FECHA DEL INFORME:	30/09/2019	**PROCESO AUDITADO:**	Gestión Contractual
LIDER DEL PROCESO:	Coordinadora Grupo de Gestión Contractual	**AUDITADOS:**	Catalina Franco Gómez - Coordinadora Grupo de Contratos Juan Guillermo Muriel – Profesional Especializado Yennifer Quiceno – Técnico Administrativo Claudia Stella Cortés – Coordinadora de Riesgos No Financieros
AUDITOR LÍDER:	Adriana Aranguren	**EQUIPO AUDITOR:**	Adriana Aranguren
LUGAR Y FECHA DE REALIZACIÓN DE AUDITORÍA:	Sede Principal Oficina Grupo de Gestión Contractual Piso 8. 17/09/2019	**CRITERIOS DE AUDITORÍA:**	Norma Técnica ISO 27001:2013 Lineamientos de MinTIC del Modelo de Seguridad y Privacidad de la Información, Política de Gobierno Digital y Política de Seguridad Digital. Documentación del Sistema de Gestión de Seguridad de la Información. Planes de mejoramiento. Normatividad aplicable.

1. OBJETIVO

Evaluar el cumplimiento o la conformidad del Sistema de Gestión de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información, de acuerdo con los requisitos de las normas técnicas vigentes aplicables, normativos y de la Entidad; en el proceso de Gestión Contractual, identificando oportunidades de mejora.

2. ALCANCE

Se auditó la gestión general del proceso teniendo en cuenta las actividades realizadas del año 2018 hasta la fecha, con base en el ciclo PHVA y el cumplimiento de normas y lineamientos transversales del Sistema de Gestión de Seguridad de la Información, en lo aplicable al proceso.

3. FORTALEZAS

Se destaca la buena disposición para la atención de la auditoría por parte de los auditados y la disponibilidad de la información.

4. RESULTADOS

CRITERIO DE AUDITORIA	NO CONFORMIDAD	OPORTUNIDAD DE MEJORA
Norma ISO 27001:2013 Anexo A Dominio A.8 Gestión de activos A.8.1. Responsabilidad sobre los activos A.8.2. Clasificación de la información A.8.2.3 Manipulación de		Se debe revisar y ajustar el inventario de activos de información, dado que actualmente se considera que todos los activos del proceso contienen información pública. Sin embargo, es necesario revisar si los datos personales sensibles de los contratistas deberían considerarse información clasificada y anonimizarse para su publicación. En ese caso, el expediente

la información Modelo de Seguridad y Privacidad de la Información. Fase: Planificación Inventario de activos de Información. Ley 1712 de 2014 Decreto 103 de 2015 Decreto 1081 de 2015 Resolución 3564 de 2015		contractual tendría confidencialidad de información clasificada, de manera parcial. Igualmente, es necesario incluir las propuestas de los procesos de subasta como información clasificada, cuyo plazo de confidencialidad sería hasta el momento de la apertura de los sobres. Estos cambios deben reflejarse en el registro de activos de información y el índice de información clasificada.
Norma ISO 27001:2013 6.1.2. Apreciación de los riesgos de seguridad de información 6.1.3. Tratamiento de los riesgos de seguridad de información Anexo A A.15. Relación con proveedores Modelo de Seguridad y Privacidad de la Información. Fase: Planificación Identificación, valoración y tratamiento de riesgo Fase: Implementación Implementación del plan de tratamiento de riesgos		Se recomienda definir y documentar una minuta del contrato base o proforma, la cual incluya las cláusulas estándar definidas de seguridad, privacidad, derechos de autor y protección de datos personales. Así mismo, se deberían establecer unas obligaciones específicas de los proveedores, en su calidad de “Encargados del tratamiento de datos personales” y para los contratistas con roles críticos para la seguridad de la información, para los casos que aplique. Para los controles de la causa CSI30-Contratistas ejecutan acciones no autorizadas, del riesgo RSI4- Falla de confidencialidad por inadecuado manejo de proveedor en temas de seguridad digital; se debería incluir el seguimiento al cumplimiento de las cláusulas y obligaciones en materia de seguridad digital, por parte de los supervisores de contrato.
Norma ISO 27001:2013 Anexo A A.13.2. Intercambio de información A.15.1. Seguridad en la relación con proveedores		Se recomienda definir y exigir que se conforme un acuerdo de intercambio de información, como requisito para establecer relación contractual con terceros con los cuales se requiera intercambiar datos de manera continua, en especial cuando se puede tratar de información clasificada o reservada.

5. CONCLUSIONES

Se han logrado el objetivo y alcance de la auditoría y se puede concluir, con base en la muestra auditada, que el proceso evidencia cumplimiento respecto a los requisitos de la norma técnica ISO 27001:2013 y demás criterios aplicados. Sin embargo, se detectaron en la auditoría tres oportunidades de mejora, las cuales se recomienda analizar, con el fin de definir e implementar acciones que permitan evitar no conformidades en el futuro. El proceso no tenía planes de mejoramiento pendientes, por no conformidades de la anterior auditoría de seguridad de la información.

6. OBJECIONES DEL AUDITADO NO RESUELTAS

No aplica.