FECHA DEL INFORME:	30/09/2019	**PROCESO AUDITADO:**	Administración de la cartera
LIDER DEL PROCESO:	Coordinador Grupo de Administración de Cartera	**AUDITADOS:**	José Eduardo Parada - Coordinador Grupo de Administración de Cartera Ingrid Johana Ortiz – Profesional Universitario Grupo de Administración de Cartera
AUDITOR LÍDER:	Adriana Aranguren	**EQUIPO AUDITOR:**	Adriana Aranguren
LUGAR Y FECHA DE REALIZACIÓN DE AUDITORÍA:	Sede Principal Oficina Grupo de Administración de Cartera Piso 4. 13/09/2019	**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 Administración de la Cartera, 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 6.1. Acciones para tratar los riesgos y oportunidades Modelo de Seguridad y Privacidad de la Información. Fase: Planificación Identificación, valoración y tratamiento de riesgo		Se recomienda revisar la identificación de riesgos de seguridad digital del proceso, de manera que se incluya por ejemplo el riesgo de falla de disponibilidad de los recursos tecnológicos, cuyo impacto en caso de materializarse es considerable.

Norma ISO 27001:2013 Anexo A A.15 Relación con proveedores A.18.1. Cumplimiento de los requisitos legales y contractuales		Se recomienda incluir las responsabilidades específicas respecto a la Ley 1581 de 2012, en los contratos con terceros “encargados del tratamiento de datos personales” de los beneficiarios de la entidad, con el fin de distribuir la facturación física y electrónica, (ver Decreto 1377 de 2013, Capítulo V, artículo 25).

Norma ISO 27001:2013 Anexo A A.13.2.2. Acuerdos de intercambio de información	No se tiene establecido un acuerdo de intercambio de información con el proveedor de distribución de facturación física (UT Cadena). Esto incumple con el control A.13.2.2 Acuerdos de Intercambio de información, del Anexo A de la Norma ISO 27001:2013. Se debe revisar que el intercambio permanente de información se realice por un FTP seguro y que los entregables digitales de la ejecución del contrato que contengan información sensible se entreguen encriptados en el medio magnético utilizado o considerar una modificación en el mecanismo de intercambio.	

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 presenta una “no conformidad” con respecto a los requisitos de la norma técnica ISO 27001:2013 y demás criterios aplicados. Ésta debe ser corregida y analizada para definir e implementar acciones correctivas, de acuerdo con el procedimiento de la entidad. Así mismo, se detectaron en la auditoría dos 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.