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

FECHA: 30/11/2018				INFORME Nº 1			
SISTEMA DE GESTIÓN							
CALIDAD		SG-SST		SIGESPI	X	AMBIENTAL	

PROCESO (S) AUDITADO (S): SIGESPI

AUDITOR LÍDER: Luis Ernesto Vargas Ayala

AUDITORE(S) ACOMPAÑANTE(S): Luis Ernesto Vargas Ayala

OBJETIVO DE LA AUDITORIA: Verifcar la conformidad del Sistema de Gestión de Seguridad de la Información, con los requisitos establecidos en ISO 27001:2013; considerando la capacidad del sistema de gestión para determinar que la entidad cumple con los requisitos de la norma.

ALCANCE DE LA AUDITORIA: Comprenderá el sistema de gestion de seguridad de la información en las instalaciones de Superservicios Carrera 18 No 84-35 y Calle 19 sede Uconal, tomando como muestra de la aplicación de controles de seguridad de la información en los procesos de Talento Humano, Adquisición de Bienes-Contratación y Dirección Técnica de Energía, Grupo coordinacion SUI; datacenter y sitio alterno de contingencia.

PERSONAL ENTREVISTADO: Procesos de: Gestion de Tecnologica de la Información - Seguridad de la Informacion, Direccion Estratégica, Gestión del Talento Humano, Direccion Técnica de Energia, Adquisición de Bienes y Servicios. Se encuentran en las actas de entrevistas y reuniones realizadas.

DOCUMENTOS ANALIZADOS (CRITERIOS)
SO 27001:2013
Requisitos Normativos
Ley 1581 de 2012; Proteccion de datos personales.
Ley 1008 de 2018 - Gobierno Digital.
Resolución 20115000009075 SSPD políticas de seguridad de la información, complementada con el subproceso Sistema de Gestión en Seguridad de la Informaciónn SGSI-SP-001.
Ley 1712 de 2014 - Ley de transparencia y del derecho de acceso a la información pública
Decreto 415 de 2016 - Fortalecimiento de institucional en materia de Tecnologías de la Información
Gobierno Digital

ASPECTOS RELEVANTES:
- Se destaca avance en la implementacion del SGSI con respecto a la visita anterior.

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):
- Incumplimiento en la entrega oportuna del informe de auditoría que afecte el plan anual 2018

OPORTUNIDADES DE MEJORA	REQUISITO NORMA
Revisar el contexto en el marco de Gobierno digital y de Riesgos. Además, definir la prioridad para asignar valoración. Relacionar las estrategias con los objetivos del sistema y periodo de revisión.	4.1
Establecer la parte interesada "cliente externo" (prestadores de servicios objeto de supervisión, vigilancia, control, reguladores CRAG y CREG).	4.2
Definir en el contexto de la organización, partes interesadas diferente a prestadores de servicios. Incluir la interrelación de seguridad de información con las partes interesadas y otras organizaciones.	4.3
Determinar en el objetivo estratégico "facilitar a los usuarios el acceso de la información segura".	5.1
Integrar en la política del sistema integrado de gestión, política de alto nivel.	5.2
Realizar planificación articulada, con el fin de determinar las acciones para tratar riesgos y oportunidades y objetivos de seguridad.	6.1.1
Actualizar valoración de riesgos, de acuerdo con la guía para la administración del riesgo y el diseño de controles en entidades públicas v4 de Octubre de 2018; en concordancia con el artículo 2.2.21.5.5 del decreto compilatorio 1083 de 2015.	6.1.2
Detallar la planificación del tratamiento de los riesgos.	6.1.3
Revisar el tratamiento de datos personal MC-F-024 v1 13/12/2017, en expedientes de funcionarios anteriores a la expedición del formato.	7.2
Incluir capacitación en seguridad de información, sensibilización de SGSI, según programa de cultura MC-PG-005 v2 25/06/2018. Incluir toma de conciencia de "no conformidades".	7.3
Se tiene propuesta de actualización pendiente de aprobación por el archivo general de la nación.	7.5.3

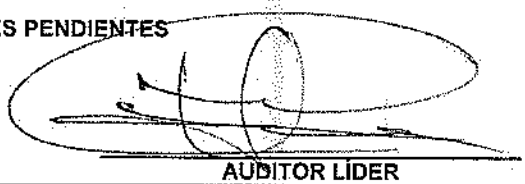
Revisar y publicar en Sigme el mapa de riesgos de proceso de gestión de tecnologías de la información de los procesos: vigilancia, inspeccion (control), participación y servicios al ciudadano, seguimiento a la gestion institucional, gestion financiera.	8.2
Implementar la primera valoracion de riesgos de seguridad de la información de los procesos. Incluir la información que se transfiere y las condiciones de Seguridad de la Informacion en la entrega, para el proceso Direccion Tecnica de Energia.	8.3
Establecer en el alcance lo que se determina necesario seguir y medir. Revisar el indicador ("Sensibilizacion en temas de seguridad y privacidad de la Información") junto con lo establecido en la hoja de vida del indicador.	9.1
Incluir en la revision por la direccion, el detalle del estado de las Acpms del SGSI.	9.3
Establecer en el proceso de seguimiento de la gestion institucional, el alcance de los criterios o categorias de las observaciones y/o oportunidadades de mejora y las acciones necesarias implementar	10.1
Definir la codificación, elaboracion, revisiòn y aprobación en el formato del documento política complementaria.	A.5.1.1
Complementar la lista de activos de tipo de software, hardware, redes, personas. Incluir el activo de software referente a SIGEP- Nómina proceso Gestión del Talento Humano	A.8.1.1 - A.8.2.1
Actualizar el procedimiento gestión de solicitudes de servicio GT-P-003 v3 18/12/2015	A.9.1.1
Revisar los accesos al sistema SIGME.	A.9.2.3
Formalizar procedimiento gestor de sincronizacion de contraseñas de las diferentes aplicaciones internas, en concordancia con la politica de control de contraseñas, en creacion y cambio.	A.9.2.4
Incluir en el manual de supervisión e interventoria, la revisión periódica de los derechos de los acceso.	A.9.2.5
Determinar en el manual de supervisión e interventoria la revisión para contratista que utilicen programas privilegiados	A.9.4.4
Definir procedimiento de criptografía con tokens en financiera y firmas digitales	A.10.1.2
Se encuentra en tratamiento mediante ACPM ACC-TI-006 separacion de ambientes.	A.12.1.4
Se tiene control de instalación de software mediante política Firewall y directorio activo. Revisar para software ejecutable liviano.	A.12.5.1
Se tiene politica de instalaciòn de software por parte del usuario en directorio activo y firewall. Revisar para software ejecutable liviano.	A.12.6.2
Determinar alta disponilidad y continuidad del servicio el firewall. En cumplimiento literal "d." política de uso de la infraestructura tecnológica.	A.13.1.1
Implementar conexiones cifradas.	A.13.1.2
Hacer extensivo los acuerdos de interoperabilidad, confidencialidad y no devulgacion.	A.13.2.4
Hacer explicito, en el contrato 597 "ADA SAS" de 2018, el "Alcance y derechos relativos al desarrollo del software y derechos de autor".	A.15.1.1
Definir en la supervisión de contratos de Personas Jurídicas el cumplimiento del sistema de gestión de seguridad de la información (compromiso de confidencialidad, compromiso de tratamiento de datos personales, derechos de autor, alcance y derechos relativos al desarrollo del software). Igualmente, en procesos que tengan subcontratación autorizada.	A.15.1.3
Determinar lineamientos de base de conocimiento institucional, fundamentado en el registro y tratamiento de incidentes de seguridad de la información y de la arquitectura de seguridad de tecnología.	A.16.1.1

Nº	NO CONFORMIDAD	REQUISITO NORMA	PROCESO
1	No se determinan los niveles de riesgo, que establecen los límites de las zonas.	6.1.2.d.3	N/A
2	No se cumple el literal "c." de la politica de dispositivos móviles en cuanto al cifrado, politicas complementarias anexo 1 del Manual del sistema integrado.	A.6.2.1	N/A
3	No se tiene implementado el etiquetado de los activos de informacion clasificada y reservada.	A.8.2.2	N/A
4	No se cancelan los derechos de acceso a la base de datos, en retiro del usuario.	A.9.2.6	N/A
5	No se cumple la politica sobre el uso de controles y llaves criptográficas, en cuanto criptografía de la informacion.	A.10.1.1	N/A
6	Se define los lineamientos de metodologia de desarrollo seguro con alcance para adquisicion de desarrollos externos. No se evidencia su aplicación en los desarrollos internos.	A.14.1.1	N/A

7	No está determinado la realización de pruebas funcionales cuando se cambia de plataforma, desde el estado inicial hasta el final de la implementación, de los controles de seguridad.	A.14.2.3	N/A
8	Se define los lineamientos de metodologia de desarrollo seguro con alcance para adquisicion de desarrollos externos. No se evidencia su aplicacion en los desarrollos internos.	A.14.2.5	N/A
9	Se define los lineamientos de metodologia de desarrollo seguro con alcance para adquisicion de desarrollos externos. No se evidencia su aplicación en los desarrollos internos.	A.14.2.8	N/A
10	No se tiene plan de continuidad del negocio y de la seguridad de la informacion.	A.17.1.1	N/A
11	No se tiene plan de continuidad del negocio y de la seguridad de la informacion.	A.17.1.2	N/A
12	No se tiene plan de continuidad del negocio y de la seguridad de la informacion.	A.17.1.3	N/A
13	No se tiene plan de continuidad del negocio y de la seguridad de la informacion.	A.17.2.1	N/A

CONCLUSIONES DE AUDITORÍA

N° DE NO CONFORMIDADES HALLADAS	13
N° DE NO CONFORMIDADES CERRADAS DURANTE LA AUDITORIA	0
N° DE NO CONFORMIDADES PENDIENTES	13
N° DE CONFORMIDADES	



AUDITOR LIDER

11/12/18