FECHA DEL INFORME:	30/08/2019	**PROCESO AUDITADO:**	Administración de activos fijos Servicios generales y apoyo logístico
LIDER DEL PROCESO:	Coordinador Grupo de Recursos Físicos	**AUDITADOS:**	Leonardo Roberto Pérez - Coordinador Grupo de Recursos Físicos Liz Andrea Choles – Técnico Administrativo y Líder MECI-Calidad Jorge Bonilla – Profesional I Giovanni Rivero – Contratista Ingeniero Civil
AUDITOR LÍDER:	Adriana Aranguren	**EQUIPO AUDITOR:**	Adriana Aranguren
LUGAR Y FECHA DE REALIZACIÓN DE AUDITORÍA:	Sede Principal Oficina Grupo de Recursos Físicos. Piso 8. 23/08/2019	**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 los procesos de Administración de activos fijos y Servicios generales y apoyo logístico, identificando oportunidades de mejora.

2. ALCANCE

Se auditó la gestión general de los procesos 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 todo el equipo de trabajo.

4. RESULTADOS

CRITERIO DE AUDITORIA	NO CONFORMIDAD	OPORTUNIDAD DE MEJORA
Norma ISO 27001:2013 7.5. Información documentada		Se deberían incluir las actividades relacionadas con la gestión de la seguridad física del Icetex en el proceso a cargo, aún cuando se realicen a través de un contrato con proveedor externo. Pueden incluirse solamente en la caracterización o generar otros documentos controlados, de acuerdo con lo

		definido dentro del sistema de gestión.
Norma ISO 27001:2013 Anexo A A.8 Gestión de 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 Resolución 3564 de 2015		Se debe revisar y ajustar el inventario de activos de información, dado que el activo “Registro de activos bienes muebles e inmuebles y activos dados de baja” corresponde al sistema de información Apoteosys (el inventario debería referirse a la base de datos del aplicativo y no al software) y aparece categorizado como “información clasificada” por Ley 1581 de 2012, pero se informa que no contiene datos personales aparte de documento de identificación, nombres y dependencia de los funcionarios que tienen asignado eventualmente un activo, los cuales son datos personales considerados públicos. En caso de mantener la clasificación debería justificarse con otra norma, en el campo “fundamento jurídico de la excepción” del índice de información clasificada y reservada.
Norma ISO 27001:2013 6.1.3. Tratamiento de los riesgos de seguridad de información Modelo de Seguridad y Privacidad de la Información. Fase:Planificación Identificación, valoración y tratamiento de riesgo Anexo A A.11.1.1. Perímetro de seguridad física A.11.1.3 Seguridad de oficinas, despachos y recursos	Se mantiene la no conformidad: “No se evidencia un control de acceso físico adecuado, lo cual se soporta al encontrar la puerta de acceso al piso 8 y al piso 4 se encontraba sin seguridad incumpliendo con el control de acceso A.11.1.1. Perímetro de seguridad física de la Norma ISO 27001:2013” (Ver observaciones en F86 Seguimiento de acciones correctivas SGSI MSPI 2017-2019, adjunto),la cual se complementa con lo observado en la presenta auditoría, en los siguientes términos: “Se presenta incumplimiento del control definido para la causa de riesgo CASI20- Robo de infraestructura de TI, equipos, medios extraíbles, dispositivo de almacenamiento o daño premeditado; dado que dentro de la seguridad física perimetral de la entidad en la sede Aguas se evidencia que no se está exigiendo el acceso por molinetes con tarjetas de proximidad en la entrada principal y tampoco en las puertas de cada uno de los pisos del edificio de oficinas. No siempre se acompaña a los visitantes para el ingreso y no se	

	entrega tarjeta de proximidad a contratistas. Esto incumple los requisitos del numeral 6.1.3.Tratamiento de riesgos de seguridad de la información y los controles A.11.1.2 Perímetro de seguridad física y A.11.1.3 Seguridad de oficinas, despachos y recursos, del Anexo A de la Norma ISO 27001:2013."	
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 deberían incluir en el sistema de gestión de riesgos de seguridad digital los riesgos asociados con el proceso de Servicios generales y apoyo logístico. Se presenta, por ejemplo, el riesgo de robo de información o activos de la entidad, dado el acceso privilegiado a las instalaciones, por parte del personal de aseo y cafetería.
Norma ISO 27001:2013 Anexo A A.11.Seguridad física y del entorno A.11.1 Áreas seguras A.13.2. Intercambio de información Ley 1581 de 2012		Se debe garantizar el respaldo de imágenes grabadas por las cámaras de seguridad, así como el manejo seguro de las grabaciones de video en caso de requerir copia, dado que se informa en auditoría que se pueden entregar por parte del proveedor a la entidad en medios removibles como USB. Dada la información sensible, se deben implementar mecanismos de encripción en ese caso, para mantener el acceso restringido. Igualmente, se deben tomar las medidas para anonimizar las imágenes o solicitar autorización de otros titulares de datos personales, en caso de atender solicitudes de acceso a videos, por parte de algún titular; en especial si se cuenta con imágenes de niñas, niños o adolescentes.
Norma ISO 27001:2013 Anexo A A.9. Control de acceso		Se recomienda asegurar que se asigne un usuario independiente para cada persona del proveedor de seguridad y de videovigilancia, que les permita el acceso a la red y los sistemas de información (registro de visitantes, puertas y molinetes y cámaras de video vigilancia), con el fin de mejorar la gestión de accesos y dar cumplimiento a las políticas respectivas.

Ley 1581 de 2012 Decreto 1377 de 2013 Capítulo III		Se recomienda instalar avisos de privacidad adicionales al de la recepción de la sede Aguas, ubicados en las zonas de ingreso a los lugares que están siendo video vigilados y monitoreados, advirtiendo que el ingreso a la zona otorga autorización para el tratamiento de los datos biométricos. Así mismo, se debería publicar aviso y autorización de tratamiento o incluirlos en las bitácoras de registro de visitantes de la Sede Elemento, piso 15. Ver Guía de protección de datos en sistemas de video vigilancia de la SIC.
Norma ISO 27001:2013 7.5.3. Control de información documentada Anexo A A.11.2.5 Retiro de activos	Se incumple con los requisitos de la Norma ISO 27001:2013 numeral 7.5.3. Control de información documentada y el control A.11.2.5 Retiro de activos por tanto se evidencia acta de apertura de libro de seguridad de 24 de julio de 2019, sin firma autorizada y sin todos los datos diligenciados completos, como números de identificación de los visitantes o funcionarios que ingresan sus equipos y serial de los mismos. Se debe cumplir con el registro y la verificación de estos datos en el momento del retiro de equipos de las instalaciones de la entidad.	

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. Además, se mantiene abierta una no conformidad proveniente de la auditoría interna anterior; relacionada con los controles de seguridad física; la cual en la auditoría interna 2017 se había detectado en los procesos de Talento Humano y se reasigna al proceso de Administración de Activos Fijos.(Ver sección 4. Para observaciones relacionadas y recomendaciones para el plan de mejoramiento, consultar F86 - Seguimiento de acciones correctivas, documento adjunto). Las no conformidades 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 seis oportunidades de mejora, las cuales se recomienda analizar, con el fin de definir e implementar acciones que permitan evitar no conformidades en el futuro. Es importante igualmente, asegurar la disponibilidad de la documentación relacionada con la ejecución del contrato del proveedor de seguridad física, en conjunto con el Grupo de Archivo.

Como parte del seguimiento del plan de mejoramiento proveniente de los resultados de la anterior auditoría interna de seguridad de la información, se cierran las 3 no conformidades pendientes, considerando que se han tomado acciones para eliminarlas; aunque se dejan observaciones y recomendaciones al respecto. Ver Formato de seguimiento F86 anexo.

6. OBJECIONES DEL AUDITADO NO RESUELTAS

No aplica.