Superservicios Superintendencia de Servicios Públicos Domiciliarios	**INFORME DE AUDITORÍA A LOS SISTEMAS DE GESTIÓN**	SIGME

FECHA: 03/11/2021				**INFORME No.1**			
SISTEMA DE GESTIÓN							
CALIDAD	x	**SG-SST**	x	**SIGESPI**	x	**AMBIENTAL**	x

PROCESO (S) AUDITADO (S): GESTION DE LA INFORMACION Y EL CONOCIMIENTO

AUDITOR LIDER: William Javier Barrera Tamayo

AUDITORE(S) ACOMPANANTE(S): María Alejandra Gaviria Valbuena

OBJETIVO DE LA AUDITORIA:
Verificar el cumplimiento de los requisitos establecidos y aplicables de las normas NTC ISO 9001:2015 (Calidad), NTC ISO 14001:2015 (Ambiental), NTC ISO 27001:2013(Seguridad y Privacidad de la Información) y NTC ISO 45001:2018 y los requisitos legales y reglamentarios aplicables al proceso en la Superintendencia de Servicios Públicos Domiciliarios" En la Superintendencia de Servicios Públicos Domiciliarios.

ALCANCE DE LA AUDITORIA:
Aplica para los servicios de vigilancia, inspección y control de la prestación de los servicios públicos domiciliarios, atendiendo los requisitos de sus partes interesadas en Bogotá D.C. (Sede Principal)

PERSONAL ENTREVISTADO:

Jair Ramírez	Contratista
John Rafael Redondo Campos	Contratista
Johanna Milena González Aguilar	Prof. Especializado
Cindy Rocío López Villanueva	Profesional Especializado
Daniel Meza	Contratista
Gabriel Camilo Pérez Castañeda	Jefe Oficina
María Ercilia Castañeda E	Profesional Especializado
Nelson Nieto Hurtado	Profesional Especializado

DOCUMENTOS ANALIZADOS (CRITERIOS)

GIC-P-001	PROCEDIMIENTO GESTION DE DATOS ABIERTOS
GIC-P-002	PROCEDIMIENTO PRODUCCIÓN DE ESTADISTICAS OFICIALES
GIC-P-003	PROCEDIMIENTO ANONIMIZACIÓN DE BASES DE DATOS
GIC-M-001	MANUAL DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES
GIC-M-002	POLÍTICA GESTIÓN DE DATOS E INFORMACIÓN
GIC-I-001	INSTRUCTIVO IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
GIC-I-002	INSTRUCTIVO PARA LA PROTECCIÓN DE LA INFORMACIÓN EN LA SUPERINTENDENCIA DE SERVICIOS PÚBLICOS DOMICILIARIOS
GIC-I-003	INSTRUCTIVO DESAROLLO DE LA GESTIÓN DE CONOCIMIENTO
GIC-I-004	INSTRUCTIVO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
GIC-I-005	INSTRUCTIVO PROCESO SIG DISPOSICIÓN FINAL
GIC-I-006	INSTRUCTIVO PRONÓSTICO DE SERIES TEMPORALES
GIC-I-007	INSTRUCTIVO DETECCIÓN DE DATOS ATÍPICOS
GIC-I-008	INSTRUCTIVO BASE DE DATOS DISPOSICIÓN FINAL

ASPECTOS RELEVANTES

4.1 Se identifican los lineamientos inherentes al proceso del el análisis del contexto interno y externo y se identifican las partes interesadas y sus requisitos pertinentes, que impactan el cumplimiento de los propósitos misionales, los resultados previstos en el SIGME y la capacidad institucional.
Se tienen en cuenta los lineamientos de seguridad de la información en el análisis del contexto.
Se establece en el documento DE-F-003 Contexto estratégico institucional, en el cual se identifican los factores y se clasifican de acuerdo al sistema de gestión.
4.2 Se identifican las partes interesadas desde el documento "DF-002 Identificación de partes interesadas" en donde se evidencian como partes directamente relacionadas al proceso como Certificación de operaciones estadísticas, DANE, DNP, Ministerios de vivienda ciudad y territorio, Entidades Territoriales.
4.3 Se ubica el alcance del sistema alineado con el proceso de Gestion de la información y el conocimiento con respecto a los requisitos de las normas NTC ISO 14001:2015, NTC ISO 45001:2018, NTC ISO/IEC 27001:2013 y NTC ISO 9001:2015.
4.4 Se tienen establecida la descripción del proceso desde el aplicativo SIGME.
Se describe el proceso desde el documento GIC-PR-001 Proceso Gestión de Información y el Conocimiento.
5/ 5.1 (9001), A.8.1 (ISO 27001) Se establecen las responsabilidades y autoridades desde la "Matriz de Roles, Responsabilidades y autoridades" en el documento "DE-R-004" desde los sistemas de gestión de calidad, ambiental, seguridad de la información y SST; y seguridad de la información en responsabilidad de los activos. Se verifica para los cargos de Oficial de Seguridad de la Información, Oficial de Protección de Datos, Interlocutor SEN y Líderes de procesos para la Gestión de Información y el Conocimiento.
5.2 A8 (ISO 27001) Se establecen las políticas complementarias, Política del SIGME, Política De Seguridad Física y del Entorno, Política de gestión de activos, Política Sobre el Uso de Controles y Llaves Criptográficas, Política De Escritorio Limpio Y Pantalla Limpia, Política De Responsabilidades Frente A La Seguridad De La Información, Política De Uso De La Infraestructura Tecnológica, Política De Uso De Internet, Política Para El Teletrabajo Y El Acceso Remoto, Política Para La Realización De Trabajo Remoto, Política De Control De Acceso Y Uso De Contraseñas, Política De Administración Del

Inventario De La Infraestructura Tecnológica entre otras.
Se puede ingresar desde la página o desde el aplicativo SIGME a través del documento código de buen gobierno o Manual de sistema integrado de gestión punto 5.6.
5.3 Se establecen los roles y responsabilidades y autoridades para las normas NTC ISO 9001:2015 NTC ISO 27001:2013 (Seguridad y Privacidad de la Información)
Se establecen las responsabilidades y autoridades del personal desde la “Matriz de Roles, Responsabilidades y autoridades” DE-R-004
Se verifica para los cargos de Oficial de Seguridad de la Información, Oficial de Protección de Datos, Interlocutor SEN y Líderes de procesos para la Gestión de Información y el Conocimiento.
Se dan a conocer a través de sensibilizaciones, se evidencia la última realizada en la fecha 13/09/2021 y Taller el 16/10/2021.
5.4 (ISO 45001) Se conoce de la existencia de los comités de Copasst y convivencia, se les comunica a través de correo electrónico y se participa por parte de los funcionarios de la elección de los mismos.
6. Se planifica el sistema de gestión de calidad, ambiental, SST y de seguridad de la información, considerando las cuestiones internas y externas revisadas en el contexto de la entidad a partir de allí se desarrolla una metodología de identificación de riesgos.
6.1/6.1.1 Se desarrolla la metodología de identificación de riesgos teniendo en cuenta:
● Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública V4 de octubre de 2018 y la NTC-ISO-IEC 27005:2009 Tecnología de la información técnica de seguridad gestión del riesgo en la seguridad de la información.
Calidad:
1. Anonimizarían de los datos: (DANE) Tratamiento con capacitación. 24/05/2021. Se evalúa la eficacia con el resultado del indicador actualmente en 0 (cumple).
2. Inadecuada gestión del conocimiento: Tratamiento con Mesas de trabajo y control de gestión del conocimiento. Acta 15/04/2021
3. Inadecuada aplicación de los procesos de calidad en el proceso estadístico: Tratamiento con identificación de las necesidades de información, verificación de las fases del diseño
Se tienen los siguientes tratamientos para los riesgos:
1. Anonimizarían de los datos: (DANE) Tratamiento con capacitación. 24/05/2021. Se evalúa la eficacia con el resultado del indicador actualmente en 0 (cumple).
2. Inadecuada gestión del conocimiento: Tratamiento con Mesas de trabajo y control de gestión del conocimiento. Acta 15/04/2021
3. Inadecuada aplicación de los procesos de calidad en el proceso estadístico: Tratamiento con identificación de las necesidades de información, verificación de las fases del diseño.
Ambiental: Riesgo residuos, energía, agua.
SST: Si bien se tiene correo de divulgación del plan de emergencias el 8 de octubre de 2021.
8.2 (ISO 27001) Valoración de riesgos de la seguridad de la información:
Gestion de cativos
Accesos físicos
Permisos:
Correos:
Acuerdos de confidencialidad
Back up
Aplicaciones tecnologías
6.1.2 (ISO 27001) La entidad define y aplica un proceso de valoración de riesgos de la seguridad de la información e incluye riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información.
6.2 Se tienen 14 objetivos estratégicos y 12 del SIGME. Todos con sus planteamientos de control y cumpliendo a la fecha para los sistemas de calidad, ambiental, SST y seguridad de la información.
6.3 Se verifica la identificación de las necesidades de cambios para el Sistema de Integrado de Gestión y Mejora considerando su propósito, consecuencias potenciales, integridad del sistema, disponibilidad de recursos y asignación o reasignación de responsabilidades y autoridades mediante metodologías que determinan dos rutas como la Catarsis: con aplicación de pasos definidos: empatía, definición, ideación e Innovación Cerrada: identificación de reto, crear equipos, reconocimientos
7 y 7.1 A.8.1.1 (ISO 27001) Se determinan los recursos necesarios para la implementación del SG y se presenta resolución SSPD20211000000045 de 4 de enero de 2021de Aceptación de presupuesto 2021, en donde se incluyen los recursos destinados al establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de calidad, ambiental, SST y de seguridad informática.
Se cuenta con inventario de activos de la información, Se registran, valoran y califican los activos de información de la entidad de acuerdo con lo establecido en el documento GIC-I-001 Instructivo identificación y clasificación de activos de información
A.8.1.2 Se administran los activos y se hacen efectivos las restricciones de acuerdo con la clasificación definida por el responsable de la producción de la información.
7.3 Se realiza la toma de conciencia en temas como la política SIGME, objetivos, aporte a los sistemas de gestión ambiental, SST, seguridad de la información y calidad a través de Intranet, correo de comunicación interna, boletín virtual infórmate, carteleras digitales, pagina Web, redes sociales
7.5/ 7.5.1/ 7.5.2/7.5.3 Se ha creado, establecido, actualizado y controlado la información documentada requerida por la norma y necesaria para la implementación y funcionamiento eficaces del SG en el aplicativo SIGME para las normas NTC ISO 9001:2015 (Calidad), NTC ISO 14001:2015 (Ambiental), NTC ISO 27001:2013 (Seguridad y Privacidad de la Información) y NTC ISO 45001:2018.
8/ 8.1 Se planifica, implementa y controlan las actividades del proceso de Información y conocimiento.
Se cuenta con las Políticas de tratamiento de datos personales:
a) Se verifica la información al Titular de forma explícita y previa, se verifica cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento, así como obtener su consentimiento expreso.
b) Se verifica la información al Titular que, por tratarse de datos personales sensibles, no está obligado a autorizar su

tratamiento.
c) Se verifica el suministro de los datos personales de los niños, niñas y adolescentes por parte de autorización de los padres de familia o representantes legales del menor.
Se toma como evidencia contrato 088 de 2021 con cláusulas 9 y 10 de manejo de datos.
Se verifica quienes se les permitir el acceso a la información.
Datos abiertos:
*Se verifica la Identificación de datos a través del instructivo GIC-I-001 Instructivo identificación y clasificación de activos de información, es decir, aquellos que se encuentran en el Registro de Activos de Información, el cual debe ser publicado en la página web de la entidad y en el portal de datos www.datos.gov.co o el que haga sus veces.
* Se verifica el proceso de anonimizarían de los datos o conjuntos de datos.
* Se verifica la radicación de una solicitud (Aranda) a la Mesa de servicios de TI, solicitando la publicación de la información en el portal www.datos.gov.co.
* Se verifica la promoción del uso de datos abiertos
* Se verifica la satisfacción del uso de datos abiertos
A.8.2 Identificación y clasificación de activos:
Se verifica el Índice de información clasificada y reservada GIC-F-002 y la clasificación de activos y el Formato Inventario y Clasificación de Activos de Información GIC-F-003
* La identificación se realiza segun las Tablas de Retención Documental (TRD) a nivel de Serie y
Subserie.
Producción de estadísticas oficiales:
*Se verifica la identificar las necesidades de información de estadística y los usuarios de esta.
*Se verifica el o GIC-F 008 Plan general de la operación estadística.
* Se revisa que se actualiza el documento metodológico en el formato GIC-F-009 Documento metodológico de la operación estadística y la ficha metodológica de la operación estadística en el formato GIC-F-010 Ficha metodológica
* A.8.3/ A.8.3.1 Se verifica el aseguramiento de la disponibilidad de los registros administrativos en el Sistema Único de Información de Servicios Públicos Domiciliarios – SUI la herramienta de inteligencia de negocios y las demás aplicaciones necesarias para el acopio, procesamiento, análisis o difusión de información estadística.
* Se verifica que la evaluación cumpla con lo especificado en el diseño de la operación estadística mediante Lista de chequeo para el proceso estadístico GIC-F-011
Gestión Del Conocimiento
Se tiene como finalidad mantener una memoria de conocimiento dentro de la entidad y transferir el conocimiento entre las personas, generando una experticia específica en campos de acción únicos que tienen las dependencias y, facilitando la toma de decisiones.
Se verifican las rutas de Conocimiento Crítico Viable (CCV), Conocimiento participativo, Buenas prácticas y Lecciones aprendidas.
Se puede verificar que existe una clasificación del conocimiento:
Se mantiene el conocimiento y se da una ubicación y acceso a documentación crítica y se garantiza la transmisión.
Incidentes:
Planificación:
Se verifica reporte: Se procede de acuerdo con el Manual de servicios tecnológicos – TI-M-002 y se verifica incidente del 17/06/2021 por fallo de aplicación de Tesorería.
Contención: Evitar propagación. Se verifican las pruebas con usuarios, se confirma acción de acceso, se validan logs de información y se revisa código fuente se provoca versión diferente.
A.8.2.2 Erradicación y recuperación: Se verifica la recuperación del Back up.
A.8.2.3 Dicha información se encuentra etiquetada y salvaguardada en las aplicaciones y en medios externos.
Lección aprendida: Se verifica que funciono bien y que deberían realizarse.
*Se tiene clasificación de incidentes de Seguridad de la Información: Tabla 8
* Se tiene clasificación de criticidad de los incidentes. Tabla 9.
*Se tienen las instrucciones para el reporte de incidentes de dato personal ante la SIC Anexo 3.
Se verifica estadística de incidentes de seguridad de la información.
A.8.1.3 Se establecen, se documentan e implementar las reglas para la seguridad de los activos y la información y se han dado a conocer a través de coreos electrónicos.
A.8.1.4 Existe un control de inventarios de la entidad para el control del manejo y devolución de activos.
Se verifica el conocimiento de los programas de:
Ambiental: programas de consumo
Salud y seguridad en el trabajo: programas de prevención
Seguridad de la información: Aplicación de seguridad a través de Anexos de ISO 27001.
8.2 (ISO 14001 y ISO45001) Se conoce superficialmente el plan de emergencias de la entidad.
NOTA:
Este tema se revisara con el proceso de Talento Humano para verificar su evidencia.
8.4.1 El proceso se asegura la conformidad de los procesos, productos y servicios suministrados externamente a través de su participación en el establecimiento de los requisitos de los mismos.
8.4.2 Se participa en el establecimiento de los controles el cual es ejecutado por el proceso de adquisición de bienes y servicios
8.4.3 Se provee la información a través de los TDR, contratos, cartas de inicio como también con los diferentes comunicados de seguimiento o terminación de servicios.
8.5 Se tienen los controles bajo condiciones controladas:
Políticas de tratamiento de datos personales:
Se realiza la verificación de actualización de la información reportada por la Supe servicios, dentro de los cinco (5) días hábiles contados a partir de su recibo.
Protección de la Información en la Superintendencia de Servicios:
Se verifican los controles de Data así:
A6.2.2 (Teletrabajo)
Se verifica que el equipo en donde se realiza el teletrabajo se encuentra conectado a través de los canales seguros dispuestos por la entidad.

Se cuenta con las BPN y solicitudes a través del aplicativo (ARANDA)
A7.2.2 (Capacitación)
Se verifica el plan de capacitación en seguridad y privacidad de la información
Se ejecuta el programa de cultura en seguridad y privacidad de la información.
A8.1.2 (Propietario Activos de Información) A8.2.1 (Clasificación Información) A8.2.2 (Etiquetado Información) Se verifica el etiquetado de los documentos físicos y digitales del Proceso/Dependencia/Grupo
A9.2 (Registro y cancelación del registro de
usuarios) Se verifican los derechos de acceso del personal a los sistemas de información de la
Súper servicios y también cancelación.
A11.1.3 (Seguridad de oficinas, recintos e instalaciones.) Se verifican las condiciones de seguridad física y ambiental en las oficinas de la Supe servicios.
Se cerífica la protección del área de ingreso y acceso con biometría en la entrada acceso al centro de cómputo.
A12.3.1 (Respaldo de la información) Se verifica el respaldo de la información relevante para el Proceso/ A13.2.3 (Mensajería Electrónica) Se verifica el correo electrónico con implementación de mecanismos para la protección adecuada de la información.
Se cuenta con Herramientas de Fortnite y política de uso de correos electrónico institucional.
Se verifica la aplicación y conocimiento de los programas de:
Ambiental: GA-PG-001 Programa Manejo de Residuos Sólidos, GA-PG-002 Programa Gestión Eficiente de La Energía, GA-PG-003 Programa Uso Eficiente del Agua y GA-PG-004 Programa Buenas Prácticas Sostenibles, en donde se tienen las evidencias de la participación de comunicaciones y ejecuciones de aplicabilidad de las mismas.
Salud y seguridad en el trabajo: GH-PG-002 Programa Entorno Laboral Saludable y GH-PG-005 Programa Prevención Desordenes Musculo Esquelético en donde se evidencias las pausas activas y sensibilizaciones en temas de ergonomía, en noviembre de 2020, 27 de octubre de 2021.
Seguridad de la información: Se evidencia la protección de la información en correos electrónicos, accesos, manejo de SIGME, solicitud de acceso y retiros de SIGME.
9/ 9.1 Se tiene indicadores de cumplimiento a gestión de calidad, ambiental, SST y seguridad de la información con estadística como cumplimiento de las operaciones estadísticas al 100% semestral.
Para gestión del conocimiento se tiene 1. La evaluación de la satisfacción de clientes de los espacios formales para compartir el conocimiento y de las herramientas de uso y apropiación del conocimiento de la entidad con resultado de 4 (cumple), con frecuencia semestral.
2. Evaluación del cliente de la gestión del conocimiento resultado de 4 (cumple). Con frecuencia semestral.
3. Porcentaje de variables sin anonimizar cumple con el 0% semestral.
9.2 No se han desarrollado auditorías al proceso año 2020 pues el proceso es nuevo para auditorias.
9.3 La frecuencia de realización dela Revisión por la Dirección es anual con corte 01 de junio.
Se incluyen las entradas de las normas NTC ISO 9001:2015 (Calidad), NTC ISO 14001:2015 (Ambiental), NTC ISO 27001:2013 (Seguridad y Privacidad de la Información) y NTC ISO 45001:2018 junto con el Decreto 1072 del 2015 y la Resolución 0312 del 2019 (Seguridad y Salud en el Trabajo)
Actualmente se encuentra en revisión.
10/ 10.1 La entidad ha determinado y seleccionado las oportunidades de mejora e implementado las acciones necesarias para cumplir con los requisitos del cliente y mejorar su satisfacción.
10.2 Se tiene 5 acciones correctivas
Se verifica acción correctiva AC-GIC-002 del 21/07/2021, AC-GIC-004 del 19/07/2021. Y se encuentra cerradas a la fecha.
10.3 Actualmente se tienen 3 acciones de mejora se verifica la acción AC-GIC-001 y se encuentra cerrada.

RIESGOS DEL PROCESO (bajo criterio de los auditores, el grado de riesgo que puede tener un proceso frente al cumplimiento total o parcial de los requisitos auditados):

Fallas en los servicios de energía, servicios de conexión, falta de disponibilidad de la información, demoras o fallas en el funcionamiento en las herramientas de consulta de la entidad.

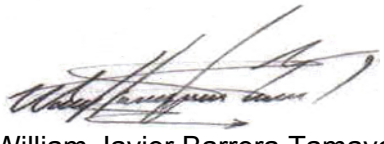
OPORTUNIDADES DE MEJORA	REQUISITO NORMA
No hay oportunidades de mejora	No Aplica

No.	NO CONFORMIDAD	REQUISITO NORMA	PROCESO
	No hay no conformidades	No aplica	No aplica

CONCLUSIONES DE AUDITORÍA

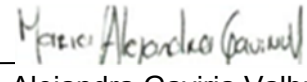
El equipo auditor llega a la conclusión de que el proceso ha establecido, mantenido y mejorado su sistema de gestión integral de acuerdo a los requisitos de la(s) norma(s), NTC ISO 9001:2015 (Calidad), NTC ISO 14001:2015 (Ambiental), NTC ISO 27001:2013(Seguridad y Privacidad de la Información) y NTC ISO 45001:2018 de igual manera el proceso ha demostrado la capacidad del sistema para lograr que se cumplan los requisitos para los servicios incluidos en el alcance, así como las políticas y los objetivos de la Organización desde la Gestion de la información y el conocimiento.

No. DE NO CONFORMIDADES HALLADAS	**0**
No. DE NO CONFORMIDADES CERRADAS DURANTE LA AUDITORIA	**0**
No. DE NO CONFORMIDADES PENDIENTES	**0**
No. DE CONFORMIDADES	**0**



William Javier Barrera Tamayo
AUDITOR LÍDER

Lida Cubillos Hernández
AUDITADO



María Alejandra Gaviria Valbuena
AUDITOR

Gabriel Camilo Pérez Castañeda
AUDITADO