El futuro es de todos — APC Colombia Agencia Presidencial de Cooperación Internacional	**INFORME DE AUDITORÍA** Código: C-FO-017 - Versión: 01 - Fecha: Octubre 7 de 2021

I. AUDITORIA SISTEMAS DE GESTIÓN			
Sistema de Gestión de Seguridad de la Información	X	Sistema de Gestión de Seguridad y Salud en el Trabajo	

II. INFORMACIÓN GENERAL DE LA AUDITORÍA

Objetivo:	Verificar el cumplimiento de los requisitos de la norma: NTC-ISO/IEC 27001:2013		
Alcance:	1. Direccionamiento Estratégico y Planeación 2. Gestión de Comunicaciones. 3. Identificación y Priorización de Cooperación Internacional 4. Preparación y Formulación de Cooperación Internacional 5. Implementación y Seguimiento de Cooperación Internacional 6. Gestión de Talento Humano 7. Gestión Contractual 8. Gestión Jurídica 9. Gestión de Tecnologías de la Información 10. Gestión Financiera 11. Gestión de Servicio al Ciudadano 12. Gestión de administración de Recursos y donaciones en especie 13. Gestión Administrativa 14. Evaluación, Control y Mejoramiento		
Criterios:	☐ NTC-ISO/IEC 27001: 2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. ☐ Políticas, procedimientos, instructivos y demás documentos aplicables a la seguridad de la información. ☐ Legislación definida en la especificación del proceso y otros documentos normativos aplicables a seguridad de la información.		
Proceso/ Dependencia o Dirección/ Proyecto/ Servicio auditado:	TODOS LOS PROCESOS, OBJETO DEL ALCANCE DEL SGSI.	Fecha de apertura: 01/10/2021	Fecha de cierre: 04/10/2021
Auditados:	Asesor con funciones de Coordinador del Grupo de Planeación, Directora General, Profesional Especializado con funciones de Coordinador del Grupo de Talento Humano, Profesional Especializado con funciones de Coordinación del Grupo de Tecnologías de la Información, Profesional Especializado con funciones de Coordinación del Grupo Financiera y Servicios Administrativos / Profesional Especializado con funciones de Coordinación del Grupo de Tecnologías de la Información, Profesional Especializado con funciones de Coordinación del Grupo de Tecnologías de la Información, Profesional Especializado con funciones de Coordinación del Grupo de Gestión Contractual, Gestión Jurídica, Asesor con funciones de Control Interno.		
Equipo auditor:	Auditor líder:	ALEX ALBERTO RODRÍGUEZ CUBIDES	
	Auditor:	MARÍA DEL PILAR DUARTE FONTECHA	
	Auditor:	OSCAR IVAN ORTIZ BOHORQUEZ	
	Auditor:	DIANA ALEXANDRA BRICEÑO SIERRA	
	Auditor:	MARIA VICTORIA LOSADA TRUJILLO	
	Auditor:	JULIO IGNACIO GUTIERREZ VARGAS	

III. DESARROLLO DE LA AUDITORÍA

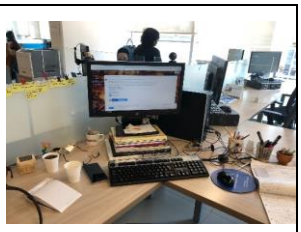
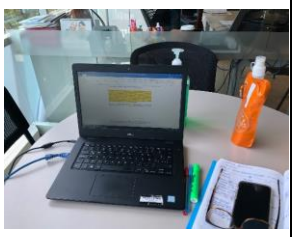
La auditoría interna al sistema de gestión de seguridad de la información, se realizó de acuerdo al plan de auditoría. Algunas entrevistas duraron más de lo previsto, pero todos los requisitos de la norma, fueron verificados. No obstante la contingencia COVID-19, la auditoría interna se desarrolló en las instalaciones de la entidad, en forma presencial.

IV. FORTALEZAS Y DEBILIDADES IDENTIFICADAS

Como fortaleza se destaca: Compromiso y competencia de los funcionarios que lideran el sistema de gestión de seguridad de la información, en la entidad.

V. HALLAZGOS DE LA AUDITORÍA

No conformidad u observación	Numeral - literal de la norma o requisito incumplido	Descripción del hallazgo u observación (¿Qué, Cómo, Cuándo, Dónde se incumplió?)	¿Es un hallazgo u observación reincidente de auditorías anteriores? Si-No	Documento o registro de evidencia del hallazgo u observación
1	6.1	En entrevista con el proceso de planeación y en la revisión documental, se evidencia que no se han identificado las oportunidades que es necesario tratar.	No	Entrevista con el funcionario del proceso responsable.
2	A.7.2.2	No se evidencia un programa de capacitación para la toma de conciencia en temas de seguridad de la información.	No	Plan de inducción, sin temas de seguridad de la información.
3	A.8.1.4	No se evidencia un procedimiento para devolución de activos.	No	Revisión documental.
4	A.5.1.1	No fue evaluada la eficacia de la comunicación de la Política de Seguridad de la Información.	No	Entrevista con los líderes del sistema de gestión de seguridad de la información.
5	A.6.1.1	No se evidenció la asignación formal de responsabilidades del SGSI.	No	Existe el Comité Institucional de Gestión y Desempeño. Resolución 507 del 5 de Diciembre de 2017, sin embargo no se evidencia la asignación de Responsable de la Seguridad de la Información al funcionario Angela Katherine Piñeros Forero – Cargo: Profesional Especializado Grado 20 con Funciones de Coordinación del Grupo de Tecnologías de Información.
6	A.11.1.4, A.11.2.1, A.11.2.3	En visita al data center de la entidad, se observaron los siguientes elementos y/o situaciones que generan riesgo para la seguridad de la información: - Material Inflamable (Escritorio / Techo Falso). - Seguridad de los equipos (Equipos sin anclaje al rack). - Cableado desorganizado. - Racks con llave expuesta.	No	

7	A.11.2.8	Durante el recorrido por las instalaciones de la Agencia, se observaron dos puestos de trabajo con sesiones de usuario abiertas desatendidas. Es decir, sin presencia del funcionario, propietario del usuario asignado.	No	 
8	A.10	La Agencia ha adquirido 18 certificados digitales a la entidad de certificación digital abierta - GSE, para sus funcionarios, quienes los utilizarán para firmar documentos en Orfeo, sin embargo, dichos certificados tienen un ciclo de vida y unas condiciones de uso, las cuales los funcionarios deben acatar y dar cumplimiento. Dichas condiciones se encuentran estipuladas en la Declaración de Prácticas de Certificación y en las Políticas de Certificación de GSE. Se evidencia que uno de los certificados entregados, está vigente y no ha sido solicitada su revocación, no obstante el dueño del mismo, ya no pertenece a la entidad.	No	Entrevista con el supervisor del contrato suscrito entre la Agencia y GSE.
9	A.18.1.1	No se ha identificado toda la legislación aplicable a la entidad. Ejemplo: Decreto 1377 de 2013.	No	Entrevista con funcionarios de los procesos: Gestión Jurídica y Tecnología de Información.
10	A.17.1	El procedimiento de contingencia de Tecnología de Información, se encuentra desactualizado. En adición en las pruebas no se incluye la participación de los usuarios finales.	No	Entrevista con funcionarios del proceso: Gestión de Tecnología de Información.

VI. CONCLUSIONES DE LA AUDITORÍA

La Agencia debe culminar su etapa de implementación del Sistema de Gestión de Seguridad de la Información, realizar mediciones a los indicadores planteados con una mayor frecuencia, determinar la causa raíz de las no conformidades detectadas y plantear los planes de acción para su cierre efectivo.

APROBADO POR:	
ELABORADO POR:	Alex Rodríguez