidad, transparencia, equidad y participación en todas las etapas del proceso de gestión de la información.
- Promover la interoperabilidad y fortalecimiento de los sistemas de información en salud, facilitando el flujo oportuno de datos entre diferentes niveles del sistema y sectores involucrados en la salud pública.
- La finalidad es que el bienestar individual y colectivo se vea reflejado en territorios más seguros, con comunidades empoderadas en el cuidado de la salud y con instituciones mejor organizadas para enfrentar riesgos en salud pública.

2.2. Marco metodológico y operativo

El Proceso Integral e Integrado de la Vigilancia de la Salud Pública (VSP), es un proceso de monitoreo crítico de los determinantes y condiciones de la salud colectiva que permite fundamentar la evaluación de las acciones emprendidas, implica que su abordaje contemple la vigilancia demográfica, (estructura y dinámica poblacional), vigilancia epidemiológica (condiciones de salud), servicios de salud (respuesta a estas condiciones de salud) y la relación de las condiciones ambientales y la salud (vigilancia sanitaria y ambiental). El desarrollo de este abordaje a través de diferentes métodos y estrategias (vigilancia pasiva, activa, rutinaria, intensificada, centinela)

Se mantendrá a través de nueve (9) componentes:

1. Sistema Nacional de Vigilancia en Salud Pública (SIVIGILA)
2. Análisis Demográfico – Estadísticas Vitales (EEVV)
3. Vigilancia Vida Saludable y Condiciones No Transmisibles
4. Vigilancia Convivencia Social y Salud Mental
5. Vigilancia Seguridad Alimentaria y Nutricional (SIVAN)
6. Vigilancia Salud Materna/Infantil y Salud Sexual y Reproductiva (SSR/SMI)
7. Vigilancia de Vida Saludable y Enfermedades Transmisibles
8. Gestión del Riesgo para la Atención de Urgencias y Emergencias en Salud Pública
9. Vigilancia Comunitaria para el Abordaje de la Salud Pública

Por lo tanto, las actividades técnicas contempladas en este componente se desarrollarán teniendo en cuenta las fichas técnicas de cada subsistema de la Vigilancia en Salud Pública para la Vigencia. Además, para el adecuado funcionamiento del Sistema Nacional de Vigilancia en Salud Publica en el Distrito, es indispensable que las subredes dispongan de la totalidad del talento humano requerido por el subsistema, para dar respuesta de manera oportuna a los productos establecidos en la matriz programática y presupuestal de GSP- PSPIC; los cuales se encuentran costeados en los productos donde participa el subsistema.

Para el análisis de información de VSP, en caso de requerirse y según el alcance de la información, se puede articular con el equipo de georreferenciación y análisis epidemiológico de VSP local, para identificar y proyectar posibles ejercicios de localización de los indicadores definidos y sus posibles desagregaciones espaciales (UPZ, barrio, sector, manzana) y/o de lugar (IPS, UPGD, albergues, centros educativos, etc).

La Vigilancia en Salud Pública Distrital, incorpora el monitoreo de eventos que son de gran impacto en la salud de la población de la ciudad y que aún no están considerados en el sistema nacional de Vigilancia de la Salud pública. Tener la capacidad de vigilar estos eventos que superan el modelo nacional, implica una estructuración de procesos y la creación de sistemas informáticos, denominando la completa operación integrada de los mismos “Gestión de la Información para la VSP”, conformada por los siguientes Sistemas de información y subsistemas:

1. SIVIGILA (Sistema nacional de vigilancia en salud pública)
2. EEVV (Estadísticas Vitales)
3. SISVEA (Sistema de vigilancia epidemiológica y ambiental)

4. SIVIM (Sistema de vigilancia epidemiológica de la violencia intrafamiliar, el maltrato infantil y la violencia sexual)
5. SIVELCE (Sistema de vigilancia epidemiológica de las lesiones de causa externa)
6. SISVECOS (Sistema de vigilancia epidemiológica de la conducta suicida)
7. VESPA (Sistema de vigilancia epidemiológica del abuso de sustancias psicoactivas)
8. SISVAN (Sistema de vigilancia alimentaria y nutricional)
9. SISVESO (Sistema vigilancia epidemiológica de la salud oral)
10. SIVISTRA (Sistema vigilancia epidemiológica ocupacional de las y los trabajadores en la economía informal)
11. Crónicas
12. Enfermedades Huérfanas
13. VEBC (Vigilancia Epidemiológica Basada en Comunidad)
14. Atención de urgencias y emergencias en salud pública

Proceso de gestión zonal y de la información de la Vigilancia en Salud Pública

La Gestión Zonal en Vigilancia en Salud Pública se entiende como el conjunto de procesos, mecanismos organizativos y operativos que permiten coordinar, articular y fortalecer las acciones de vigilancia en un territorio delimitado (zona, distrito o área de influencia). Su finalidad es garantizar la recolección, análisis, interpretación y uso oportuno de la información en salud, teniendo en cuenta las particularidades sociales, culturales, epidemiológicas y ambientales de cada contexto territorial.

La gestión zonal:

- Facilita la descentralización de los procesos de vigilancia, acercando la toma de decisiones a la realidad local.
- Promueve la articulación interinstitucional e intersectorial, involucrando a las comunidades y actores clave en la identificación y control de riesgos.
- Optimiza el flujo de información entre las fuentes primarias, las subredes, los niveles distritales y nacionales.
- Contribuye al fortalecimiento de la capacidad de respuesta local, mejorando la eficiencia en la detección temprana de alertas y el control de brotes.

En síntesis, la Gestión Zonal constituye un pilar estratégico de la vigilancia en salud pública, ya que integra la dimensión territorial con la gestión de la información,

permitiendo intervenciones más pertinentes, eficaces y sostenibles en beneficio de la salud colectiva.

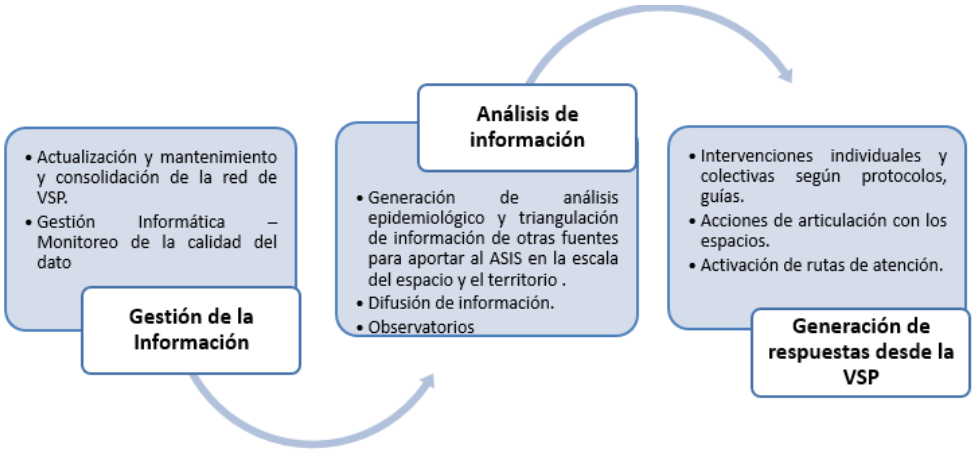
Objetivos de la Gestión Zonal de Vigilancia en Salud Pública

1. Integrar los procesos zonales de vigilancia en salud pública con los sistemas de información distritales y nacionales, asegurando un flujo oportuno y estandarizado de datos.
2. Optimizar la recolección, procesamiento, análisis y difusión de la información, garantizando confiabilidad y accesibilidad para los diferentes actores del sistema.
3. Fortalecer la infraestructura tecnológica y los mecanismos de seguridad de la información, asegurando la integridad, confidencialidad y disponibilidad de los datos.
4. Capacitar y acompañar técnicamente al talento humano responsable de la vigilancia en salud pública en el uso de herramientas informáticas, sistemas de reporte y protocolos establecidos.
5. Promover la coordinación interinstitucional y zonal para la consolidación de la información y la articulación de respuestas frente a eventos de interés en salud pública.
6. Implementar estrategias innovadoras de análisis de datos, incluyendo herramientas de inteligencia artificial y analítica avanzada, para mejorar la detección temprana de riesgos y el monitoreo epidemiológico.
7. Garantizar el uso ético y legal de la información, en concordancia con las políticas de protección de datos personales y la normativa vigente.
8. Evaluar periódicamente el desempeño del sistema de gestión zonal y de información, generando mejoras continuas que fortalezcan la vigilancia en salud pública.

Los elementos básicos que componen la Acción de Gestión de la información para la VSP son:

a. Ficha de caracterización de fuentes primarias de información.
b. Formatos o fichas epidemiológicas en donde se capturan las variables básicas que permiten la caracterización y definición del caso.
c. Herramientas informáticas, que facilitan el manejo de estas variables y el análisis de estas. (Aunque en la mayoría de los casos comparten el nombre del subsistema que soportan, algunas de estas herramientas agrupan varios subsistemas de información.)

Figura 1. Metodología de la operación de la Vigilancia en Salud Pública.



En esta transición se mantiene el planteamiento de un enfoque orientado a dar cumplimiento a la misión de la Vigilancia en Salud Pública del Distrito, que se opera en la mayoría de los casos desde el Plan de Intervenciones Colectivas, a través de las cuatro subredes integradas de servicios de salud; buscando dar una respuesta integral a la gobernanza, la atención primaria en salud y la gestión del riesgo.

Este escenario propuesto refleja la dinámica de la Vigilancia en Salud Pública del Distrito Capital, en donde no es suficiente contar con datos crudos, sino que los mismos deben ser procesados, garantizando calidad, oportunidad y análisis que soporten la toma de decisiones (información para la acción), además de su utilización para la gestión del conocimiento desde la investigación y uso de la academia.

Lo anterior implica disponer de un proceso unificado, definido por etapas e identificando responsables en el ciclo de la información que permita el seguimiento continuo de actividades de “extremo a extremo” del ciclo. Así, la gestión de la información hace parte del modelo de operación propuesto para la VSP del Distrito Capital, en donde cada actuación se articula, no desde una estructura piramidal sino a través de una transversalidad de su accionar.

Los Sistemas de Información en Salud (SIS), comprenden el principal soporte, para la adecuada toma de decisiones, la subdirección de Vigilancia y Control en Salud Publica de la Secretaria de Salud de Bogotá, tiene como meta, crear el “SISTEMA INTEGRADO DE INFORMACIÓN DE VIGILANCIA EN SALUD PUBLICA DISTRITAL (SIIVSPD)”. con el fin de potencializar el uso de la información, y contando con sistema de información dinámico que pueda adaptarse a los cambios en la vigilancia en salud pública y las

estrategias que se generen desde los diferentes componentes y subsistemas de información.

El sistema integrado de información permite gestionar los recursos informacionales internos y externos con el fin de generar servicios y productos que respondan a las necesidades de la vigilancia en salud pública. Este enfoque asegura que el sistema opere de manera eficiente, segura y costo–efectiva, aprovechando al máximo los recursos de información para la mejora continua y la toma de decisiones en todos los niveles: desde la fuente primaria hasta el nivel distrital.

Objetivos del Sistema de Gestión de la Información

- Determinar las necesidades internas de información (funciones, actividades y procesos administrativos) y satisfacerlas de manera eficiente.
- Identificar las necesidades externas de la organización y atenderlas oportunamente.
- Desarrollar la base de información de la organización y garantizar su accesibilidad.
- Optimizar el flujo de información y fortalecer los niveles de comunicación organizacional.
- Desarrollar y garantizar la operatividad de la estructura informacional.
- Manejar eficientemente los recursos institucionales de información y optimizar su valor estratégico.
- Garantizar la integridad, accesibilidad y protección de las bases históricas institucionales.
- Evaluar periódicamente la calidad e impacto de la información en la gestión y el desarrollo organizacional.
- Optimizar la base y la estructura informacional para incrementar productividad y rendimiento de la inversión.
- Establecer y supervisar procedimientos de seguridad de la información organizacional.
- Capacitar al personal en el uso y manejo responsable de los recursos informacionales.
- Contribuir a la modernización y optimización de procesos organizacionales y administrativos.
- Garantizar la calidad de los productos informacionales, asegurando su eficacia y pertinencia.

2.2.1. Funciones del Sistema de Gestión Zonal

1. Coordinar la gestión zonal de la vigilancia en salud pública, asegurando la implementación de los lineamientos, protocolos y políticas definidos por el nivel nacional y distrital.

2. Fortalecer la articulación interinstitucional e intersectorial en el territorio, garantizando la integración de esfuerzos entre EPS, IPS, entes territoriales y demás actores que producen o usan información en salud pública.
3. Consolidar, validar y analizar la información proveniente de las fuentes primarias de los diferentes subsistemas de vigilancia, asegurando calidad, oportunidad y confiabilidad.
4. Identificar, priorizar y gestionar los eventos de interés en salud pública a nivel zonal, garantizando la notificación oportuna y la respuesta articulada frente a brotes, emergencias o riesgos en salud.
5. Implementar estrategias de monitoreo y evaluación zonal que permitan hacer seguimiento a indicadores, planes de acción y compromisos establecidos en salud pública.
6. Optimizar los recursos disponibles en el nivel zonal, garantizando eficiencia en el uso del talento humano, tecnológico y financiero en los procesos de vigilancia.
7. Fortalecer las capacidades técnicas y operativas del personal zonal, a través de capacitaciones, asistencia técnica y acompañamiento en la gestión de la vigilancia.
8. Fomentar el uso y la apropiación de herramientas tecnológicas y sistemas de información, asegurando que el nivel zonal cumpla con los requerimientos del sistema integrado de información en salud pública.
9. Promover la retroalimentación y socialización periódica de resultados de la vigilancia en salud pública con actores locales y distritales para la toma de decisiones informadas.
10. Velar por la confidencialidad, seguridad y uso ético de la información, cumpliendo las políticas y normativas sobre protección de datos.

2.2.2. Funciones del Sistema de Gestión de la Información

1. Socialización y articulación: Difundir las estrategias definidas de gestión de la información a líderes y responsables técnicos de los 14 subsistemas de VSP.
2. Ciclo de vida de la información: Evaluar la trazabilidad de la información desde su recolección hasta su disposición final.
3. Gestión de almacenamiento: Administrar medios de almacenamiento seguros, garantizando acceso controlado, respaldo y recuperación de bases de datos históricas y actuales.
4. Requerimientos técnicos: Definir y socializar los mínimos técnicos de equipos de cómputo para el personal responsable de la información, articulando con el área TIC (sin atribuir al ingeniero de sistemas de la subred tareas de mantenimiento físico).
5. Optimización del uso de la información: Maximizar su aprovechamiento, reduciendo costos de obtención, definiendo responsables y garantizando su ciclo continuo.
6. Custodia de recursos: Elaborar y actualizar la matriz de levantamiento de información de los 14 subsistemas de VSP (equipos de cómputo, bases de datos y talento humano).
7. Control y protección de datos: Garantizar el cumplimiento de la normativa de habeas data, asegurando acceso controlado a la información sensible.

8. Capacitación continua: Desarrollar capacitaciones bimensuales en plataformas de información en salud pública (ej. SIVIGILA 4.0, SIVIGILA DC), o según los lineamientos del nivel central.
9. Reuniones de articulación: Coordinar espacios de trabajo entre líderes distritales de gestión de la información, ingenieros de sistemas de subredes, líderes de subsistemas y comités técnicos.
10. Gestión de requerimientos: Coordinar con el área TIC y la coordinación de salud pública las necesidades tecnológicas, sistemas de información y bases de datos.
11. Gestión centralizada: Tramitar con el área TIC los requerimientos transversales para el fortalecimiento de la vigilancia en salud pública.

2.2.3. Políticas de protección y tratamiento de datos personales

Seguridad de la Información en los Procesos integrales e integrados de Vigilancia en Salud Pública (VSP)

La seguridad de la información resultante de los procesos integrales e integrados de Vigilancia en Salud Pública (VSP) se garantiza mediante la implementación de mecanismos que protegen la integridad y la confidencialidad de los datos, asegurando que la información sea confiable, completa y accesible únicamente para los actores autorizados.

Este proceso no es responsabilidad exclusiva de las Subredes de servicios de salud, sino que compromete a todas las instituciones productoras y generadoras de datos relevantes, en tanto aportan insumos esenciales para el desarrollo social y la toma de decisiones en salud pública. Dichos datos incluyen variables sensibles de identificación personal que requieren un manejo responsable y bajo estrictos estándares de protección.

En este sentido, la Secretaría Distrital de Salud (SDS) ha desarrollado y adoptado lineamientos específicos que rigen la seguridad de la información:

- **Política de Seguridad de la Información – SDS-TIC-POL-001 V.12:**

  Su objetivo principal es garantizar que los recursos de software, hardware y sistemas de información de la SDS sean utilizados exclusivamente para los fines para los que fueron creados, dentro del marco normativo previsto. Esta política busca salvaguardar la **confidencialidad, integridad y disponibilidad de la información** institucional.

- **Política de Protección de Datos Personales – SDS-TIC-POL-003 V.3:**

  Establece los lineamientos para el tratamiento adecuado de los datos personales, asegurando el cumplimiento de la normatividad vigente en materia de habeas data, protección de la intimidad y derechos de los titulares de la información.

Con la aplicación de estas políticas, la Secretaría Distrital de Salud y las instituciones vinculadas a los procesos de VSP fortalecen la gobernanza de los datos, consolidando un sistema seguro, confiable y ético que respalde la toma de decisiones en beneficio de la salud pública y la protección de los derechos de los ciudadanos.

2.2.4. Implementación de nuevas estrategias para el análisis de información

Los Grupos de Gestión de la Información de la Secretaría Distrital de Salud y de las Subredes, en su propósito de optimizar los procesos de recolección, procesamiento y análisis de datos, adelantarán esfuerzos orientados a la incorporación de nuevas estrategias basadas en inteligencia artificial (IA) y analítica avanzada.

La implementación de estas herramientas permitirá:

- **Automatizar procesos** de clasificación, depuración y consolidación de datos, reduciendo errores humanos y tiempos de respuesta.
- **Detectar patrones y tendencias epidemiológicas** con mayor rapidez y precisión, facilitando la identificación de alertas tempranas y eventos inusuales en salud pública.
- **Fortalecer la capacidad predictiva** del sistema de vigilancia, permitiendo anticiparse a posibles brotes y emergencias sanitarias.
- **Mejorar la visualización y comprensión de la información**, mediante el uso de modelos de análisis en tiempo real y tableros interactivos.
- **Apoyar la toma de decisiones basada en evidencia**, ofreciendo a los profesionales y epidemiólogos insumos estratégicos para intervenciones oportunas y efectivas.

De esta forma, la integración de la inteligencia artificial en los procesos de vigilancia en salud pública **transformará significativamente la manera en que los equipos técnicos procesan y utilizan los datos**, contribuyendo a una gestión más eficiente, innovadora y acorde con los desafíos actuales de la salud pública.

Aquí hay algunas estrategias que se pueden considerar:

1. Integración de Machine Learning

- Modelos Predictivos: Utiliza algoritmos de machine learning para predecir tendencias y comportamientos futuros basados en datos históricos.
- Análisis de Sentimientos: Aplica técnicas de procesamiento de lenguaje natural (NLP) para analizar opiniones y emociones en datos textuales, como IEC, unidades de análisis, encustas.

2. Análisis de Big Data

- Data Lakes: Implementa un enfoque de data lake para almacenar grandes volúmenes de datos no estructurados, permitiendo análisis más flexibles.

- Herramientas de Visualización: Usa herramientas como Tableau o Power BI para crear visualizaciones interactivas que faciliten la comprensión de patrones y tendencias en los datos.

3. Automatización de Procesos

- RPA (Robotic Process Automation): Automatiza tareas repetitivas que involucran la recopilación y el análisis de datos, liberando tiempo para análisis más complejos.
- ETL Inteligente: Mejora procesos de Extracción, Transformación y Carga (ETL) utilizando IA para mejorar la calidad de los datos.

4. Análisis en Tiempo Real

- Streaming de Datos: Implementa soluciones que permitan el análisis de datos en tiempo real, utilizando herramientas como Apache Kafka para procesar flujos de datos continuos.
- Alertas Proactivas: Configura sistemas que envíen alertas automáticas basadas en patrones de datos inusuales o eventos específicos.

5. Personalización y Segmentación

- Segmentación Dinámica: Utiliza IA para segmentar audiencias de manera dinámica, adaptando estrategias de marketing o productos a grupos específicos en tiempo real.
- Recomendaciones Personalizadas: Implementa sistemas de recomendación que analicen el comportamiento del usuario para ofrecer productos o servicios personalizados.

6. Colaboración Interdisciplinaria

- Equipos Multidisciplinarios: Fomenta la colaboración entre expertos en datos, analistas de negocio y personal operativo para obtener diferentes perspectivas en el análisis.
- Capacitación Continua: Ofrece capacitación en IA y análisis de datos a todo el personal para que puedan contribuir al proceso.

7. Ética y Gobernanza de Datos

- Transparencia en los Modelos: Asegúrate de que los modelos de IA sean interpretables y comprensibles para los usuarios, promoviendo la confianza en los resultados.
- Políticas de Privacidad: Implementa políticas sólidas para la gestión y el uso de datos, garantizando el cumplimiento de normativas como el GDPR.

8. Pruebas y Evaluación Continua

- Iteración y Mejora: Establece un ciclo de prueba y aprendizaje continuo, donde se evalúen y ajusten los modelos y estrategias de análisis regularmente.
- Métricas de Éxito: Define KPIs claros para medir la efectividad de las nuevas estrategias y realizar ajustes basados en los resultados obtenidos.

Implementar estas estrategias no solo mejorará el análisis de información, sino que también ayudará a las organizaciones a ser más ágiles y proactivas en la toma de decisiones.

Continuaremos con la implementación de R, R Studio y Visual Code,Power BI los cuales utilizaremos para la programación de rutinas de depuración automatizadas

2.2.5. Características Generales para los equipos de cómputo para PII de VSP:

Las características mínimas de los computadores utilizados para el proceso de sistematización de la información del Proceso integral e integrado de Vigilancia en Salud Publica, se relacionan por herramienta informática, al igual que el tipo de plataforma y bases de datos, la subred deberá garantizar un puesto de trabajo y un equipo de cómputo según sus necesidades, durante toda la vigencia del convenio.

Recurso tecnológico mínimo requerido:

2.2.5.1. Hardware

Las características mínimas de los computadores utilizados para el proceso de sistematización de la información de la vigilancia en salud pública se relacionan en el documento denominado

"Anexo 8 Insumos Requeridos para la Operación GSP- PSPIC y la Gestión de la Salud Pública \ Vigilancia Epidemiológica \ materiales e insumos \ equipos de cómputo para tareas básicas de equipos operativos, lideres y apoyos".

Para los procesadores de los equipos de gama media, se podrán homologar de la siguiente manera por:

- **Intel i5 de decima generación por i7, i9 de sexta generación o superior, XEON de segunda generación o superior**
- **AMD Ryzen 5 de tercera generación por Ryzen 7, 9 de segunda generación**

Para los procesadores de los equipos de gama alta, se podrán homologar de la siguiente manera por:

- **Intel i7 de decima generación por i9 de sexta generación o superior, XEON de segunda generación o superior**
- **AMD Ryzen 7 de tercera generación por Ryzen 9 de segunda generación**

El tiempo de vida útil de los equipos de cómputo será de 5 años, para los equipos nuevos, y que cumplan con las garantías de mantenimiento, suministro de corriente y

manipulación adecuados por parte del usuario y para equipos de segunda mano o que no cumplan con alguno de los requisitos mínimos de mantenimiento, energía, o manipulación será de 3 años de vida útil a partir de su instalación.

Los equipos se definen según las actividades y tares desarrolladas de la siguiente manera:

- **Los equipos de cómputo de gama media se definen para: GESTIÓN DE LA INFORMACIÓN EN SALUD PUBLICA**
- **Los equipos de cómputo gama alta se definen para: TAREAS DE INGENIERÍA y DISEÑADORES, GEÓGRAFOS.**
- **Los equipos de cómputo portátiles gama media se definen para: GRUPO DE ATENCION HUMANIZADA PARA LA DEFUNCIÓN – GAHD Y y VIGILANCIA BASADA EN COMUNIDAD**
- **Las impresoras portátiles se definen para: GRUPO DE ATENCION HUMANIZADA PARA LA DEFUNCIÓN – GAHD.**

(La configuración solicitada es la mínima requerida para el manejo de la información por parte de los técnicos y profesionales del área de vigilancia en salud pública)

Una (1) impresora y escáner para el área de vigilancia en salud pública.

2.2.5.2. Software

En el marco de la gestión de la información en salud pública, la disponibilidad de herramientas tecnológicas confiables constituye un requisito esencial para garantizar la calidad de los procesos analíticos y de toma de decisiones. En este sentido, la utilización de software de ofimática licenciado y de software especializado en epidemiología reviste una importancia estratégica.

El software de ofimática licenciado asegura el cumplimiento de normativas legales y de estándares de seguridad informática, minimizando los riesgos asociados al uso de programas no autorizados, tales como la pérdida de integridad de los datos, vulnerabilidades frente a ciberataques y posibles sanciones jurídicas. Asimismo, su utilización garantiza la compatibilidad de formatos, la estabilidad en el procesamiento de información y la disponibilidad de actualizaciones que optimizan el rendimiento operativo. Estas características resultan críticas para la elaboración de informes técnicos, análisis estadísticos preliminares, consolidación de bases de datos y la comunicación institucional.

Por su parte, el software epidemiológico constituye un componente especializado indispensable para la vigilancia en salud pública. Estas plataformas permiten el procesamiento y análisis avanzado de datos poblacionales y clínicos, la detección

temprana de eventos de interés en salud pública, la modelación predictiva de tendencias epidemiológicas, así como la georreferenciación y visualización de la distribución espacial de enfermedades. El uso de estas herramientas posibilita la generación de evidencia científica robusta que respalda la formulación de políticas sanitarias, la evaluación de intervenciones y la optimización de recursos en los diferentes niveles de gestión del sistema de salud.

En conjunto, la implementación de software de ofimática licenciado y software epidemiológico fortalece la capacidad institucional para desarrollar procesos de análisis confiables, oportunos y alineados con los lineamientos técnicos nacionales e internacionales, consolidando así la respuesta integral frente a los desafíos en salud pública.

Los softwares requeridos son:

- Office 365 versión profesional o 2019 Profesional o superior
- R, R Studio
- Visual Code
- Navegador (Edge, Mozilla, Crhome)
- Quamtun Qgis
- Antivirus (Según disponibilidad de la subred)
- Microsoft Teams
- Power BI Desktop
- Genopro
- Power BI Desktop
- EpiInfo Ultima Version

Los requerimientos de software son definidos según las actividades de cada profesional, es importante aclarar que se pueden requerir aplicativos que no se encuentran en el listado dependiendo de las necesidad o novedades que se presenten en el proceso de la vigilancia en salud pública, aquellos que sean de licencia libre serán solicitados al equipo de gestión de la información de cada subred para que sean gestionados al área TIC, y para aquellos que requieran algún tipo de licenciamiento espacial o de costo, se realiza por los medios oficiales de la Secretaria de Salud de Bogota.

2.2.5.3. Servicio de Internet

Con el fin de garantizar la transferencia oportuna de información de notificación inmediata y rutinaria, cada equipo de cómputo deberá disponer de un servicio de Internet con una velocidad mínima garantizada de 20 Mbps (megabits por segundo), tanto de subida como de bajada. Esta capacidad debe estar disponible en todo momento para cada equipo, constituyendo la condición mínima requerida para el adecuado funcionamiento de los procesos de vigilancia.

Adicionalmente, las unidades deben contar con equipos de comunicación permanente (teléfonos fijos o móviles institucionales) que permitan mantener la comunicación continua y efectiva con los actores involucrados en la vigilancia.

Es importante precisar que la velocidad de conexión está directamente relacionada con la configuración de la subred, por lo cual se deberá asegurar la disponibilidad y calidad del servicio contratado.

La gestión de la información en salud pública se soporta en el uso de plataformas institucionales como Sivigila 4.0, Sivigila D.C., RUAF, Microsoft Teams, correo electrónico institucional, entre otras, que requieren de canales efectivos, estables y funcionales para su operación, la subred garantizara la disponibilidad de un canal de internet, funcional y de calidad, las 24 horas al día, los 7 días de la semana.

Nota Importante:

Las actividades y productos generados en el marco de la vigilancia en salud pública deben ser entregados dentro de los tiempos establecidos en las fichas técnicas correspondientes. La **falta de conectividad a Internet no constituye justificación válida para incumplimientos**. Únicamente el referente distrital, mediante oficio, podrá autorizar avales para la entrega extemporánea de información, de acuerdo con la situación particular.

2.2.6. Gestión de Correos Electrónicos Institucionales por Proceso

Importancia de contar con un correo electrónico por procesos

La implementación de correos electrónicos institucionales asignados a cada proceso responde a la necesidad de garantizar una gestión organizada, segura y eficiente de la información dentro de la entidad. A diferencia de un único correo para todos los procesos, esta estrategia asegura una trazabilidad clara y evita riesgos administrativos y de seguridad.

- **Trazabilidad y responsabilidad:** Cada proceso tiene funciones y competencias específicas; disponer de un correo exclusivo permite identificar con precisión la procedencia, seguimiento y resolución de cada comunicación, evitando confusiones sobre quién es responsable de dar respuesta.
- **Organización de la información:** Al centralizar toda la comunicación en un solo correo se genera saturación, pérdida de mensajes importantes y dificultad en la clasificación. Los correos por procesos permiten segmentar, ordenar y archivar la información de acuerdo con el flujo documental correspondiente.
- **Confidencialidad y seguridad:** Algunos procesos manejan información sensible o reservada (ejemplo: historias clínicas, resultados de laboratorio, talento humano,

vigilancia en salud, contratación). Al tener un correo por proceso se garantiza que solo el equipo autorizado acceda a la información, reduciendo riesgos de filtración o acceso indebido.

- **Eficiencia en la gestión:** Con un correo por proceso se facilita la atención oportuna de solicitudes, la priorización de asuntos críticos y la distribución equitativa de la carga laboral, evitando retrasos que ocurren cuando todas las comunicaciones llegan a un solo buzón.
- **Continuidad y reemplazos de personal:** Los correos institucionales por procesos garantizan la continuidad del servicio, ya que no dependen de una persona en particular. En caso de rotación de personal, vacaciones o ausencias, el acceso puede mantenerse para el equipo del proceso sin afectar la atención de los requerimientos.
- **Cumplimiento normativo y auditorías:** La asignación de correos por procesos facilita el cumplimiento de políticas de gestión documental, transparencia y auditoría, permitiendo evidenciar de manera clara el flujo de información y las actuaciones de cada área.

En conclusión, un correo electrónico único para todos los procesos genera sobrecarga, desorden y riesgos de seguridad, mientras que un correo institucional por procesos fortalece la eficiencia, la transparencia y la gobernanza de la información.

Normas para el Uso Adecuado de los Correos Institucionales

El correo electrónico institucional es una herramienta oficial de comunicación que garantiza la gestión transparente, segura y eficiente de la información dentro de la entidad. Su uso debe estar alineado con las políticas de seguridad informática, la normatividad vigente y los principios de confidencialidad, eficiencia y responsabilidad.

1. Uso Exclusivamente Institucional: El correo institucional se utilizará únicamente para actividades relacionadas con las funciones y responsabilidades del cargo o proceso asignado.

No está permitido el uso del correo institucional para fines personales, comerciales, proselitistas, ni para actividades ajenas a la misión de la entidad.

2. Confidencialidad y Seguridad de la Información: Está prohibido compartir contraseñas o credenciales de acceso.

La información sensible o reservada debe ser manejada exclusivamente por los responsables autorizados del proceso.

En caso de identificar intentos de fraude, phishing o correos sospechosos, estos deben reportarse de inmediato al área de tecnología o sistemas.

3. Responsabilidad en la Comunicación: Todo mensaje enviado desde el correo institucional representa oficialmente a la entidad, por lo que debe mantener un lenguaje formal, respetuoso y acorde con los lineamientos de comunicación institucional.

Se debe garantizar que las respuestas a solicitudes o comunicaciones externas se den en los tiempos establecidos por la normatividad vigente.

4. Organización y Gestión Documental: Los correos electrónicos deben clasificarse, archivarse y gestionarse conforme a las tablas de retención documental o lineamientos de gestión de la información establecidos.

No se deben eliminar mensajes que contengan información relevante para auditorías, procesos administrativos o seguimiento de casos.

5. Uso Responsable de Recursos Tecnológicos: Evitar el envío masivo de correos innecesarios que puedan congestionar la red institucional.

No adjuntar archivos que contengan virus, software no autorizado o información que comprometa la seguridad de los sistemas.

Utilizar los canales de almacenamiento institucional (servidores, nube corporativa, intranet) en lugar de sobrecargar el correo con archivos de gran tamaño.

6. Continuidad y Acceso por Procesos: Los correos institucionales deben ser creados y administrados por procesos, no por personas, con el fin de garantizar la trazabilidad y continuidad en caso de cambios de personal.

El acceso a los correos institucionales debe estar regulado y controlado por el área de sistemas o la dependencia responsable de la gestión tecnológica.

El uso adecuado del correo institucional garantiza transparencia, seguridad, eficiencia y trazabilidad en la gestión administrativa y en los procesos de vigilancia en salud pública.

Con el fin de garantizar la seguridad, autenticidad y trazabilidad de la información institucional, se establece que únicamente serán válidos los correos electrónicos que pertenezcan a los dominios oficiales autorizados por la entidad.

En consecuencia:

Todo funcionario, contratista o colaborador deberá utilizar únicamente las cuentas institucionales asignadas.

No se permitirá el uso de correos personales (ejemplo: *@gmail.com, *@hotmail.com, *@yahoo.com, entre otros) para la gestión de trámites, envío de reportes, notificaciones o intercambio de información oficial.

El uso de correos no autorizados se considerará una falta a la política de seguridad de la información y podrá generar sanciones administrativas o contractuales.

Los dominios válidos serán definidos, administrados y actualizados exclusivamente por el área de tecnología o la dependencia encargada de la infraestructura informática.

Los correos oficiales válidos para él envío de información, solo podrán ser de cualquiera de los siguientes dominios:

- @saludcapital.gov.co
- @subrenorte.gov.co
- @subredcentrooriente.gov.co
- @subresuroccidente.gov.co
- @subresur.gov.co

CORREO REQUERIDOS POR SUBSISTEMA O PROCESO

Un correo electrónico por localidad

	Cantidad Correos Totales
• SIVIGILA (Uno (1), por cada localidad)	20

Un correo por subsistema de información por subred:

Grupo	**Total X Grupo**
• CRONICOS	1
• SIVISTRA	1
• SISVESO	1
• GESTIÓN DE LA INFORMACIÓN	1
• TRASMISIBLES	1
• SALUD SEXUAL Y REPRODUCTIVO	1
• SISVAN	1
• URGENCIAS Y EMERGENCIAS	1
• ESTADÍSTICAS VITALES	1
• GRUPO GAHD (Subred Norte)	2
• VIGILANCIA BASADA EN COMUNIDAD	1
• GEOGRAFICO	1
• SALUD MENTAL	1

Los correos deberán tener las siguientes características, 50 Gb de espacio para correo, 500 Gb de espacio de almacenamiento en OneDrive, deberán ser licencias corporativas, debido a la alta rotación, los correos serán asignados al líder del procesos el cual deberá controlara el acceso a cada correo y de ser necesario, cambiar la clave de acceso, por intentos de accesos no autorizados, rotación de personal

El plazo máximo para contar con los correos por procesos institucionales, será el 31 de octubre de 2025

Nota Importante:

La firma en los correos institucionales es un requisito fundamental porque:

Identificación y responsabilidad: Permite reconocer con claridad quién envía la comunicación, en representación de qué proceso o dependencia, evitando mensajes anónimos o confusos.

Validez institucional: Cada correo enviado representa oficialmente a la entidad. La firma estandarizada refuerza la seriedad, formalidad y legitimidad de la información.

Transparencia y trazabilidad: La firma garantiza que la comunicación pueda ser rastreada a un responsable o dependencia, lo cual es clave en procesos administrativos, auditorías y vigilancia en salud pública.

Imagen corporativa: Proyecta una presentación uniforme y profesional de la institución, fortaleciendo la confianza frente a actores internos y externos.

Cumplimiento normativo: Apoya las políticas de gestión documental y de seguridad de la información, que exigen trazabilidad en las comunicaciones oficiales.

Ejemplo de Firma Institucional en un correo

Atentamente,

_____

Ruben Dario Rodriguez Camargo
Profesional Universitario – Proceso de Vigilancia en Salud Pública
Secretaría de Salud Distrital
Correo: rdrodriguez @saludcapital.gov.co
Teléfono: (601) 3649090 – Ext. 123
www.saludcapital.gov.co

Este mensaje y sus anexos son de carácter confidencial. Si usted no es el destinatario autorizado, por favor elimínelo e informe al remitente. El uso inadecuado de esta información está prohibido por la ley.

3. Gestión Zonal Para la Vigilancia en Salud Pública:

Realizar la gestión técnica y operativa de la vigilancia en salud pública en la Subred Integrada de Servicios de Salud según los lineamientos operativos y protocolos establecidos para la atención de los eventos de interés en salud pública emitidos por el nivel nacional y distrital

Producto:

Gestión Zonal en los Niveles Meso y Micro de la Salud Pública del Proceso Integral e Integrado de Vigilancia en Salud Pública

Unidad de medida; Avance mensual al plan de acción

Forma de reporte de ejecución del producto: Mensual

Perfil

Profesional especializado 2 (Referentes gestión): Profesional de ciencias de la salud, con posgrado en epidemiología y con 3 años de experiencia específica en procesos de vigilancia en salud pública.

Profesional Universitario 1: Profesional de ciencias de la salud, sociales, económicas e ingenierías, administración (empresas, hotelera, entre otros) Se valora experiencia en salud, salud pública o vigilancia en salud publica
Experiencia mínima 6 meses relacionada

Tecnólogo: tecnólogo administrativo, bases de datos, mercadeo, salud ocupacional, entre otros. Mínimo 6 meses de experiencia relacionada

3.1. Descripción de la actividad

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
1. Participar en la mesa de gestión territorial APSocial del GSP-PSPIC	Mensual	**Profesional especializado 2 o universitario 1**	1. Acta con listado de asistencia. Nota: Desde la SDS, se entregará metodología para el desarrollo de la Instancia

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
Socialización de logros y dificultades evidenciadas en la o las localidades que lidere, así como, análisis para la toma de decisiones. Desarrollar acciones que permitan la articulación de los procesos locales, garantizando la adecuada operación de los subsistemas, y haciendo énfasis en los diferentes espacios del GSP-PSPIC, incluyendo el modelo territorial. 2. Desarrollar el plan de acción de la vigilancia en salud pública, en articulación con los líderes operativos de VSP, realizando seguimiento administrativo financiero, y presupuestal, y garantizando el cumplimiento de las metas, lineamientos y protocolos. El plan de acción se debe enviar desde el correo institucional del líder del componente de VSP consolidado los 5 primeros días hábiles del mes siguiente a la ejecución por correo electrónico DMWalteros@saludcapital.gov.co 3. Realizar procesos de inducción y reinducción a los equipos técnicos que desarrollan la VSP, garantizando la gestión del conocimiento y el cumplimiento de las especificaciones técnicas requeridas, oportuna y eficientemente. Realizar procesos de fortalecimiento de capacidades a los entornos sobre notificación obligatoria (iniciando el convenio y/o cuando se requiera 4. Realizar seguimiento técnico, financiero, poblacional, y territorial, al proyecto de inversión- con calidad y oportunidad, en coherencia a los procesos de reporte al informe de gestión y operación de la subred para cada periodo.	El desarrollo de las actividades es diario, semanal y con reporte mensual según la especificidad y tiempos necesarios.		2.Plan de acción de la vigilancia en salud pública, aprobado y con avances mensuales, 2.1 Actas de reunión y listados de asistencia de la validación del plan de acción 3. Actas de reunión y listados de asistencia de inducción, entrenamiento o fortalecimiento de los procesos. Actas o soportes de inducción, reinducción, a los procesos de VSP. 4.Digitación y ajustes proyecto inversión en la herramienta dispuesta por la SDS, en las metas de VSP de manera oportuna.

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
Cumplimiento de los Actividades y metas, según lo definido en los documentos operativos, lineamientos, y según especificidades de cada subsistema. 5.Controlar y evaluar los procesos de pre- auditoría, de seguimiento físico, financiero, y de verificación de actividades, conforme a los documentos operativos, y lineamientos; a fin de garantizar criterios de calidad, oportunidad e integralidad en la operación de la VSP, generando planes de mejora según necesidad. Con profesional universitario 1 6. Planear y liderar la reunión de líderes y referentes, teniendo en cuenta actualizaciones de alertas epidemiológicas, indicadores trazadores, evaluación de ajustes de eventos al SIVIGILA, como mínimo una vez al mes. Planear y liderar la reunión mensual con el equipo de Vigilancia en Salud Pública enfocada en procesos de fortalecimiento técnico y avances de la ejecución del convenio en relación con los temas técnicos, administrativos y financieros. 6. Preparar, presentar y realizar informes y análisis periódicos y a demanda, del seguimiento técnico, administrativo y financiero de la vigilancia en salud pública en la Subred Integrada de Servicios de Salud. 7. Participar en el análisis y revisión de los indicadores trazadores en salud cuando se convoque, con el fin de aportar en el análisis estadístico de los datos presentados, incluyendo los determinantes encontraron en las investigaciones epidemiológicas			Actas de participación en espacios de gestión de los procesos de VSP. 5. Actas o soportes de seguimiento o pre-auditoria a los procesos de VSP y presentación de auditoría. 6.Actas y listados de asistencia de reunión 6.Presentación de informes según requerimientos de SDS. Oficios y correos electrónicos de respuesta y/o envío de información requerida. 7. Matriz de indicadores, análisis y seguimiento 8. Actas y listados de asistencia de reunión 9.Matriz de base de talento humano con seguimiento. 10.Respuesta PQR con respuestas gestionadas 11.Mensualización validad con acta de seguimiento

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
de campo y las demás acciones desarrolladas por la VSP. 8.Participación en socialización de resultados de asistencia técnicas a UPGDs públicas y privadas con el propósito de identificar y optimizar procesos clave para el fortalecimiento de la Vigilancia en Salud Pública. 9. Revisión base de talento humano SDS que ejecuta las acciones de vigilancia en salud publica en el marco de la ejecución del convenio GSP – PSPIC, asegurando el cumplimiento de actividades por los perfiles requerido, establecidos en el anexo 9 del convenio. 10.Proyectar respuestas a PQR y demás solicitudes que tengan que ver con la información y procesos que se ejecuten de la vigilancia en salud Publica en el marco del convenio y en articulación con la Secretaría Distrital de Salud, teniendo en cuenta que se debe entregar información oficial validada desde la SDS. Realizar verificación e informe mensual de puntos críticos, en donde se evidencie las causas y posibles acciones de subsanación de la subejecución del componente de Vigilancia en salud Publica de acuerdo con las líneas del plan programático y presupuestal 11.Realizar y verificar en conjunto con las lideres técnicas el proceso de mensualización de metas de la vigilancia en Salud pública y de ser necesario adelantar los procesos de reprogramación necesarios para dar cumplimiento a la ejecución del convenio 12.Administrar, custodiar y controlar la información producida en la vigilancia en salud pública según criterios de			12.Verificación de información, acciones de confidencialidad con seguimiento en VSP 13.Matriz de seguimiento de eventos priorizados 14. Actas y listados de asistencia de reunión 15. Actas y listados de asistencia de reunión

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
confidencialidad y uso definidos, toda vez que en el marco de las investigaciones que se desarrollan en salud pública, de las actuaciones de investigación, vigilancia y control, así como de los procesos administrativos sancionatorios, el Estado está llamado a proteger la intimidad personal y familiar y el buen nombre de quienes en estos intervienen. Lo anterior, con sustento en el artículo 15 superior y en el artículo 4º de la Ley Estatutaria 1581 de 2015 "Por la cual se dictan disposiciones generales para la protección de datos personales"; así como de manera especial, en acatamiento de lo dispuesto en el artículo 2.8.8.1.2.5 del Decreto 780 de 2016, que estipula: "La información relativa a la identidad de las personas, obtenida durante el proceso de vigilancia en salud pública, es de carácter confidencial y será utilizada exclusivamente por parte de las autoridades sanitarias para fines de la vigilancia, o por las autoridades judiciales, siempre que medie solicitud previa del juez de conocimiento. 13.Coordinar en articulación con los líderes operativos, las acciones, para el análisis de eventos de salud priorizados, generando las alertas necesarias en el marco de ejecución del GSP PSPIC. 14. Atender requerimientos, elaborar respuestas a consultas y peticiones, del equipo de interventoría o seguimiento GSP PSPIC, auditoria y entes de control, con calidad y oportunidad; respecto a la operación de la vigilancia en salud pública en la Subred Integrada de Servicios de Salud.			

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
15. Asistencia a reuniones citadas por la SDS del líder del componente de VSP 16. Asistencia y participación a los COVE distritales (en caso de cruce de agendas podrá asistir el Universitario 1)			
1. Apoyar el seguimiento periódico a los indicadores de interés en salud pública para la subred integrada de servicios de salud, generando alertas oportunamente, frente al aumento de casos o situaciones colectivas que afecten la salud de la población, esto incluye los indicadores de VSP priorizados de los planes de cuidado de la salud. 2.Apoyo a la revisión integral y consolidación del plan de acción, garantizando el cumplimiento de criterios técnicos que requiere el proceso, implementando de manera efectiva el seguimiento periódico, para realizar ajustes y reportes de avance 3.Apoyar en la elaboración y presentar de manera oportuna, actas, bases de datos, matrices, presentaciones e informes requeridos para el GSP-PSPIC con el fin de mostrar las acciones realizadas desde el proceso de vigilancia en salud pública 4.Apoyar procesos de auditoria/seguimiento a los subsistemas de acuerdo al perfil según se requiera. 5. Participación en mesas de articulación con los diferentes actores del PSPIC y actores comunitarios, a demanda con el fin de articular acciones en el marco del modelo Mas Bienestar entre el PIC y las acciones de participación social.	El desarrollo de las actividades es diario, semanal y con reporte mensual según la especificidad y tiempos necesarios.	**Profesional universitario 1 (operativo),**	1. Matriz de indicadores, análisis y seguimiento 2.Plan de acción de la vigilancia en salud pública, aprobado y con avances mensuales 3.Informes seguimiento administrativo o matriz o seguimiento 4. Actas y listados de asistencia 5. Actas de mesas de articulación cuando aplique 6. Soporte seguimiento informes bimestrales 7.Seguimiento SEGPLAN 8.Soporte de cargue de la consolidación aplicativo Th 9.Acta y listado de asistencia de participación cuando aplique

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
6.Elaborar y Consolidación de manera oportuna de informes bimestrales y trimestral de gestión que permitan mostrar las acciones realizadas desde el proceso de vigilancia en salud pública, con el fin de dar brindar información técnica que permita aportar al desarrollo del modelo Mas Bienestar 7.Realizar el seguimiento periódico al SEGPLAN y a los indicadores GESI asociados, con el propósito de monitorear el cumplimiento de metas, evaluar el avance de las acciones programadas y contribuir a la toma de decisiones informadas en el marco de la gestión en salud pública 8.Apoyar la consolidación de los soportes en el aplicativo de talento humano, en coordinación con el tecnólogo, con el fin de asegurar la integridad, organización y disponibilidad de la información requerida para la adecuada gestión de la vigilancia en salud pública 9.Participación en las mesas SIVIGILA transmisibles cuando se requiera, con el fin de recibir línea técnica y realizar procesos de articulación para dar respuesta oportuna de acuerdo a las acciones desarrolladas por la vigilancia en salud publica en el marco del convenio GSP – PSPIC 10.Apoyar temas administrativos, técnicos y operativos que se requiera desde la Gestión Zonal de VSP			
1. Garantizar el flujo de información epidemiológica, que se genera a partir de la operación	El desarrollo de las actividades es diario, semanal y con reporte	Tecnólogo	1.Soporte de seguimiento o control del fujo de la información

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
de la vigilancia en salud pública de la subred, bajo los principios de integridad, disponibilidad, y confidencialidad de la información, en el marco de la gestión informática. **2.** Realizar la consolidación y cargue de los soportes que se ingresaran al aplicativo de talento humano en articulación con profesional universitario 1 3. Realizar la solicitud, inventario, y control del flujo de insumos requeridos para cada uno de los subsistemas de acuerdo con lo especificado en el anexo 8 y la demanda presentada por situaciones de contingencia, registrando la entrada y salida de cada uno de ellos 4. Elaboración del cronograma mensual de vehículos por cada subsistema de acuerdo a requerimiento, teniendo en cuenta asignación por anexo 8 y priorización por necesidades operativas y contingencias diarias del proceso, además de la verificación y solicitud de planillas de manera que se garantice el uso apropiado del recurso. 5.Garantizar el flujo de información epidemiológica, que se genera a partir de la operación de la vigilancia en salud pública de la Subred, bajo los principios de integridad, disponibilidad, y confidencialidad de la información, en el marco de la gestión informática en articulación con el ingeniero de sistemas. 6. Realizar la gestión documental teniendo en cuenta las normas de archivo vigentes, contabilizando el número de folios máximo para cada carpeta, ingreso al FUID y transferencias al archivo central de acuerdo con la periodicidad requerida.	mensual según la especificidad y tiempos necesarios		2. Soporte de cargue de la consolidación aplicativo Th 3. Seguimiento, inventario anexo 8 4. Cronograma de operación de vehículos VSP 5.Seguimiento flujo de información 6.Revisión gestión documental 7.Seguimiento al cronograma 8.Soporte de acciones técnicas 9. Actas de seguimiento a los equipos dispuestos en anexo 8 10.Soporte de mesas de ayuda.

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
7.Solicitar, consolidar y realizar seguimiento diario al diligenciamiento del cronograma de actividades solicitado por secretaria Distrital de Salud, teniendo en cuenta la calidad y concordancia de cada una de las variables, además de realizar el cargue de la información de acuerdo con la periodicidad y la metodología que defina nivel central. 8.Apoyar las acciones técnicas de fortalecimiento en conjunto con el ingeniero de sistemas. 9. En conjunto con el ingeniero de sistemas realizar actas de seguimiento a los equipos dispuestos por el anexo 8 (celulares, computadores, impresoras). 10.Crear las mesas de ayuda requeridas para el adecuado funcionamiento del área relacionada con infraestructura, insumos biomédicos, entre otras de las cuales se tenga competencia.			

En el marco del Modelo Territorial de Salud MAS Bienestar, cuyo objetivo es mejorar el bienestar, la calidad de vida y la salud de la ciudadanía de Bogotá mediante un modelo de salud basado en Atención Primaria Social, así como fortalecer la gobernabilidad y gobernanza territorial por medio de una acción sectorial e intersectorial efectiva, que incida positivamente en los determinantes sociales de la salud y mejore las condiciones de vida y salud de personas, familias y comunidades, desde las acciones de apoyo de la gestión de la salud pública y del plan de salud pública de intervenciones colectivas, se, reconocen cinco temas que transversalizan la operación, y que deben ser de conocimiento y apropiación por parte de los equipos integrales de salud (técnicos operativos de los entornos cuidadores y procesos transversales), para lo cual, se contará con los respectivos documentos operativos.

Estos temas transversales se dividen en dos categorías:

- Temas que implican procesos de intervención y cuyas fichas técnicas, están inmersos dentro de las carpetas de la coordinación GSP- PSPIC. (Carpeta: Temas_transversales)

- Temas transversales de procesos de Educación en Salud Pública, a través de los cuales se favorece la socialización, demanda de servicios, programas y acciones, y participación de la población que se interviene desde las acciones de la GSP-PSPIC. (Carpeta: Fichas_tecnicas).

3.1.1. A la primera categoría pertenecen:

- **Activación de rutas y canalizaciones:** Es el proceso mediante el cual se da continuidad a la atención desde otros actores a personas, familias y comunidades a las que se les identificaron riesgos, necesidades y situaciones desde acciones colectivas por medio de la aplicación de sus diferentes tecnologías; por tanto, la canalización hace parte de una acción resolutiva del PSPIC. Teniendo en cuenta que los entornos y procesos transversales operan el PSPIC en los territorios, es ineludible que reconozcan y apropien la ficha técnica del procedimiento de canalización para la activación de rutas integrales de atención en el GSP – PSPIC a la oferta distrital sectorial e intersectorial, documento de jerarquía fundamental sobre otro, toda vez que estandariza su operación y delimita los alcances de los diferentes niveles de operación del PSPIC.

- **Gestión del sistema de información – GESI:** Conjunto de procesos relacionados con la disponibilidad de los sistemas de información, para facilitar el control del proceso del ciclo de vida de la Información de las acciones realizadas por los entornos cuidadores con criterios de calidad, continuidad, oportunidad, pertinencia, accesibilidad, seguridad, integralidad, durante la etapas de planeación, ejecución, seguimiento y evaluación de las acciones colectivas desarrolladas en el marco del Plan de Salud Pública de Intervenciones Colectivas – PSPIC y GSP, para la toma de decisiones estratégicas para el mejoramiento de la salud.

- **Educación en Salud Pública:** La articulación del equipo de Educación para la Salud Pública con los entornos, temas y procesos de la Gestión de la Salud Pública y el Plan de Salud Pública de Intervenciones Colectivas (GSP-PSPIC) se fundamenta en el desarrollo y fortalecimiento de capacidades personales, institucionales y sociales. Esta articulación se concreta a través de la asistencia técnica, que incluye acompañamiento, capacitación, orientación y asesoría para la implementación de procesos educativos dialógicos.

La asistencia técnica proporcionada por el equipo de Educación para la Salud Pública tiene como objetivo crear escenarios formativos que permitan al talento humano en salud que opera en el GSP-PSPIC la oportunidad de desarrollar las capacidades necesarias para liderar procesos educativos dialógicos, en coherencia con lo planteado en el Modelo de Salud MAS Bienestar. En este sentido, la educación para la salud pública no es

transmitir información, sino generar procesos de producción y reproducción cultural que incidan en las formas de vida, condiciones y estilos de vida de la población.

Lo anterior en el entendido que parte de las horas destinadas para el fortalecimiento de capacidades, estarán en la lógica de los procesos de Educación para la Salud Pública.

3.1.2. A la segunda categoría pertenecen:

De otro lado y con relación a los temas transversales que hacen parte del proceso Educación en Salud Pública - ESP, se contemplan: autorregulación, donación de sangre, donación y trasplante de órganos, infección respiratoria aguda – IRA notificación de eventos de interés en salud pública y educación en prevención en control de infecciones, por lo cual, para su orientación técnica, se contará con fichas técnicas específicas que deben ser de conocimiento de los equipos operativos.

- **Autorregulación:** Busca aportar a los procesos de prevención y control de los factores de riesgo sanitarios, así como del monitoreo de los factores ambientales, a través de la sensibilización de la población sobre los aspectos que se deben tener en cuenta para minimizar o controlar los efectos en salud por inadecuadas condiciones sanitarias o ambientales, complementario con la sensibilización acerca de la responsabilidad que tienen los propietarios de los establecimientos sobre el cumplimiento de la normatividad sanitaria. Por tal motivo se promueve en la comunidad la estrategia de autorregulación, donde los proveedores o productores de bienes o servicios pueden inscribirse para la revisión de la norma sanitaria según la actividad económica, el registro, la verificación del cumplimiento normativo con base en una lista de chequeo, la solicitud de la visita sanitaria y la autorregulación posterior y de manera permanente.

Teniendo en cuenta el contexto mencionado, la Secretaría Distrital de Salud implementó en Bogotá, esta estrategia, la cual puede ser consultada a través de la página web “negocios saludables – negocios rentables”, (http://autorregulacion.saludcapital.gov.co/), donde los proveedores o productores de bienes o servicios pueden inscribirse siguiendo los pasos allí establecidos, los cuales incluyen la revisión de la norma sanitaria según la actividad económica, el registro, la verificación del cumplimiento normativo con base en una lista de chequeo, la solicitud de la visita sanitaria y la autorregulación posterior y de manera permanente. Adicionalmente, la invitación a que los establecimientos se vinculen a los programas de excelencia sanitaria que brinda la Secretaría Distrital de Salud.

- **Notificación de eventos de interés en salud pública:** El sistema nacional de vigilancia en Salud Pública es definido en el Decreto 780 de 2016 en su Artículo 2.8.8.1.1.3 como “Conjunto de usuarios, normas, procedimientos, recursos técnicos, financieros y de talento humano, organizados entre sí para la recopilación, análisis, interpretación, actualización, divulgación y evaluación sistemática y oportuna de la

información sobre eventos en salud, para la orientación de las acciones de prevención y control en salud pública". (Art. 3 de/Decreto 3518 de 2006).

La vigilancia en salud pública, función esencial asociada a la responsabilidad estatal y ciudadana de protección de la salud, consistente en el proceso sistemático y constante de recolección, análisis, interpretación y divulgación de datos específicos relacionados con la salud (1), incorpora el monitoreo de eventos que son de gran impacto en la salud de la población bogotana a través de las cuatro subredes integradas de servicios de salud.

En cumplimiento de la responsabilidad Distrital de protección de la salud y en pro del mejoramiento de la calidad y la notificación de los eventos de interés en Salud Pública (EISP), se desarrolla el componente con el fin de definir las líneas de acción para la gestión del subsistema SIVIGILA en la vigilancia de los eventos de interés en salud pública, identificando y recolectando información oportuna y veraz que permita el análisis de la situación de salud de la población bogotana, apoyando la toma de decisiones en el sistema de Salud.

Desde la Secretaría Distrital de Salud, se estandarizaron los productos y las acciones a desarrollar para garantizar su operación, desde la adaptación de los lineamientos nacionales para el Distrito Capital con el fin de dar cumplimiento a la meta de mantener en operación los Subsistemas de Vigilancia en Salud Pública, consolidando la red para la ciudad y la gestión de implementación en las localidades del Distrito de las intervenciones de vigilancia en Salud Pública.

La red de operadores de la VSP la forman instituciones públicas y privadas del sector salud u otros sectores de la ciudad de Bogotá, que captan y notifican eventos de interés en salud pública, generando la información necesaria para el subsistema de vigilancia en salud pública del Distrito Capital. En el modelo establecido se constituyen en el canal de entrada y se reconocen como Unidades Primarias Generados del Dato (UPGD) o Unidades Informadoras (UI) (2).

UPGD: "Entidad pública o privada que captura la ocurrencia de eventos de interés en salud pública y genera información útil y necesaria para los fines del sistema de vigilancia en salud pública-SIVIGILA" (1, 2).

Las localidades deberán recibir las fichas o planos de notificación de eventos captados por los entornos cuidadores y urgencias y emergencias, previamente caracterizados; verificar y garantizar la digitalización en el sistema SIVIGILA (articulación interna de la subred); y enviar con la notificación rutinaria semanal o inmediata, previa evaluación de cumplimiento en la definición de caso, si el entorno no realiza el ingreso al aplicativo, la subred deberá garantizar el ingreso de estas en aplicativo sivigila como corresponsable. Es de aclarar la responsabilidad del entorno con el sistema SIVIGILA; sin embargo, la subred debe articular entre sus procesos; en la matriz de articulación se aclaró la responsabilidad y obligatoriedad de quien capta el EISP "Notificación de eventos de

interés en salud pública captados dentro de sus actividades (artículo 2.8.8.1.1.2 decreto 780 de 2016)".

Eventos que se pueden notificar directamente por cada entorno/proceso

ENFERMEDADES GRUPO EVENTO CÓDIGO

ENFERMEDADES	GRUPO	EVENTO	CÓDIGO
Trasmisibles	Zoonóticos	Agresión por animal potencialmente trasmisor de la rabia	300
	Inmunoprevenibles	Varicela Individual	831
	Trasmitidas por alimentos	Enfermedad transmitida por alimentos o agua ETA (Brote)	349
	Inmunoprevenibles	Parotiditis Individual	620
	Inmunoprevenibles	Brote parotiditis	621
	Inmunoprevenibles	Brote Varicela	830
	Inmunoprevenibles	Brote de EDA	996
	Inmunoprevenibles	Brote por ERA	991
	Transmisibles	IRA Virus Nuevo	346
Salud Materno Infantil	Salud Materno Infantil	Morbilidad Materno Extrema	549
Vigilancia nutricional	Vigilancia nutricional	Desnutrición aguda en menores de cinco años	113

Así como en el Decreto 3518 de 2006, Artículo 20. Notificación obligatoria. Todos los integrantes del Sistema de Vigilancia en Salud Pública, Sivigila, que generen información de interés en salud pública, deberán realizar la notificación de aquellos eventos de reporte obligatorio definidos en los modelos y protocolos de vigilancia, dentro de los términos de estructura de datos, responsabilidad, clasificación, periodicidad y destino señalados en los mismos y observando los estándares de calidad, veracidad y oportunidad de la información notificada.

Para los eventos establecidos en el instrumento codificación eventos sivigila INS, el cual puede ser consultado en la página web del INS (https://www.ins.gov.co/Direcciones/Vigilancia/Paginas/SIVIGILA.aspx) o aquellos que representen un riesgo para la salud pública de los habitantes del Distrito.

Nota: los espacios convocados a nivel subred, serán asumidos por referentes o apoyos del entorno/proceso; los espacios convocados a nivel local serán asumidos por las personas delegadas para las mesas locales del cuidado por la salud, según el documento operativo de la Coordinación GSP-PSPIC.

4. Gestión de la información para los subsistemas de la vigilancia en salud pública:

Realizar la gestión técnica y operativa de los sistemas de información para la vigilancia en salud pública en la Subred Integrada de Servicios de Salud, garantizando la administración, seguridad, disponibilidad e integridad de los datos, de acuerdo con los lineamientos, protocolos y políticas establecidos por el nivel nacional y distrital.

Producto:

Gestión de la Información en los Subsistemas de la Vigilancia en Salud Pública, asegurando la calidad, oportunidad y confidencialidad de los datos, y el soporte tecnológico para el proceso integral e integrado de la VSP.

Unidad de medida; Mensual

Forma de reporte de ejecución del producto: Mensual

Perfil

Profesional Universitario 2, (Ingeniero de Sistemas, con mínima dos años (2) de experiencia en sistemas de información en salud pública y conocimientos que garantiza la gestión de la información. (La experiencia de los dos años puede ser como técnico en sistemas))

Descripción de la actividad

4.1. Apoyo Técnico al Área

Realizar apoyo técnico al área de vigilancia en salud pública, y articulación interna en la subred, en los procesos de gestión informática y soporte mesa de ayudad o el área TIC

Apoyo con la organización del equipo técnico en la proyección de cronogramas de disponibilidad, en los diferentes procesos que se requieran.

4.2. Coves distritales y Locales

Cuando hablamos del Comité Distrital de Vigilancia Epidemiológica (COVE Distrital) nos referimos a una instancia técnica, intersectorial y de coordinación que funciona a nivel distrital o territorial para fortalecer el Sistema de Vigilancia en Salud Pública.

El Comité Distrital de Vigilancia Epidemiológica es el órgano de articulación y análisis que reúne a las autoridades sanitarias del distrito, representantes de las diferentes instituciones prestadoras de servicios de salud, aseguradores y sectores relacionados, con el fin de coordinar, consolidar, analizar y dar respuesta a la información epidemiológica generada en el territorio.

- Ámbito: opera a nivel de ciudad o distrito.
- Conformación: Secretaría Distrital de Salud (líder), hospitales públicos y privados, EPS, IPS, laboratorios, y en algunos casos sectores como educación, ambiente o servicios públicos.
- Funciones clave:
    1. Coordinar la vigilancia epidemiológica en todo el distrito.
    2. Analizar la información de salud pública y la situación epidemiológica local.
    3. Recomendar acciones de prevención y control de eventos de interés en salud pública.
    4. Articular la respuesta ante brotes, epidemias y emergencias sanitarias.
    5. Capacitar y retroalimentar a los COVES institucionales.

- Integra la información de todos los actores del sistema de salud del distrito.
- Fortalece la toma de decisiones en salud pública con base en evidencias.
- Optimiza la respuesta interinstitucional ante emergencias sanitarias.
- Permite retroalimentar a las instituciones de salud para mejorar la calidad de los reportes al SIVIGILA.

El COVE Distrital es el espacio de coordinación y análisis a nivel territorial que asegura que la vigilancia epidemiológica no se quede en cada institución, sino que se traduzca en decisiones colectivas de salud pública para proteger a toda la población del distrito.

Para el desarrollo de los coves distritales las subredes apoyaran según el cronograma en la logística del COVE distrital

1. El equipo distrital y el equipo local definirán en conjunto la agenda, el lugar, con una duración no mayor a dos horas.
2. Él envió por correo electrónico de la agenda, el lugar de realización y si se requiere el link de inscripción, a cada una de las UPGD y UI distritales
3. El listado de asistencia se realizar por medio de formularios virtuales.
4. Elaboración del acta, la cual será realizado en un plazo máximo de 5 días hábiles siguientes al cove y será remitida al nivel distrital al grupo responsable del cove en el mes.

Cronograma de los responsables de la organización y apoyo de las subredes del COVE distrital y local para el año 2025, 2026 y 2027

MES	FECHA	GRUPO RESPONSABLE VSP	SUBRED DE APOYO	GRUPO DE APOYO DE LA SUBRED Y ORGANIZADOR DEL COVE LOCAL EN EL MES
Octubre	1 de octubre de 2025	Salud Mental	Sur	Salud Mental
Noviembre	5 de noviembre de 2025	Vigilancia Comunitaria	Sur Occidente	Vigilancia Comunitaria
Diciembre	3 de diciembre de 2025	Gestión de la Información	Centro Oriente	Gestión de la Información
Enero	21 de enero de 2026	Nutrición	Sur Occidente	Nutrición
Febrero	11 de febrero de 2026	No Trasmisibles	Sur	No Trasmisibles
Marzo	4 de marzo de 2026	Trasmisibles - Eventos Respiratorios	Sur Occidente	Trasmisibles - Eventos Respiratorios
Abril	8 de abril de 2026	Salud Ambiental	Centro Oriente	Salud Ambiental
Mayo	6 de mayo de 2026	Sivigila	Norte	Sivigila
Junio	3 de junio de 2026	Estadísticas Vitales	Sur	Estadísticas Vitales
Julio	1 de julio de 2026	Salud Sexual y Reproductiva	Centro Oriente	Salud Sexual y Reproductiva
Agosto	5 de agosto de 2026	Urgencias y Emergencias	Norte	Urgencias y Emergencias
Septiembre	2 de septiembre de 2026	Trasmisibles - Eventos EPV	Sur	Trasmisibles - Eventos EAPV
Octubre	7 de octubre de 2026	Salud Mental	Sur Occidente	Salud Mental
Noviembre	4 de noviembre de 2026	Vigilancia Comunitaria	Centro Oriente	Vigilancia Comunitaria
Diciembre	2 de diciembre de 2026	Subdirección de VSP	Norte	Gestión de la Información
Enero	13 de enero de 2027	Nutrición	sur	Nutrición
Febrero	10 de febrero de 2027	No Trasmisibles	Sur Occidente	No Trasmisibles
Marzo	3 de marzo de 2027	Trasmisibles - Eventos Respiratorios	Centro Oriente	Trasmisibles - Eventos Respiratorios
Abril	7 de abril de 2027	Salud Ambiental	Norte	Salud Ambiental
Mayo	5 de mayo de 2027	Sivigila	Sur	Sivigila
Junio	2 de junio de 2027	Estadísticas Vitales	Sur Occidente	Estadísticas Vitales
Julio	7 de julio de 2027	Salud Sexual y Reproductiva	Sur	Salud Sexual y Reproductiva
Agosto	4 de agosto de 2027	Urgencias y Emergencias	Centro Oriente	Urgencias y Emergencias
Septiembre	1 de septiembre de 2027	Trasmisibles - Eventos EAPV	Sur Occidente	Trasmisibles - Eventos EAPV
Octubre	6 de octubre de 2027	Salud Mental	Centro Oriente	Salud Mental
Noviembre	3 de noviembre de 2027	Vigilancia Comunitaria	Norte	Vigilancia Comunitaria
Diciembre	1 de diciembre de 2027	Subdirección de VSP	Sur	Gestión de la Información

El líder de la gestión de la información deberá socializar la agenda a todo el equipo de vigilancia de la subred, explicando y definiendo las actividades que deberán realizar los equipos responsables del apoyo al cove, y deberá soportar esta actividad con el acta y el

listado de firmas, este soporte será enviado el último día hábil del mes de octubre, al correo rdrodriguez@saludcapital.gov.co

4.3. Infraestructura Tecnológica

La infraestructura tecnológica en el marco de la gestión de la información en salud pública se refiere al conjunto de recursos físicos, lógicos y organizativos que permiten el almacenamiento, procesamiento, análisis, transmisión y protección de los datos de salud. Esta infraestructura constituye la base operativa que soporta los sistemas de información y garantiza la disponibilidad, integridad, seguridad y accesibilidad de la información en tiempo real.

Incluye componentes como:

- **Hardware:** servidores, computadores, dispositivos móviles, unidades de almacenamiento y redes de comunicación.
- **Software:** sistemas de información en salud (HIS, SIVIGILA, etc.), bases de datos, plataformas de visualización, herramientas de análisis estadístico y sistemas de respaldo.
- **Conectividad:** acceso a internet, redes internas seguras (intranet), VPN y canales de comunicación en línea entre diferentes niveles del sistema.
- **Seguridad informática:** mecanismos de control de acceso, cifrado, autenticación, copias de seguridad y protocolos de recuperación ante fallos.
- **Soporte técnico y talento humano:** personal capacitado para la operación, mantenimiento y actualización de los sistemas y equipos tecnológicos.

Una infraestructura tecnológica adecuada permite **gestionar la información de forma eficiente, segura y oportuna**, facilitando la toma de decisiones basadas en evidencia, la vigilancia en salud pública, la articulación intersectorial y la respuesta rápida ante emergencias sanitarias.

Activos de Información

4.3.1. Hardware

La disponibilidad tecnológica es fundamental para el desarrollo de la gestión de la información, en la Vigilancia en Salud Publica, requiere la disponibilidad de equipos de cómputo con la capacidad de procesamiento y almacenamiento, adecuadas para el

cumplimiento de las actividades requeridas; por lo cual se requiere realizar el inventario para detectar, equipos deteriorados o caducados. stock obsoleto, equipos que desaparecen, adicionalmente nos ayuda a hacer un buen plan de mantenimiento y, por ende, garantizar la continuidad de su uso.

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
Ficha de inventarios de activos de información acorde a los equipos disponibles para la vigilancia en salud pública.	Se realizar en el mes de: Octubre de 2025 Febrero de 2026 Febrero de 2027	Título Profesional en Ingeniera de Sistemas	1. Ficha de INVENTARIO DE ACTIVOS DE INFORMACIÓN, HARDWARE, enviado por correo electrónico

4.3.2. Software

Los equipos deberán contar con los aplicativos necesarios para el desarrollo de la gestión de la información, los cuales son

- Microsoft Windows 10 versión profesional, (**Nota Importante:** El soporte principal para Windows 10 finaliza el 14 de octubre de 2025. Después de esa fecha, Microsoft dejará de ofrecer actualizaciones de seguridad y soporte técnico para Windows 10. **Consecuencias:** No más actualizaciones de seguridad ni soporte técnico, por lo cual las subredes dispondrán de 6 meses hasta el 14 de abril de 2026, para actualizar el sistema operativo de los equipos de computa a Windows 11 profesional.

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
Ficha de inventarios de activos de información acorde a los softwares disponibles para la vigilancia en salud pública	Se realizar en el mes de: Octubre de 2025 Febrero de 2026 Febrero de 2027	Título Profesional en Ingeniera de Sistemas	1. Ficha de INVENTARIO DE ACTIVOS DE INFORMACIÓN, SOFWARE, con el número de licencias disponibles, enviado por correo electrónico

Los productos serán enviados el día:

- El primer reporte será enviado por correo electrónico como máximo plazo el 31 de octubre de 2025.
- El Segundo reportes será enviado por correo electrónico como máximo plazo el 27 de febrero de 2026.
- El tercer reporte será enviado por correo electrónico como máximo plazo el 26 de febrero de 2026.

4.4. Protocolos de transferencia de información

La transferencia de información en vigilancia en salud pública es un proceso clave que garantiza el flujo oportuno, seguro y estandarizado de datos entre los diferentes actores del sistema de salud. Para ello, se implementan protocolos específicos que definen las normas, procedimientos y herramientas que deben seguirse para asegurar la calidad, confidencialidad y utilidad de la información transmitida.

Estos protocolos son esenciales para mantener la continuidad y eficiencia del sistema de vigilancia, permitiendo detectar eventos de interés en salud pública, monitorear tendencias epidemiológicas y activar respuestas tempranas frente a emergencias sanitarias.

Entre las generalidades más relevantes de estos protocolos se destacan:

1. **Estandarización de formatos y contenidos** Se establecen estructuras y campos de información uniformes (como fichas de notificación, códigos CIE-10, variables mínimas requeridas), que facilitan la interoperabilidad entre sistemas y la comparación de datos entre regiones o instituciones.

2. **Periodicidad y rutas de notificación** Se definen frecuencias claras (diaria, semanal, inmediata, etc.) y canales formales para el envío de datos desde los prestadores de servicios de salud hacia las entidades territoriales, y de allí al nivel nacional o internacional si es necesario.

3. **Medios de transmisión** Los protocolos especifican si la transferencia se realiza por medios electrónicos (plataformas web, bases de datos en línea, correo institucional seguro), físicos (en casos excepcionales), o a través de sistemas integrados de información en salud (como SIVIGILA en Colombia).

4. **Seguridad y confidencialidad** Todo protocolo debe incluir medidas de protección de datos sensibles, control de accesos, autenticación de usuarios y trazabilidad de la información para evitar filtraciones o manipulaciones no autorizadas.

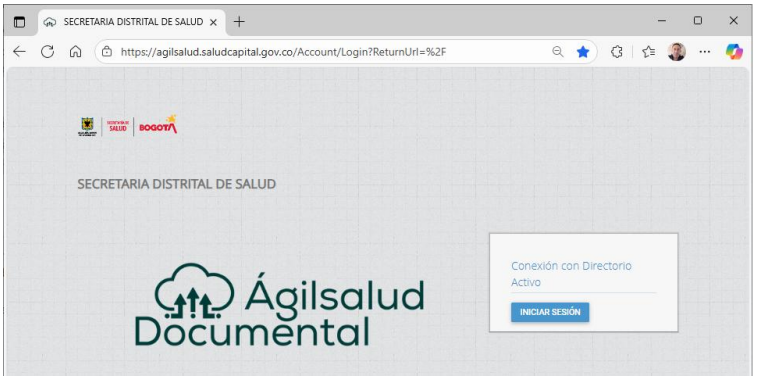
5. **Validación y calidad de datos** Se establecen mecanismos de revisión, depuración y validación de los registros antes, durante y después de su

transferencia, garantizando que los datos sean precisos, completos y consistentes.

6. **Capacitación y responsabilidad institucional** Los protocolos también determinan roles y responsabilidades para cada actor del sistema (IPS, EPS, entes territoriales, institutos nacionales), así como los requerimientos de formación continua para el personal involucrado.

En conjunto, los **protocolos de transferencia de información en vigilancia en salud pública** son una herramienta estratégica que permite asegurar la **fluidez, utilidad y seguridad del dato epidemiológico**, constituyendo la base para la respuesta sanitaria, la formulación de políticas y la protección de la salud colectiva.

El medio de comunicación oficial entre la Secretaria de Salud de Bogotá y las subredes será, la plataforma web de Agisalud Documental, en la cual se radicaron las comunicaciones oficiales



Los correos institucionales serán el único medio de comunicación escrito aprobado, y tendrán valides, en procesos de auditoría, entrega de productos y cumplimiento de actividades.

Nota Importante: Los correos utilizados por las subredes deberán ser de dominio institucional, identificando la subred a al que pertenecen y deberán ser firmados por el funcionario que genera el correo, con el nombre del funcionario, cargo, subsistema, área a la que pertenece, subred y numero de contacto, de lo contrario "***no tendrán validez oficial en ninguno de los procesos o como soportes de la gestión realizada***."

Para los referentes de la gestión de la información de cada subred, deberán contar con un correo institucional con al menos 50 gb de espacio, y disponibilidad de espacio en

el OneDrive de al menos 500 gb, de espacio disponible, el correo deberá ser con las siguientes características de nombre según la subred como:

- Subred Norte: givsp@(dominio del hospital).gov.co
- Subred Centro Oriente: givsp@(dominio del hospital).gov.co
- Subred Sur Occidente: givsp@(dominio del hospital).gov.co
- Subred Sur: givsp@(dominio del hospital).gov.co

Cada subsistema de información deberá contar con un correo institucional con las mismas características, garantizando todos los protocolos de trasferencia de información.

Se deberá enviar el inventario de correos disponibles por subsistema de información, y deberá incluir, correo electrónico, nombre del funcionario responsable y celular de contacto.

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
Ficha de inventarios de activos de información acorde a los correos por subsistema de información para la vigilancia en salud pública	Se realizar en el mes de: Octubre de 2025	Título Profesional en Ingeniera de Sistemas	1. Ficha de INVENTARIO DE ACTIVOS DE INFORMACIÓN, CORREOS ELECTRÓNICOS POR SUBSISTEMA DE INFORMACIÓN enviado por correo electrónico
	Mensual		1. Ficha de INVENTARIO DE ACTIVOS DE INFORMACIÓN, CORREOS ELECTRÓNICOS POR SUBSISTEMA DE INFORMACIÓN enviado por correo electrónico, con las novedades presentadas el último día hábil del mes

Los productos serán enviados el día:

El primer reporte será enviado por correo electrónico como máximo plazo el 31 de octubre de 2025.
Las novedades se enviaron en último día hábil del mes.

4.5. Gestión Documental

La gestión documental se refiere al conjunto de procesos, normas y herramientas que permiten la organización, producción, recepción, procesamiento, circulación,

almacenamiento, conservación y disposición final de los documentos relacionados con la vigilancia, análisis y toma de decisiones en salud pública.

Estos documentos pueden ser físicos o electrónicos, e incluyen registros de notificación, fichas epidemiológicas, reportes estadísticos, actas, resoluciones, informes técnicos, comunicaciones oficiales y demás soportes que contienen información vital para el funcionamiento del sistema.

Su objetivo principal es:

Garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información documental, asegurando que esté accesible para quienes la requieran, en el momento oportuno, y conforme a la normativa legal vigente.

1. **Clasificación y organización documental:** Establecimiento de series documentales y tipologías específicas para los procesos de salud pública.
2. **Digitalización y archivo electrónico:** Conversión de documentos físicos a formatos digitales y uso de sistemas informáticos para su almacenamiento y gestión.
3. **Control de versiones y trazabilidad:** Registro de modificaciones, responsables y fechas para garantizar la transparencia y la auditoría documental.
4. **Acceso y consulta controlada:** Definición de niveles de acceso para proteger la confidencialidad de datos sensibles, especialmente cuando contienen información personal o clínica.
5. **Conservación y disposición final:** Aplicación de tablas de retención documental que determinen el tiempo de archivo, migración a otros formatos o eliminación segura según valor administrativo, legal o histórico.

En resumen, la gestión documental dentro del sistema de información en salud pública es una función **estratégica y normativa** que fortalece la eficiencia administrativa, mejora la calidad del dato, asegura el cumplimiento legal y respalda las acciones de vigilancia, intervención y evaluación en salud.

Gestión de respaldo de información para los 14 subsistemas de información

La Secretaria de Salud de Bogotá, considera que toda la información de sus sistemas informáticos debe ser protegidos de posibles daños, por lo que debe ser respaldada con cierta frecuencia, para asegurar el proceso de recuperación.

Bajo esta premisa, el referente de la gestión de la información deberá considerar soluciones de respaldo para equipos de escritorio, sistemas de información y aplicaciones (códigos fuentes, bases de datos, etc.) que se consideren críticos para las

subredes. Igualmente, garantizar la disponibilidad de infraestructura adecuada de respaldo y asegurar su disponibilidad cuando sea requerida la copia, incluso después de un desastre o falla de un dispositivo.

Cada respaldo que se realice, manual o automático, deberá quedar registrado en un LOG de copias o soporte de la gestión realizada

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
En reunión con el equipo de gestión de la información, de la secretaria de salud y subredes se definirán los activos de información que requieren respaldo de seguridad (Backup)r	Se realizar en el mes de: Octubre de 2025	Título Profesional en Ingeniera de Sistemas	Acta de reunión con la definición de cada base a la cual se le realizara respaldo
Realizar respaldos de información por cada activo de información, las bases de datos tendrán el acumulado del año 2024 (Iniciando el 1 de enero de 2024 a la fecha de corte)	Mensual		Log de respaldo y verificación de los backups por mes, si la subred no cuenta con servidores de respaldo, deberá contar con medio de respaldo alterno. Generar listado de la información respaldad los cortes de información

Los productos serán enviados el día:

El último día hábil del mes por correo electrónico.

Los reportes serán enviados al correo rdrodriguez@saludcapital.gov.co y cargado al OneDrive en la carpeta dispuesta para la subred

- \OneDrive - Saludcapital\- CONVENIO_GSP_20250901_20270630\Gestion de la Informacion Subred\1_Subred_Norte
- \OneDrive - Saludcapital\- CONVENIO_GSP_20250901_20270630\Gestion de la Informacion Subred\2_Subred_Centro Oriente
- \OneDrive - Saludcapital\- CONVENIO_GSP_20250901_20270630\Gestion de la Informacion Subred\3_Subred_Sur_Occidente
- \OneDrive - Saludcapital\- CONVENIO_GSP_20250901_20270630\Gestion de la Informacion Subred\4_Subred_Sur

La disponibilidad de los accesos se realizará a los correos oficiales de la subred para la gestión de la información

4.6. Seguridad de la Información

Manejo de información personal, 'Habeas data'

La confidencialidad, en informática, es un principio fundamental de la seguridad de la información que garantiza el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.

- Ley 1266 de 2008 "*Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*"

- Artículo 3 del Decreto 235 de 2010, modificado por el Artículo 1 del Decreto 2280 de 2010, establece que "*para efectos de formalizar el intercambio de información de manera ágil, oportuna y confiable, las entidades públicas o los particulares encargados de una función administrativa podrán emplear el mecanismo que consideren idóneo para el efecto, tales como cronograma de entrega, plan de trabajo, protocolo o convenio, entre otros*."

- Artículo 9 de la Ley 1581 de 2012, menciona respecto a la autorización del titular que. "*Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior*."

- Artículo 4 de la Ley 1581 de 2012, menciona que para el tratamiento de datos personales se aplica de manera armónica Principio de confidencialidad, por el cual "*todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma*."

Que, por lo expuesto, la información recibida por parte de las UPGD y UI por medio de notificaciones, recolección o cualquier otro medio, están cubiertas por la ley de habeas data y tratamiento de datos personales y el uso de esta información será de uso exclusivo del área de vigilancia en salud pública de la subred y el uso se restringe solo para los fines establecidos según los lineamientos, decretos y circulares para la Vigilancia en Salud Publica, tanto para los técnicos y profesionales, cada funcionario tienen la responsabilidad de su custodia y adecuado uso, adicionalmente los documentos como actas, intervenciones epidemiológicas, unidades de análisis, estudios de caso y todos aquellos que contengan información de pacientes o evaluación de instituciones; Las

notificaciones y documentos serán de uso exclusivo para la subred y el área de vigilancia en salud pública de la Secretaria de Salud de Bogota.

El envió de casos residentes de otras subredes (comunicación inter local) para el desarrollo de intervenciones epidemiológicas o vistas de salud pública, también cuentan con la protección del tratamiento de datos personales y normas establecidas.

No se entregará información de ningún subsistema, de forma parcial o completa a personas naturales o empresas fuera de la subred, cualquier solicitud de información deberá ser por medio de oficio dirigida a la Subdirección de Vigilancia y Control en Salud Publica de la secretaria de Salud de Bogotá, enviada por correo certificado.

Le excepción son los requerimientos judiciales, los cuales tiene carácter legal y de obligatorio cumplimiento.

Para las diferentes áreas de la subred que requieran información de Salud Pública, se deberá solicitar por medio escrito (oficio o correo electrónico) al líder de vigilancia en salud pública, en cual se especificara cual va a ser el uso de la información solicitada, se deberá definir las variables, el periodo y el evento, y se deberá diligenciar y firmar el "Formato de Trasferencia de Información", el responsable que recibe (receptor), debe ser un funcionario activo de la subred, de planta o contratista.

La Secretaria Distrital de Salud desarrollo la "Política de Seguridad de la Información" SDS-TIC-POL-001 V.8, cuyo objetivo principal está encaminado a garantizar los lineamientos de seguridad de la información de la SDS (recursos de software, recursos de hardware, sistemas de información) se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto, asegurando la confidencialidad de la información; y la "Política de protección de datos personales SDS-TIC-POL 003 V.2.

Bajo este contexto, dentro la seguridad de la información de la Vigilancia en Salud Pública, las Subredes y el talento humano asignado deberán adoptar los siguientes procedimientos:

- Confidencialidad de la información: "toda persona que intervenga en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación"

Por su naturaleza, marco normativo, importancia y especificidad de los datos que maneja el Sistema de Vigilancia en Salud Pública, la información resultante tiene una alta sensibilidad, tal como lo indica el Artículo 5 de la Ley 1581 de 2012 y el Artículo 2.8.8.1.2.5 del Decreto 780 de 2016, en donde se especifica: "La información relativa a la Identidad de las personas, obtenida durante el proceso de vigilancia en salud pública, es de carácter confidencial y será utilizada exclusivamente por parte de las autoridades sanitarias para fines de la vigilancia, o por las autoridades judiciales, siempre que medie solicitud previa del juez de conocimiento. Para el efecto, el Ministerio de la Protección Social reglamentará la obtención, uso, administración y seguridad de la información de salud".

Las subredes deben ser garantes que el talento humano asignado cumpla con las directrices, por lo cual se deberá diligenciar el Formato de transferencia de información **SDS-TIC_014 V.2** por cada uno de los participantes de los subsistemas, al inicio de vigencia, en cada adición y cuando ingrese talento humano nuevo.

Por consiguiente, **el manejo y uso de esta información implica una responsabilidad legal para los administradores de los datos de la VSP**. Para ello la Subdirección de Vigilancia en Salud Pública de la Secretaría Distrital de Salud, establece que:

- El uso de la información de vigilancia en salud pública tiene varias finalidades, que todos los administradores de la información deben conocer y garantizar y está descrita en el Decreto 780 de 2016 en su artículo 2.8.8.1.1.4.

La reproducción y/o entrega a terceros de las bases de datos de cada uno de los subsistemas de Vigilancia en Salud Pública, debe regirse bajo la normatividad vigente. El uso indebido de esta información debe ser notificado de forma inmediata a la Secretaría Distrital de Salud y a las entidades judiciales competentes.

"Acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley 1581 de 2012 y la Constitución".

- Las instituciones deben garantizar la seguridad de la información, aplicando las medidas que sean necesarias para garantizar la integridad de los datos, evitar adulteración, pérdida, consulta o uso no autorizado.

El producto es el control de la información suministrada a las diversas áreas de la subred contando con el formato de transferencia de información completamente diligenciado.

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
Se generará un repositorio escaneado de los formatos de trasferencia de información por mes	Se realizar en el mes de: Octubre de 2025	Título Profesional en Ingeniera de Sistemas o Tecnólogo	Formato de Trasferencia de Información, para el inicio del convenio todos los funcionarios (Contratistas y de Planta), deberán diligenciar el formato de confidencialidad dando claridad la fecha de inicio y ficha de fin del contrato. El tecnólogo podrá apoyar a la entrega y solicitud del formato a los funcionarios nuevos, todos los formatos diligenciados deberán ser cargados al repositorio establecido para este fin, administrado por el ingeniero de sistemas. Los formatos en PDF serán envidos por correo según lo establecidos en el

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
			equipo de gestión de la información.
	Mensual		Formato de Trasferencia de Información, de forma mensual se entregarán las novedades según el ingreso de funcionarios nuevos Nota: Si la información es periódica solo se deberá diligenciar un solo formato aclarando que la entrega se realizara indefinidamente y si es por solo una ocasión se deberá diligenciar el formato de trasferencia con la claridad de una sola entrega

Los productos serán enviados el día:

El último día hábil del mes por correo electrónico.

4.7. Soporte Tecnológico

4.7.1. Capacitaciones y evaluación de procesos

La capacitación son un papel primordial para el logro de tareas y proyectos, dado que es el proceso mediante el cual los trabajadores adquieren los conocimientos, herramientas, habilidades y actitudes para interactuar en el entorno laboral y cumplir con el trabajo que se les encomienda.

Las acciones de capacitación permiten adquirir conocimientos teóricos y prácticos, que las personas actualicen sus conocimientos y adquieran nuevos, que fortalezcan su capacidad de respuesta ante los cambios del entorno o de sus requerimientos laborales, incrementen su desempeño dentro de la subred o institución y estén más preparadas para el día a día, lo cual les dará mayor confianza personal al desarrollar otras aptitudes y actitudes.

En un mundo donde la única constante es el cambio, obtener el beneficio del aprendizaje continuo es una oportunidad para mantener la vigencia laboral y desarrollar e innovar en los procesos de trabajo.

En este orden de ideas, la capacitación laboral busca que las tareas se realicen con calidad, productividad, estabilidad, permanencia y en un buen ambiente de trabajo.

Entre los beneficios destacan:

- Calidad y mejora en las tareas,
- Reducción en tiempos y supervisión,
- Solución de problemas con diferente visión,
- Sensibilización ante nuevos retos,
- Desarrollo ético y motivación del personal,
- Creación de equipos de trabajo de alto desempeño,
- Seguridad y autoestima en los trabajadores,
- Mayor especialización, a la vez que flexibilidad en sus tareas.

Debido a la dinámica de salud pública, cambio en los lineamientos según el comportamiento de las enfermedades y la adaptación de las herramientas informáticas a estos cambios y principalmente al constante cambio de personal en las subredes y en mayor medida en las UPGD y UI, es necesario implementar espacios de capacitación constante, con el fin de unificar y estandarizar criterios, formatos y procedimientos.

Los ingenieros deberán garantizar una capacitación de Sivigila 4.0 o Sivigila DC o herramienta informática que sea parte de la vigilancia en salud pública, el objetivo es poder desarrollar las capacitaciones con calidad, contando con los técnicos de los diferentes subsistemas de información de las subredes o expertos externos, que puedan contribuir a una adecuada trasferencia del conocimiento.

Deberán convocar al 100% de las UPGD y UI en la vigencia de convenio, en importante aclarar que las capacitaciones se podrán desarrollar de forma virtual a través de Microsoft Teams, distribuyendo al 100% de las instituciones entre los 2 meses del convenio, con el objetivo de poder atender la mayor cantidad de inquietudes presentadas, en el producto iniciara de acuerdo a cronograma definido en comite gestión de la información , debido al tema de logista, convocatoria y reagenda miento debido a que tiene muchas variables que no dependen del funcionario, el objetivo es diseñar, agendar, realizar, verificar el cumplimiento de los asistentes y verificar a que institucione representan, se deberá contar con la lista de asistencia que deberá contar con:

Fecha de reunión
Código de habilitación de la UPGD o UI

Nombre de la razón social
Nombre completo
Apellido completo
Numero de Documento
Celular o teléfono de contacto con extensión
Correo electrónico al cual será enviado el certificado de asistencia

Para las capacitaciones se realizará, un pre-test y al finalizar un post test y solo se enviará correo certificando la asistencia a quienes diligencien los formularios enviados durante el fortalecimiento técnico (pre-test, pos-test y listado de asistencia).

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
Capacitaciones de las plataformas Sivigila 4.0, Sivigila DC o el tema que aporte a los sistemas de información en salud pública, a las UPGD y UI del distrito capital. Este espacio podrá ser utilizado por referentes distritales o locales, según las necesidades del momento, por emergencias, brotes, cambios en protocolos, implementación de nuevas estrategias, etc. La capacitación por ser un espacio al cual se convocaran UPGD y UI, se desarrollará según cronograma establecidos por el equipo de gestión de la información, y será organizado por una subred de forma mensual.	Se realizar en el mes de: Octubre de 2025	Título Profesional en Ingeniera de Sistemas	En acta se definirán los responsables de forma mensual y se iniciara en el mes de noviembre, con la subred norte
	Mensual		Grabación de la capacitación, lista de asistencia y resultados del pre y pos test, generando un informe de resultados. Y las inquietudes que pudieran surgir en la capacitación

Los productos serán enviados el día:

El último día hábil del mes por correo electrónico.

4.7.2. Monitoreo y seguimiento de la calidad del dato de las fuentes de información de VSP (depuración, precrítica, critica, ajuste y realimentación dato, evaluación de indicadores)

La falta de la calidad en los datos es uno de los principales problemas a los que se enfrentan los responsables de sistemas de información, pues representa claramente uno de los problemas "ocultos" más graves y persistentes en los sistemas de información en salud publica

Cómo definimos la calidad de los datos

Según lo que plantea la norma ISO 9000: 2000, la calidad se podría definir como "*el grado en el que un conjunto de características inherentes cumple con los requisitos, esto es, con la necesidad o expectativa establecida, generalmente implícita u obligatoria*".

David Loshin, President of Knowledge Integrity, Inc: "*Para ser capaces de relacionar los problemas de la calidad de datos con su impacto en el negocio, tenemos que ser capaces de clasificar tanto nuestras expectativas de calidad de datos, como los criterios de impacto en la empresa*".

Dr Kaoru Ishikawa (1988), a su vez, considera que: "*En su interpretación más estrecha, calidad significa calidad del producto, pero en su interpretación más amplia significa calidad del trabajo, calidad del servicio, calidad de la información, calidad del proceso, calidad de la dirección y calidad de la empresa*".

Para poder obtener un buen control de calidad se requiere cubrir todo un procedimiento para poder lograr nuestro objetivo, que es mejorar la calidad

La importancia a la calidad de sus datos generara los siguientes beneficios a la información:

- Minimizar los riesgos en los errores de análisis, especialmente en los relacionados con la gestión de la información.
- Ahorro de tiempo y recursos, haciendo un mejor uso de la infraestructura tecnológica y sistemas para explotar su información.
- Toma de decisiones oportunas, en base a información confiable, validada y limpia.
- Adaptación a estándares o regulaciones internacionales sobre el manejo de información, permitiendo facilidad al momento de ejecutarlas.
- Mejorar la confianza.

Depuración de datos

La depuración de datos consiste en el proceso de detección y corrección de datos incorrectos o corruptos de una base de datos. El proceso se utiliza principalmente cuando contiene datos incorrectos, incompletos, inexactos o irrelevantes que son identificados, y luego modificados, sustituidos o eliminados.

Si queremos asegurarnos de que los datos se utilizan de la manera más productiva y significativa posible, de forma que podamos añadir valor, se debe dar mucha importancia a la calidad utilizando herramientas y depuración.

Se pueden lograr beneficios, algunos de los cuales pueden conducir a reducir los costes operativos y maximizar las ganancias.

Mejora la eficiencia: Mediante la depuración de datos, se elimina el problema de datos incorrectos o contaminados. Podemos crear listados más eficientes. En el proceso los datos han de estar limpios, actualizados y exactos, siguiendo con regularidad las rutinas de calidad.

La duplicación de datos es otro aspecto que puede ser erradicado. El impacto de la duplicación es directamente proporcional al tiempo que permanecen en la base de datos.

Mejora el proceso: En una organización se duplican los datos, podrían estar limpios inicialmente, pero los errores pueden surgir en cualquier momento.

Con unos datos limpios se puede realizar mucho mejor la analítica que puede ofrecerte un completa inteligencia de negocios (business intelligence), lo cual contribuirá al éxito a largo plazo.

Agiliza las Tareas: La eliminación de la duplicación de datos puede ayudar a optimizar y ahorrar mucho dinero. Y acompañar en la determinación de si algunos flujos de trabajo pueden ser modificados o identificar una oportunidad para lanzar un nuevo servicio.

Aumenta rendimiento: Tener una base de datos limpia y bien mantenida puede evitar que se utilice información desactualizada. Al trabajar con registros limpios maximizamos la eficiencia y la productividad del personal.

Aumentan las respuestas: Si se trabaja en la mejora de la coherencia y el aumento de la veracidad de los datos a través de la depuración, se pueden mejorar drásticamente las tasas de respuesta, lo que se traduce en mayores beneficios

Diferenciar entre los que se pueden detectar de forma automática, y los "enigmáticos", que requieren contextualización, intervención humana.

Variedad: La información procede de distintas fuentes y su estructura puede ser mucha, poca o directamente ninguna. Por ello, es imposible poder aplicar una misma métrica de calidad a todos ellos (Bases de datos SQL (o no SQL), propias o de terceros, Datos del CRM, Hojas de cálculo, Informes de transacciones…)

Ésta gran variedad de se traduce frecuentemente en grandes diferencias semánticas (campos con nombre idénticos pero significados muy diferentes, según el departamento), o inconsistencias sintácticas (por ejemplo sellos temporales inútiles, **etc.**). Las primeras, se

pueden reducir considerablemente si disponemos de los metadatos adecuados de las distintas fuentes. Para las segundas, habrá que esperar a la fase de Data Engineering, donde se seleccionan los campos útiles para las predicciones y se descartan los que aportan ruido. Por ejemplo, los campos con valores aleatorios, o campos dependientes etc.

Volumen: Hay que definir métricas de calidad, dejar de trabajar con valores absolutos, para pasar a hacerlo con aproximaciones e intervalos de confianza.

Velocidad: Si los procesos de depuración de los datos no son los adecuados, para cuando se ha verificado su calidad, estos datos han perdido su valor para el negocio. No obstante, este incremento de velocidad se consigue a costa de sesgar la información.

Veracidad: La veracidad de los datos tiene que ver con los posibles sesgos en la información, el ruido, y los datos anormales. Además los datos pueden ser poco consistentes o poco fiables (según su origen, proceso de captura de la información, procesado, infraestructura de seguridad etc.).

Esta desconexión entre las fuentes de la información y los usuarios finales es la causa principal de los problemas de calidad de los datos desde la perspectiva de la Veracidad

Valor: El "Valor" del dato es mucho más tangible, nos permiten "medir" su calidad, y definir estrategias para mejorarla. El dato es bueno si me sirve para lo que yo quiero hacer con él.

Por lo expuesto con anterioridad, la calidad de la información de la notificación recibida por parte de las fuentes primarias de información es de vital importancia para un adecuado análisis, por esta razón los ingenieros apoyaran a los profesionales de los diversos subsistemas, a construir rutinas de depuración, para la evaluación, depuración y control de la información recibida.

Nota Importante: *La solicitud para el apoyo técnico se deberá realizar por medio de correo electrónico del lider del componente que lo requiera, el correo deberá tener la solicitud del apoyo técnico, los documentos, manuales, fichas y documentos necesarios para el desarrollo solicitado, un documento donde se explique clara mente lo que se requiere, las bases que se deberán gestionar y el cronograma propuesto por el componente, es importante que el desarrollo sea acompañado por el profesional encargado del subsistema.*

La calidad de datos es la cualidad de un conjunto de información recogida en una base de datos, un sistema de información o un data warehouse que reúne entre sus atributos la exactitud, completitud, integridad, actualización, coherencia, relevancia, accesibilidad y confiabilidad necesarias para resultar útiles al procesamiento, análisis y cualquier otro fin que un usuario quiera darles.

Los subsistemas de información cuentan con procesos estandarizados de captura de información, sin embargo, se presenta la novedad que la información recolectada no cuenta con la calidad necesaria, por este motivo implementar estrategias de evaluación y apoyo en metodologías de evaluación de información, con el objetivo de mejorar la calidad de la información.

1. Evaluación del manejo de herramientas por parte de los técnicos de los subsistemas de información
2. Generar espacios de capacitación de las dificultades evidenciadas
3. Evidenciar la información o variables que presentan el mayor volumen de inconsistencias
4. Definir estrategias y metodologías de depuración de la información, apoyando a los referentes de cada componente según lo soliciten
5. Programar rutinas de depuración con el apoyo de los referentes
6. Evaluación constante de la calidad del dato

Las subredes deben garantizar que el talento humano asignado para el producto de Gestión de la Información, tengan las capacidades suficientes y el conocimiento adecuado para el manejo de los datos para la vigilancia en salud pública, deberá conocer la normatividad, instrumentos, protocolos, lineamientos y documentos necesarios para el procesamiento y evaluación de la información notificada.

Actividad Inicial

La estandarización de fichas técnicas en los subsistemas de cada Subred de Salud es fundamental porque:

1. Unifica criterios y procedimientos
    - Garantiza que todas las subredes utilicen el mismo formato, variables e indicadores, evitando duplicidad, vacíos o diferencias en la forma de reportar la información.
    - Facilita la comparabilidad entre subsistemas (epidemiología, laboratorio, salud ambiental, gestión zonal, etc.).
2. Asegura calidad y confiabilidad de los datos
    - Mejora la oportunidad, completitud y consistencia de la información que se reporta al nivel distrital y nacional.
    - Reduce errores de interpretación y garantiza que cada dato recolectado tenga el mismo significado en todo el sistema.
3. Fortalece la toma de decisiones en salud pública
    - Permite contar con información homogénea que sirve para el análisis, planeación y priorización de intervenciones en salud.
    - Favorece la evaluación de resultados y el seguimiento a metas establecidas en vigilancia y control.
4. Optimiza recursos y procesos
    - Disminuye tiempos en la recolección, procesamiento y consolidación de datos.
    - Facilita la interoperabilidad entre sistemas de información de las subredes.
5. Cumple con la normatividad y lineamientos nacionales
    - Responde a los protocolos definidos por el Instituto Nacional de Salud (INS) y las secretarías de salud.
    - Asegura la articulación del nivel local con el distrital y nacional dentro del SIVIGILA.

La estandarización de las fichas técnicas por subsistema en cada subred es clave para garantizar uniformidad, calidad y comparabilidad de la información, lo que fortalece la vigilancia en salud pública y asegura que las decisiones se basen en evidencia confiable, optimizando recursos y respondiendo de manera más eficaz a las necesidades del territorio.

Los ingenieros de sistemas lideres de cada subred iniciar con la estandarización de los formatos utilizados en cada uno de los proceso, por lo cual se generan cronogramas y responsables de cada una de los desarrollos de las fichas, es importante aclarar que la implementación de cada formato será acompañado por los lideres de los diferentes subsistemas de información distritales.

Detalle de la actividad	Periodicidad	Perfiles del talento humano	Soportes o medios de verificación
Cronograma de estandarización de formatos distritales y por subred.	Se realizar en el mes de: Octubre de 2025	Título Profesional en Ingeniera de Sistemas	Acta de actividades y cronograma de desarrollo, esta actividad también deberá tener reuniones mensuales evaluando, dificultades, inquietudes presentadas, capacitaciones si se requieren.
	Mensual		Reunión de seguimiento
Apoyo Técnicos a procesos de depuración o automatización de procesos, en la gestión de la calidad de la información, mediante solicitud escrita por parte de los subsistemas del área de vigilancia en salud pública, los cuales enviara mediante correo electrónico la solicitud de apoyo, especificando, el tipo de apoyo, los insumos requeridos para el apoyo, y en reunión se definirán los tiempos y entregas.	*Mensual según requerimientos*		*Según cronograma establecido en la reunión de apoyo se entregaran los soportes mensuales, si no se realiza solicitud de apoyo se deberá enviar un correo electrónico al líder informando que para el mes no se solicitó soporte técnicos, con copia a la coordinación de la subres*

4.7.3. Asistencia técnica remota

La asistencia técnica remota consiste en una intervención técnica a distancia sobre un computador. El único requisito es que este computador pueda conectarse a Internet. El técnico realiza la reparación o configuración desde la subred, tomando el control total del ordenador del cliente. La seguridad y privacidad están garantizadas por las características del soporte técnico y la metodología utilizada.

Los beneficios que ofrece el soporte remoto son muchas; entre ellas podemos destacar las siguientes:

Soporte Remoto

1. Velocidad: La dinámica actual; exige respuestas veloces a cualquier posible situación anormal que pueda surgir. Es aquí donde reside una de las ventajas indiscutibles del soporte remoto; pues permite a la subred contactar al servicio de asistencia de forma rápida para solicitar soluciones inmediatas. En un gran número de casos, el funcionamiento correcto y completo de una aplicación puede restablecerse rápidamente mediante la adición de un parche, de una actualización, o con un cambio de configuración (por ejemplo, Sivigila). Estos ajustes pueden ser aplicados de forma rápida por un técnico; a través del soporte remoto. De esta manera, los usuarios minimizan los tiempos de inactividad; al reducir el tiempo de respuesta que podría necesitar la llegada del soporte in situ.

2. Disponibilidad: El soporte remoto permite que las subredes tengan acceso a una asistencia rápida; desde cualquier punto geográfico donde exista una conexión a internet. Así, las UPGD o UI pueden sentir la confianza de contar con un servicio capaz de responder de forma eficiente; incluso en contexto donde las características de la organización exigen la movilidad constante de usuarios y equipos.

3. Rentabilidad: Usualmente la presencia física de un técnico implica cargos extra relacionados con los gastos de transporte. Estos cargos; pueden elevar de forma considerable. En la asistencia remota, por el contrario, la inversión del cliente cubre exclusivamente el servicio del acceso a internet el cual es cubierto por la organización.

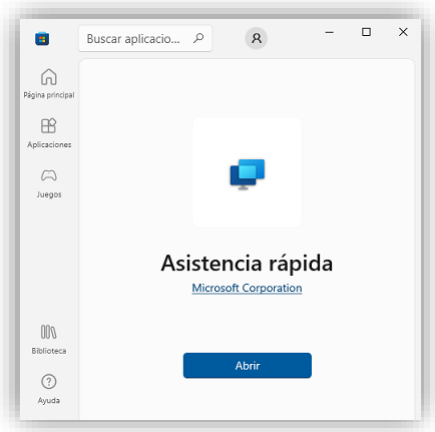
4. Eficiencia: A través de este servicio se pueden resolver un 90% de incidencias de TI. En el caso del desempeño de soluciones de software; hay proveedores que han logrado una mayor efectividad al responder de forma eficiente ante al menos un 99% de las solicitudes de sus clientes. Esto resulta de gran utilidad para cualquier organización pues lleva al mínimo la necesidad de solicitar la presencia física de un técnico.

5. Intercambio de aprendizaje: El soporte remoto implica una interacción en tiempo real. Lo que quiere decir que a medida que el técnico hace ajustes en un sistema; el cliente puede ver todo lo que sucede desde su pantalla. Esto da la oportunidad a los usuarios en las UPGD y UI de aprender cómo resolver por sí mismos; situaciones relacionadas con el desempeño de sus aplicaciones. Lo que representa la garantía de un servicio de valor; pues disminuye la necesidad de la organización de solicitar constantemente el servicio de soporte.

6. Mayor satisfacción: Al obtener resoluciones más rápidas, precisas y eficientes, los usuarios en las UPGD y UI pueden alcanzar una mayor satisfacción y confianza en las herramientas que utilizan en su entorno. De esta manera se optimizan los flujos de trabajo y se garantizan mejores resultados.

Se requiere el uso de herramientas de acceso remoto de alta calidad y de comunicación encriptada; que asegure la protección de la información sensible de la organización y que la gran mayoría de UPGD y UI puedan acceder sin incurrir en costos.

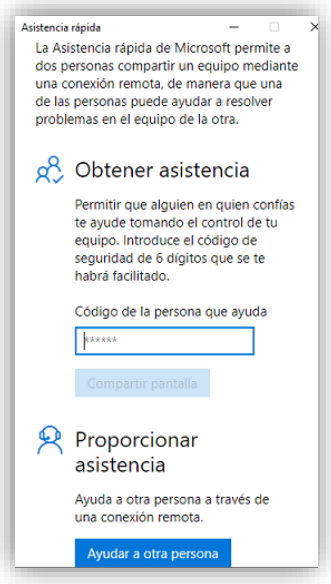
Por lo cual se propone el uso de “Asistencia Rápida” o” Quick Assist” de Microsoft, esta herramienta disponible para Windows 10 licenciado o superior, está disponible de forma libre en Microsoft Store.



Descripción

Con la aplicación Asistencia rápida, puedes recibir o proporcionar asistencia al equipo a través de una conexión remota. Se puede usar para conectarse de forma remota a un dispositivo y, a continuación, ver su pantalla, realizar anotaciones o tomar el control total. Además, los usuarios pueden solucionar problemas, diagnosticar problemas graves y proporcionar instrucciones a los usuarios directamente en sus dispositivos. Recuerda compartir la Asistencia rápida solo con personas de confianza, ya que pueden acceder a tu PC.

El soporte se conecta a un servicio en la nube de Microsoft iniciando Quick Assist e iniciando sesión con una cuenta de Microsoft (se admiten cuentas de MSA y AAD); Quick Assist mantendrá una conexión con el servicio en la nube de Microsoft y el soporte recibirá un código de conexión, el usuario que necesita asistencia también inicia la Asistencia rápida y conecta la misma sesión especificando el código de conexión. De esta forma, ambos clientes pueden usar conexiones salientes al servicio en la nube de Microsoft y el servicio en la nube actúa como un intermediario entre ambos clientes. Esto permite una conectividad flexible a clientes remotos donde sea que estén.



La implementación de esta solución deberá ser realizada con el apoyo del área de tecnología de la información y comunicaciones (TIC) de cada subred.

Los ingenieros responsables de la gestión de la información del área de vigilancia en salud pública de cada subred, realizaran la labor de empalme entre el área TIC y solo para los técnicos del área de salud pública que realicen asistencias técnicas de mantenimiento y apoyo a las UPGD y UI, es importante contar con las actas de las reunión con TIC, y definir con los lideres que técnicos requieren de esta solución de accesos virtual. La reunión con TIC se realizará en el mes de septiembre y dependiendo de la respuesta de ellos se realizar la implementación a los técnicos.

Si el área de TIC de cada subred no puede garantizar el uso del aplicativo “Asistencia Rápida”, y su adecuado funcionamiento, deberá generar estrategias de soporte virtual, como AnyDesk o TeamViewer o cualquier aplicativo que permita el cumplimiento del soporte rápido y con calidad y que permita grabará la asistencia, para fines de auditoría; los acuerdos deberán quedara en acta firmada y enviada a la secretaria como gestión de la información.

Entrega de Productos Mensuales

Los productos serán enviados al correo rdrodriguez@saludcapital.gov.co y cargado al OneDrive en la carpeta dispuesta para la subred

- \OneDrive - Saludcapital\- CONVENIO_GSP_20250901_20270630\Gestion de la Informacion Subred\1_Subred_Norte

- \OneDrive - Saludcapital\- CONVENIO_GSP_20250901_20270630\Gestion de la Informacion Subred\2_Subred_Centro Oriente
- \OneDrive - Saludcapital\- CONVENIO_GSP_20250901_20270630\Gestion de la Informacion Subred\3_Subred_Sur_Occidente
- \OneDrive - Saludcapital\- CONVENIO_GSP_20250901_20270630\Gestion de la Informacion Subred\4_Subred_Sur

La disponibilidad de los accesos se realizará a los correos oficiales de la subred para la gestión de la información

5. Indicadores

Monitoreo y seguimiento

N°.	Nombre del indicador	Frecuencia de medición	Fórmula	Fuente	Responsable del cálculo
1	Porcentaje de Cumplimiento en el plan de acción de la Vigilancia en Salud pública	Mensual	Total de Actividades administrativas y técnicas de la VSP realizadas / Total de Actividades administrativas y técnicas de la VSP programadas	Plan de acción de la VSP	**Profesional especializado 2 (Referentes gestión).** Profesional Universitario 1
2	Relación de computadores disponibles por talento humano en salud pública	Mensual	Numero de computadores disponibles para VSP / Numero de profesionales asignados a la gestión de al información	Plan de acción de la VSP	**Profesional especializado 2 (Referentes gestión de la información).** Profesional Universitario 2

Referencias Bibliográficas

- Ministerio de Salud. Decreto 780 del 06 de mayo de 2016, por medio del cual se expide el Decreto Único Reglamentario del Sector Salud y Protección Social. https://www.minsalud.gov.co/Normatividad_Nuevo/Decreto%200780%20de%202016.pdf
- Política de seguridad de la información de la Secretaria Distrital de Salud. http://sdsisolucion/IsolucionCalidad/Administracion/frmFrameSet.aspx?Ruta=Li4vRnJhbWVTZXRBcnRpY3Vsby5hc3A/UGFnaW5hPUJhbmNvQ29ub2NpbWllbnRvNFNEUy9mL2ZjZTM2Yzg4M2ZjNjRmNDdiNmFmZDk1MTBlYWQ4NGE3L2ZjZTM2Yzg4M2ZjNjRmNDdiNmFmZDk1MTBlYWQ4NGE3LmFzcCZJREFSVElDVUxPPTQzMjI1
- Plan de acción de la Secretaria Distrital de Salud de Bogotá D.C.
- Plan de Desarrollo “Un nuevo contrato social y ambiental para la Bogotá del siglo XXI”, 2020-2024.
- Instituto Nacional de Salud. Lineamientos Nacionales. Vigilancia y control en Salud Pública. Dirección de Vigilancia y Análisis del riesgo en Salud Pública. Bogotá, 2025
- Ministerio de Salud y Protección Social. Ley estatutaria 1581 de 2012 y los decretos que la reglamentan, por la cual se dictan disposiciones generales para la protección de datos personales. Decreto 235 de 2010, por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
- Secretaria Distrital de Salud, Documento Operativo Vigilancia en Salud Pública, Componente Análisis y realimentación desde la vigilancia en Salud Pública 2025.
- Davis,G. y Olsón., (1985) Management Information Systems: Conceptual foundations, Structure and Development. 2a ed.Nueva York: McGrawhill, Citado en Moreiro, G. (1998) Introducción al estudio de la información y la documentación. Medellín: Editorial Universidad de Antioquia.
- Barroso, J.,(2009) Propuesta de pautas para el diseño de un Sistema de Gestión de Información en la empresa ECIMETAL. Tesis de Licenciatura. Cuba, Departamento de Bibliotecología y Ciencia de la Información, Universidad de La Habana.
- Moreiro,G., (1998) Introducción al estudio de la información y la documentación. Medellín: Editorial de Antioquía.
- Ponjuán, G., (1998) Gestión de la información en las organizaciones: principios, conceptos y aplicaciones. Santiago de Chile.
- Ponjuán,G., (2000). Aplicaciones de Gestión de información en las organizaciones. El profesional de la información y su dominio de las técnicas y herramientas de la Gestión. Tesis de Doctorado. Cuba, Departamento de Bibliotecología y Ciencia de la Información, Universidad de La Habana.
- Ponjuán,G., (2004a) Gestión de la Información: dimensiones e implementación para el éxito organizacional. Rosario, Ediciones Nuevo Paradigma.
- Paez, U., (1990) ¿Qué es la gestión de Información?. INFOLAC. Citado en Prendes, L., (2005). La Gestión de Información. Estudio del tema en los Congresos INFO. Tesis de Licenciatura. Cuba, Departamento de Bibliotecología y Ciencia de la Información, Universidad de La Habana.
- White.,(1985) Intelligence management en: Cronin,B. Information management: from strategies to action. London.
- Woodman L. (1985) Information management in large organizations. En: Information management from strategies to action. London: ASLIB.
- Asistencia Remota - INFORMATICA 7
- Servicio de análisis y depuración de contenidos de la base de datos
- Introducción a la Calidad de Datos: Definición, Control y Beneficios
- Política de seguridad de la información de la Secretaría Distrital de Salud. http://sdsisolucion/IsolucionCalidad/Administracion/frmFrameSet.aspx?Ruta=Li4vRnJhbWVTZXRBcnRpY3Vsby5hc3A/UGFnaW5hPUJhbmNvQ29ub2NpbWllbnRvNFNEUy9mL2

ZjZTM2Yzg4M2ZjNjRmNDdiNmFmZDk1MTBlYWQ4NGE3L2ZjZTM2Yzg4M2ZjNjRmNDdiNmFmZDk1MTBlYWQ4NGE3LmFzcCZJREFSVElDVUxPPTQzMjI1

Control de cambios

VERSIÓN	FECHA DE APROBACIÓN	RAZÓN DE CREACIÓN O ACTUALIZACIÓN
1	25/09/2025	Inicio convenios interadministrativos GSP-PSPIC octubre 2025
2	11/12/2025	Revisión y ajuste de ficha técnica convenio GSP-PSPIC

	ELABORÓ	REVISÓ	APROBÓ
Nombre (s)	Jennifer Carolina García Sarmiento Ruben Dario Rodriguez Camargo	Diana Marcela Walteros Acero Marcela Martínez Contreras Claudia Milena Cuellar Diana Sofia Ríos	María Belén Jaimes Sanabria Patricia Eugenia Molano Builes
Firma (s)			
Cargo	Profesionales especializados	Subdirectora de Vigilancia en Salud Pública Subdirectora de Acciones Colectivas Subdirectora de Gestión y Evaluación de Políticas Subdirectora de Determinantes en Salud	Directora de epidemiologia, análisis y gestión de políticas en Salud Colectiva Directora de Salud Colectiva
Fecha	Diciembre de 2025	Diciembre de 2025	Diciembre de 2025