FECHA DEL INFORME:	30/09/2019	**PROCESO AUDITADO:**	Gestión de Servicios Tecnológicos
LIDER DEL PROCESO:	Director de Tecnología	**AUDITADOS:**	Martha Robayo – Analista II- Dirección de Tecnología Mauricio Cajicá- Coordinador de Infraestructura de TI Claudia Cortés – Coordinadora de Riesgos no Financieros Angela Chaparro – Administrador Aranda. KGV Servicios Jimmy Edisson Díaz – Profesional Universitario I Mercy Macedo – Gestor de Servicios TI
AUDITOR LÍDER:	Adriana Aranguren	**EQUIPO AUDITOR:**	Adriana Aranguren
LUGAR Y FECHA DE REALIZACIÓN DE AUDITORÍA:	Sede Edificio Elemento Piso 15 6/09/2019 y 9/09/2019	**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 de Servicios Tecnológicos, 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 mejora de los controles de seguridad informática, que se implementarán a través de la contratación de un SOC; dentro del contrato interadministrativo de prestación de servicio derivado del convenio marco entre Icetex e Internexa.

4. RESULTADOS

CRITERIO DE AUDITORIA	NO CONFORMIDAD	OPORTUNIDAD DE MEJORA
Norma ISO 27001:2013 Anexo A		Para el activo identificado como “CUSTODIA DE CONTRASEÑAS DE

Dominio A.8 Gestión de activos A.8.2.3 Manipulación de la información Modelo de Seguridad y Privacidad de la Información. Fase: Planificación Inventario de activos de Información.		LOS SISTEMAS", documento físico con las contraseñas de administrador de sistemas sensibles, para uso en caso de contingencia; se recomienda incrementar las medidas de seguridad, guardando el sobre sellado en caja fuerte u/o implementando división de información en dos componentes, para que fuese necesaria la aprobación de dos perfiles privilegiados, con el fin de tener acceso a las claves
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 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		Para el activo denominado en el inventario "BASES DE DATOS DE SISTEMAS DE INFORMACIÓN" se recomienda detallarlo por cada una de las bases de los diferentes aplicativos y analizar si es necesario justificar con normatividad distinta, de acuerdo con la información que contiene cada una. Es importante porque del inventario se obtiene la información para el Índice de información clasificada y reservada, registro de activos y Registro Nacional de Bases de Datos.
Norma ISO 27001:2013 6.1.2. Apreciación de los riesgos de seguridad de información Modelo de Seguridad y Privacidad de la Información. Fase: Planificación Identificación, valoración y tratamiento de riesgo		Se observan los siguientes aspectos por mejorar en la gestión de los riesgos de seguridad de la información del proceso: • Para el Riesgo 4, causa 30-Contratistas ejecutan acciones no autorizadas, tanto la causa como el control son muy generales. Se deberían implementar y relacionar en el mapa de riesgos los controles específicos de verificación de cumplimiento a las obligaciones de seguridad de los proveedores de tecnología, dada la criticidad de los roles desempeñados. • Para la Causa 34 -Hw o Sw con vulnerabilidades de seguridad, desactualizado u obsoleto, del riesgo 7, de falta de disponibilidad por denegación; la causa está

		redactada como debilidad de un control. • El riesgo 10 - Falla de integridad por virus informático, debería replantearse como “falla de integridad por ataque cibernético” y la causa 16 redactarse en términos de vulnerabilidades de seguridad perimetral; debilidades o brechas de seguridad en el perímetro y punto final; el antimalware configurado, actualizado y con mantenimiento apropiado realmente es un control. • La Causa 45 del mismo riesgo: Desactualización de antimalware, realmente no es una causa, es una debilidad de control, que debe redefinirse.
Norma ISO 27001:2013 6.1.3. Tratamiento de los riesgos de seguridad de información		Se han detectado deficiencias en la aplicación de restricciones en la navegación de usuarios de las regionales (evidenciado en visitas de Atención al usuario de las sedes de Cúcuta e Ibagué). Se debe reforzar este control de seguridad lógica perimetral, presente en la matriz de riesgos, control 25 frente a la causa 45 del riesgo de: Falla de integridad por virus informático.
Norma ISO 27001:2013 Anexo A A.16. Gestión de Incidentes de Seguridad de la Información Modelo de Seguridad y Privacidad de la Información. Fase: Implementación Implementación del plan de tratamiento de riesgos		Se debería revisar la gestión de riesgos de seguridad digital, en coordinación con la gestión de riesgo operativo; dado que incidentes como los de la pérdida de integridad en la información de Signature (No.1924) y para Comité de Crédito, deberían también ser tratados con el procedimiento de incidentes de seguridad de la información y el cierre debería darse únicamente cuando se hayan implementado las acciones correctivas definitivas, que permitan evitar que se vuelva a presentar.
Norma ISO 27001:2013 Anexo A A.12.6.1.Gestión de las vulnerabilidades técnicas	Se presenta incumplimiento de los requisitos de la Norma ISO 27001:2013, Anexo A, Control A.12.6.1 Gestión de las vulnerabilidades técnicas; puesto que no se presenta un plan de remediación como respuesta al último análisis de vulnerabilidades, correspondiente al primer semestre de 2019;lo cual se refleja también en el incumplimiento del indicador “Gestión de	

	vulnerabilidades de la plataforma tecnológica" del proceso de Riesgo Operativo.	
Norma ISO 27001:2013 Anexo A A.12.6.2. Restricción en la instalación de software Procedimiento: A7-1-09 Inventario de software y hardware y control de software legal		Se deberían analizar las causas y tomar acciones correctivas para los casos en los cuales se detecta software no autorizado en los equipos de cómputo del ICETEX; como revisar si el usuario cuenta con usuario administrador de la máquina autorizado y si debe conservar dichos privilegios o si la Mesa de Servicios o la Dirección de Tecnología instala software o asigna permisos sin contar con la debida autorización, por ejemplo.
Norma ISO 27001:2013 Anexo A A.8.1.1. Inventario de activos A.8.1.2. Propiedad de los activos	Se presenta incumplimiento de los requisitos de la Norma ISO 27001:2013, Anexo A, A.8.1.1 Inventario de activos y A.8.1.2 Propiedad de los activos; puesto que se detectan inconsistencias en la información registrada en el inventario sobre la dependencia, serial y placas de los equipos de cómputo asignados a Rosa Maria González, Jefe (E) de Control Interno y el computador en uso por parte de Adriana Aranguren, que aún aparece a nombre del contratista Luis Francisco Santos, que no labora desde diciembre de 2018 con la entidad. Aunque se están haciendo actualizaciones del inventario, se recomienda tomar acciones correctivas para evitar que se vuelva a presentar, como la coordinación junto con los Grupos de Recursos Físicos, Talento Humano y Gestión contractual, de manera que las novedades de personal y contratos; así como la asignación o retiro de equipos de cómputo sean reportados a Tecnología y actualizados en el inventario de manera oportuna. El inventario de activos de hardware, software e infraestructura debe ser integrado en el inventario de activos del Sistema de Gestión de Seguridad de la Información.	
Norma ISO 27001:2013 Anexo A A.9. Control de acceso		Se recomienda evaluar la implementación de un formato o aceptación de responsabilidad específica para el otorgamiento de

A.9.3. Responsabilidades del usuario Procedimiento Asignación / Retiro de accesos a sistemas de información: A7-1-05 Gestión de accesos.		derechos de acceso privilegiados, para funcionarios y contratistas que por sus funciones o responsabilidades tengan este tipo de acceso.
Norma ISO 27001:2013 Anexo A A.9.2. Gestión de acceso de usuario	Se presenta incumplimiento de los requisitos de la Norma ISO 27001:2013, Anexo A, A.9.2. Gestión de acceso de usuario; puesto que se detectó en seguimiento al plan de mejoramiento de hallazgos de la revisoría fiscal que en los listados de usuarios de las bases de datos, sistema Core y Apoteosys se presentan usuarios genéricos, sin identificación de responsable, funcionarios que no tienen actualizada la dependencia a la cual pertenecen; entre otros.	
Ley 1712 de 2014 Decreto 1081 de 2015	Se presenta incumplimiento de los requisitos de la Ley 1712 de 2014, Artículo 11 y Decreto 1081 de 2015, Artículo 2.1.1.2.1.11. Publicación de Datos Abiertos; puesto que se evidencia que se tienen publicados un conjunto de datos abiertos básicos desactualizados en el portal DatosAbiertos.com.	
Norma ISO 27001: 2013 Anexo A A.14.2. Seguridad en el desarrollo y en los procesos de soporte A.17.2.1. Disponibilidad de los recursos de tratamiento de la información		Se requiere mejorar el soporte sistemas de información, dado que se presentaron fallas de disponibilidad en la funcionalidad del aplicativo “Cuenta de cobro a proveedores”, utilizado por el Grupo de Recursos Físicos para generar cuentas de cobro para tarjetas de proximidad perdidas, durante el mes de agosto de 2019.. A pesar de que se evidenció correo informando a TI, en la presente auditoría no se logró tener información respecto al soporte de dicho aplicativo. Se recomienda incluir y mantener actualizada dentro del inventario de activos la información de soporte y líder técnico de cada sistema de información, módulo o aplicativo.
Norma ISO 27001: 2013 Anexo A A.14.2.5. Principios de	Se mantiene la no conformidad: “No se evidencia control sobre todos los desarrollos realizados dentro de	

construcción de sistemas seguros	cada una de las áreas, incumpliendo de esta forma con lo establecido en la Norma ISO 27001:2013 en el Control A.14.2.5 Principios de construcción de los sistemas seguros".	

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 cuatro "no conformidades" con respecto a los requisitos de la norma técnica ISO 27001:2013 y demás criterios aplicados. Igualmente, se mantiene una no conformidad de la auditoría interna anterior del SGSI. Éstas deben ser corregidas y analizadas para definir e implementar acciones correctivas, de acuerdo con el procedimiento de la entidad. Así mismo, se detectaron en la auditoría ocho oportunidades de mejora, las cuales se recomienda analizar, con el fin de definir e implementar acciones que permitan evitar no conformidades en el futuro.

6. OBJECIONES DEL AUDITADO NO RESUELTAS

No aplica.