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

FECHA: 11 / Noviembre de 2020				**INFORME Nº 01-2020**			
SISTEMA DE GESTIÓN							
CALIDAD	**x**	**SG-SST**	**x**	**SIGESPI**	**x**	**AMBIENTAL**	**x**

PROCESO (S) AUDITADO (S)
Gestion de Tecnologias de la Información

AUDITOR LÍDER:
Mario Fernando Brand

AUDITORE(S) ACOMPAÑANTE(S):
Cristel Xiomara Gómez Pinzón

OBJETIVO DE LA AUDITORIA:
Verificar la implementación y eficacia del SIGME y su conformidad con:
• Los requisitos establecidos por la Entidad .
• Los requisitos establecidos por las normas ISO 9001:2015 (9K), ISO 14001:2015 (14K), , ISO 45001:2018 (45K), ESTÁNDARES MÍNIMOS RES 0312 2019 // DUR 1072:2015 (D1072) e ISO 27001:2013 (27K)
• Los requisitos legales y reglamentarios aplicables al proceso

ALCANCE DE LA AUDITORIA:
Inicia desde la programación de la auditoria hasta el seguimiento de la ejecución y verificación de las actividades del proceso de Gestion de Tecnologias de la Información -Daniel Joaquin Rodríguez

PERSONAL ENTREVISTADO:
Carlos Prada , Jazmín Flechaz Muñoz, Elizabeth Sanabria, David Rodriguez,José Córdoba Nieto,Daniel Joaquín Rodríguez Morales, Alexis Montoya Tellez,Andrés Felipe Rincón Valencia,Yeison David Niño,Oscar Puentes,Paola Rincon,Carlos Ubaque,Diana Toro,Jeisson Gutierrez, Edwin Cortes

ISO 14001:2015-ISO 45001:2018
numerales 5.1.,5.2,5.3,6.2,6.1.2,8.1,8.2 - Decreto 1072 del 2015
articulos 2.2.4.6.8 y 2.2.4.6.11 y 2.2.4.6.14 Resolución 0312 del 2019
numeral 2.1.1, 2.8.1,3.1.9,3.2.1,4.2.2 y 5.1.1
9001
5.2 Política;
6.1 Planificación- Acciones para abordar riesgos y oportunidades,
6.2 Objetivos de calidad y planificación,
7.1. 1. Recursos,
7.5 Información documentada,
8.1 Planificación y control operacional,
8.7 Control de las Salidas No Conformes,
9 Evaluación de Desempeño,
10. Mejora Continua

ISO 27001

A.5POLÍTICAS DE SEGURIDAD
A.6ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION
A.7SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
A.8GESTIÓN DE ACTIVOS.
A.9CONTROL DE ACCESOS
A10CIFRADO.
A11SEGURIDAD FÍSICA Y AMBIENTAL.
A12SEGURIDAD EN LA OPERATIVA
A13SEGURIDAD EN LAS TELECOMUNICACIONES
A14ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
A15RELACIONES CON SUMINISTRADORES.
A16GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
A17ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
A18CUMPLIMIENTO.

ASPECTOS RELEVANTES: **Compromiso por parte del personal** **Conocimiento frente al SIGME**
RIESGOS DEL PROCESO **Fallas en los servicios de energía, servicios de conexión , plataforma Google Meets, falta de disponibilidad de la información, demoras o fallas en el funcionamiento en las herramientas de consulta de la entidad, ausencia de los auditados, ausencia de los auditores por calamidades**

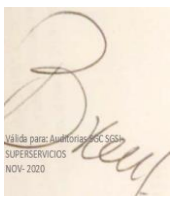
OPORTUNIDADES DE MEJORA	REQUISITO NORMA
Fortalecimiento de las políticas de TI- en el cubrimiento y la transferencia de la información (Ejem. Dispositivos móviles, Riesgos, Ciberseguridad, Manejo de medios)	**27001: A.5.1- A.5.2**
Se debe fortalecer la administración del riesgo informático a todos los niveles del proceso. fortaleciendo. el contexto, identificación del riesgo, Estimación del riesgo,, evaluación del riesgo,,Tratamiento del riesgo,aceptación del riesgo.En lo posible manejar lo como un área independiente al area de TI	**9001-5.1.1, 6.1, 9.1.327001-27005 Gestión del riesgo de la seguridad de la información**
La alta dirección de la empresa debe apoyar activamente la seguridad al interior de ella, mediante un compromiso demostrado definiendo roles y responsabilidades posteriormente implementar un plan de trabajo detallando actividades fechas, responsables, alcance, objetivos, etc.Todo esto alineado a las necesidades de la organización	**27001 numeral:17**
Para generar un plan de recuperación del negocio optimo se debe alinear y madurar el plan de recuperación de desastres al plan de continuidad del negocio. fortalecimiento la identificación de amenazas, identificación de riesgos, tratamiento de los mismos, manejo de crisis, comunicación de crisis, análisis de impacto del negocio . etc	**27001 A:17**
Evaluar la independencia del proceso de seguridad de la información de la dirección de sistemas ya que: **1. Facilidad de alineación con la estrategia de la organización.** **2. Independencia, imparcialidad y objetividad** **3. El apoyo de gerencia suele ser mayor y por ende la cultura es más fácil de fomentar, los presupuestos relativamente más amplios y el provecho para la empresa puede ser mayor** **4. Control a nivel corporativo de la seguridad de la información: lo cual significa que los directivos de la compañía hacen parte del modelo de seguridad de la información y están comprometidos con el mismo** **5. Creación de un comité de seguridad de la información: involucramiento de áreas funcionales y técnicas (TI) para aportar al beneficio de la seguridad de la información.** **6. Participación del área de auditoría: mayor compenetración de esta área en el tema de seguridad de la información, con aportes valiosos al respecto de acuerdo a sus metodologías de auditoría** **7.Puede interactuar con otras áreas de la organización (seguridad física, Riesgos operativos, Auditoría/contraloría/Control interno).**	**ISO 27001 Numeral 4,**
La información en las empresas, constituyen los activos más valiosos intrínsecamente, las organizaciones deben desarrollar estrategias que permitan, certificar la disponibilidad, integridad, confidencialidad y auditabilidad , siendo solventado con el uso de buenas prácticas que se adapte a la realidad organización y al software que en esta se desarrolla. por ese motivo se recomienda Alinear los procesos de desarrollo de software a buenas prácticas internacional. Como por ejemplo ISO 33000, CMMI, Código Seguro ETC. con el objetivo de mitigar los posibles riesgos y maximizar las oportunidades del los procesos de la SUPERSERVICIOS.	**27001 A 12.2- A12.5 A 12.6**

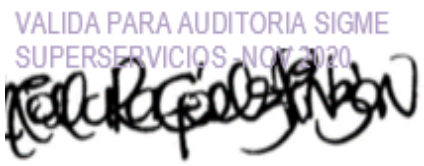
Nº	NO CONFORMIDAD	REQUISITO NORMA	PROCESO
1	**No se evidencia actualizada la matriz de roles y responsabilidades de los funcionarios que hacen parte del área de sistemas, la cual fue presentada por líder del proceso (Gestión Tecnologías de la Información). Generado un incumplimiento a la norma ISO 27001 y 9001. Para dejar evidencia basta con definir el organigrama y la matriz RACI donde se describa todos los perfiles y obligaciones de acuerdo a su puesto de trabajo.**	**9001—5.3 27001–A.6.1.1-A 6.1.2 A 7.2.2**	**Gestion de Tecnologias de la Información**
2	**No se evidencia el informe de la visita al lugar donde se custodian las copias de respaldo, generando incumplimiento a la norma ISO 27001, y a las políticas de respaldo de la información.Para dejar evidencia basta realizar una visita al lugar donde se custodian las copias de respaldo dejando constancia documentada de los posibles riesgos y proponer controles si se requiere todo alineado a las buenas prácticas de protección de la información**	**9001- 7.5 27001- A.12.3**	**Gestion de Tecnologias de la Información**

CONCLUSIONES DE AUDITORÍA

Se evidencia conocimiento por parte de los integrantes del proceso en las actividades propias del mismo

Nº DE NO CONFORMIDADES HALLADAS	**2**
Nº DE NO CONFORMIDADES CERRADAS DURANTE LA AUDITORIA	**0**
Nº DE NO CONFORMIDADES PENDIENTES	**0**
Nº DE CONFORMIDADES	**0**





MARIO BRAND	**CRISTEL XIOMARA GOMEZ**	**Daniel Joaquin Rodríguez**
AUDITOR SGC-SIGESPI	**AUDITOR SGA-SG SST**	**AUDITADO**