INFORME DE AUDITORÍA INTERNA No.: 14

FECHA DE EMISIÓN DEL INFORME	**Día:**	17	**Mes:**	09	**Año:**	2020

1. PROCESO:	Sistema de Gestión de Seguridad de la Información NTC-ISO-27001:2013
2. LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):	Líder Estratégico: Director de Informática y Desarrollo 1. Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones, 2. Coordinador Grupo de Sistemas y Arquitectura y Tecnología 3. Coordinador Grupo Arquitectura de Datos. 4. Jefe Oficina Asesora de Planeación.
3. OBJETIVO DE LA AUDITORÍA:	Evaluar el cumplimiento del Sistema de Gestión de Seguridad de la Información de acuerdo con los requerimientos de la NTC-ISO/IEC 27001:2013, así como los controles establecidos en el Anexo A de la norma.
4. ALCANCE DE LA AUDITORÍA:	Se realizó auditoría al Sistema de Gestión de Seguridad de la Información de la entidad, mediante prueba selectiva y/o muestreo a las actividades realizadas durante el periodo comprendido entre el 10 de agosto de 2019 al 11 de septiembre de 2020, fecha de finalización de esta auditoría. Esta norma se aplicó a los procesos de Gestión del Talento Humano, Gestión de Infraestructura física, Gestión Contractual, Gestión Documental, Oficina Asesora de Planeación y Gestión de Infraestructura y Tecnologías de Información. No fue necesario, incorporar hechos adicionales en el desarrollo de la auditoría.
5. CRITERIOS DE LA AUDITORÍA:	Se evaluó la conformidad de la norma NTC-ISO 27001:2013 La efectividad de los controles definidos en el Anexo A de la norma NTC-ISO 27001:2013 A.5 Políticas de la Seguridad de La Información - A5.1.1, A5.1.2

	A.6 Organización de la Seguridad de la Información - A6.1.1, A6.1.2, A6.1.3, A6.1.4, A6.1.5, A6.2.1, A6.2.2 A.7 Seguridad de los Recursos Humanos - A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1 A8 Gestión de Activos - A8.1.1, A8.1.2, A8.1.3, A8.1.4, A8.2.1, A8.2.2, A8.2.3, A8.3.1, A8.3.2, A8.3.3 A9 Control de Acceso - A9.1.1, A9.1.2, A9.2.1, A9.2.2, A9.2.3, A9.2.4, A9.2.5, A9.2.6, A9.4.1, A9.4.2, A9.4.3; A9.4.4, A9.4.5 A11 Seguridad Física y del Entorno - A11.2.4, A11.2.6, A11.2.7. A12 Seguridad de las Operaciones - A12.1.1; A12.1.3, A12.1.4, A12.2.1, A12.3.1, A12.4.1, A12.4.2, A12.4.3, A12.4.4, A12.5.1, A12.6.1, A12.6.2, A12.7.1 A13 Seguridad de las Comunicaciones - A13.1.1, A13.1.2, A13.1.3, A13.2.1, A13.2.2, A13.2.3, A13.2.4

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	18	**Mes**	08	**Año**	2020	**Desde:**	18/08/2020 D / M / A	**Hasta:**	18/09/2020 D / M / A	Día	18	Mes	09	Año	2020

6. HALLAZGOS DE LA AUDITORÍA

6.1 ASPECTOS FUERTES DEL PROCESO:

1. Se identificó liderazgo en la operación del Sistema de Gestión de Seguridad de la Información NTC-ISO 27001:2013 durante la Emergencia Sanitaria, decretada por el Gobierno Nacional. También, se observó evolución y madurez del Sistema de seguridad de la Información, donde se ha mantenido la seguridad de la información y los servicios como: audiencias virtuales, trámites y servicios en línea, sin suspender el servicio a los usuarios.

2. Considerando el número reducido de funcionarios y contratistas encargados de la gestión de la Seguridad de la Información en la Entidad, se observa compromiso y resultados en las labores de gestión de seguridad de la información.

6.2 OBSERVACIONES

1. Con las nuevas herramientas en la nube que ha venido adquiriendo e implementando la Entidad, como el caso de Teams, donde se pueden compartir archivos y grabar reuniones, que a su vez quedan alojadas en un repositorio público, es necesario socializar a los funcionarios en general, sobre la importancia de no dejar allí información confidencial, con el fin de, evitar posibles fugas de información.

6.2 OBSERVACIONES

2. Por instrucciones de la Secretaría General, ante la ausencia de un funcionario, por vacaciones, licencia no remunerada o incapacidad, se debe inhabilitar el acceso a la Red, por el tiempo que dure esta. Las directrices una vez se den, deben quedar documentadas y controladas en el Sistema de Gestión Integrado, teniendo en cuenta que tiene afectación directa sobre un activo de información y ayuda a mantener el enfoque y la disciplina hacia el objetivo deseado. Adicionalmente, es preciso reforzar el control que actualmente se ejecuta sobre esta directriz, dado que, en la revisión efectuada, el equipo auditor encontró un caso, donde no fue reportada al grupo de Sistemas la novedad de una licencia no remunerada, que va del 7/10/2019 al 25/9/2020, como área encargada de ejecutar dicho control.

3. En el documento GC-G-002 Guía: Administración de Riesgos Institucionales, versión 006, del 17 de julio de 2020, no especifica claramente que debe hacer un Líder en caso de materializarse un riesgo del proceso, solamente hace mención de qué hacer, cuando se materializa un riesgo de corrupción.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
1. Toma de conciencia de las políticas de seguridad de la información y del Sistema de Gestión Integrado. El equipo auditor, realizó un trabajo de campo mediante la aplicación de dos (2) encuestas para obtener información del conocimiento de los funcionarios y contratistas sobre el Sistema de Seguridad de la Información definido por la Entidad. La primera de ellas, relacionada con la política y la segunda con el conocimiento de sus funciones y responsabilidades con el sistema de Seguridad de la información. Para la primera se tomó una muestra sesenta y tres (63) funcionarios a los que se les envío por correo electrónico los días 26 de agosto y 1 de septiembre de de 2020, que incluía un cuestionario con seis (6) preguntas relacionadas con la Política del Sistema de Gestión Integrado y el Documento de Políticas, necesarias para el Sistema, se obtuvo respuesta de veintinueve (29) funcionarios, obteniendo como resultado, que el 93% de los encuestados, conoce la Política del Sistema de Gestión Integrado, frente un 7% que dice no conocerla. El 90% conoce donde se encuentra ubicada, frente a un 10% que dice no saber. Con respecto a si conocen el documento de Políticas donde están definidas las aplicables a todo el Sistema de Gestión Integrado, incluidas las de Seguridad de la Información, el 31% conoce el documento de Políticas y su ubicación, frente a un 69% que no las conoce. Adicionalmente, el día 11 de septiembre de 2020 se aplicó una segunda encuesta, a 24 directivos, líderes de procesos y coordinadores, para saber	Norma NTC-ISO-IEC 27001: 2013 numeral 7.3 Toma de conciencia

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
que funcionarios conocían su funciones y responsabilidades frente al Sistema de Gestión de Seguridad de la Información, para lo cual se obtuvo respuesta de nueve (9) de ellos, obteniendo como resultado que el 56% las conoce, frente a un 44% que no. A la pregunta que si sabe dónde están definidas esas funciones y responsabilidades, el 22% manifestó si saber, frente al 78% que no lo sabe. Lo anterior evidencia que falta fortalecer las sensibilizaciones, enfocadas a la interiorización del documento de políticas y su ubicación, al igual que el conocimiento y ubicación del documento donde están definidas las funciones y responsabilidades frente al Sistema de Seguridad de la Información. Y de esta manera, mejorar la concientización de funcionarios y contratistas sobre el conocimiento, aplicación y cumplimiento de las mismas. En consecuencia, se incumple la Norma NTC-ISO-IEC 27001:2013 numeral 7.3 Toma de conciencia.	
2. Restricción de Acceso a la Información de los Repositorios de SharePoint. Teniendo en cuenta que la Seguridad de la Información es transversal y aplica a todos los procesos definidos en el Sistema de Gestión Integrado de la Entidad, el equipo auditor tomó como muestra siete (7) repositorios de SharePoint, utilizados por los diferentes procesos para almacenar información sensible, evidenciando debilidad en el control por parte de los propietarios de la información, en el caso de los repositorios de: Acuerdos de Insolvencia en Ejecución, Régimen Cambiario, Administración de Personal y Contratos, al no solicitar oportunamente al área técnica, el retiro de los permisos de acceso ante el traslado de funcionarios o al terminar el tiempo definido, para desarrollar una actividad puntual, como es el caso de las auditorías internas. Situación que de alguna manera pone en riesgo la confidencialidad de la información que allí se almacena. En consecuencia, se incumple A9.4.1 Restricción del acceso a la información.	Norma NTC-ISO-IEC 27001: 2013 Anexo A numeral A9.4.1 Restricción del acceso a la información.
3. Competencias del Oficial de Seguridad de la Información Siendo el Rol del Oficial de seguridad un pilar importante dentro de la gestión de Seguridad de la Información, en la actualidad no hay claridad de quién debe asumir la responsabilidad en la Entidad, ni se determina donde se encuentra ubicado en la estructura organizacional.	Norma NTC-ISO-IEC 27001: 2013 numeral numeral 7.2 Competencia

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
Adicionalmente, no hay evidencia que dé cuenta de la definición de las competencias requeridas para desempeñar el Rol de Oficial de Seguridad de la Información en la Entidad. En este sentido, la Entidad debe tomar las acciones necearías de manera inmediata, para reducir o gestionar los riesgos asociados con las debilidades actuales, que permitan el aseguramiento y madurez del Sistema de Seguridad de la Información. En consecuencia, se incumple lo dispuesto en el numeral 7.2 de la NTC-ISO 27001:2013	

7. CONCLUSIONES DE LA AUDITORÍA

De la auditoria adelantada al Sistema de Gestión de Seguridad de la Información NTC-ISO 27001:2013, el equipo auditor concluye:

- En la revisión efectuada a los riesgos de seguridad de la información, solo se cuenta con un modelo para el proceso de Gestión Integral, se requiere diseñarlos, analizarlos y evaluarlos en el contexto de seguridad de la información y definirlos para todos los procesos en el Nivel Central e Intendencias Regionales, de la implementación de los riesgos es necesario mantener la información documentada en el software que tiene diseñado la Entidad para tal fin.

- Con el análisis de riesgos de gestión, se deben identificar y evaluar los riesgos asociados al llevar los datos a la nube parcial o totalmente.

- Las actividades del Director de Informática y Desarrollo quien debe garantizar la aplicación de los permisos definidos de los activos de información que custodia, se deben articular con el rol del Oficial de Seguridad de la Información de velar, verificar y aprobar los cambios que impacten el cumplimiento de los permisos de acceso, definir con claridad el rol de oficial de seguridad para que facilite ejercer un papel independiente en el monitoreo eficaz del Sistema de Gestión de Seguridad de la Información.

- Las acciones que se estructuren dentro del plan de mejoramiento de la auditoría externa, deben cumplirse dentro del término establecido para cada una de ellas, y que dichas acciones contribuyan a erradicar la causa raíz de las no conformidades, de manera efectiva.

- Consecuencia de la Emergencia Sanitaria decretada por el Gobierno Nacional, no todos los mantenimientos se pudieron ejecutar en las fechas programadas inicialmente, sin embargo, contratos de mantenimiento como Digiturno, aires acondicionados, sistema de extinción de incendios, UPS ya se han venido reprogramando y realizando.

7. CONCLUSIONES DE LA AUDITORÍA

- Los informes generados de las pruebas periódicas de las vulnerabilidades técnicas realizados a los sistemas de información, deben llevar la fecha de emisión del mismo.

- Actualmente no hay contrato para el Almacenamiento y Custodia de Medios Magnéticos, todos estos medios que estaban bajo custodia, ahora se encuentran ubicados en el Centro de Cómputo de la Entidad. Si bien, estos ya presentan deterioro y obsolescencia, se les debe establecer el procedimiento para darles disposición final.

- Si bien, dentro del proceso de gestión Integral, fue objeto de una no conformidad relacionada con los documentos obsoletos del SGI, dado que están sin la debida protección y con acceso a todos los funcionarios de la Entidad, debido a falla técnica en la plataforma, es algo que requiere pronta solución.

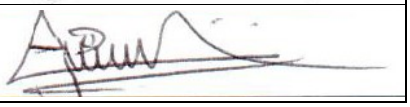
- Referente a las actividades auditadas al Sistema de Gestión de Seguridad de la Información NTC-ISO-27001:2013, de acuerdo con lo dispuesto en la Norma NTC-ISO 14001:2015, cumplen con las acciones propuestas en los numerales, 4.1, 4.2, 4.3, 4.3, 4.4, 5.1, 5.2, 5.3, 6.1, 6.2, 7.1, 7.4, 7.5, 8.1, 8.2, 8.3, 9.1, 9.2, 9.3, 10.1, 10.2 No obstante se identificaron no conformidades referentes a los numerales 7.3, 7.2, los cuales impiden tener la gestión del Sistema totalmente asegurada.

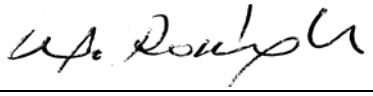
- En cuanto a los controles del anexo de la Norma NTC-ISO 14001:2015 cumplen con las acciones propuestas en los numerales A5.1.1, A5.1.2; A6.1.1, A6.1.2, A6.1.3, A6.1.4, A6.1.5, A6.2.1, A6.2.2; .7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1; A8.1.1, A8.1.2, A8.1.3, A8.1.4, A8.2.1, A8.2.2, A8.2.3, A8.3.1, A8.3.2, A8.3.3; A9.1.1, A9.1.2, A9.2.1, A9.2.2, A9.2.3, A9.2.4, A9.2.5, A9.2.6, A9.4.2, A9.4.3; A9.4.4; A9.4.5; A11.2.4, A11.2.6; A11.2.7.; A12.1.1; A12.1.3, A12.1.4; A12.2.1; A12.3.1; A12.4.1; A12.4.2; A12.4.3; A12.4.4; A12.5.1; A12.6.1; A12.6.2; A12.7.1; A13.1.1; A13.1.2; A13.1.3; A13.2.1; A13.2.2; A13.2.3; A13.2.4 No obstante se identificaron no conformidades referentes a los numerales A9.4.1, los cuales impiden tener la gestión del Sistema totalmente asegurada.

En total se identificaron **tres (3) observaciones y tres (3) no conformidades**, que requieren estructuración de acciones preventivas y correctivas que permitan garantizar la mejora continua del Sistema de Seguridad de la Información y por ende la madurez del Sistema de Gestión Integrado, el Sistema de Control Interno y la Gestión Institucional.

Para constancia se firma en Bogotá D.C., a los 18 días del mes de septiembre del año 2020

8. RESPONSABLES INFORME DE AUDITORÍA

Nombre Completo	Responsabilidad	Firma
Arnulfo Suárez Pinzón	Jefe Oficina de Control Interno	
Miguel Darío Quintana Sánchez	Auditor Líder	

8. RESPONSABLES INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad**	**Firma**
Wilma Rocío Pedrozo Ulloa	Auditor	

9. ANEXOS
Resultado de la Encuesta conocimiento de la política y el Resultado de la Encuesta de Responsabilidades.