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

FECHA: 26-07-2022				**INFORME No. 01**			
SISTEMA DE GESTIÓN							
CALIDAD		**SG-SST**	x	**SIGESPI**	x	**AMBIENTAL**	x

PROCESO (S) AUDITADO (S)
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

AUDITOR LÍDER:; PAOLA ANDREA ANGEL, MAURICIO GONZÁLEZ

AUDITORE(S) ACOMPAÑANTE(S): WILLIAM CALLEJAS BASTO; CARLOS ROSAS ACEVEDO

OBJETIVO DE LA AUDITORÍA: Verificar el cumplimiento de los requisitos establecidos y aplicables de la norma NTC ISO 14001:2015, 45001:2018 y la 27001:2013, para el Sistema de gestión ambiental, Seguridad y salud en el trabajo y seguridad y privacidad de la información y los requisitos legales y reglamentarios aplicables en la Superintendencia de Servicios Públicos Domiciliarios

ALCANCE DE LA AUDITORÍA: Aplica para los servicios de vigilancia, inspección y control de la prestación de servicios públicos domiciliarios, para la atención de los requisitos de sus partes interesadas

PERSONAL ENTREVISTADO: John Rafael Redondo Campos, Daniel Fernando Sanmiguel Cespedes, Claudia Paola Andrade Murillo, Jazmin Argenis Flechaz Muñoz, Lenni Durbay Muñoz Jiménez, Daniel Joaquin Rodríguez Morales, David Mauricio Rodríguez Escobar, Mauricio Mancera Marin

DOCUMENTOS ANALIZADOS (CRITERIOS): NTC ISO 14001:2015, NTC ISO 27001:2013, NTC ISO 45001:2018, Decreto 1072 de 2015, Resolución 0312 de 2019 y documentos propios de la organización enmarcados en sus Sistema Integrado de gestión, como lo son:

- Contexto estratégico institucional
- Identificación partes interesadas y sus requisitos pertinentes
- Manual del Sistema Integrado de Gestión y Mejora Versión
- Resolución 20201000050165 del 11-11-2020
- Resolución No. 20211000153595 del 13-05-2021
- Resolución No. SSPD 20211000391444 DEL 11-08-2021
- Matriz de roles, responsabilidades y autoridades
- Manual de políticas complementarias del SIGESPI.
- Gestión de Activos de Información
- Responsabilidades de los usuarios
- Controles contra códigos maliciosos
- Acuerdos de confidencialidad o de no divulgación
- Identificación de la legislación
- aplicable y de los requisitos contractuales
- Matriz de comunicaciones del sistema integrado de gestión y mejora
- Código de buen gobierno
- Instructivo para la administración de riesgos
- Identificación de peligros, evaluación valoración de riesgos y determinación de controles
- Instructivo para la administración de riesgo
- Declaración de aplicabilidad SIGESPI NORMA NTC ISO/IEC 27001:2013
- Plan de trabajo
- Resolución 20211000886495 del 30-12-2021.
- Manual de funciones
- Plan institucional de capacitaciones
- Diagnóstico de necesidades de aprendizaje individual
- Programa de Toma de Conciencia y Formación para los Sistemas de Gestión que Integren SIGME y el Sistema de Control Interno
- Procedimiento gestión de cambios
- Plan de Prevención, Preparación y Respuesta ante Emergencias
- Instructivo para el seguimiento, medición, análisis y evaluación en el SIGME.
- Inspección áreas de trabajo
- Inspección y control de botiquines y elementos de primeros auxilios
- Hoja de vida e inspección del extintor
- Inspección de seguridad puesto de trabajo del teletrabajador
- Inspección al uso y estado de los elementos de protección personal
- Inspección a puesto con video terminales
- Inspección orden y aseo
- Inspección de gabinetes contra incendios
- Inspección de transporte vertical
- Procedimiento auditorías internas de gestión e informes de ley
- Procedimiento de acciones correctivas, preventivas, de mejora y correcciones
- Control de acceso
- Áreas seguras
- Seguridad de las comunicaciones

- Gestión de incidentes de Seguridad de la información

ASPECTOS RELEVANTES

- El proceso demuestra entendimiento y buen manejo del sistema integrado de gestión y mejora SIGME
- Se observa conocimiento, entendimiento y adecuada gestión de Riesgos de Seguridad.
- Se observa un proceso maduro en la segregación de funciones en donde el oficial de seguridad hace parte de los procedimientos con la revisión y verificación de solicitudes de vpn, gestión de incidentes, adquisiciones entre otras.
- Se cuenta con un proceso de gestión de conocimiento por medio de pares en donde cada colaborador comparte el conocimiento crítico.

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, falta de disponibilidad de la información, demoras o fallas en el funcionamiento en las herramientas de consulta de la entidad, ausencia de los auditados o ausencia del equipo auditor por calamidades

OPORTUNIDADES DE MEJORA	REQUISITO NORMA
• Fortalecer trazabilidad entrega RAEES por parte del proceso Gestión de la Tecnologías de la Información a la Dirección Administrativa	NTC ISO 14001:2015 8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL
• Fortalecer la segregación de residuos en los puntos ecológicos de incidencia al proceso de Gestión de la Tecnologías de la Información	NTC ISO 14001:2015 8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL
• Es importante que se realice la socialización del DE-M-004 Manual de políticas complementarias del SIGESPI teniendo en cuenta su reciente actualización.	NTC-ISO-IEC 27001 A.5.1.1 Políticas para la seguridad de la información
• Se recomienda tomar los cursos relacionados con seguridad de la información que ofrecen los diferentes proveedores, esto con el fin de mantener actualizados a los funcionarios.	NTC-ISO-IEC 27001 A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
• Se recomienda involucrar formalmente al oficial de Seguridad de la Información en el comité de Gestión de Cambios para que pueda participar en temas críticos relacionados con confidencialidad Integridad y disponibilidad de la Información.	NTC-ISO-IEC 27001 12.1.2 Gestión del cambio
• Implementar mecanismos que permitan controlar el uso de medios removibles y busquen mitigar la fuga de información	NTC-ISO-IEC 27001 A.8.3.1 Gestión de medios removibles
• Se recomienda la habilitación de la política que obligue o solicite el cambio de contraseña o implementar controles al respecto	NTC-ISO-IEC 27001 9.4.3 Sistema de gestión de contraseñas
• Se recomienda complementar y actualizar la política de bloqueo de sesión conforme a lo configurado en la política de directorio activo.	NTC-ISO-IEC 27001 11.2.8 Equipos de usuario desatendidos
• Se recomienda buscar alternativas diferentes frente a la salida de este, por cuanto depende únicamente de la huella biométrica y en casos de emergencia pueden existir escenarios de riesgo que no permitan la adecuada evacuación del centro de datos.	NTC-ISO-IEC 27001 9.1.1 Política de control de acceso

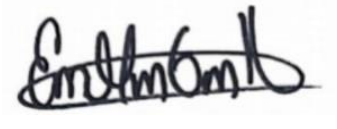
No.	NO CONFORMIDAD	REQUISITO NORMA	PROCESO
1	No se cuenta con matriz de inventario de activos actualizada y falta establecer la valoración de activos, y propietarios de los activos	NTC-ISO-IEC 27001 A.8 GESTIÓN DE ACTIVOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

CONCLUSIONES DE AUDITORÍA:

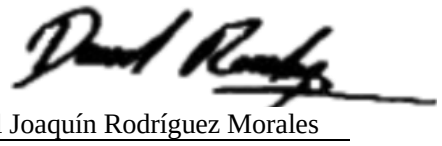
El equipo auditor concluye que el proceso se ha establecido mantenido y mejorado de manera integral conforme con los requisitos de las normas;ISO 14001:2015,ISO 45001:2018, Decreto 1072 de 2015, Resolución 0312 de 2019 e ISO 27001:2013

No. DE NO CONFORMIDADES HALLADAS	**1**
No. DE NO CONFORMIDADES CERRADAS DURANTE LA AUDITORIA	**0**
No. DE NO CONFORMIDADES PENDIENTES	**1**
No. DE CONFORMIDADES	**1**

Paola Andrea Ángel
AUDITOR LÍDER



Mauricio González
AUDITOR LÍDER



Daniel Joaquín Rodríguez Morales
AUDITADO